# Netcool Configuration Manager 6.4.2

*User Guide*

2023-4219-01

**Note**

Before using this information and the product it supports, read the information in “Notices” on page 337.

This edition applies to version 6.4.2 of IBM Tivoli Netcool Configuration Manager (5725-F56) and to all subsequent releases and modifications until otherwise indicated in new editions.

# Contents

# About this publication

IBM Tivoli Netcool Configuration Manager provides network management and configuration capabilities. Specifically, Netcool Configuration Manager provides the configuration management capabilities for network devices and extensive configuration policy thresholding capabilities.

The *IBM Tivoli Netcool Configuration Manager User Guide* guide describes how to access reports, use devices, and execute the different utilities to maintain and support auto-discovery.

## Intended audience

This publication is intended for users working with IBM Tivoli Netcool Configuration Manager.

## What this publication contains

This publication contains the following sections:

- Chapter 1, “Getting started,” on page 1

  Provides information on how to
- Chapter 3, “Configuring network devices,” on page 39

  Provides information on how to configure network devices.
- Chapter 4, “Managing network compliance,” on page 201

  Provides information on how to perform network compliance management tasks.
- Chapter 5, “Using the DASH portlets,” on page 295

  Provides information on the TIP portlets. Specifically, it describes the Netcool Configuration Manager Activity Viewer and the configuration tasks that you can perform with it.
- Chapter 6, “Viewing reports,” on page 311

  Provides information on how to access and view reports.
- Chapter 7, “Setting user preferences,” on page 327
- Provides information on how to set system user properties for various UIs.

## Publications

This section lists publications in the Netcool Configuration Manager PDF document set. The prerequisite publications in the IBM Tivoli Network Manager IP Edition and IBM Tivoli Netcool/OMNIbus library are also listed here. The section also describes how to access Tivoli publications online and how to order Tivoli publications.

### Netcool Configuration Manager PDF document set

The following documents are available in the Netcool Configuration Manager library:

- *IBM Tivoli Netcool Configuration Manager Installation and Configuration Guide*

  Describes how to install IBM Tivoli Netcool Configuration Manager. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up IBM Tivoli Netcool Configuration Manager.
- *IBM Tivoli Netcool Configuration Manager User Guide*

  Describes user tasks for IBM Tivoli Netcool Configuration Manager, such as how to access reports, use devices, and execute the different utilities to maintain and support Auto-Discovery. This publication is for users working with IBM Tivoli Netcool Configuration Manager.

- *IBM Tivoli Netcool Configuration Manager Administration Guide*

  Describes administration tasks for IBM Tivoli Netcool Configuration Manager, such as how to set up user accounts, create and manage the OS registry, administer database and policy exports and imports, and perform housekeeping and security tasks. This publication is for administrators who are responsible for the maintenance and availability of IBM Tivoli Netcool Configuration Manager.
- *IBM Tivoli Netcool Configuration Manager Reference Guide*

  Contains reference information about IBM Tivoli Netcool Configuration Manager.
- *IBM Tivoli Netcool Configuration Manager API Guide*

  Provides information about how to use the Java API to programmatically access IBM Tivoli Netcool Configuration Manager.
- IBM Tivoli Netcool Configuration Manager NSM REST API Guide

  Describes the Service Management Interface API.
- *IBM Tivoli Netcool Configuration Manager Integration Guide*

  Describes how to integrate Netcool Configuration Manager with Tivoli Netcool/OMNIbus and Network Manager.
- *IBM Tivoli Netcool Configuration Manager Quick Start Guide*

  Gets you started with a typical installation for IBM Tivoli Netcool Configuration Manager.
- *IBM Tivoli Netcool Configuration Manager Release Notes*

  Gives important and late-breaking information about IBM Tivoli Netcool Configuration Manager. This publication is for deployers and administrators, and should be read first.

## Prerequisite publications: IBM Tivoli Network Manager IP Edition

To use the information in this publication effectively when dealing with an integrated installation of Netcool Configuration Manager, Network Manager, and Tivoli Netcool/OMNIbus, you must have some prerequisite knowledge, which you can obtain from the Network Manager documentation, especially the following publications:

- *IBM Tivoli Network Manager IP Edition Release Notes*

  Gives important and late-breaking information about IBM Tivoli Network Manager IP Edition. This publication is for deployers and administrators, and should be read first.
- *IBM Tivoli Network Manager Getting Started Guide*

  Describes how to set up IBM Tivoli Network Manager IP Edition after you have installed the product. This guide describes how to start the product, make sure it is running correctly, and discover the network. Getting a good network discovery is central to using Network Manager IP Edition successfully. This guide describes how to configure and monitor a first discovery, verify the results of the discovery, configure a production discovery, and how to keep the network topology up to date. Once you have an up-to-date network topology, this guide describes how to make the network topology available to Network Operators, and how to monitor the network. The essential tasks are covered in this short guide, with references to the more detailed, optional, or advanced tasks and reference material in the rest of the documentation set.
- *IBM Tivoli Network Manager IP Edition Product Overview*

  Gives an overview of IBM Tivoli Network Manager IP Edition. It describes the product architecture, components and functionality. This publication is for anyone interested in IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*

  Describes how to install IBM Tivoli Network Manager IP Edition. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Administration Guide*

  Describes administration tasks for IBM Tivoli Network Manager IP Edition, such as how to administer processes, query databases and start and stop the product. This publication is for administrators who are responsible for the maintenance and availability of IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Discovery Guide*

  Describes how to use IBM Tivoli Network Manager IP Edition to discover your network. This publication is for administrators who are responsible for configuring and running network discovery.

- *IBM Tivoli Network Manager IP Edition Event Management Guide*

  Describes how to use IBM Tivoli Network Manager IP Edition to poll network devices, to configure the enrichment of events from network devices, and to manage plug-ins to the Tivoli Netcool/OMNIbus Event Gateway, including configuration of the RCA plug-in for root-cause analysis purposes. This publication is for administrators who are responsible for configuring and running network polling, event enrichment, root-cause analysis, and Event Gateway plug-ins.

- *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*

  Describes how to use IBM Tivoli Network Manager IP Edition to troubleshoot network problems identified by the product. This publication is for network operators who are responsible for identifying or resolving network problems.

- *IBM Tivoli Network Manager IP Edition Network Visualization Setup Guide*

  Describes how to configure the IBM Tivoli Network Manager IP Edition network visualization tools to give your network operators a customized working environment. This publication is for product administrators or team leaders who are responsible for facilitating the work of network operators.

- *IBM Tivoli Network Manager IP Edition Management Database Reference*

  Describes the schemas of the component databases in IBM Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the component databases directly.

- *IBM Tivoli Network Manager IP Edition Topology Database Reference*

  Describes the schemas of the database used for storing topology data in IBM Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the topology database directly.

- *IBM Tivoli Network Manager IP Edition Language Reference*

  Describes the system languages used by IBM Tivoli Network Manager IP Edition, such as the Stitcher language, and the Object Query Language. This publication is for advanced users who need to customize the operation of IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Perl API Guide*

  Describes the Perl modules that allow developers to write custom applications that interact with the IBM Tivoli Network Manager IP Edition. Examples of custom applications that developers can write include Polling and Discovery Agents. This publication is for advanced Perl developers who need to write such custom applications.

- *IBM Tivoli Monitoring for Tivoli Network Manager IP User's Guide*

  Provides information about installing and using IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition. This publication is for system administrators who install and use IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition to monitor and manage IBM Tivoli Network Manager IP Edition resources.

## Prerequisite publications: IBM Tivoli Netcool/OMNIbus

To use the information in this publication effectively when dealing with an integrated installation of Netcool Configuration Manager, Network Manager, and Tivoli Netcool/OMNIbus, you must have some prerequisite knowledge, which you can obtain from the Tivoli Netcool/OMNIbus documentation, especially the following publications:

- *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*

Includes installation and upgrade procedures for Tivoli Netcool/OMNIbus, and describes how to configure security and component communications. The publication also includes examples of Tivoli Netcool/OMNIbus architectures and describes how to implement them.

- *IBM Tivoli Netcool/OMNIbus User's Guide*

  Provides an overview of the desktop tools and describes the operator tasks related to event management using these tools.

- *IBM Tivoli Netcool/OMNIbus Administration Guide*

  Describes how to perform administrative tasks using the Tivoli Netcool/OMNIbus Administrator GUI, command-line tools, and process control. The publication also contains descriptions and examples of ObjectServer SQL syntax and automations.

- *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*

  Contains introductory and reference information about probes and gateways, including probe rules file syntax and gateway commands.

- *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide*

  Describes how to perform administrative and event visualization tasks using the Tivoli Netcool/OMNIbus Web GUI.

## Accessing terminology online

The IBM Terminology website consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology website at the following Web address:

http://www.ibm.com/software/globalization/terminology

## Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center website at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp

**Note:** If you print PDF documents on other than letter-sized paper, set the option in the **File** > **Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

## Ordering publications

You can order many Tivoli publications online at the following website:

http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following website:

   http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss
2. Select your country from the list and click **Go**. The **Welcome to the IBM Publications Center** page is displayed for your country.
3. On the left side of the page, click **About this site** to see an information page that includes the telephone number of your local representative.

# Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully.

With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

# Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education website:

https://www.ibm.com/training/search?query=tivoli

# Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

**Online**
Go to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html and follow the instructions.

**IBM Support Assistant**
The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, go to http://www.ibm.com/software/support/isa

# Conventions used in this publication

This publication uses several conventions for special terms and actions and operating system-dependent commands and paths.

## Typeface conventions

This publication uses the following typeface conventions:

**Bold**

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:** and **Operating system considerations:**)
- Keywords and parameters in text

***Italic***

- Citations (examples: titles of publications, diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a *point-to-point* line)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data
- Variables and values you must provide: ... where *myname* represents....

**Monospace**

- Examples and code examples

- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

## Operating system-dependent variables and paths

This publication uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace **$***variable* with **%***variable***%** for environment variables, and replace each forward slash (**/**) with a backslash (****) in directory paths. For example, on UNIX systems, the $NCHOME environment variable specifies the directory where the Network Manager core components are installed. On Windows systems, the same environment variable is %NCHOME%. The names of environment variables are not always the same in the Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to $TMPDIR in UNIX environments.

If you are using the bash shell on a Windows system, you can use the UNIX conventions.

# Chapter 1. Getting started

The Getting Started section is intended for anyone who uses Netcool Configuration Manager to manage and configure network resources.

**Note:** Before proceeding, ensure that Netcool Configuration Manager - Base has been installed on all servers, and that each Netcool Configuration Manager - Base instance has been started.

## Launching Netcool Configuration Manager - Base

Launch the Netcool Configuration Manager - Base GUI using the web portal. This provides options for the Netcool Configuration Manager - Base Webstart GUI, Netcool Configuration Manager - Compliance and Account Management.

This task describes how to launch Netcool Configuration Manager - Base and log in using the web portal.

1. Using a browser, launch the Netcool Configuration Manager - Base web portal from: `http://<ncmserver-hostname-ip>:<port-number>`. The port number will have been specified during installation.
2. When presented with the Netcool Configuration Manager - Base login screen, you should login using the Netcool Configuration Manager default administrator name and password specified during installation. Click on the **Login** icon to proceed.
3. The user can launch the Netcool Configuration Manager - Base Webstart GUI, Netcool Configuration Manager - Compliance GUI, Reporting (optional) or Account Management from here. Choose Netcool Configuration Manager - Base Webstart GUI link and enter your default administrator name and password specified during installation. Click on the **Login** icon to proceed.

Next, you should set the time zone.

## Setting time zone

For display purposes, it is recommended that you set the system time zone appropriate to your location.

When set, all times shown in the application will be converted to your timezone with the exception of the times shown in the UOW log, which will remain in GMT. When the timezone is set, it only applies against the username that was used to set the timezone.

1. Select **File** > **Preferences**.
2. Navigate to the **User Information** preference along the left hand side of the screen.
3. Configure the **Time Zone** using the drop down menu.
4. When complete select **Apply**, and then select **OK** to proceed.

Next, you should set the resource visibility.

## Setting Resource Browser visibility

For the purposes of Resource Browser visibility, it is recommended that you set the visibility options. This allows you to view the resource types (for example, Command Set and Configuration) you require. Not all resource types are visible by default.

This task describes how to set Resource Browser visibility.

1. Select **File** > **Preferences**.
2. Navigate to the **Resource Browser** preference along the left hand side of the screen.
3. The **Resources** visibility can be configured using the checkbox listing. Against each resource type option you wish to have visibility to, you must select the checkbox. At a minimum, it is recommended you select Authentication and Work Server resource types.

4. When complete select **Apply**, and then select **OK** to proceed.

Next, you should create a work server resource.

## Setting up a worker server resource

A worker server resource defines how work will be distributed in the system. A worker server resource is required if work will be executed.

This task describes how to set up a worker server resource.

1. Navigate to the **System Manager** .
2. Select the **Servers** folder within the Systems Manager.
3. You can see the worker server on your deployment in the **Servers** folder.
4. You can also edit the default worker server to add a second worker server. Navigate to the Resource Browser, highlight the work server resource named *Work Distribution*, then right click and select **Edit**.
5. Right click on the first line, and select **Edit**. Enter the name of the second worker server. Remember to set the **Ignore** flag to `false`.
6. Select **File** > **Save** to complete the change.

Next, you should create an authentication resource.

## Setting up an authentication resource

When Netcool Configuration Manager sets up the communication between itself and a device, it builds a list of credentials to use when authenticating. An authentication resource must be set up for this reason. This allows the users to specify user login credentials, as well as SNMP device login community string credentials.

Netcool Configuration Manager cannot support authentication resource VTMOS types in the following formats: unknown/*/*/* or */unknown/*/* or */*/unknown/* or */*/*/unknown for IDT auto. While defining VTMOS field values, an 'UNKNOWN' value can not be used for a singular field.

1. You can edit the default authentication resource. Navigate to the Resource Browser, highlight the authentication resource, then right click and select **Edit**.
2. The authentication resource username and password can be edited, as well as SNMP information.
3. Select **File** > **Save** to complete the changes.

Next, you can create an FTP resource. This is an optional step.

## Configuring an FTP resource

When Netcool Configuration Manager is transferring configuration information to and from a device, it can be set up to use either streaming or FTP. If you disable streaming, then you must configure an FTP resource, as described here.

The default RAD setting for most devices is:

**Streaming**
For retrieving the configuration

**FTP**
For pushing changes to the device

You must check the device RAD for these settings.

If you opt to disable streaming, you follow this procedure to set up an FTP resource.

Netcool Configuration Manager attempts to locate an FTP resource by looking into the same realm as the device, then moving up the realm tree until the top realm is reached. If an FTP resource is not found, then Netcool Configuration Manager looks for a default file transfer resource by reading the following locations:

**From the rseries.properties file**

deviceConstants/FTP_HOST

deviceConstants/FTP_PATH

**From System properties**

FTP Username

FTP Password

- If any of the above parameters are included in a file transfer resource, then the value in the file transfer resource overrides the default value.
- If either Host or Path is modified in the `rseries.properties` file, then a Netcool Configuration Manager worker server restart is required.

**Note:** Modifying either User name or Password does not require a restart.

1. Navigate to the Resource Browser.
2. Select **File** > **New** > **File Transfer**.

   The **New File Transfer** screen is displayed.
3. Use the following table to help you complete the information required.

*Table 1. New File Transfer screen fields*

| Field | Description |
|---|---|
| Name | The name specified at install time to identify the FTP resource.<br>**Restriction:** `ftpInfo` and `altFtpInfo` are the only two names that can be given to an FTP resource. |
| Vendor | Using the drop down menu, select the Vendor for the FTP resource. |
| Type | Using the drop down menu, select the Type for the FTP resource. |
| Model | Using the drop down menu, select the Model for the FTP resource. |
| OS | Using the drop down menu, select the OS for the FTP resource. |

4. Click **OK** to complete the FTP resource creation.
5. Right-click the FTP resource in the Resource Browser, and select **Edit** from the drop-down menu.
6. Click **Add** to enter the following FTP details:

*Table 2. FTP details*

| Field | Description |
|---|---|
| Name | Enter one of the following names: `ftpInfo` or `altFtpInfo`. |
| Host | This property defines the host for the FTP server, which can be an Netcool Configuration Manager server or an external server, or left blank in order to use the FTP server details entered at install time (as stored in the `rseries.properties` file).<br>**Note:** For environments which require that each Netcool Configuration Manager worker server run an FTP server, leave this property blank.<br>**Tip:** The host information will be sent to the devices, and so may need to be set as an IP rather than an alias or hostname that might only be resolvable on the Netcool Configuration Manager server. |
| Username | Enter the FTP username. |
| Password | Enter the password for the ftp user. |

| Table 2. FTP details (continued) | |
|---|---|
| **Field** | **Description** |
| Path | This is the path on the local worker server where files are stored during the file transfer.<br>Leave this blank when the path property is to be retrieved from the `rseries.properties` file of the worker server running the UOW. |
| Mode | **Select**<br>For passive FTP mode<br>**Unselect**<br>For Active FTP mode |

## Changing server pool sizes

The default worker server pool sizes can be configured to meet the system requirements.

This task describes how to adjust the default thread count.

1. Navigate to the Systems Manager.
2. To modify the worker server pool sizes, right click on the worker server and choose **Change pool settings** from the pop-up menu.
3. The **Change Server Pool Sizes** screen is displayed. The max normal pool size can be configured to address the number of threads set on a worker server. This needs to be optimized based on device real estate, but generally a value between 20 and 40 threads is applicable. The range will be affected by the amount of heap available to the JVM and to the number of database connection available.
4. Click **OK** to save changes to the server pool size.

Next, you can configure Netcool Configuration Manager - Compliance security.

## Importing devices

Netcool Configuration Manager - Base allows both manual and automated initial input of your network device information into the database. When importing an existing device into the database, the system also writes the running configuration to the stored/candidate configuration on the device, ensuring that all three configurations (current, running, stored) are in sync.

This task describes how to import a device into Netcool Configuration Manager - Base.

1. Navigate to the Resource Browser.
2. Select **File** > **New** > **Network Resource**.
3. The **New Network Resource** screen is displayed. Use the following table to help you complete the information required.

| Table 3. New Network Resource screen fields | |
|---|---|
| **Field** | **Description** |
| Name | A unique name to identify the network resource. |
| Vendor | Using the drop down menu, select the Vendor for the network resource. |
| Type | Using the drop down menu, select the Type for the network resource. |
| Model | Using the drop down menu, select the Model for the network resource. |

| *Table 3. New Network Resource screen fields (continued)* | |
|---|---|
| **Field** | **Description** |
| OS | Using the drop down menu, select the OS for the network resource. |

4. Select **OK** to complete the network resource creation.
5. The network resource can be edited, by right clicking on the network resource within the Resource Browser and select **Edit**.
6. Select the Resource Browser in the navigation tree.

   Your resources display.
7. Select or Search for the network resources you want to import.
8. Click to highlight the desired resource, and then right click and select **Import**. (Use `Ctrl-click` to select multiple resources.)

   The **Import Network Resource** wizard displays.

   Any resources that you selected in the Resource Browser are preselected here. You can add more resources and adjust the order on this panel. Use the buttons in the middle of the panel to add, remove, and rearrange resources to be imported.
9. Click **Next**.

   The **Configure Failure Options** wizard displays.
10. Select one of the fields from the **Configure Failure Options** wizard using the following table as a guide, and then click **Next**.

| Field | Description |
|---|---|
| **Ignore All Errors** | Indicates that you do not want the UOW to stop processing, regardless of how many failures occur. |
| **Fail After Total Errors** | Select the maximum number of failures you want to occur before the UOW stops processing. |
| **Fail After Percent Errors** | Select the maximum percentage of failures you want to occur before the UOW stops processing. This option is useful when there are a large number of command sets being applied to a large number of resources. If your desired percentage does not equal a whole number, the number of failures necessary to cause termination is rounded up. For example, if you select 51% and there are 2 command sets and 5 resources, the formula is as follows:<br>`Max # of failures: (51/100) x (2x5) = 5.1 = 5` |

   The **Password Override** wizard displays.
11. Select one of the fields from the **Password Override** wizard using the following table as a guide, and then click **Next**.

| Field | Description |
|---|---|
| **Override ITNCM Authentication** | Select this check box to override the default Netcool Configuration Manager authentication information. |
| **Login Name** | Provide the login name for the device you are accessing. |
| **Password** | Provide the password for the device you are accessing. |

| Field | Description |
|---|---|
| **Enable Password** | Provide the device enable password for the device you are accessing. |
| | Select this check box if you will always use this authentication for your resource. |

The **Execution Priority** wizard displays.

12. The default execution priority is low. Choose the appropriate priority and click **Next**.

    The **Schedule Work** wizard displays.

13. Select either immediate or scheduled execution. If you select scheduled execution, additional fields are displayed asking for the execution window. Provide the start date and time, and the end date and time for executing the work. From this dialog you can also specify a recurring schedule for the UOW. Click **Next** when complete.

    The **Describe Work** wizard displays.

14. Type a description and click **Finish**.
15. You can check the status of the Import Network Resource UOW processing. Navigate to the Queue Manager and select the "Work Currently Executing" queue. When the UOW has completed, it appears in the "Work That Is Finished" queue.
16. The device will now be listed under the root realm in the Resource Browser. It will be in a managed state.
17. You can also discover a device instead of manually importing it. Refer to the Admin guide for further information on Auto-Discovery.

# Running Netcool Configuration Manager - Compliance policies

Netcool Configuration Manager - Compliance should also be configured using the following procedures.

## Importing sample compliance policies

You can import sample compliance policies. These policies have been installed by default, and after you have imported them they will be available in the Netcool Configuration Manager - Compliance UI.

Before sample policies can be viewed, access permissions must be granted.

**Note:** Policies exported from a previous version of Netcool Configuration Manager can be imported into the most current version, but some errors may be reported.

1. Locate the sample policy folder:
   `/opt/IBM/tivoli/netcool/ncm/compliance/db/export/samplePolicies`
2. Copy the sample policies from the original location to the following directory:
   `/opt/IBM/tivoli/netcool/ncm/compliance/db/export/tables`

   You can use the following command:

   ```
   cp /opt/IBM/tivoli/netcool/ncm/compliance/db/export/samplePolicies/
   sample_policies.tar
   /opt/IBM/tivoli/netcool/ncm/compliance/db/export/tables
   ```

3. Locate the `/opt/IBM/tivoli/netcool/ncm/compliance/db/export/tables` directory and access the `sample_policies.tar` tar file. You can use the following command:
   `tar xvf sample_policies.tar`

   **CAUTION:** This step overwrites existing policies. Back up existing policy xml files, if required.

4. In the `/opt/IBM/tivoli/netcool/ncm/compliance/bin/utils` directory, run the following script to install the sample policies, and merge these with any existing policies:
   `./dbImport.sh`

5. To grant access privileges to the users who requires read access to the sample policies, use **AdminUser SecurityRealm Access Control**, and then add the user to **Allowed Groups**.

## Setting Netcool Configuration Manager - Compliance security

Netcool Configuration Manager - Compliance security must be setup to configure security permissions for policy realms. If the user does not have the appropriate realm permissions, they will not have visibility to policies.

This task describes how to set policy realm permissions in the Netcool Configuration Manager - Compliance security.

1. Login to the Netcool Configuration Manager - Compliance UI.
2. Select **Admin** > **User Security Options**.
3. Select the **Realm Access Control** tab.
4. Select **New Realm** to create a new realm in Netcool Configuration Manager - Compliance. When the **New Realm** screen is displayed, enter a realm name and select **OK**.
5. Then, select **Add Group(s)** to assign permissions to the newly created realm. When the **Select Groups** screen is displayed, choose one or more groups to add, and select **OK**.
6. Select **Close** to complete.

## Executing a policy

Policy execution describes the various methods that may be used to invoke and run compliance policies can be validated against the network. It also describes the steps a user must take in order to execute the policies that have been created on the network.

Please note in the event that realms are moved or renamed, any previously scheduled policies which are set to execute against devices involved in the changed realms shall execute against zero devices. This is only an issue if the realms are changed while the Netcool Configuration Manager - Compliance server is stopped.

Policy execution can be triggered by a number of events: on demand initiation, scheduled initiation and automatic initiation.

**Note:** Please ensure that the correct security access is obtained before attempting to execute any policies. The user must be a member of a group who has "Execution" rights. This enables the user to execute compliance entities.

The following outlines the steps required to execute an ad-hoc policy.

1. Navigate to the policy in the Execution tab, either right click and select execute policy or select the 'Execute' icon
2. The **Create & Execute Adhoc Process** screen will be displayed. This screen requests a name and description to be added for the purposes of the policy execution. The Name field will be pre-filled with the server date and time. The name field is mandatory. Click Next to progress.
3. The **Select Devices** screen shall be displayed.
4. The Devices/Realms that are required to execute the Policy against should be selected. Using the navigation tree in the Device pane, select the necessary devices or realms.

   The Check device coverage button will inform if all devices in selection are covered by the policies, which will allow the user to continue to the next step. If there is a problem with the device coverage, the **Policy Coverage Check** screen will be displayed. This will give a reason such as: Policy not applicable or No rule applicable.
5. Click Next on the **Select Device** screen to progress
6. Immediately before the **Parameters** screen is displayed, a pop-up box will appear to confirm the user would like to view parameters. Select ‘Yes' to view the parameters (if any) from the selected policies. If parameters have been used in any of the policy definitions that are included in a process, the appropriate override value must be provided in this screen if required.

7. The **Report Options** screen is displayed. The following table describes the options available.

*Table 4. Report options*

| Option | Description |
|---|---|
| Generate Report | When checked this will generate a report each time that the policy is executed. By default this is unchecked. |
| Report Type | Options are Summary, Policy, Device and Validation Detail.<br>**Summary** reports provides a bar chart showing the results by result category, and another bar chart showing the breakdown of failed results by severity.<br>**Policy** reports list the compliance validation results for each device. The results can be further interrogated to produce the Validation Detail report.<br>**Device** Reports list the compliance validation results for each policy. The results can be further interrogated to produce the Validation Detail report.<br>The **Validation Detail** reports provides a further level of information on the Device/Policy reports to determine what impact the evaluation criteria had on the result. |
| Show Results | User can choose which Results they wish to report on. By default all validation results are shown, but the user can opt to exclude any of the following results: Pass, Exempt, Fail, Not Assessed |
| Show Severity Levels | User can choose which Severity Levels they wish to report on: Severity 1-5. By default all Severity Levels shall be included in the report, but users have the option to exclude certain severity levels from the report |

**Note:** The Show Results and Show Severity Levels report options are greyed out if the "Summary" report type is chosen. The Summary report is based on all validation results (i.e. Passed, Failed, Exempt, Not Assessed), and also includes all severity levels.

Please enter the information as required, and click Next to continue to the next screen.

8. The **Distribution** screen is displayed. This is an optional screen. Please note that report distribution and report storage options are only available for Scheduled reports.

   As part of report distribution, an e-mail message can be constructed using the template provided. The E-mail body is free-text and can be used to add any comments as required. There are a number of file types supported for the Report email attachment, including: PDF, HTML, Excel, Text, RTF, XML, PostScript and Result File.

   Report Storage provides ability to save the report result on the server for retrieval at a later date. Report storage when checked will store the report in the "Saved Reports" tab for later retrieval.

9. Click Finish to complete the Policy execution.

10. When the policy executes, the user interface defaults to the Process Execution Summary in the Results tab. The progress of the policy execution can be tracked with the help of this screen. In the **Process Execution Summary** screen, a policy executed will have an execution type of "AdHoc".

**Related tasks**

Applying policies (via wizard)
Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

## Creating a compliance process

Use this procedure to define a new Compliance Process. Defining a new Compliance Process requires access to the User Interface wizard.

In defining Compliance Processes, a user must specify against which devices the process must run. For example, it is possible to run a process against all devices that must adhere to the set of policies that are included in the process. But it is also possible to set up a process that runs against only a sub-set of these devices, for example all devices in a part of the network that share the same NTP server. It is simple for a user to copy an existing Process, and modify some its components in order to create a new Process.

You can define the process parameters during the creation of the Compliance Process or later.

Follow the steps outlined under 'Procedure' to create a Compliance Process.

1. Select **CreateProcess**.

   The **Name and Description** window displays. Mandatory fields are denoted by an * (asterisk). Policy selection is also required at this stage.
2. Use the following descriptions as a guide to entering the appropriate information in the **Name and Description** window.

   **Name**
   Specifies the name used to identify the process. This field takes a maximum of 255 characters. This is a mandatory field.

   **Description**
   Specifies a brief narrative attached to the Policy whose purpose is to explain its function or use. This field takes a maximum of 4000 characters.

   **Revision**
   Specifies an automatically generated number that is given an initial value of one. Each time the Policy is edited, the revision number is incremented by one. This is for versioning control.

   **Enable process for automatic validations**
   When selected this option indicates that the policies selected within this process may be used by automatic processes.

   **Policy Selection**
   Policies to be included in the validation procedure should be selected here. Select the Policy/ Policies required from the navigation pane, and select using the arrows in the middle of the panel. A new Policy may be created at this stage using the **Create new** icon; this invokes the **Create a Policy** window.
3. Click Next on the **Name and Description** window.

   The **Pre-Emptive Options** window displays.
4. Use the following descriptions as a guide to entering the appropriate information in the **Pre-Emptive Options** window.

   **Enable Pre-Emptive Compliance Options for this Process**
   Specifies a check box that enables or disables the specified Compliance Process for pre-emptive compliance.

**Policy Name**
Specifies a list of Policies to be included. Policies that are not enabled for pre-emptive compliance appear in the list, but are greyed out. The user does not have the ability to enable them for pre-emptive compliance.

5. Click Next on the **Pre-Emptive Options** window.

   The **Select Devices** window displays.

6. Use the following descriptions as a guide to entering the appropriate information in or to making use of the icons at the bottom of the **Select Devices** window.

   **Retrieve Realms Button**
   Populates realms created

   **Device/Realm Selection drop-down menu**
   Options to view devices, realms, VTMOS device and VTMOS realm.

   **Check Device Coverage Button**
   Checks if Policies cover all devices selected.

   **Note:** The Check Device Coverage button will inform if all devices in the selection are covered by the policies, which will allow the user to continue to the next step in creating a Compliance Process. If there is a problem with the device coverage, the **Policy Coverage Check** window screen will be displayed. This window displays a reason such as: Policy not applicable or No rule applicable.

   **Search for Devices**
   Conduct a search on devices based on Name, Realm, Status, Synced at, and VTMOS.

   If sub-realms are employed in your realm structure, and you want to include these sub-realms in your selection, you must check the **Include Subrealms** checkbox. By default this is checked.

   The Devices/Realms that are required to execute the Process against should be selected. Using the navigation tree in the Device pane, select the necessary devices or realms.

7. Click **Next** on the **Select Devices** window.

   The **Parameters** window displays.

   You cannot add any new parameters here, but if you edit an existing parameter when creating a new policy that will create a process parameter in the 'Process Parameter' tab in the Process Administration GUI.

8. Select an existing parameter that exists in one of the included definitions, and then click **View** > **Edit**. Use the following descriptions as a guide, and note that not all of the following fields are editable:

   **Name**
   Specifies the name of the parameter. Parameters that have already been created in any of the Compliance definitions or through parameter administration display in this window.

   **Type**
   Specifies the type of the parameter, either LOCAL or GLOBAL.

   **Description**
   Specifies a description for the parameter.

   **Current Value**
   Specifies the current value for the parameter.

   **Default Value**
   Specifies the default value for the parameter.

   **Realm**
   Specifies the realm.

9. Click Next on the **Parameters** window.

   The **Process Schedule** window displays.

10. Use the following descriptions as a guide to entering the appropriate information in the **Process Schedule** window.

**Unscheduled**
Specifies a radio button used to specify an unscheduled execution of a Compliance Process.

**Scheduled**
Specifies a radio button used to specify a scheduled execution of a Compliance Process.

**Recurring Schedule**
Specifies radio buttons used to specify a scheduled or recurring execution of a Compliance Process. The recurring schedule is offered on an hourly, daily, weekly, monthly, or yearly basis.

**Server Time:**
Specifies the user's preference for date and time on the UI.

**Scheduled Monthly**
Specifies radio buttons used to specify the day and month if the Monthly radio button is selected.

11. Click Next on the **Process Schedule** window.
12. The **Choose a Save Location** window displays.
13. Navigate through the tree structure, and choose the location where you want to save the newly created Compliance Process. Otherwise, it is possible to create a new folder from here if required.
14. Click Finish on the **Choose a Save Location** window to complete the creation of the Compliance Process.

You can create another Compliance Process by following these instructions.

**Related tasks**

Editing process parameters
Use this procedure to edit process parameters.

Searching for devices
Searches may be performed on column names which appear in the devices tab. The devices search is invoked by clicking on the search icon. The Search By Column screen appears on the left hand side of the user interface.

Creating pre-emptive policies
Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device, allowing you to evaluate the impact of configuration changes against pre-defined compliance policies for a device. In order to run a pre-emptive compliance, you first create or modify existing policies to make them suitable for execution in a pre-emptive manner. You then create a compliance process to apply the pre-emptive policy to a device.

## Viewing results

Netcool Configuration Manager - Compliance will run the validation of devices against policies and generate the validation results. All results across all validations will be stored in the Netcool Configuration Manager - Compliance database, and are available for review by the user until they are removed through house keeping.

The user may only view those Processes/Devices/Actions for which they have security permissions for. This is controlled through both Netcool Configuration Manager - Base and **Admin** > **User Security Options**.

The Results screens are flexible and easy to use, the user has the abilities to:

- Sort the results based on column headers
- Increase and decrease column width to better view the data
- Hide and unhide rows and columns
- Access Summary and detailed information by allowing the user to drill down on specific devices to view configuration level detail
- Use customizable Paging feature for easy navigation through results
- Export Policies in the Validations screen

The Results page gives the user access to compliance validation results based on their level of security. There are a number of different views in the Results tab, where validation results can be viewed and analyzed. Whilst the Home page provides a summary of all devices on the network, the Results tab indicates policy status in a greater level of detail.

Users have various methods to review these results. They can review results in context of the ad-hoc, unscheduled, scheduled or automated process that generated the results. Users only interested in policy violations may want to review the notifications that were generated during the various compliance validations. Users also have the ability to perform a detailed search through the results and immediately see the result of their search.

Remedial actions may be generated for devices that violate a policy. These remedial actions will be placed in the remedial actions queue. Network engineers can approve the remedial actions in this queue, which will then trigger a configuration change action to run against the device to bring the device back into compliance.

**Related tasks**

Viewing pre-emptive policies and results

Use the pre-emptive compliance functionality to check proposed configuration changes to a device against predefined compliance policies for that device. Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device. The capability is intended to enable customers to evaluate the impact of configuration changes against predefined compliance policies for a device.

Viewing device configurations

There are a number of options available for viewing device configurations. They can be viewed as Native Commands, Stored 'Show' Commands, or Modelled Configurations (for smart model devices).

Applying policies (via wizard)

Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

# Chapter 2. Discovering network devices

Use this information about Netcool Configuration Manager to perform network discovery tasks.

## Overview

To perform discovery, you use the Auto-Discovery tool in conjunction with the BulkLoader utility, only in a stand-alone installation. If Netcool Configuration Manager is integrated with Network Manager, use the ITNM discovery driver to perform discovery.

### The Auto-Discovery tool

The Auto-Discovery tool is used in conjunction with the BulkLoader utility. A device seed file provides login credentials and is fed into the Auto-Discovery tool.

The Auto-Discovery tool will connect to devices using either TELNET or SSH, sending the necessary show commands to that device. Using the CLI that is returned, the Auto-Discovery tool will then determine the Vendor, Type, Model, and Operating System (VTMOS) of each network resource.

The output generated by the Auto-Discovery tool is the `BulkLoad.csv` file, which is used by the BulkLoader utility to load devices into the Netcool Configuration Manager database.

For more information on the BulkLoader utility, see the *IBM Tivoli Netcool Configuration Manager Administration Guide*.

### The DeviceInfo.txt file

The `DeviceInfo.txt` file contains the information passed to the script that executes the Auto-Discovery tool. In this file, you specify password groups, realms, and device IP addresses, all of which are required for most administrative tasks. In the `DeviceInfo.txt` file, you also specify the results directory where the Auto-Discovery tool writes all of its output result files.

For more information on the `DeviceInfo.txt` file, see “Editing DeviceInfo.txt” on page 18 and “Deviceinfo.txt syntax” on page 18.

### The Auto-Discovery tool results directory

The Auto-Discovery tool results directory is specified in the `DeviceInfo.txt` file and can be in any location. The Auto-Discovery tool writes all of its output result files in this auto discovery results directory. If the specified results directory name does not exist, the Auto-Discovery tool creates it.

The Auto-Discovery tool creates two CSV files, a log file, and one text file that contains the results of the auto discovery operation. The Auto-Discovery tool uses the following naming scheme for all of the output result files:

```
realm_name-date-fileandextension
```

An example name for one of the CSV files is `IBM-test-juniper-20070308-BulkLoad.csv`.

The following table describes each of the output result files.

| Output result file name | Description |
|---|---|
| `BulkLoad.csv` | Created as a result of the devices it has "discovered" in a form that the BulkLoader utility will be able to recognize. Details included are: realm, hostname, vendor, type, model, and os. In addition, the following custom RAD feature is included, so these can be used if required: |

| Output result file name | Description |
|---|---|
| | `"com-type, ssh-type, streaming, username, password, enable-password, althostname, port"` |
| `TelnetScan.csv` | Contains the details of each device, including login information and VTMOS. |
| `LoginResults.txt` | Contains the results of login to each device. Displays details of account name and password, and indicates whether the login was successful or not. |
| `Auto-Discovery.log` | Contains a log of completed scans applied to all of the specified IP addresses. Includes date/time stamp, and indicates location to view the result of successful scans. |

The Auto-Discovery tool creates a file that the BulkLoader utility (executed by specifying the `BulkLoader` keyword when executing the `icosutil` utility) uses to import the device or devices into the Netcool Configuration Manager database. This is attached to the results folder as `bulkload.csv`. This is the most important file produced by the utility, and contains all the information required for the bulk import into theNetcool Configuration Manager database.

The other output files are useful for problem resolution, in the case where a particular device cannot be discovered.

## The command.properties file

The `command.properties` text file contains show commands. Show commands are the commands that the Auto-Discovery tool sends to a device to make sure the device has logged in once. Once the device is logged in, the show commands return CLI for determining VTMOS.

You can modify the `command.properties` text file to add, remove, and edit the show commands that the Auto-Discovery tool uses.

For more information on the `command.properties` file, see “Configuring Auto-discovery commands” on page 21.

## The ad.properties file

The `ad.properties` file contains information used to configure how the Auto-Discovery tool executes.

For more information on the `ad.properties` file, see “Configuring Auto-Discovery properties” on page 21.

## Support for new devices

The Auto-Discovery tool uses five external XML files to parse the CLI from a device to discover a VTMOS. In order to add support for a new device, three of these files: `RegexList.xml`, `MapVendor.xml`, and `MapType.xml` require an update. The other two files: `MapModel.xml` and `MapOS.xml` only require an update if the model number and OS obtained from the CLI needs to be mapped to a different model number and OS.

**Note:** If support for a new device is added, a ticket should be raised to ensure support for this addition is available in the next release of the product. The Regular expression (Regex) entries as well as CLI output retrieved from the device should also be included.

# About head end devices

Head end devices are another type of resource on which Netcool Configuration Manager operates. Specifically, Netcool Configuration Manager provides a framework that makes it easier to administer and use head end devices. A head end device is a central control device required by some networks (for example, Local Area Networks (LANs) or Metropolitan Area Networks (MANs)). Head end devices provide centralized functions such as re-modulation, re-timing, message accountability, contention control, diagnostic control, and access to a gateway. A head end device can also refer to a central control device within CATV systems that provides centralized functions such as re-modulation.

Generic examples of head end devices include the following:

- Devices that model their internal architecture as virtual devices (for example, the Juniper ERX head end device, which supports multiple virtual routers).
- Devices that facilitate virtual networks (for example, hypervisors and BNT devices that support hypervisors).
- Software devices (for example, the CISCO Nexus, which emulates a set of blade switches managed by a blade supervisor).
- Rack controllers that act as a head end controller for cards in a shelf.
- TL-1 gateways for Sonet and SDH transmission devices.
- EMS systems that manage a set of vendor specific devices.
- Head end devices that act as supervisors for CATV or Telephony services.

Head end devices manage one or more virtual or physical devices. These virtual or physical devices are referred to as head end managed devices.

## Understanding conventional head end devices

A conventional head end device acts as the configuration controller for one or more head end managed devices. Changes made to the head end configuration can be targeted at specific head end managed devices. System administrators apply these changes to specific head end managed devices through some internal protocol.

Conventional head end devices are the most common form of head end device. Examples of conventional head end devices include:

- Hypervisors — Hypervisors are software programs designed to manage multiple operating systems running on the same computer system. Typically, hypervisors manage the operating systems' processor, memory, and other resources.
- Rack controllers
- Devices such as the Juniper ERX that model their configuration in terms of virtual routers. Another example is the CISCO Nexus, which provides access to the virtual blade servers through an FSM head end.

## Understanding head end device and managed device redundancy

The term redundant is used to describe one or more components in a computer or network system that serves as a backup system to protect the main system in the event of a failure. There are a number of relationships associated with redundancy that can exist between devices and the head end devices that manage them. System administrators need to understand these relationships to effectively manage head end devices and their associated managed devices.

### Head end device redundancy

A single device could be managed by more than one head end device. For example, a device could exhibit physical redundancy with two head end devices, where one head end device serves as the main backup and the other serves as a secondary or standby backup. In the case of a transmission ring, any device

within the ring can perform the role of a head end device. Thus, the associated head end managed devices could be managed by one or more of the head end devices in the transmission ring.

Netcool Configuration Manager handles redundancy at the head end device level by duplicating both the head end devices and the devices that they manage. This approach can be expressed as 1 head end device to *N* head end managed devices.

### Stand alone device redundancy

A single device could operate within a protection group of *N* identical devices. While one device within the group is designated the master, the remaining devices are designated as standbys ready to take over the responsibility of the master upon a failure. Device redundancy can also exist at the virtual device level. For example, VMware (and other hypervisor vendors) can move a Virtual Machine (VM) between servers (hypervisors) transparently to the end user. However, this mechanism relies on the virtual network employed by the VMs to be replicated on both the original and target servers.

Netcool Configuration Manager handles redundancy at the device level by treating each device for which access is possible as a unique device. This approach ignores any protection agreement between devices (for example, where cards/blades provide physical redundancy). In the case where redundancy of devices is forced due to vendor constraints, Netcool Configuration Manager again treats each instance of the device as unique. For example, in the case of VMware where vswitches are replicated on all instances of hypervisor for which VM protection is enabled, Netcool Configuration Manager treats each instance of vswitch as a unique device. Likewise, Netcool Configuration Manager regards all instances of hypervisor as unique.

## Understanding the discovery process for head end devices

Device discovery is the process of “finding” devices and adding these devices to Netcool Configuration Manager for the purpose of configuration management.

Users can initiate the discovery of both head end and non-head end devices. However, the discovery of head end managed devices is the responsibility of the head end driver and will be triggered each time the driver is requested to “reconcile” the configuration of the head end device configuration.

Users can also manually add devices through the Netcool Configuration Manager API or Netcool Configuration Manager client.

## Understanding the methods used to discover and add devices

Use this information to review the existing methods Netcool Configuration Manager provides to discover and add stand alone devices and head end devices. This information also identifies the method Netcool Configuration Manager uses to discover and add devices to be managed by head end devices.

A user can add a new stand alone device or head end device to Netcool Configuration Manager by using one of the following methods:

- Device synchronization with Network Manager
- Manual addition of the device through the Netcool Configuration Manager API or Netcool Configuration Manager client GUI
- Discovery of the device through the Netcool Configuration Manager discovery mechanism

For head end managed devices, Netcool Configuration Manager automatically adds them when they are discovered through their associated head end devices.

In all of the these discovery methods, Netcool Configuration Manager determines if the device is a head end device through the driver associated with that device. Furthermore, once a device is discovered, Netcool Configuration Manager must determine the VTMOS for the device. The following table summarizes how Netcool Configuration Manager determines the VTMOS for the device, based on the discovery method.

| Discover/add device method | How Netcool Configuration Manager determines the VTMOS for the device |
|---|---|
| Device synchronization with Network Manager | The device synchronization process creates a device discovery unit of work (UOW). Part of this UOW is to access the device and apply a set of commands to the device. The response to these commands is parsed using a set of user defined regular expressions, from which the VTMOS is identified.<br>When the device is imported for the first time, a driver is identified based on this VTMOS. On access to the device, the driver will issue commands of its own to identify the VTMOS. If another driver offers better support for this device then a user can confirm acceptance of the new driver. |
| Manual addition of the device through the Netcool Configuration Manager API or Netcool Configuration Manager client | The user specifies the VTMOS when creating the device. If the VTMOS is entirely wrong for the device, then discovery fails. If however the VTMOS results in a driver being chosen which can at least access the device then the actual VTMOS “could” be determined (based on how “near” the original VTMOS is). The actual VTMOS will be used in subsequent accesses to the device which will result in the correct driver being chosen. |
| Discovery of the device through the Netcool Configuration Manager discovery mechanism | Identical to device synchronization with Network Manager |
| Netcool Configuration Manager auto discovery | The auto discovery feature currently does not support the automatic discovery of head end devices. |
| Discovery of conventional head end devices | A conventional head end device knows the VTMOS for its head end managed devices. There is no need to employ the current Network Manager discovery process. New devices discovered should have the same VTMOS as the parent head end device, except for the type field which should distinguish the head end managed device as a `vdevice`. This retains sufficient information in the VTMOS to relate it to a specific version of the OS. This type could be further refined to `vrouter`, `vswitch`, and `vbridge`if required.<br>**Note:** The previous description describes a VMWare and HMC environment. A virtual device can have a different VTMOS (including vendor) than the head end device that manages it. |

## Understanding the discovery of head end devices with Network Manager IP Edition

Use this information to learn how Netcool Configuration Manager discovers head end devices in conjunction with Network Manager IP Edition.

Currently Netcool Configuration Manager synchronizes the list of managed devices with Network Manager IP Edition through an API. There is no direct access to the NCIM database. In a standalone environment, without the presence of Network Manager IP Edition, Netcool Configuration Manager carries out the task of device discovery.

# Editing DeviceInfo.txt

Use this information to learn how to set up and maintain the `DeviceInfo.txt` file. This information includes creating the file and adding password groups, realms, and device IP addresses, all of which are required for most administrative tasks.

The `DeviceInfo.txt` file must be created in order to pass parameters to the script that executes the Auto-Discovery tool. The name of this file is arbitrary, as long as it has an extension of `.txt`. You must make sure to specify this file when calling the script that executes the Auto-Discovery tool.

The location of the `Auto-Discovery.jar` file is unimportant as long as the directory path has been fully qualified.

1. Navigate to an appropriate directory where you want the `DeviceInfo.txt` file to reside. The following example shows the use of the `cd` command on a Linux or Unix system to navigate to an appropriate directory:

   ```
   cd /opt/IBM/tivoli/netcool/ncm/autodiscovery/devicefiles
   ```

2. Using a text editor, create a file called `DeviceInfo.txt` (or any other meaningful file name). The following example uses the vi editor (on Linux or Unix) to create a `DeviceInfo.txt` file:

   ```
   vi DeviceInfo.txt
   ```

3. Use the appropriate syntax to populate the contents of the `DeviceInfo.txt` file with password groups, realms, and device IP addresses.

Here is a complete example of the previous steps:

```
cd /opt/IBM/tivoli/netcool/ncm/autodiscovery/devicefiles
vi DeviceInfo.text
```

For details on the syntax used to populate a `DeviceInfo.txt` file, see "Deviceinfo.txt syntax" on page 18.

## Deviceinfo.txt syntax

Use this information to understand the syntax used to add password groups, realms, and device IP addresses to the `DeviceInfo.txt` file.

### Purpose

The `DeviceInfo.txt` file is used to pass parameters to the script that executes the Auto-Discovery tool.

### Syntax

```
a:username
p:password
e:password
d:location of results folder
r:realm
device IP address
.
.
.

[r:realm]
[device IP address]
.
.
.
```

**a:** ***username***
Specifies the name of the user.

**p:** ***password***
Specifies the password of the user.

**e:** ***enable password***
Specifies that the password of the user be enabled.

**r:** ***realm***
Specifies the realm. The realm is followed by one or more IP addresses. Use the realm syntax to specify as many realms as necessary to create multiple realms. At least one realm must be created.

**Note:** There must be no blank lines in between the lines of syntax. Otherwise, the Auto-Discovery tool may fail.

## Syntax for adding a password group

The following example shows the syntax used to add a password group. This password group is used to log onto a device.

```
a:acc1
p:pwd1
```

The account name is preceded by `a:` and the password for that account by `p:`. The `DeviceInfo.txt` file must contain at least one password group. Multiple password groups may be added if required.

## Order for using multiple password groups

When using multiple password groups in the `DeviceInfo.txt` file, the order in which they are entered may affect the performance of Auto-Discovery. To facilitate the most efficient discovery, arrange password groups that are most commonly used first. The reason being that for every password group, a connection is opened to each device. This ensures that the minimum number of connections to the password groups are established.

## Syntax for adding an enable password

The following example shows the syntax used to add an enable password:

```
e:epwd1
```

The enable password is preceded by `e:`. The `DeviceInfo.txt` file must contain at least one enable password. Multiple enable passwords can be added, simply by repeating the line in the text file with a different password.

The enable password used has no dependency on the password group used. Once Auto-Discovery has logged onto a device, it can attempt a number of passwords to gain access to enable mode.

## Syntax for adding a results directory

The following example shows the syntax used to add a results directory on a Windows operating system platform:

```
d:.\results
```

The results directory is preceded by `d:`. This is the directory where the Auto-Discovery tool creates the output files. For example, the location might be in the current working directory in a folder called `\results`.

The results directory will be written to any location provided. The naming of this file is arbitrary, as long as the directory is specified. If the directory name specified does not exist, the Auto-Discovery tool will create it.

## Syntax for adding a realm

The following example shows the syntax used to add a realm on a Windows operating system platform:

```
r:example\devices
```

The realm is preceded by an `r:` (the letter`r:` followed by a colon). This is the name of the realm that will be written to the `BulkLoad.csv` file. When using the Bulk import utility to import the CSV file into Netcool Configuration Manager, this is the realm the devices will be held under.

The specified realm should be a valid host realm. If the specified realm does not exist in Netcool Configuration Manager, the Bulk Loader will fail. The `-cr` command can be used to create a realm, if the realm you are importing to does not already exist.

For further information about Adding Realms, see the *IBM Tivoli Netcool Configuration Manager Administration Guide*.

## Syntax for adding device IP addresses

The following example shows the syntax used to add a device IP address:

```
182.178.29.1
```

Specifying device IP addresses does not require any preceding characters. They are inserted into the files as shown. All individual device IP addresses should be listed. IP ranges are also accepted. For example: `182.178.29.*`. Host names may also be used.

### Sample

The following example shows a sample `DeviceInfo.txt` file with multiple user accounts, enable passwords, realms, and IP addresses:

```
a:acc1
p:pwd1
e:epwd1
a:acc2
p:pwd2
e:epwd2
d:.\results
r:example/devices
10.216.254.*
10.216.255.1
10.216.255.2
r:example/devices2
10.216.255.3
10.216.255.4
10.216.255.5
10.216.255.6
10.216.255.7
10.216.255.8
10.216.255.9
10.216.255.10
10.216.255.11
```

Using the `DeviceInfo.txt` file sample, Auto-Discovery will use the following password groups to log onto devices:

```
log onto devices:
Group 1 (account=acc1,password=pwd1)
Group 2 (account=acc2,password=pwd2)
Group 3 (account=acc3,password=pwd3)
```

Once logged onto a device, one of the following enable passwords will be used to access enable mode:

```
epwd1, epwd2
```

All results files created by Auto-Discovery will be placed in the current working directory called `results`. The realm name for performing the bulk importing of devices into Netcool Configuration Manager will be `example/devices`. Auto-Discovery will attempt to discover all the devices listed after the realm name.

## Configuring Auto-discovery commands

Show commands are the commands that Auto-Discovery sends to a device to make sure the device has logged in once. Once the device is logged in, the show commands return CLI for determining VTMOS.

The show commands are kept in a text file called `command.properties`. This text file may be modified to add, remove, and edit show commands that Auto-Discovery uses.

## Configuring Auto-Discovery properties

To configure Auto-Discovery tool properties, edit the `ad.properties` file. This file contains properties used to configure how the Auto-Discovery tool executes.

The following example is a sample of the `ad.properties` file that contains the properties used to configure how the Auto-Discovery tool should execute.

```
connectionType=ssh,telnet,snmpv3,https
customRad=false
delayBetweenConnectionAttempts=1000
hostNames=false
logIntoEnableMode=true
numberOfThreads=10
ssh1Cipher=3des
ssh2Ciphers=
ssh2MacAlgos=
ssh2LogFile=
ssh2LogLevel=0
sshPort=22
sslPort=443
telnetPort=23
timeOut=30
```

This task requires you to edit the properties in the `ad.properties` file.

1. Using a text editor, open the `ad.properties` file
2. Use the following table to learn about each property and its valid values.

| Property | Description |
|---|---|
| `autoAnswerLoginPrompts` | Specifies a string list of possible auto answer login prompts displayed by devices. Separate each prompt with a `,` (comma). |
| `autoAnswerPrompts` | Specifies a string list of possible auto answer prompts displayed by devices. Separate each prompt with a `,` (comma). |
| `commandErrorMsgs` | Specifies a string list of possible command error messages displayed by devices. Separate each message with a `,` (comma). |
| `connectionType` | Specifies the connection type. The connection types currently supported are TELNET and SSH. Either type may be used, or else a combination of the two. If a combination is used, Auto-Discovery will use the connection types in the order they are supplied. In the example provided SSH is used first to connect to the device, and if no connection can be established then TELNET is used. The default order is specified by `ssh,telnet`. |
| `customRad` | Specifies whether the custom RAD feature is used when bulk importing into Netcool Configuration Manager. The parameter for creating a custom RAD is a boolean, and can be set to true or false. By default this value is set to false. |
| `delayBetween ConnectionAttempts` | Specifies the delay, in milliseconds, between connection attempts with different user ID groups as well as between sending the different enable passwords. |

| Property | Description |
|---|---|
| enableSuccessMsgs | Specifies a string list of possible success messages displayed by devices when the enable command is run. Separate each message with a , (comma). |
| hostNames | Specifies a Boolean value that indicates whether the host name is to be used in the discovery output file instead of the IP address. The default value is false. |
| ignorePromptsEnding | Specifies a string list of possible prompts displayed by devices that the tool should ignore. Separate each prompt with a , (comma). |
| loginErrorMsgs | Specifies a string list of possible login error messages displayed by devices. Separate each message with a , (comma). |
| logIntoEnableMode | A boolean parameter. If set to true, autodiscovery attempts to log into enable mode on the device. If false, it does not. The default for this parameter is "true". |
| numberOfThreads | Specifies the number of threads that Auto-Discovery uses, which is the number of devices it can discover at a time. The default value for this property is 10. |
| passwordPrompts | Specifies a string list of possible password prompts displayed by devices. Separate each prompt with a , (comma). |
| replaceChars | Specifies a string list of possible characters to replace, like escape characters. Separate each string with a , (comma). |
| ssh1Cipher | Specifies the preferred cipher used when connecting to a device via SSH1 protocol. The default value is 3des. You can specify multiple ciphers. Separate each cipher with a , (comma). For the values to use, refer to the documentation for your devices, Java Runtime Environment, and Java Security Provider. |
| ssh2Ciphers | Specifies the preferred cipher used when connecting to a device via SSH2 protocol. The default value is aes128-cbc. You can specify multiple ciphers. Separate each cipher with a , (comma). For the values to use, refer to the documentation for your devices, Java Runtime Environment, and Java Security Provider. |
| ssh2LogFile | Specifies the file name where the tool writes the mindterm communication logs. |
| ssh2LogLevel | Specifies the level of mindterm communication logs that should appear in the log file. The default value is 0. Allowed values are any integer from 0 to 7. The following list shows the allowed values and their meanings:<br>• 0 EMERGENCY<br>• 1 ALERT<br>• 2 ERROR<br>• 3 WARN<br>• 4 NOTICE<br>• 5 INFO<br>• 6 DEBUG<br>• 7 DEBUG2 |

| Property | Description |
|---|---|
| ssh2MacAlgos | Specifies the preferred MAC Algorithms used when connecting to a device via SSH2 protocol. You can specify multiple MAC algorithms. Separate each algorithm with a , (comma). For the values to use, refer to the documentation for your devices, Java Runtime Environment, and Java Security Provider. If this value is not provided, then the MAC algorithm that is configured on the device is used. |
| sshPort | Specifies the device port used by SSH to establish a connection. The default is 22. |
| sslPort | Specifies the port used for SSL connections. The default is 443. |
| timeout | Specifies the connection time out value, which is the value, in seconds, indicating when the device connection will time out. By default this value is set to 20. |
| telnetPort | Specifies the device port used by TELNET to establish a connection. The default is 23. |
| timeOut | Specifies the device connection timeout, in seconds. By default this value is set to 20. |
| usernamePrompts | Specifies a string list of possible username prompts displayed by devices. Separate each prompt with a , (comma). |

3. After you complete your edits, save and close the ad.properties file.

You can now run the script that executes the Auto-Discovery tool.

## About customizing Regexlist.xml

The RegexList.xml file contains Regex for determining a device's VTMOS. These expressions are all embedded inside the <regexlist> XML tags.

Regular expression (Regex) is a string that is used to describe or match a set of strings, according to syntax rules.

The XML files used to add support for new devices are parsed using an XML parser. XML has a special set of characters that cannot be used in normal XML strings, and must be replaced by an alternative set of characters. The following table identifies the characters that cannot be used in normal XML strings and their associated alternative characters:

| XML character that cannot be used in normal XML strings | Alternative character |
|---|---|
| & (ampersand) | &amp; |
| < (less than symbol) | &lt; |
| > (greater than symbol) | &gt; |
| " (double quote) | &quot; |
| ' (single quote) | &#39; |

The following example shows an invalid XML string:

```
<value>model->2621<value>
```

This example shows a valid XML string:

```
<value>model-&gt;2621</value>
```

The > (greater than symbol) in the first XML string has been replaced with its alternative (>) in the second string. This makes the string valid.

The examples that follow describe how to:

- Configure a Regex for discovering a vendor, model, and os
- Configure a Regex for discovering a new vendor, model, and os

## Customizing Regexlist.xml

The RegexList.xml file contains Regex for determining a device's VTMOS. These expressions are all embedded inside the <regexlist> XML tags.

Before editing the RegexList.xml file, you must be familiar with Regex and XML.

In order to add support for new devices, the CLI is obtained from the device, and read in as a string. Regex is applied to this string, which in turn extracts the VTMOS information for a particular device.

**Note:** A CLI is a prompt-driven user interface to an operating system or application. The Windows Command Prompt application in a Windows operating system is an example of a CLI.

This task assumes that you are familiar with the XML tags described in the following table:

| XML tag | Description |
|---|---|
| <vendor> | At the beginning of the RegexList.xml example file are the Regex for determining a device's vendor. This is embedded inside <device> tags. The name attribute in the <vendor> tag indicates that everything enclosed within these tags apply to CISCO devices only. |
| <model> | The <model> tags indicate that all Regex contained within these tags are to be used for parsing the CLI string from the device, in order to determine the model. Multiple <regex> tags can be embedded inside the <model> tags. Inside the <regex> tags are two further tags called <value> and <range>. The actual Regex is embedded inside the <value> tags. The <range> tag holds a single, or a range of digits that indicates which word(s) to extract as the model from the string returned. |
| <os> | The <os> tags indicate that everything contained within these are to be used for parsing the CLI string from the device. This will then be used to determine the operating system. Multiple <regex> tags can be embedded inside the <os> tags. Inside the <regex> tags are two additional tags called <value> and <range>. The actual Regex is embedded inside the <value> tags. The <range> tag holds a single, or a range of digits that indicates which word(s) to extract as the model from the string returned. An asterisk (*) embedded inside these tags will return the complete result from the Regex. |

1. Open the RegexList.xml file for editing.
2. Add the new Regex for discovering a new vendor, by embedding in the <device> tags within the <regex> tags (refer to the Example section). There are now two Regex for determining the vendor of the device: CISCO and Juniper.
3. Add the new Regex for discovering a new model by embedding the additional set of <regex> tags within the <model> tags. There are now two Regex for determining a CISCO device model.
4. Add the new Regex for discovering a new os by embedding the additional set of <regex> tags within the <os> tags. There are now two Regex for determining a CISCO device operating system.

   **Note:** The <model> and <os> tags can contain multiple <regex> tags. The order in which Auto-Discovery will use the model and os Regex will be the order in which they are embedded.
5. When you are satisfied with your edits, save and exit the RegexList.xml file.

The following `RegexList.xml` file example is used to illustrate the XML tags referenced in the previous procedure:

```
<regexlist>
    <device>[Cc][Ii][Ss][Cc][Oo]</device>* Used to discover vendor
    <vendor name="Cisco">
        <model>* Used to discover model
            <regex>
                <value>(?<=[Cc][Ii][Ss][Cc][Oo][\s])[\d]+</value>
                <range>*</range>
        </model>
        <os>* Used to discover operating system
            <regex>
                <value>(?<=[Vv]ersion[\s])[.|(|)|A-Z|a-z\d]+</value>
                <range>*</range>
            </regex>
        </os>
    </vendor>
</regexlist>
```

If this example `RegexList.xml` is used to parse the CISCO CLI example in “CLI examples” on page 36, the following would be returned:

```
vendor=CISCO, model=2651, os=12.4(5A)
```

If this example `RegexList.xml` is used to parse the Juniper CLI example in “CLI examples” on page 36, the following would be returned:

```
vendor=JUNOS, model=M5, os= 6.2R2.4
```

**Note:** The Regex in the `<device>` tags returns `JUNOS` as the vendor. In the `<vendor>` tags the `name` attribute is `Juniper`. Using MapVendor.xml, `JUNOS` will be mapped to output the actual vendor as Juniper.

You can now configure the `MapVendor.xml` file.

For instructions on how to configure the `MapVendor.xml` file, see “Customizing MapVendor.xml” on page 27.

To study a complete working example of a `RegexList.xml` file, see “RegexList.xml example” on page 25.

# RegexList.xml example

The `RegexList.xml` example contains the Regex for determining device VTMOS for these vendors: CISCO, Alcatel, and Motorola.

## Purpose

This example shows how to populate the XML tags associated with specifying Regex for determining device VTMOS.

### Sample

Study the following example to learn how to populate the XML tags associated with specifying Regex for determining device VTMOS.

```
<regexlist>
<!-- device vendor-->
<device>LE-[0-9]*</device>
<!-- WWP -->
<device>[Cc][Ii][Ss][Cc][Oo]</device>
<device>[Aa][Ll][Cc][Aa][Tt][Ee][Ll]</device>
<device>[Jj][Uu][Nn][Ii][Pp][Ee][Rr]</device>
<device>[Jj][Uu][Nn][Oo][Ss]</device>
<device>[Mm][Oo][Tt][Oo][Rr][Oo][Ll][Aa]</device>
<device>[Ee][Xx][Tt][Rr][Ee][Mm][Ee]</device>
<!-- CISCO DEVICE MODEL & OS -->
```

```
<vendor name="Cisco">
<model>
<regex>
<value>(?<=[Cc][Ii][Ss][Cc][Oo][\s])((((\d){3,5}))(?=.*[\S]|
processor|revision)|(?<=[Cc][Ii][Ss][Cc][Oo][\s]
[A-Za-z][A-Za-z])((((\d){3,5}))(?=.*processor|revision)|
(?<=[Cc][Ii][Ss][Cc][Oo][\s][A-Za-z][A-Za-z][A-Za-z]
[A-Za-z][A-Za-z])((((\d){3,5}))(?=.*processor|revision)|
(?<=[Cc][Ii][Ss][Cc][Oo][\s][A-Za-z])((((\d){3,5}))
(?=.*processor|revision)|(?<=[Cc][Ii][Ss][Cc][Oo][\s]
[A-Za-z][A-Za-z][-][A-Za-z]|Model:[\s][A-Za-z][A-Za-z]
[-][A-Za-z])((((\d){3,5}))(?=.*processor|revision|
[\s])|PIX[\s|-]Firewall</value>
<range>*</range>
</regex>
<regex>
<value>(?<=[Cc][Ii][Ss][Cc][Oo][\s])([\S]*)(?=.*processor|
revision)</value>
<range>*</range>
</regex>
</model>
<os>
<regex>
<value>(?<=SW:[\s]|Version[\s])[\d][\d|.|(|)|A-Z|a-z]*</value>
<range>*</range>
</regex>
</os>
</vendor>
<!-- ALCATEL DEVICE MODEL & OS -->
<vendor name="Alcatel">
<model>
<regex>
<value>ALCATEL.*[\d]{3,5}</value>
<range>3</range>
</regex>
</model>
<os>
<regex>
<value>[Ss]oftware[Vv]ersion.*[Aa][Ll][Cc][Aa][Tt][Ee][Ll]
<value>
<range>4</range>
</regex>
<regex>
<value>.*(?<=ALCATEL)</value>
<range>1</range>
</regex>
</os>
</vendor>
<!-- JUNIPER DEVICE MODEL & OS -->
<vendor name="Juniper">
<model>
<regex>
<value>(?<=([Mm]odel:[\s]|product-name>|description>|
host-name>))[A-Z|a-z|\d]+</value>
<range>*</range>
</regex>
<regex>
<value>Chassis.*</value>
<range>3</range>
</regex>
</model>
<os>
<regex>
<value>(?<=Software Suite \[|version>)([\d|.| |a-z|A-Z]*)
</value>
<range>*</range>
</regex>
</os>
</vendor>
<!-- WWP DEVICE MODEL & OS -->
<vendor name="Wwp">
<model>
<regex>
<value>Platform [Nn]ame.*\|.*[\\n\\f\\r\\t\|]*</value>
<range>4</range>
</regex>
<regex>
<value>[Oo][Pp][Ee][Rr].*\|.*[\\n\\f\\r\\t]*</value>
<range>3</range>
</regex>
</model>
<os>
```

```
<regex>
<value>Installed Package.*[\\n\\f\\r\\t]*</value>
<range>4</range>
</regex>
</os>
</vendor>
<!-- MOTOROLA DEVICE MODEL & OS -->
<vendor name="Motorola">
<model>
<regex>
<value>(?<=Description:[\s][A-Za-z][A-Za-z]
[A-Za-z][\s]|Chassis[\s][A-Za-z][A-Za-z]
[A-Za-z])([\d]){3,5}</value>
<range>*</range>
</regex>
</model>
<os>
<regex>
<value>SW [Vv]ersion.*[\\n\\f\\r\\t]*</value>
<range>3</range>
</regex>
</os>
</vendor>
<!-- EXTREME DEVICE MODEL & OS -->
<vendor name="Extreme">
<model>
<regex>
<value>#.*[Cc]onfiguration generated</value>
<range>2</range>
</regex>
<regex>
<value>[Bb]lackdiamond|[Ss]ummit|[Aa]lpine</value>
<range>*</range>
</regex>
</model>
<os>
<regex>
<value>[Vv]ersion.*[Bb]y</value>
<range>2</range>
</regex>
</os>
</vendor>
</regexlist>
```

## Customizing MapVendor.xml

The `MapVendor.xml` file is used by Auto-Discovery to map a unique string obtained from the CLI to that vendor name of that device.

Before editing the `MapVendor.xml` file, you must be familiar with XML.

This task assumes that you are familiar with the XML tags described in the following table:

| XML tag | Description |
|---|---|
| `<vendorlist>` | The file contains `<vendorlist>` tags. Embedded inside are `<vendor>` and `<output>` tags. The `name` attribute in each `<vendor>` tag indicates that everything enclosed within these tags apply to the specified vendor, which in this example are CISCO and Juniper devices only. |

1. Open the file for editing.
2. Edit the XML tags according to your needs. Use the Example section as a guide.
3. When you are satisfied with your edits, save and exit the file.

Consider the following XML tags in a sample file:

```
<vendorlist>
<vendor name="CISCO"> 1
<output>Cisco</output> 2
</vendor>
</vendorlist>
```

Now consider the following return from the Auto-Discovery tool when it uses a RegexList.xml file to parse the CISCO CLI:

```
vendor=CISCO  1
model=2651  2
os=12.4(5A)
```

The Auto-Discovery tool:

1. Compares the value `CISCO` returned to `vendor` with the value specified in the `name` attribute of the `<vendor>` tag. The values match.
2. Returns the value specified in the `<output>` tag, if the values in `vendor` and `<vendor>` match. In this example, returns the device vendor as Cisco.

Consider the following XML tags for Juniper in a sample file:

```
<vendor name="JUNOS">  1
<output>Juniper</output>  2
</vendor>
</vendorlist>
```

Now consider the following return from the Auto-Discovery tool when it uses a RegexList.xml file to parse the Juniper CLI:

```
vendor=JUNOS  1
model=M5  2
os=6.2R2.4
```

The Auto-Discovery tool:

1. Compares the value `JUNOS` returned to `vendor` with the value specified in the `name` attribute of the `<vendor>` tag. The values match.
2. Returns the value specified in the `<output>` tag, if the values in `vendor` and `<vendor>` match. In this example, returns the device vendor as Juniper.

You can now configure the `MapModel.xml` file.

For instructions on how to configure the `MapModel.xml` file, see “Customizing MapModel.xml” on page 29.

To study a complete working example of a file, see “MapVendor.xml example” on page 28.

# MapVendor.xml example

The `MapVendor.xml` file is used by Auto-Discovery to map a unique string obtained from the CLI to that vendor name of that device.

## Purpose

This example shows how to populate the XML tags associated with mapping a unique string obtained from the CLI to that vendor name of that device.

### Sample

Study the following example to learn how to populate the XML tags associated with mapping a unique string obtained from the CLI to that vendor name of that device.

```
<vendorlist>
    <vendor name="CISCO">
        <output>Cisco</output>
    </vendor>
    <vendor name="JUNIPER">
        <output>Juniper</output>
    </vendor>
    <vendor name="JUNOS">
        <output>Juniper</output>
    </vendor>
```

```
    <vendor name="WWP">
        <output>Wwp</output>
    </vendor>
    <vendor name="LE-311">
        <output>Wwp</output>
    </vendor>
    <vendor name="LE-310">
        <output>Wwp</output>
    </vendor>
    <vendor name="MOTOROLA">
        <output>Motorola</output>
    </vendor>
    <vendor name="EXTREME">
        <output>Extreme</output>
    </vendor>
    <vendor name="ALCATEL">
        <output>Alcatel</output>
    </vendor>
</vendorlist>
```

## Customizing MapModel.xml

The `MapModel.xml` file is used by Auto-Discovery to map a unique string obtained from the CLI to the model number of a device.

Before editing the `MapModel.xml` file, you must be familiar with XML.

This task requires that you become familiar with the XML tags described in the following table:

| XML tag | Description |
|---|---|
| `<vendorlist>` | The `MapModel.xml` file contains `<vendorlist>` tags. Embedded inside are `<vendor>`, `<model>`, and `<output>` tags. The `name` attribute in the `<vendor>` tags indicates that everything enclosed within these tags apply to the specified vendor, which in this example are CISCO and Juniper devices only. The `name` attribute in each `<model>` tag is used to match the model number returned in a CLI call. |

1. Open the `MapModel.xml` file for editing.
2. Edit the XML tags according to your needs. Use the Example section as a guide.
3. When you are satisfied with your edits, save and exit the `MapModel.xml` file.

Consider the following XML tags in a sample `MapModel.xml` file:

```
<vendorlist>
<vendor name="Cisco"> 1
<model name="UBR7246VXR"> 2
<output>7246</output> 3
</model>
</vendor>
</vendorlist>
```

Now consider the following return from the Auto-Discovery tool when it uses a `RegexList.xml` file to parse the CISCO CLI:

```
vendor=Cisco 1
model=2651 2
os=12.4(5A)
```

The Auto-Discovery tool:

1. Compares the value `Cisco` returned to `vendor` with the value specified in the `name` attribute of the `<vendor>` tag. The values match.
2. Compares the value `2651` returned to `model` with the value specified in the `name` attribute of the `<model>` tag. These values do not match.
3. Returns the value specified in the `<output>` tag, if the values in `model` and `<model>` match.

Because the values specified in `model` and `<model>` do not match, the Auto-Discovery tool performs no mapping of the model numbers for a CISCO device. Thus, the model number remains as it is.

Consider the following XML tags for Juniper in a sample `MapModel.xml` file:

```
<vendor name="Juniper"> 1
<model name="OLIVE"> 2
<output>M40</output> 3
</model>
</vendor>
</vendorlist>
```

Now consider the following return from the Auto-Discovery tool when it uses a `RegexList.xml` file to parse the Juniper CLI:

```
vendor=Juniper 1
model=OLIVE 2
os=6.2R2.4
```

The Auto-Discovery tool:

1. Compares the value `Juniper` returned to `vendor` with the value specified in the `name` attribute of the `<vendor>` tag. The values match.
2. Compares the value `OLIVE` returned to `model` with the value specified in the `name` attribute of the `<model>` tag. These values match.
3. Returns the value specified in the `<output>` tag (in this case M40), because the values in `model` and `<model>` match.

   Thus, the Auto-Discovery tool performs a mapping of the model numbers for a Juniper device because the values specified in `model` and `<model>` match.

You can now configure the `MapType.xml` file.

For instructions on how to configure the `MapType.xml` file, see "Customizing MapType.xml" on page 31.

To study a complete working example of a `MapModel.xml` file, see "MapModel.xml example" on page 30.

# MapModel.xml example

The `MapModel.xml` file is used by Auto-Discovery to map a unique string obtained from the CLI to the model number of a device.

## Purpose

This example shows how to populate the XML tags associated with mapping a unique string obtained from the CLI to the model number of a device.

### Sample

Study the following example to learn how to populate the XML tags associated with mapping a unique string obtained from the CLI to the model number of a device.

```
<vendorlist>
    <vendor name="Juniper">
        <model name="OLIVE">
            <output>M40</output>
        </model>
    </vendor>
    <vendor name="Extreme">
        <model name="ALPINE">
            <output>BLACKDIAMOND</output>
        </model>
    </vendor>
    <vendor name="Cisco">
        <model name="CAT6K-MSFC">
            <output>6509</output>
```

```
        </model>
        <model name="PIX FIREWALL">
            <output>PIX FIREWALL</output>
        </model>
        <model name="PIX-FIREWALL">
            <output>PIX-FIREWALL</output>
        </model>
        <model name="CAT6K-MSFC2">
            <output>6506</output>
        </model>
        <model name="CATALYST">
            <output>6509</output>
        </model>
        <model name="RSP2">
            <output>7507</output>
        </model>
        <model name="RSP4">
            <output>RSP4</output>
        </model>
        <model name="RSP8">
            <output>RSP8</output>
        </model>
        <model name="RSP4+">
            <output>7505</output>
        </model>
        <model name="MSFC">
            <output>MSFC</output>
        </model>
        <model name="MSFC2">
            <output>6509</output>
        </model>
        <model name="MSFC3">
            <output>MSFC3</output>
        </model>
        <model name="C5RSM">
            <output>C5RSM</output>
        </model>
        <model name="UBR7246VXR">
            <output>7246</output>
        </model>
    </vendor>
</vendorlist>
```

## Customizing MapType.xml

The MapType.xml file is used by Auto-Discovery to determine a device type, after having determined the device model.

Before editing the MapType.xml file, you must be familiar with XML. You should also have edited a MapModel.xml file.

This task requires that you become familiar with the XML tags described in the following table:

| XML tag | Description |
|---|---|
| <vendorlist> | The MapType.xml file contains <vendorlist> tags. Embedded inside are <vendor>, <model>, and <type> tags. The name attribute in the <vendor> tags indicates that everything enclosed within these tags apply to the specified vendor, which in this example are CISCO and Juniper devices only. The name attribute in each <model> tag is used to match the model number returned in a CLI call. The type tag specifies the type of the device. |

1. Open the MapType.xml file for editing.
2. Edit the XML tags according to your needs. Use the Example section as a guide.
3. When you are satisfied with your edits, save and exit the MapType.xml file.

Consider the following XML tags in a sample MapType.xml file:

```
<vendorlist>
<vendor name="Cisco"> 1
<model name="2621"> 2
```

```
<type>Router</type> 3
<model>
</vendor>
</vendorlist>
```

Now consider the following return from the Auto-Discovery tool when it uses a `RegexList.xml` file to parse the CISCO CLI:

```
vendor=Cisco 1
model=2651 2
os=12.4(5A)
```

The Auto-Discovery tool:

1. Compares the value `Cisco` returned to `vendor` with the value specified in the `name` attribute of the `<vendor>` tag. The values match.
2. Compares the value `2651` returned to `model` with the value specified in the `name` attribute of the `<model>` tag. These values match.
3. Returns the value specified in the `<type>` tag, if the values in `model` and `<model>` match.

   Because the values specified in `model` and `<model>` match, the Auto-Discovery tool returns the device type of `Router` (the value specified in the `<type>` tag).

Consider the following XML tags for Juniper in a sample `MapType.xml` file:

```
<vendor name="Juniper"> 1
<model name="M40"> 2
<type>Router</type> 3
<model>
</vendor>
</vendorlist>
```

Now consider the following return from the Auto-Discovery tool when it uses a `RegexList.xml` file to parse the Juniper CLI:

```
vendor=Juniper 1
model=M40 2
os=6.2R2.4
```

The Auto-Discovery tool:

1. Compares the value `Juniper` returned to `vendor` with the value specified in the `name` attribute of the `<vendor>` tag. The values match.
2. Compares the value `M40` returned to `model` with the value specified in the `name` attribute of the `<model>` tag. These values match.
3. Returns the value specified in the `<type>` tag, if the values in `model` and `<model>` match.

   Because the values specified in `model` and `<model>` match, the Auto-Discovery tool returns the device type of `Router` (the value specified in the `<type>` tag).

You can now configure the `MapOS.xml` file.

For instructions on how to configure the `MapOS.xml` file, see “Customizing MapOS.xml” on page 33.

To study a complete working example of a `MapType.xml` file, see “MapType.xml example” on page 32.

## MapType.xml example

The `MapType.xml` file is used by Auto-Discovery to determine a device type, after having determined the device model.

### Purpose

This example shows how to populate the XML tags associated with mapping a unique string obtained from the CLI to determine a device type.

**Sample**

Study the following example to learn how to populate the XML tags associated with mapping a unique string obtained from the CLI to determine a device type.

```
<vendorlist>
    <vendor name="Cisco">
        <!-- 2600 -->
        <model name="2610">
            <type>Router</type>
        </model>
        <model name="2612">
            <type>Router</type>
        </model>
        <!-- 65xx -->
        <model name="6506">
            <type>Switch</type>
        </model>
        <model name="6509">
            <type>Switch</type>
        </model>
    </vendor>
    <vendor name="Motorola">
        <model name="64000">
            <type>Cmts</type>
        </model>
    </vendor>
</vendorlist>
```

## Customizing MapOS.xml

The `MapOS.xml` file is used by Auto-Discovery to map a unique string obtained from the CLI to that device's operating system.

Before editing the `MapOS.xml` file, you must be familiar with XML.

This task requires that you become familiar with the XML tags described in the following table:

| XML tag | Description |
|---|---|
| `<vendorlist>` | The `MapOS.xml` file contains `<vendorlist>` tags. Embedded inside are `<vendor>`, `<os>`, and `<output>` tags. The `name` attribute in the `<vendor>` tags indicates that everything enclosed within these tags apply to the specified vendor, which in this example are CISCO and Juniper devices only. The `name` attribute in each `<os>` tag is used to match the os number returned in a CLI call. |

1. Open the `MapOS.xml` file for editing.
2. Edit the XML tags according to your needs. Use the Example section as a guide.
3. When you are satisfied with your edits, save and exit the `MapOS.xml` file.

Consider the following XML tags in a sample `MapOS.xml` file:

```
<vendorlist>
    <vendor name="Cisco"> 1
        <os name="10.5"> 2
        <output>10.3</output> 3
        </os>
    </vendor>
</vendorlist>
```

Now consider the following return from the Auto-Discovery tool when it uses a RegexList.xml file to parse the CISCO CLI:

```
vendor=Cisco 1
model=2651
os=12.4(5A) 2
```

The Auto-Discovery tool:

1. Compares the value `Cisco` returned to `vendor` with the value specified in the `name` attribute of the `<vendor>` tag. The values match.
2. Compares the value `12.4(5A)` returned to `os` with the value specified in the `name` attribute of the `<os>` tag. These values do not match.
3. Returns the value specified in the `<output>` tag, if the values in `os` and `<os>` match.

   Because the values specified in `os` and `<os>` do not match, the Auto-Discovery tool performs no mapping for a CISCO device with an os string of `12.4(5A)`. Thus, the os number remains as it is.

Consider the following XML tags for Juniper in a sample `MapOS.xml` file:

```
<vendor name="Juniper"> 1
<model name="M4"> 2
<output>M40</output> 3
</model>
</vendor>
</vendorlist>

<vendorlist>
    <vendor name="Juniper"> 1
        <os name="6.2R2.4"> 2
            <output>6.0</output> 3
        </os>
    </vendor>
</vendorlist>
```

Now consider the following return from the Auto-Discovery tool when it uses a RegexList.xml file to parse the Juniper CLI:

```
vendor=Juniper 1
model=M40
os=6.2R2.4 2
```

The Auto-Discovery tool:

1. Compares the value `Juniper` returned to `vendor` with the value specified in the `name` attribute of the `<vendor>` tag. The values match.
2. Compares the value `6.2R2.4` returned to `os` with the value specified in the `name` attribute of the `<os>` tag. These values match.
3. Returns the value specified in the `<output>` tag (in this case `6.0`), because the values in `os` and `<os>` match.

   Thus, the Auto-Discovery tool performs a mapping of the os numbers for a Juniper device because the values specified in `os` and `<os>` match.

To study a complete working example of a `MapOS.xml` file, see “MapOS.xml example” on page 34.

# MapOS.xml example

The `MapOS.xml` file is used by Auto-Discovery to map a unique string obtained from the CLI to the os number of a device.

## Purpose

This example shows how to populate the XML tags associated with mapping a unique string obtained from the CLI to the os number of a device.

### Sample

Study the following example to learn how to populate the XML tags associated with mapping a unique string obtained from the CLI to the os number of a device.

```
<vendorlist>
    <vendor name="Juniper">
        <os name="OS">
```

```
            <output>OS</output>
        </os>
    </vendor>
    <vendor name="Cisco">
        <os name="OS">
            <output>OS</output>
        </os>
    </vendor>
</vendorlist>
```

# Executing the Auto-Discovery tool

To execute the Auto-Discovery tool, specify the command appropriate to the operating system you are running.

The Auto-Discovery tool is available for AIX and Linux, and is executed from the command line. The Auto-Discovery tool is invoked by calling the applicable Auto-Discovery script along with the name of the text file that contains the host names or IP addresses of those devices to be discovered.

The syntax for the executing the Auto-Discovery tool is as follows:

```
script_name text_file_name.txt
```

To execute the Auto-Discovery tool on Linux or AIX, execute the `autodiscover.sh` script from the command line and follow it with the name of the text file. For example:

```
./autodiscover.sh DeviceInfo.txt
```

### Sample output of Auto-Discovery

The following example demonstrates the output expected after the Auto-Discovery tool has been successfully executed.

The following is a sample `DeviceInfo.txt` file used by the Auto-Discovery tool:

```
a:cisco
p:cisco
e:cisco
d:./results
r:vmware/Devices
r2501a
r2501b
r2503a
r2503b
r2514a
r2610a
r2610b
r2509a
```

The output of a successful execution of the `autodiscover.sh` script and the `DeviceInfo.txt` file would look like the following:

```
./autodiscover.sh DeviceInfo.txt

-------------------------------------------------------------------------------
Begin Scan :
Device Info File: DeviceInfo.txt
Number Of Threads: 10
Custom Rad: false
TimeOut: 20
-------------------------------------------------------------------------------
Attempting Login with the following Account / Password group
***** Using Account: cisco *****
***** Using Password: cisco *****
-------------------------------------------------------------------------------
Connected to r2503a
Device VTMOS - Cisco/Router/2500/12.2(1D)
-------------------------------------------------------------------------------
Connected to r2514a
Device VTMOS - Cisco/Router/2500/12.1(3)T
-------------------------------------------------------------------------------
```

```
Connected to r2610a
Device VTMOS - Cisco/Router/2610/12.1(16)
--------------------------------------------------------------------------
Connected to r2501a
Device VTMOS - Cisco/Router/2500/12.1(3)T
--------------------------------------------------------------------------
Connected to r2501b
Device VTMOS - Cisco/Router/2500/12.1(3)T
--------------------------------------------------------------------------
Connected to r2610b
Device VTMOS - Cisco/Router/2610/12.1(16)
--------------------------------------------------------------------------
Connected to r2509a
Device VTMOS - Cisco/Router/2509/12.3(19)
--------------------------------------------------------------------------
Connected to r2503b
Device VTMOS - Cisco/Router/2500/12.0(4)
--------------------------------------------------------------------------
Finished Scan - Date: 20070903
```

To view the results files created as part of the execution, see the results file located in the `./results/` directory. The results file produced for the `bulkimport` utility would look as follows:

```
#realm, hostname, vendor, type, model, os,*"com-type,ssh type,streaming,
username,password,enable-password,alt-hostname,port"
vmware/Devices,r2503a,Cisco,Router,2500,12.2(1D)
vmware/Devices,r2514a,Cisco,Router,2500,12.1(3)T
vmware/Devices,r2610a,Cisco,Router,2610,12.1(16)
vmware/Devices,r2610b,Cisco,Router,2610,12.1(16)
vmware/Devices,r2501a,Cisco,Router,2500,12.1(3)T
vmware/Devices,r2501b,Cisco,Router,2500,12.1(3)T
vmware/Devices,r2509a,Cisco,Router,2509,12.3(19)
vmware/Devices,r2503b,Cisco,Router,2500,12.0(4)
```

**Note:** It is a requirement that a Resource Access Document (RAD) is created or exists in the destination realm prior to the use of the `Bulkload.csv` by the Bulkload utility.

The RAD specifies the method by which the devices are communicated via (ssh or telnet), and in addition the credentials used by the Bulkload utility to interact with the device.

The Auto-Discovery script that executes the Auto-Discovery tool requires a text file with any name and an extension of `.txt`. For the purposes of illustrating the contents of this text file, subsequent examples use a text file called `DeviceInfo.txt`. The text file that you supply to the Auto-Discovery script is integral in establishing logon connections to the network devices in a realm.

For more information on the `DeviceInfo.txt` file, see “Deviceinfo.txt syntax” on page 18.

# Auto-Discovery Logs

This information describes the information available in Auto-Discovery logs.

A UOW log file is generated to record the sequence of events which take place during the submission of a UOW. Auto-Discovery logs information as a UOW. A log file is created regardless of the outcome of the UOW. This detail can help determine issues when the UOW fails.

The types of information Auto-Discovery logs contain are: unknown type, success, parsing fail, connection fail and authentication fail.

# CLI examples

Use this information to study CLI examples for the CISCO 2621 router and the Juniper M40 router.

## CISCO 2621 router CLI example

The following example shows the CLI for the CISCO 2621 router.

```
Cisco IOS Software, C2600 Software (C2600 ADVIPSERVICESK9-M),

Version 12.4(5a), RELEASE SOFTWARE (fc3)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 13-Jan-06 19:19 by alnguyen
ROM: System Bootstrap, Version 12.2(7r) [cmong 7r], RELEASE SOFTWARE (fc1)
2600l-xm uptime is 7 weeks, 20 hours, 44 minutes
System returned to ROM by power-on
System restarted at 17:40:52 UTC Tue Mar 20 2007
System image file is "flash:2:c2600-advipservicesk9-mz.124-5a.bin"
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco 2621XM (MPC860P) processor (revision 1.0) with 118784K/12288K bytes of
memory

Processor board ID JAD0628050B
M860 processor: part number 5, mask 2
2 FastEthernet interfaces
1 ATM interface
32K bytes of NVRAM.
16384K bytes of processor board System flash partition 1 (Read/Write)
32768K bytes of processor board System flash partition 2 (Read/Write)
Configuration register is 0x2102
```

## Juniper M40 router CLI example

The following example shows the CLI for the Juniper M40 router.

```
Hostname: jpe2
Model: M5
JUNOS Base OS boot [6.2R2.4]
JUNOS Base OS Software Suite [6.2R2.4]
JUNOS Kernel Software Suite [6.2R2.4]
JUNOS Packet Forwarding Engine Support (M20/M40) [6.2R2.4]
JUNOS Routing Software Suite [6.2R2.4]
JUNOS Online Documentation [6.2R2.4]
JUNOS Crypto Software Suite [6.2R2.4]
```

# Chapter 3. Configuring network devices

Use this information about Netcool Configuration Manager to perform device configuration tasks after devices have been discovered.

The following topics relate to network device configuration:

- Command sets
- Command filters
- Device configuration
- Queues
- Resources

Netcool Configuration Manager provides the following tools used in network device configuration:

| Tool | Description |
|---|---|
| Netcool Configuration Manager GUI (hereinafter referred to as the Resource Browser) | Use the Resource Browser to perform tasks related to command sets, command filters, and resources. You also use the Resource Browser to launch the IDT. |
| Command Set Editor | Use the Command Set Editor to edit command sets. |
| Configuration Editor | Use the Configuration Editor to edit native command sets (that is, device configurations). |
| Queue Manager | Use the Queue Manager to view and manage the queues of approval tickets and work. Depending on the security privileges, the user can approve or reject work, requeue work, and dequeue work using the Queue Manager. |
| Activity Viewer | Use the Activity Viewer to display information about configuration and compliance events recorded against network devices in a sequential timeline view. This data is extracted from historical and audit logs. You access the Activity Viewer from Network Manager or Tivoli Netcool/OMNIbus.<br>**Note:** The Activity Viewer can only be used when Netcool Configuration Manager is operating in an integrated environment, that is, with Network Manager and Tivoli Netcool/OMNIbus. |
| Command Filter Test Tool | Use the Command Filter Test Tool when editing or adding Permit and Deny statements in a command filter to test what commands will be permitted and denied. You access the Command Filter Test Tool through the Resource Browser. |
| Netcool Configuration Manager Accounts Administration Homepage | Use the Accounts Administration Homepage to assign command filters. |

Netcool Configuration Manager also provides the IBM Tivoli Netcool Configuration Manager Device Terminal (hereinafter referred to as IDT).

Use the IDT to create one or more sessions to perform configuration operations on network devices. Read the topics associated with the IDT to learn how to:

- Set IDT system properties
- Change IDT display settings
- Run command sets from IDT
- Run IDT scripts
- Change the IDT JVM configuration
- View the device log

# Using IDT

The following topics provide an overview of IDT.

## About using IDT

Use the IDT to access a device through a TELNET, SSH1 or SSH2 session. IDT provides full access to all commands on the network device, and allows access to the native command line.

### Architecture in which the IDT operates

IDT provides a seamless communications channel to all of the network devices that Netcool Configuration Manager manages through the use of the following components:

- Resource Browser
- Netcool Configuration Manager Presentation server
- SSH Daemon (this may be run on either the Worker or Presentation server).

The Netcool Configuration Manager client ALWAYS connects to the network device through the Netcool Configuration Manager Presentation server.

### IDT and the security framework

The IDT functionality integrates fully with the Netcool Configuration Manager security framework. Groups, users, and access permissions for IDT are controlled within the Netcool Configuration Manager account management environment.

In Netcool Configuration Manager, account management refers to the administration of groups, users, and the permissions of those groups and users. All rights are allocated at the group level. Users inherit access rights on the basis of group membership. As new users are added, they are assigned to a group that grants them the appropriate permissions to perform the functions that Netcool Configuration Manager permits.

In order to gain access to IDT; users need to belong to a group which has the 'IDT Access' group activity. This activity provides access to IDT via the Tools menu.

IDT Acess is only required for login to a device via IDT. The user does not require any activities to view their own logs. They do however require IDT Administration to view other users' logs. Additionally, the user may belong to the "IDT Administration", “IDT Allow AutoLogin”, “IDT Allow Manual Login”, or the "IDT Enable Mode" group activities.

For further information about the Netcool Configuration Manager account management environment, see the *IBM Tivoli Netcool Configuration Manager Administration Guide*.

### How to access IDT

Users launch IDT from the Resource Browser by right clicking on the selected device(s), and selecting **Tools** > **Device Terminal** (**Auto Login**/**Manual Login**) from the menu. Alternatively if the device is highlighted, users can select **Tools** > **Device Terminal** (**Auto Login**/**Manual Login**) from the Tool bar. The **Device Terminal Manual Login** option will only be activated if the “IDT Allow Manual Login” activity is chosen in the Netcool Configuration Manager account management.

Multiple IDT sessions may be opened concurrently, and users can view multiple active IDT sessions side by side in a tabbed format. This provides the advantage of being able to compare configurations and settings quickly.

These sessions can also be viewed as separate panes on the desktop. The IDT sessions are logged as either active or inactive. The activity status of IDT sessions at any given time can be viewed within Netcool Configuration Manager by selecting **Tools Active Terminals**. If the session has disconnected for any reason and the session is still displayed as active in the dialog, you can manually set it to inactive by right clicking on the server and select the Mark Session As Closed icon.

All connection paths to the device will be tried automatically using the details provided in the RAD. Additionally, all supplied authentication credentials will be tried. Each IDT session is represented as a tab on the device terminal screen. This window is almost indistinguishable from a standard TELNET or SSH session. If any Message of the Day or other text describing the device has been set, this will be displayed prior to the request for login credentials if using TELNET. If using SSH, the Message of the Day will not be seen until after the request for login credentials. The maximum number of active IDT sessions that each client can run at a given time may be configured in the `IDT Terminal Throttle` system property. When the device has been accessed, the user may be warned about pending work - both Pending and Waiting to Execute UOWs. Users will also be warned if there is an existing IDT session.

**Related tasks**

Setting IDT system properties.
Use the **System Properties** option to set IDT system properties.

Changing IDT display properties.
Use the **Change Font** option to change the font type and size and the **Colour Scheme** option to change the color scheme within single or multiple IDT sessions.

Running command sets in an IDT session
Use the **Apply Native Cmd Set** option to define and apply an unlimited number of commands (using native command sets) directly to one or more devices.

Changing IDT SSH Daemon configuration
Each Netcool Configuration Manager server has an SSH Daemon process that routes IDT sessions to another Netcool Configuration Manager server or to the network device.

Changing the IDT JVM configuration
By default, IDT is run as an internal component. However if a performance enhancement is required, the IDT Daemon has the ability to run on its own JVM. Use this procedure to configure the IDT JVM.

Viewing the Device Log
Login credentials, commands and responses, alongside results are recorded in the Device Log.

## Setting IDT system properties.

Use the **System Properties** option to set IDT system properties.

Follow these steps to set or change IDT system properties.

1. Access **Tools** > **System Properties**.
2. The following table describes the available IDT system properties available:

*Table 5. IDT System properties*

| System Property | Description |
|---|---|
| IDT Allow Connections from Presentation | Specifies whether to allow automatic connections from the Presentation server. |
| IDT Buffer Size | Specifies the maximum size of the scrollback buffer in IDT. Use this system property to configure the number of lines to view when using the scroll function. |

*Table 5. IDT System properties (continued)*

| System Property | Description |
|---|---|
| IDT Connection View | User can choose the view when connecting to a device. For example, a user might see a logon script, an animation, a combination of the two, or nothing. |
| IDT Default UOW Description | Provides user with the ability to set the description that is used by default when IDT submits a UOW. |
| IDT Device Output Delay | The delay in milliseconds, for logging command responses. |
| IDT Device Output Limit | Limits the number of characters logged for any device output. A limit of Zero will return all output. |
| IDT Display UOW Confirmation | Displays a confirmation and UOW ID when the UOW has been submitted successfully. |
| IDT Inactivity Timeout Period | Number of minutes a session will stay connected during user inactivity. The default is 15 minutes. However, any timeout set on the device will override this property. |
| IDT Regex Match String | Regex commands may be entered, and searched upon before forcing synchronization. This is only valid if the "IDT Synchronization Disconnect Action" is set to "Regex Match Synchronization". |
| IDT Synchronization Disconnect Action | The synchronization action to perform once a user has disconnected from a device can be chosen. The options are: Force Synchronization Without Prompt, Force Synchronization, Regex Match Synchronization Without Prompt, Regex Match Synchronization, Prompt Synchronization, or No Action. |
| IDT Terminal Throttle | This configures the maximum number of terminal sessions that each client can be running at any given time. |
| IDT UOW Conflict Connectionn | Action to take when connecting to a device associated with active UOWs. |
| IDT Use Main Server For Connection | Device connection is facilitated by an IDT Presentation server. Otherwise, it is facilitated by a user's Presentation server. |
| IDT User Conflict Connection | Action to take when connecting to a device which has already had an active IDT session. This may warn the user, prevent connection or take no action. |

3. Choose the system property that you want to set or change, and select **Update**.
4. Once the changes have been made. Choose **Close**.

**Related concepts**

About using IDT

Use the IDT to access a device through a TELNET, SSH1 or SSH2 session. IDT provides full access to all commands on the network device, and allows access to the native command line.

## Changing IDT display properties.

Use the **Change Font** option to change the font type and size and the **Colour Scheme** option to change the color scheme within single or multiple IDT sessions.

Users can change the font type and size within the IDT session, both for a single IDT session and across all open IDT sessions. Users can also change the color scheme of the IDT session to improve readability.

Follow these steps to set or change the IDT font type and size and the color scheme.

1. To change or set the font type and size:
   a) From the IDTTool bar, select **Tools** > **Change Font**.
   b) When the **Change Font** window is displayed, edit the font type and size as required, and then select **Apply to All** to apply the font changes across all open IDT sessions. Or, select **Apply to Current** to apply the font changes to the currently selected IDT session only.
2. To change the color scheme:
   a) From the IDT Tool bar, select **Tools** > **Colour Scheme**. To apply the colour scheme changes to the currently open IDT session, select **Apply to Current**. To apply the colour scheme changes to all open IDT sessions, select **Apply to All**. The options for both **Apply to Current** and **Apply to All** are: **Black on White**, **White on Black**, and **Green on Black**.

      After you select an option, the color scheme of the current IDT session will be updated accordingly. Any changes to fonts and color schemes are saved to the database, and are retained for the next time the user logs in.

Within the IDT session, you can copy and paste items to and from the command line by using the Copy and Paste UI icons or the Edit menu.

**Related concepts**

About using IDT

Use the IDT to access a device through a TELNET, SSH1 or SSH2 session. IDT provides full access to all commands on the network device, and allows access to the native command line.

## Running command sets in an IDT session

Use the **Apply Native Cmd Set** option to define and apply an unlimited number of commands (using native command sets) directly to one or more devices.

The user must belong to the IDT Administration group activity, as well as either the IDT Allow Manual Login or IDT Allow Automatic login group activities. In addition the "IDT Synchronization Disconnect Action" system property must be set to "Prompt Synchronization".

The following procedure explains how to execute a native command set in an IDT session. These allow the user to send native (Command Line Interface, or CLI) commands to the active terminal session through the IDT interface. This option on IDT is dependent on the current state. If the user is not in configuration mode the commands will be sent to the device but not applied.

1. In the Resource Browser, right click on the selected device or devices, and select **Tools** > **Device Terminal (Auto/Manual)** from the menu. Alternatively if the device is highlighted, select **Tools** > **Device Terminal (Auto/Manual)** from the Tool bar.
2. From the Tool bar, select **Tools** > **Apply Native Cmd Set**. The **Native Command Set Selection** window is displayed.
3. Select the required native command set from the displayed realms, and then select **OK** to execute. This action will apply the selected native command set to the IDT session.

An active IDT session can be disconnected by typing 'exit' into the session window, or alternatively by selecting the **Disconnect** button. After disconnecting from an active IDT session, you can reconnect to the session by selecting the **Reconnect** button.

To close the IDT terminal, select the **Close Terminal** button, or **File** > **Close Terminal**. Alternatively, press the **cross-hair (X)** in the corner of the browser window. The user will be asked to provide confirmation to exit IDT. All methods of exiting a session will result in a Config Sync with the "IDT Synchronisation Disconnect Action" system property configured properly.

**Related concepts**

About using IDT

Use the IDT to access a device through a TELNET, SSH1 or SSH2 session. IDT provides full access to all commands on the network device, and allows access to the native command line.

## Changing IDT SSH Daemon configuration

Each Netcool Configuration Manager server has an SSH Daemon process that routes IDT sessions to another Netcool Configuration Manager server or to the network device.

The main purpose of the SSD Daemon is to provide a secure tunnel to route session information from the IDT client to the device. Depending on the server configuration, this may route information from **client** > **presentation server** > **network device**, or **client** > **presentation server** > **worker server** > **network device**.

The SSH Daemon can operate in three modes:

**mainserver**
The 'mainserver' mode is normally configured on a presentation server.

If you have a deployment with more than one presentation server, then by setting one of the servers to 'mainserver' means that all IDT sessions will route through this server.

If all presentation servers are configured as 'mainserver', IDT will pick the first one in the list.

**server**
The 'server' mode is the opposite of 'mainserver', and is normally configured on a presentation server.

If you have a deployment which has more than one presentation server, then by setting all of the servers to 'server' means that all IDT sessions will route through the presentation server to which the user has connected.

**worker**
The 'worker' mode is always configured on a worker server, and should only be changed if the worker is reconfigured into a presentation server.

This task describes how to run the `changeIDTDaemon.sh` script.

1. Change to the following directory:

```
cd /opt/IBM/tivoli/netcool/ncm/bin/utils/idt
```

2. Run the `changeIDTDaemon.sh <mode>` script, for example `changeIDTDaemon.sh server`

**Related concepts**

About using IDT

Use the IDT to access a device through a TELNET, SSH1 or SSH2 session. IDT provides full access to all commands on the network device, and allows access to the native command line.

## Changing the IDT JVM configuration

By default, IDT is run as an internal component. However if a performance enhancement is required, the IDT Daemon has the ability to run on its own JVM. Use this procedure to configure the IDT JVM.

Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command as follows:

```
/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh stop
```

Follow these steps to configure the IDT JVM.

1. Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop Netcool Configuration Manager server command:

   ```
   ./itncm.sh stop
   ```
2. Access the `/opt/IBM/tivoli/netcool/ncm/config/server` directory. Edit the `config.xml` file to remove the Netcool Configuration Manager IDT component (see example below). Save the changes when complete.
3. Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory. Edit the `itncm.sh` script by changing the `IDT_STANDALONE=FALSE` Boolean value to `IDT_STANDALONE=TRUE`. Save the changes when complete.

```
<component>
<name>SSHDaemonComponent
</name>
<class>com.intelliden.core.idt.daemon.SSHDaemonComponent
</class>
</component>
```

Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the start Netcool Configuration Manager server command:

```
./itncm.sh start
```

**Related concepts**

About using IDT

Use the IDT to access a device through a TELNET, SSH1 or SSH2 session. IDT provides full access to all commands on the network device, and allows access to the native command line.

## Viewing the Device Log

Login credentials, commands and responses, alongside results are recorded in the Device Log.

1. The Device Log is categorized by User ID. Users with IDT administration access can view the logs of any user who accessed the network device in an IDT session, by selecting appropriately from the User ID drop down selection box. However, users with no IDT administration access can only view logs made against their own login. The drop down menu is not populated with other User IDs.
2. The `IDTArchive` utility is available as part of the `icosutil` script, and is used for archiving IDT session logs from Netcool Configuration Manager network resources based upon user criteria.

   **IDT Allow Connections from Presentation**
   Gives users the choice to allow automatic connections from the Presentation server.

**Related concepts**

About using IDT

Use the IDT to access a device through a TELNET, SSH1 or SSH2 session. IDT provides full access to all commands on the network device, and allows access to the native command line.

# Using command sets

Command sets are snippets of resource configurations that can be applied across multiple network resources. Command sets use standard configuration syntax and markup to identify the commands.

**Related concepts**

Using command set groups

Command set groups are collections of device-specific command sets that all perform the same configuration change. You use command set groups when you want to apply the same change to devices of a different VTMOS.

**Related tasks**

Editing command set groups

After you create a command set group, you must edit it. You can also rename an existing command set group, or move it to a different realm.

# Overview of command sets

Use this information to acquire an understanding of command sets.

Command sets can be parameterized so that some values can be modified at run time. Command sets are defined on a specific VTMOS, and it is important to ensure that all commands included in the command set apply to the VTMOS chosen.

Command sets are applied as a unit of work (UOW), and therefore can be scheduled and approved.

**Note:** When creating a modeled command set, the list of VTMOS labels from which you can select has been filtered to only display the labels for Smart Model drivers. Standard driver VTMOS are excluded.

An example of the use of command sets is a network administrator wanting to change the SNMP contact of all the Cisco 26xx routers on the network to the same value, without having to create individual configuration change UOWs for each resource.

## About command sets

**Native command sets**

Native command sets allow you to send CLI commands to one or more network resource at a time. The information from these commands is shown in the UOW log.

Native command sets can be used to modify commands on both managed and modeled network resources, and can be scheduled like any other UOW.

Native command sets include two modes of operation:

**Configuration change**

Used to change the configuration on a network resource.

**Interrogation**

Used to issue informational requests, such as show diag or show version.

When a native command set contains a script that attempts to send a restricted command via the device interface, it will be rejected when the script attempts to execute.

**Note:** This apples to interrogation command sets only, and not to configuration change command sets.

**Realms and security**

In order to create and apply command sets, you must belong to a group with the appropriate access privileges. A command set can be created in any realm, and can then be applied to network resources in any other realm, as long as appropriate rights for each realm are allocated.

**Using command sets as default configurations**

Command sets are ideally suited for use as default configurations to seed new resources. For example, if there are many resources of the same VTMOS, a parameterized template could be created using a command set that would be applied to each resource, thus saving time on manually configuring each device.

A second common application for command sets is to apply identical configuration stanzas to multiple devices, for example to apply login banners, manage VLANs and trunks, or manage SNMP settings.

**Wildcards**

For modeled command sets, wildcards are supported in command set elements, allowing a comparison to be made against any previous value, thus making command sets more general and reusable.

**Parameters**

Parameters allow the reuse of command sets, as each time the command set is applied, the value of the parameterized value can be defined. A default value may be used for any parameterized field. The user applying the command set is prompted to provide values for any parameterized fields.

**Failures**

A UOW task is considered a failure when a command set does not execute successfully against a resource. If there are multiple modifications within a command set, and one change in the command set fails, the application of the command set to that particular network resource is stopped.

When a command set is being applied, the number of failures allowed before the UOW containing the command set(s) should stop processing may be specified. This is specified in the **Configure Execution Options** display window.

If a modeled command set does not make a change to a configuration, this does not necessarily mean a failure has occurred. The command set may have been designed to change a configuration if the criteria matches. Or the command set may only change a value based on the current value. For example a command set may state that **banner/motd** will be changed to "new message" only if the current value is "test message."

Native command sets, however, will simply execute the commands, and the device will merge or modify the commands in the way one would expect when entering them on the CLI.

After any configuration change failure, Netcool Configuration Manager uses the value of the **ResourceErrorRecovery** flag to determine how to roll back the change.

**Multiple command sets**

Multiple command sets can be applied to a network resource at the same time.

The same command set can also be added multiple times to the same UOW, which means the same command set will be applied to each network resource specified in the UOW multiple times. This is particularly useful when adding list commands, because a single command set that adds a parameterized list command can be created. Examples would be when adding NTP servers or SYSLOG servers.

Multiple command sets may be applied to a single resource or to multiple resources. Take into account any dependencies when the command sets and resources are being ordered.

## Modeled command set processing

Use this information to learn how a modeled command set is processed, from submission to completed UOW.

**Note:** A device must be in synch before applying a command set.

**Parameter substitution**

When a command set is submitted, XML representing the command set logic is added to the UOW. If any parameterized values existed in the command set, those parameters are replaced by their actual values (supplied by the user submitting/applying the command set).

**Device processing**

Before applying a command set to the configuration running on a resource, the command set is applied to a copy of the current configuration in the database. Each configuration change (add, delete, match/replace, and so forth) within the command set is examined to determine if the requested change can be made. If the command set results in any changes, the copy of the current configuration is saved as a draft configuration. If no changes would result from the application of the command set, the next work component is processed, or if that was the only work component, the UOW is shown as completed with a successful status.

Before applying the draft configuration to the device, the system compares running versus stored (the two versions of the configuration on the network resource), and running versus current (the copy stored in the database). If any differences are found, the application of that command set to that resource is considered a failure.

If the comparisons are the same, the draft configuration that was created at the beginning of processing is applied to the network resource, and the "old" current configuration becomes a versioned configuration. The "new" current configuration is named "application of command set x" where x is the name of the command set that was just applied.

This process continues for each work component contained within the UOW. See the following section for a description of how work components are ordered within a command set UOW.

**Work processing order**

When multiple command sets are applied against multiple network resources, there are two different ways in which the command sets can be applied to the device. These are 'Apply Device at a time', and 'Apply Command Set at a time'.

**Apply Device at a time**

If this option is chosen each and every command set will be applied to the first resource. Only when each command set has been applied, will the command sets then be applied to the next resource. The following table shows the order in which individual work components are processed when multiple command sets are applied to multiple network resources.

*Table 6. Work component processing order when multiple command sets are applied to multiple network resources*

| Command set | Resource 1 | Resource 2 |
|---|---|---|
| **Command Set 1**<br>• config chg A<br>• config chg B | 1. Command set 1, change A is applied to Resource 1.<br>2. Command set 1, change B is applied to Resource 1. | 5. Command set 1, change A is applied to Resource 2.<br>6. Command set 1, change B is applied to Resource 2. |
| **Command Set 2**<br>• config chg A<br>• config chg B | 3. Command set 2, change A is applied to Resource 1.<br>4. Command set 2, change B is applied to Resource 1. | 7. Command set 2, change A is applied to Resource 2.<br>8. Command set 2, change B is applied to Resource 2. |

**Apply command set at a time**

This option represents the processing order in case a UOW is submitted "Command Set at the time", in which case the first command set is executed against all devices before a second command set is executed against all devices, and so on. The following table shows the order in which individual work components are processed when multiple command sets are applied to multiple network resources.

*Table 7. Work component processing order when multiple command sets are applied to multiple network resources*

| | **Command Set 1**<br>• **config chg A**<br>• **config chg B** | **Command Set 2**<br>• **config chg A**<br>• **config chg B** |
|---|---|---|
| **Resource 1** | 1. Command set 1, change A is applied to Resource 1.<br>2. Command set 1, change B is applied to Resource 1. | 5. Command set 2, change A is applied to Resource 1.<br>6. Command set 2, change B is applied to Resource 1. |
| **Resource 2** | 3. Command set 1, change A is applied to Resource 2.<br>4. Command set 1, change B is applied to Resource 2. | 7. Command set 2, change A is applied to Resource 2.<br>8. Command set 2, change B is applied to Resource 2. |

**Note:** Each work component represents a unique resource change, in which the device is locked, the change is made, the old ’current becomes a versioned configuration, and a new current configuration is created.

**Related tasks**

Applying native command sets (via wizard)

Native command sets are defined by your administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying native command sets** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager.

Applying modeled command sets (via wizard)
Modeled command sets are defined by an administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying modeled command sets** wizard. You access the wizard from either the Activity Viewer or from the Network View, Hop View and Path View in Network Manager.

**Related reference**

JavaScript within native command set scripting
Native command sets support JavaScript scripting functionality that will allow the creator to add their own logic flow around sending native commands to network resources and the ability to execute or return data from external commands.

## JavaScript within native command set scripting

Native command sets support JavaScript scripting functionality that will allow the creator to add their own logic flow around sending native commands to network resources and the ability to execute or return data from external commands.

### Syntax

The first line of the native command set must be `//#javascript` or `//#js` to indicate to the workflow engine that scripting mode has been enabled.

The script must include a function named `execute` that accepts three parameters and returns `true` or `false` to indicate that the unit of work (UOW) has succeeded or failed.

**Note:** The parameter names are not fixed.

Here is an example of the script syntax:

```
//#javascript
function execute(scriptAuditLogger, deviceInterface, systemInterface) {
    //enter javascript logic here
    return true;
}
```

This could also be written as:

```
//#javascript
function execute(logger, device, system) {
    //enter javascript logic here
    return true;
}
```

At script runtime, the workflow engine passes three classes corresponding to the function parameters to the script. Whatever names are chosen for the parameters, the names must be used within the body of the function.

**Restriction:** Do not use the $ character when creating JavaScript within native command set scripting, for example in a regular expression. Use `#single_dollar#` instead (including the hashtags). Netcool Configuration Manager interprets the $ character as the beginning of a substitution variable, which allows the use of parameters in Native Command Sets. A single $ character is therefore interpreted as the beginning of a substitution, and if there is no closing $ character, an error occurs.

### Methods

In order to describe the methods that are available for each class, the parameter names in the first example from the Syntax section will be used.

The scriptAuditLogger class that is passed into script function supports the following methods for sending messages to the unit of work log:

*Table 8. Methods that support the scriptAuditLogger class*

| Method | Description | Example |
|---|---|---|
| void info(String message) | Sends an audit log message to the UOW log. | scriptAuditLogger.log(“This message will appear in Unit of work log”); |
| void error(String message, Exception exception) | Sends an audit log error message to the UOW log. | scriptAuditLogger.error(“This operation has failed”, e); |

The deviceInterface class that is passed into the script function provides the ability to send native commands to the network resource. The following table describes the methods for sending native commands to a network resource.

*Table 9. Methods that support the deviceInterface class*

| Method | Description | Example |
|---|---|---|
| String send(String command) | Sends a command to device and returns response. | var response = deviceInterface.send(“show ip interface brief”); |
| String send(String command, String responseRegExp) | Sends a command to device and returns result of running a regular expression on the response. Only the first group match is returned. | var response = deviceInterface.send(“show ip interface brief”, “^(\w+)\s”); |
| String sendAndExpect(String command, String expectedResponse | Sends a command to a device, waits for the expected response, and returns the device's response. Use this method when an interactive command is to be sent. | deviceInterface.sendAndExpect("copy run start", "[startup-config]?"); deviceInterface.send("\r"); |
| String sendAndExpect(String command, String expectedResponse, String responseRegExp) | Sends a command to a device, waits for the expected response, and returns the result of running a regular expression on the response. Only the first group match is returned. Use this method when an interactive command is to be sent. | |

The systemInterface class that is passed into the script function provides the ability to execute external commands, retrieve data from external commands, and execute file operations to create, update and delete files, and to SFTP a file to a specified server.

*Table 10. Methods that support the systemInterface class*

| Method | Description | Example |
|---|---|---|
| public Path createFile (String filePathName, String content) throws Exception | Method to create a file, given the absolute file path and the content as a String. You need to add `sun.nio.fs.UnixPath` as an allowed class to System Properties to use this method. | `var response = system.createFile(source,"initial content of file\n");` |
| public Path updateFile (String filePathName, String content) throws Exception | Method to update a file, given the absolute file path and the content as a String. You need to add `sun.nio.fs.UnixPath` as an allowed class to System Properties to use this method. | `var response = system.updateFile(source,"appended update to file\n");` |
| public void deleteFile (String filePathName) throws Exception | Method to delete a file given the absolute file path, | `system.deleteFile(source);` |
| public boolean sftpFile (String sourceFilePathName , String destinationFilePathName , Map<String,String> options) throws Exception | Method to SFTP a file to a specified server. You need the `java.util` package in System Properties as an allowed java package to use this method. | `var source="/home/icosftp/testJSCreatedFile.xml";`<br>`var response = system.createFile(source,"initial content of file\n");`<br>`var destination="/home/timo/testJSCreatedFile.xml";`<br>`var options=new java.util.HashMap();`<br>`options.put("username","user1");`<br>`options.put("password","pass1");`<br>`options.put("remoteHost","10.168.1.1");`<br><br>`system.sftpFile(source,destination,options);` |
| String executeSystemCommand (String shellName, String shellArgs, String command, String checksum) | Executes a system command and returns the output of the system command.<br><br>The system command is a file that contains a shell script. The user must calculate a checksum for the file using icosutil. The checksum must then be entered in a native command set. | var response = systemInterface.executeSystemCommand (“/bin/sh”, “-c”, “getNetStat.sh”, “<generated checksum>”);<br><br>To generate a checksum for the getNetStat.sh script on the server run the following command: `<install_dir>;/bin/icosutil CalculateChecksum getNetStat.sh`<br><br>**Important:** If an external script is modified after a checksum has been generated, then a new checksum must be generated and the native command set script must be updated. |

| *Table 10. Methods that support the systemInterface class (continued)* | | |
|---|---|---|
| **Method** | **Description** | **Example** |
| String executeSystemCommand (String shellName, String shellArgs, String command, String responseRegExp, String checksum) | Executes a system command and returns the result of running a regular expression on the output of the system command. Only the first group match is returned.<br><br>The system command is a file that contains a shell script. The user must calculate a checksum for the file using icosutil. The checksum must then be entered in a native command set. | var response = systemInterface.executeSystemCommand (“/bin/sh”, “-c”, “getExternalData.sh”, “^(w+)\s“, <generated checksum>”);<br><br>To generate a checksum for the getExternalData.sh script on the server run the following command: `<install_dir>;/bin/icosutil CalculateChecksum getExternalData.sh`<br><br>**Important:** If an external script is modified after a checksum has been generated, then a new checksum must be generated and the native command set script must be updated. |

## Restricted commands

**Restriction:** The following notes do not apply to a configuration change native command set.

Restricted commands are not permitted within an interrogation native command set that does not contain a script. For example, a user is prohibited from saving the following interrogation native command set:

```
reload
```

However, a user is allowed to save the following interrogation native command set:

```
//#javascript
function execute(scriptAuditLogger, deviceInterface, systemInterface) {
    var command = “reload”;
    deviceInterface.send(command);
    return true;
}
```

**Note:** Despite it being permitted to save this interrogation native command set, however, it would fail at runtime, because a restricted command within an interrogation native command set is prohibited from being sent to a device.

## Disabling scripting

An administration user, that is, a user with View System and Manage System activities, can disable the scripting functionality by setting the following system property to false:

**Scripting – Enable script execution**

The system checks this property at runtime, and if set to 'false', will not allow scripts to be run.

The default setting is 'true'

## Disabling external system commands

An administration user, that is, a user with View System and Manage System activities, can disable external system commands by setting the following system property to false:

**Scripting – Enable external system command execution**
The system checks this property at runtime, and if set to 'false', will not allow scripts to be run.

The default setting is 'true'

## Allowing classes and packages in scripting

To allow external Java classes and packages to be used in a script, the following system properties need to be configured:

**Note:** In order to change system properties a user must have View System and Manage System activities assigned to their user group.

**Scripting - Classes allowed in a script**
This system property stores a list of allowed Java classes. It is checked at runtime to determine if classes in a script are permitted.

The default list is empty, which means that no classes are permitted until a system administrator has added them to this list.

The allowed classes list is comma-separated, for example:

```
java.lang.String
```

```
java.lang.String, java.lang.StringBuilder, java.util.ArrayList
```

**Scripting - Packages allowed in a script**
This system property stores a list of allowed Java packages. It is checked at runtime to determine if packages in a script are permitted.

The default list is empty, which means that no packages are permitted until a system administrator has added them to this list.

The allowed classes list is comma-separated, for example:

```
java.util
```

```
java.util, java.util.regex, java.text
```

## Setting scripting timeout

An administration user, that is, a user with View System and Manage System activities, can edit the appropriate system property to define the length of time that scripts within a command set or compliance definition are allowed to run without completing before they are stopped:

**Scripting - Maximum script execution time**
The default script execution limit is 10 minutes, and a system administrator can set a time limit between one and 120 minutes.

If a script within a command set times out, the UOW is marked 'failed'.

## Script samples

The following script determines whether a Cisco router's clock is synchronized with an NTP server. If it is not synchronized, the IP address of the unsynchronized master is retrieved and a ping command is issued.

```
//#javascript
function execute(scriptAuditLogger, deviceInterface, systemInterface) {
    var response = deviceInterface.send("show ntp status", "(Clock is unsynchronized)");

    if (response == null) {
        scriptAuditLogger.info("Clock IS synchronized");
        return true;
    } else {
        scriptAuditLogger.info("Clock is NOT synchronized");
        response = deviceInterface.send("show ntp association",
```

```
"(#\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3})");
        if (response != null) {
            var ipAddress = response.substring(1);
            scriptAuditLogger.info("IP address of master = " + ipAddress);
            response = deviceInterface.send("ping " + ipAddress);
            scriptAuditLogger.info(response);
        } else {
            scriptAuditLogger.info("NTP master is NOT configured.");
        }
        return false;
    }
}
```

The following script finds the IP addresses of a Cisco router's interfaces and performs a naming service lookup for each IP address.

```
//#javascript
importClass(java.util.regex.Pattern);
importClass(java.util.regex.Matcher);

function execute(logger, device, system) {
    var ipAddresses = device.send("show ip int brie | ex (Interface|unassigned|down)");
    logger.info(ipAddresses);

    var regexpression = "((?:(?:25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])\\.)
{3}(?:25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9]))";
    var pattern = Pattern.compile(regexpression, Pattern.MULTILINE);
    var matcher = pattern.matcher(ipAddresses);

    while (matcher.find()) {
        var ipAddress = matcher.group();
        logger.info("Found ip address [" + ipAddress + "]. Performing nslookup...");
        var response = system.executeSystemCommand("/bin/sh",
"-c", "/home/icosuser/scripts/nslookup.sh " + ipAddress,
"57b0b52e4a43da0591f90d4b7da6f6d189b985bbf4ec787a416104910f7610ac");
        logger.info(response);
    }

    return true;
}
```

**Note:** The shell script used in this example, `nslookup.sh`, was written and saved in the `/home/icosuser/scripts` directory on the Netcool Configuration Manager server. The script consisted of one line:
`nslookup $1`

**Note:** The script's checksum was calculated using the icosutil utility.

**Related concepts**

Overview of command sets
Use this information to acquire an understanding of command sets.

**Related tasks**

Editing native command sets
After you have created or copied a native command set, you edit it using the Native Command Set Editor.

## Inline Commands for Native Command Sets

You can use inline commands for Native Command Sets.

You can only use inline commands for Native Command Sets (NCS) if Line By Line (LBL) mode is true. If the LBL is not true, Netcool Configuration Manager will remove the commands and try to send what is left to the device. To use inline commands to make configuration changes, Streaming has to be set and the sendData command will be used instead of send command.

**Note:** In the f5 example, streamFile.03, send was replaced by send Data:

```
### Stream file
streamFile.03.sendData=$stream_input$\r
streamFile.04.wait=#
streamFile.05.sleep=5000
```

```
streamFile.08.send=save sys config\r
streamFile.11.wait=#
```

## Inline commands

**ITNCM-Sleep**

This command will allow Netcool Configuration Manager to sleep for the specified milliseconds before doing the next command in the list.

Example sleeping for 2 seconds:

```
ITNCM-Sleep=2000
```

The following example is for using the sleep command in an NCS. This example is for a Juniper m7i.

```
ITNCM-Sleep=10000
ITNCM-ChangePrompt=#
set system location floor 1
ITNCM-Sleep=5000
set system location building redish
ITNCM-Sleep=5000
set system location floor 313
ITNCM-Sleep=4000
set system location rack 23
ITNCM-Sleep=2000
set system location altitude 123
ITNCM-ResetPrompt=true
```

**ITNCM-NoPrompt**

This command will cause Netcool Configuration Manager to not wait for a prompt to be returned.

When setting NoPrompt to true, ITNCM will not wait for any reply from the device.

Example:

```
ITNCM-NoPrompt=true
ITNCM-NoPrompt=false
```

The following example was for an F5 device. In this example the display threshold is set to 6. This is a device change, but we are not going into configuration mode so we are using an interrogation script.

```
cli
ITNCM-NoPrompt=true
modify preference display-threshold 6
ITNCM-NoPrompt=false
exit
```

**ITNCM-ChangePrompt**

This command will change the prompt that Netcool Configuration Manager is waiting for when executing commands in NCS.

This example changes the prompt from default prompt to '>'.

```
ITNCM-ChangePrompt=>
```

The following example shows how to use the ChangePrompt cmd in a NCS.

```
ITNCM-Sleep=10000
ITNCM-ChangePrompt=#
set system location floor 1
ITNCM-Sleep=5000
set system location building redish
ITNCM-Sleep=5000
set system location floor 313
ITNCM-Sleep=4000
set system location rack 23
ITNCM-Sleep=2000
set system location altitude 123
ITNCM-ResetPrompt=true
```

**ITNCM-ResetPrompt**

This command will reset the prompt to the default value.

The default prompt is set in the device script (example default.prompt=#):

```
ITNCM-ResetPrompt=true
ITNCM-ResetPrompt=false
```

The following is an example of how to use the ResetPrompt cmd in a NCS.

```
ITNCM-Sleep=10000
ITNCM-ChangePrompt=#
set system location floor 1
ITNCM-Sleep=5000
set system location building redish
ITNCM-Sleep=5000
set system location floor 313
ITNCM-Sleep=4000
set system location rack 23
ITNCM-Sleep=2000
set system location altitude 123
ITNCM-ResetPrompt=true
```

**ITNCM-ChangeEndOfLine**

This command will change the end of line value that follows each command.

```
ITNCM-ChangeEndOfLine=\r\n
```

**ITNCM-ResetEndOfLine**

This command will reset the end of line values back to the default value.

The default value is \n

```
ITNCM-ResetEndOfLine=true
ITNCM-ResetEndOfLine=false
```

**Inline case statement**

Inline case statement is a command that is added to the Native Command Sets (NCS) to handle the case where multiple responses to a command that is sent to the device are possible. The case statement is limited to one cmd at a time.

All of the following examples are for list net vlan on an F5 load balancer. Depending on the configuration size, the device will return a question with y/n. If the config is small, the config will be displayed without the extra prompt. When the y/n prompt is given, the device will expect a y to display the config.

**Case statement commands**

**ITNCM-Case(some number)** - is one of the expected responses that Netcool Configuration Manager will expect from the previous command.

**ITNCM-Case-Done** - lets Netcool Configuration Manager know that the case statement is done.

**ITNMC-Send** - is what Netcool Configuration Manager will sent to the device.

**ITNCM-Wait** - is what Netcool Configuration Manager will wait for from the device.

**ITNCM-Case-Loop** - is the number of times Netcool Configuration Manager will loop through the cases statement while waiting for a match. The default = 2.

**ITNCM-Case-Sleep** - is the time in milliseconds that the case statement will sleep after all the cases have been checked. The default = 1500.

**ITNMC-Case-Timeout** - is the time that the case statement will wait for each of the cases to show up in the device output before moving to check the next case. The default = 1500.

**Example One**

Add a case statement that will return a carriage return "\r" in the case of a # or y in the case of y/n) prompt.

If the LBL is not set, then the ITNCM-Case1, ITNCM-Case2 and ITNCM-Case-Done lines will be removed and everything else will be sent to the device.

```
list net vlan
ITNCM-Case1=#
\r
ITNCM-Case2=y/n)
y
ITNCM-Case-Done
```

**Example Two**

Add a case statement that will return a carriage return and a new line blank in the case of a # or y in the case of y/n) prompt. If the LBL is not set then the ITNCM-Case1, ITNCM-Case2 and ITNCM-Case-Done lines will be removed and everything else will be sent to the device.

```
list net vlan
ITNCM-Case1=#

ITNCM-Case2=y/n)
y
ITNCM-Case-Done
```

**Example Three**

Add a case statement that will not return anything in the case of a # or y in the case of y/n) prompt. If the LBL is not set then the ITNCM-Case1, ITNCM-Case2 and ITNCM-Case-Done lines will be removed and "list net vlan" and "y" will be sent to the device.

```
list net vlan
ITNCM-Case1=#
ITNCM-Case2=y/n)
y
ITNCM-Case-Done
```

**Example Four**

Add a case statement that will not return anything in the case of a # or y in the case of y/n) prompt and wait for a # before finishing. If the LBL is not set then the ITNCM-Case1, ITNCM-Case2, ITNCM-Wait and ITNCM-Case-Done will be removed and "list net vlan" and "y" will be sent to the device.

```
list net vlan
ITNCM-Case1=#
ITNCM-Case2=y/n)
y
ITNCM-Wait=#
ITNCM-Case-Done
```

**Example Five**

Add a case statement that in the case of y/n) will send a newline, then a y and then wait for a #. Or in the case of a #, will send a carriage return, then a new line blank and then wait for a # before finishing. If the LBL is not set then the ITNCM-Case1, ITNCM-Case2, ITNCM-Wait and ITNCM-Case-Done will be removed and "list net vlan" and "y" will be sent to the device.

```
list net vlan
ITNCM-Case1=y/n)
y
ITNCM-Wait=#
ITNCM-Case2=#

ITNCM-Wait=#
```

**Example Six**

Add ITNCM-Case-Loop=4 - This will cause ITNCM to loop 4 times unless a match is found sooner

Add ITNCM-Case-Sleep=25000 - ITNCM will sleep 25 sec between loops of the case statement.

Add ITNMC-Case-Timeout=25000 - ITNCM will wait 25 sec before timing out on the expected case before moving to the next case.

Add a case statement that will send a newline and wait for a # in the case of a # or y in the case of y/n) prompt and wait for a # before finishing.

Add a 2nd case statement that will not send anything for a # in the case of a # or y in the case of y/n) prompt and wait for a # before finishing.

Add ITNCM-Case-Loop=2 - set the loop count back to default.Add ITNCM-Case-Sleep=15000 - set sleep time back to default.

Add ITNMC-Case-Timeout=15000 - set sleep time back to default. If the LBL is not set then all the ITNCM-Case1, ITNCM-Case2, ITNCM-Wait, ITNCM-Case-Done, ITNCM-Case-Loop, ITNCM-Case-Sleep and ITNCM-Case_Timeout will be removed and "list net vlan","y","\r"," list all-properties " and "Y" will be sent to the device.

```
ITNCM-Case-Loop=4
ITNCM-Case-Sleep=25000
ITNCM-Case-Timeout=25000
list net vlan
ITNCM-Case1=y/n)
y
ITNCM-Wait=#
ITNCM-Case2=#

ITNCM-Wait=#
ITNCM-Case-Done
list all-properties
ITNCM-Case1=#
ITNCM-Case2=y/n)
y
ITNCM-Wait=#
ITNCM-Case-Done
ITNCM-Case-Loop=2
ITNCM-Case-Sleep=15000
ITNCM-Case-Timeout=15000
```

**Example Seven**

Is the same as 6 but will send “show sys software” between the two case statements. If the LBL is not set then all the ITNCM-Case1, ITNCM-Case2, ITNCM-Wait, ITNCM-Case-Done, ITNCM-Case-Loop, ITNCM-Case-Sleep and ITNCM-Case_Timeout will be removed and "list net vlan","y","\r","show sys software ","list all-properties " and "Y" will be sent to the device.

```
list net vlan
ITNCM-Case1=y/n)
y
ITNCM-Wait=#
ITNCM-Case2=#

ITNCM-Wait=#
ITNCM-Case-Done
show sys software
list net vlan
ITNCM-Case1=y/n)
ITNCM-Send=y
ITNCM-Wait=#
ITNCM-Case2=#

ITNCM-Wait=#
ITNCM-Case-Done
```

**Example Eight**

Add a case statement that will return a carriage return and wait for a # in the case of a # or y and wait for a # in the case of y/n) prompt. If the LBL is not set then the ITNCM-Case1, ITNCM-Case2 and ITNCM-Case-Done all the ITNCM-Send and ITNCM-Wait commands will be removed and only the show sys software, list net vlan will be sent to the device.

**Related tasks**

Editing native command sets

After you have created or copied a native command set, you edit it using the Native Command Set Editor.

## About working with command sets

Use this information to obtain an overview of the tasks that you can perform when working with command sets

The following table identifies the tasks associated with command sets. The table contains the following columns:

- Task — Specifies the command set task.
- Tool — Specifies the tool used to complete the command set task.
- Stand alone — Specifies whether the command set task applies to Netcool Configuration Manager when operating in a stand alone environment.
- Integrated — Specifies whether the command set task applies to Netcool Configuration Manager when operating in an integrated environment, that is, with Network Manager and Tivoli Netcool/OMNIbus.

| Task | Tool | Stand alone | Integrated |
|---|---|---|---|
| Creating command sets | Resource Browser | Yes | Yes |
| Copying command sets | Resource Browser | Yes | Yes |
| Editing command sets | Command Set Editor | Yes | Yes |
| Editing native command sets | Configuration Editor | Yes | Yes |
| Applying command sets | Resource Browser | Yes | No |
| Applying native command sets | Resource Browser | Yes | No |
| Applying native command sets (via wizard) | Applying native command sets portlet (wizard)<br>**Note:** Access this wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition. | No | Yes |
| Applying modeled command sets (via wizard) | Applying modeled native command sets portlet (wizard)<br>**Note:** Access this wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition. | No | Yes |
| Using command set parameters | Command Set Editor | Yes | Yes |
| Using CSV command sets | Resource Browser | Yes | Yes |
| Defining command set order | XML editor | Yes | Yes |

## Creating command sets

The procedures to follow for creating a modeled command set and a native command set are identical. Note that in the following process any reference to command sets also applies to native command sets.

**Note:** Netcool Configuration Manager does not support the creation of native command sets for head end devices and their associated managed devices.

This task describes how to create a command set. Once created, you still have to edit the command set.

1. Navigate to the realm in the Resource Browser where you want to create a single or multiple command set, or a native command set.
2. Select **File** > **New** > **Command Set**. Or, select **File** > **New** > **Native Command Set**.
3. When the **New Command Set** window displays, specify the name and VTMOS of the new command set.

   **Note:** When creating a modeled command set, the list of VTMOS labels from which you can select has been filtered to only display the labels for Smart Model drivers. Standard driver VTMOS are excluded.
4. Select **OK** to complete.

This action creates the command set in the Resource Browser under the current realm.

Next, you edit the command set.

## Copying command sets

The copy command set functionality enables you to create new command sets quickly based on information that exists in the command set you want to copy from.

This task describes how to copy a command set. Once copied, you still have to edit the command set.

**Note:** The procedures to follow for copying a modelled command set and a native command set are identical. In the following process any reference to command sets also applies to native command sets.

1. Navigate to the realm in the Resource Browser which contains the command set that you wish to copy.
2. Highlight the command set to be copied.
3. Select **Edit** > **Copy Command Set**.

The new command set is created as a copy of the original. It is named using the same name as the original, and appended with '_1'.

This command set can now be renamed and modified, that is, edited, as required.

## Editing native command sets

After you have created or copied a native command set, you edit it using the Native Command Set Editor.

1. Highlight the native command set you want to edit, and select **Edit** > **Edit** from the menu bar. Alternatively, you can select **Edit** from the right-click menu.

   The native command sets is opened in edit mode.
2. Edit the native command set.

   The Native Command Set Editor is a simple text editing window. To edit commands, enter valid CLI commands within the text editing window. Use the following descriptions as a guide, and select **File** > **Save** when done.

   **Native command set type**
   Select one of the two following native command set types:

   **Configuration change**
   Configuration change commands are used for applying a modification to the configuration.

   **Interrogation**
   Interrogation commands are used for information retrieval

   **Note:** You cannot use a combination of the two types within the same command set.

   **Line by line**
   If you select **Line by line**, you need to further define this option by choosing one of the following two options from the dop-down list:

   - **Stop at first error**
   - **Process all, ignore errors**

**Tip:** When editing native command sets for Cisco CATOS switches, use line by line mode. Non-line by line mode will not throw an error for anything in a TFTP file. Therefore, no error message is seen by Netcool Configuration Manager. This results in the UOW saying it is successful when it actually failed. In addition, there is no indicator in the UOW or `icos` logs that there was any problem. Using line by line of the native command set catches the error, fails the change, and rolls back the configuration change as needed.

**Script syntax and examples**
For more information on native command set scripting, such as syntax, methods and sample scripts, see "JavaScript within native command set scripting" on page 49.

**Related reference**

JavaScript within native command set scripting
Native command sets support JavaScript scripting functionality that will allow the creator to add their own logic flow around sending native commands to network resources and the ability to execute or return data from external commands.

Inline Commands for Native Command Sets
You can use inline commands for Native Command Sets.

## Editing modeled command sets

After you have created or copied a command set, you use the Command Set Editor to add commands and logic to each command set.

1. Highlight the modeled command set that you want to edit, and select **Edit** > **Edit** from the menu bar. Alternatively, you can select **Edit** from the right-click menu.

   The command set is opened in the Command Set Editor in edit mode.
2. Click a command in the command tree to import it into the command window. You can filter the command tree to display all commands, or an edited list. Edit the modeled command set using the following information as guidance.
   When you have completed your edits, select **File** > **Save**.

Command Set Editor icons and functionality.

**Icons along the top right panel**
Use these icons to apply markup to the commands. The markup determines whether commands are added, modified, or deleted from the configuration when it is applied.

**Bottom of screen: 'Command Set' label**
This label indicates that you are using the Command Set Editor rather than the standard GUI editor.

**Bottom of screen: Current mode**
The current mode is either 'Match' or 'Replace'.

Change this by clicking the double-up arrow at the right end of the line of icons at the top of the window.

**Bottom of screen: Save needed**
This icon indicates that a save is needed, and disappears once you have saved the Command Set.

If you make additional changes after saving, the icon reappears.

3. To build a modeled command set, you perform the following steps:
   a) Define commands to add, modify, or delete.
   b) Mark up those commands with appropriate icons to tell the system if it is adding, modifying, or deleting the commands.
   c) Save the command set.

**Tip:** Open a view of the configuration that you will be changing in the GUI editor. This will be a helpful reference for entering the parameters into the Command Set Editor. For more information, see "Importing configurations and command sets" on page 116.

The following three simple examples describe how to Add a Command, Delete a Command, and Modify a command.

**Add a Command**

1. **Define commands:** From the left pane of the Command Set Editor, select the command you wish to add. In the right pane, fill out or select the parameters as you would for a standard change in the GUI editor.
2. **Add the Mark Up:** From the right pane, highlight the command you added in the first step and click the green '+' icon from the markup options at the top. If it is greyed out, the editor is in Match mode. Click the double up-arrow on the right end of the markup icons to switch to Replace mode and you will be able to select the green '+'. (Note that if you had to change modes, highlight the command again.) Verify that the green '+' now appears on the command. Also notice that there is now an orange diamond on the top level command. This indicates that this command structure will be modified by this Command Set. The left pane also shows the mark up.
3. **Save:** Save the command set.

**Delete a Command**

1. **Define commands:** From the left pane of the Command Set Editor, select the command you wish to remove. In the right pane, fill out or select the parameters that match what you will be removing.
2. **Add the Mark Up**: From the right pane, highlight the command you defined in the first step and click the red '-' icon from the markup options at the top. If it is greyed out, the editor is in Match mode. Click the double up-arrow on the right end of the markup icons to switch to Replace mode and you will be able to select the red '-'. (Note that if you had to change modes, highlight the command again.) Verify the red '-' is now showing on the command. The left pane also shows the mark up.
3. **Save:** Save the command set.

**Modify (or match-and-replace) a Command**

This procedure differs slightly in that the Define Commands step is performed twice – once for the match portion and once for the modify portion.

1. **Define commands:** From the left pane of the Command Set Editor, select the command that you wish to modify. From the right pane, set the mode to 'Match' by clicking the double up-arrow on the top right. Fill out or select the parameters that match the existing parameters that you wish to change.
2. **Add the Mark Up:** From the right pane, while still in 'Match' mode, select the parameter to be changed, and click the blue triangle icon from the markup options at the top.
3. **Define Command:** Click the double up-arrow once to go into Replace mode (notice that the parameter value disappears). Fill in the new value.
4. **Save:** Save the command set.

For further information on modeled command set

**Related concepts**

Overview of the Configuration Editor

The Configuration Editor is an applet used for viewing and editing configurations and command sets.

## Advanced modeled command set functions

The Command Set Editor has a number of advanced functions you can use to edit modeled command sets.

### Additional Icons in the Command Set Editor

**Duplicate Roll-up**

To the right of the up and down arrows, there is an icon of two overlapping sheets of paper. This is the 'Duplicate Roll-up' icon, and it allows you to duplicate or copy a portion of the command set that you have already created.

**Duplicate Roll-up** is helpful for quickly adding several of the same items then you can edit them individually.

**Trash can**
Used to delete a highlighted item

**Sheet of paper with diagonal line across**
Marks the current widget as active or inactive

**Green equal sign**
For matching on sibling commands

Defines required criteria before another change can happen

**Green asterisk**
For adding wildcard flexibility

Placing wildcard markup on an argument tells the command set interpreter that the argument is a regular expression and not an explicit string.

**Black 'P'**
'P' for parameterization

Creates generic, reusable command sets

**Circle with diagonal line through**
Sets a command to the 'no' version

## Examples

**Example 1 – Wildcard match and replace with default value and parameterization**
The green asterisk (*) is a wildcard matching widget that allows you to make a change to a field regardless of the current value; no matching test is required. The black 'P' for parameterization allows you to create generic, reusable command sets.

1. **Define Command:** Select interface **Async** in the left pane, and click on **Add Async** in the right pane. Enter the value **1** for the Async interface number. Since this is an existing Async interface on this example device, there are no changes to be made in this portion of the command, so no markup is needed on Async 1.
2. **Add the Markup:** Select **arp timeout** under Async 1 in the left pane. Still in Match mode, on the right pane, select the box to select timeout. You need to add two pieces of markup to the timeout argument. Select the red box for the value of the timeout argument, and click the green ***** wildcard to indicate that we will match any existing value in this field. Also click the **Modify** widget (blue triangle) to indicate this argument will be modified.

   **Note:** The green wildcard (*) may also be used to match a portion of a value. For example, on an ip address field, you could supply the value `10.1.1.*` and all the values 10.1.1.0-255 would be matched.
3. **Add Markup:** Now click the double up-arrow to change to **Replace** mode. Notice the timeout parameter box is set to red again and the green asterisk (*) is gone, but the blue triangle modify icon is still on the line. Now you can enter `1000` into the red box as a default value for the change. Click the black 'P' at the top of the right pane with the other icons. A box requesting you to fill in a name for the parameter appears. Enter a descriptive name such as `arp timeout` and click **OK**. Now a black 'P' is on this line next to the blue triangle. When this command set is applied to the device, you will see the parameter name you set and be given the opportunity to either keep the default value of 1000 or change to another value for the arp timeout. So you may supply a default value, or you may add the 'P' markup, or you may have both a default value and the 'P' markup. Note that you can place the 'P' for parameterizing in either the Match or the Replace windows, or in both allowing maximum flexibility. Using 'P' on the search criteria lets you decide the value to Match at execution time. In the Command Set Editor, click on the 'P' to see the assigned parameter name.
4. Save the command set.

**Example 2 – Import a configuration**

**CAUTION:** You can import a configuration over the top of an existing command set. This clears all previously defined commands and markup.

1. Create a new (empty) modeled command set.
2. Edit the new command set to open up the Command Set Editor.
3. Click **File** > **Import** in the upper left corner of the window. Double-click on the realm where the device resides, then double-click the desired device. Select the configuration you wish to import, and click **Import**. Note the configuration list displays timestamps, which are useful in determining the right one to select.

   **Note:** This provides the exact information for matching so we do not have to enter it manually. Since only commands with mark up are utilized in the command set, all the commands that do not have mark up are ignored when the command set is submitted.

**Example 3 – Match to Change Sibling Commands**

The green equal icon (=) selects the required criteria before another change can happen. Currently this allows only searches or changes between siblings. The device modeling of the SmartModel creates a hierarchy that defines parent-child relationships. Siblings are children of the same parent, that is, two or more commands at the same command level. In an access list, the 'remark', 'permit' and 'deny' statements are siblings of each other. All are at the same level in the hierarchy, and all are under the access-list parent command. This example shows how to use the green '=' to select the match criteria to allow a sibling command to be added. The same logic also applies for 'deletes' and 'modifies' of a sibling.

1. **Define command:** Import a configuration and open the existing access list command to be changed. The starting access-list is:

   ```
   access-list 10 permit 10.10.10.10
   access-list 10 remark ACL10
   access-list 10 permit 192.168.10.0 0.0.0.255
   ```

2. **Add Markup:** While in Match mode, select the sibling line to match against. In this example, the match is against the remark ACL10 line. Select this line and click the green **=**.
3. **Add Markup:** While still in Match mode, expand the 'permit 192.168.10.0' section and click on the IP address. Click on the blue triangle on the top of the right panel to allow this address to be changed.
4. **Add Markup:** Click the double up-arrow on the top of the right panel to go into Replace mode. Expand the permit '192.168.10.0' section, and click in the empty IP address box. Fill in a default address and click the 'P' (for parameter) to allow entering a different IP address at the time of execution.
5. **Define Command:** Click **Add permit**. Select any and click log.
6. **Add Markup:** Select the **permit any log** line (defined in previous step) and click on the green **+** to add this command.
7. Save the command set.

## Notes

**Remember:** If there is no markup, there is no change.

Adding and modifying are different.

Matching criteria is case-sensitive.

Commands are interpreted by the operating system on the device and potentially redefined, for example `permit 12.13.14.1 255.255.255.255` is interpreted to permit host 12.13.14.1

Any command set that searches for permit 12.13.14.1 255.255.255.255 never finds anything because the command has been reformatted. The best way to avoid this issue is to look at the configuration. You can import the configuration into the command set and use that format.

## Applying command sets

When applying a command set, the system verifies that the running and stored (candidate) configurations on each impacted resource are the same. If these are not the same, a mismatch error will be presented. This mismatch must be resolved before submitting any changes to the resource. After a successful configuration change, the system writes the running configuration to the stored/candidate configuration on each resource, ensuring that all three configurations (current, running, stored) are in synch.

There are a number of different windows presented in both the modelled command sets and native command sets. The sequence of the windows are dependent on the type and composition of the command set.

**Restriction:** When applying native command sets ensure that the 'native compare' option is disabled in the RAD. Instead, use 'smartmodel diff', as this option will handle non-comparable lines in the configuration.

This task describes how to apply a command set.

**Note:** There are several different ways to apply a command set. A command set can be selected, and applied to one or more network resources. One or more network resources can be selected, and then a command set applied to the network resource(s). Also multiple command sets can be supplied to multiple network resources. In addition, one or more command sets can be applied to a realm.

1. Navigate to the Resource Browser, and highlight the command set required from the listing of network resources.
2. From the menu bar, select **Tools** > **Apply (Native) Command Set**.
3. When the **Select Command Sets** window is displayed choose the command sets required using the **Add/Remove** buttons in between the panels. The Move Up and Move Down icons are used for prioritizing the order in which the command sets are applied. Select **Next** to proceed.
4. The **Scope of Application** dialog displays. Using the following table as a guide, please enter the appropriate information requested. When the scope selection has been chosen, select **Next**.

*Table 11. Scope of Application dialog*

| Selection | Description |
|---|---|
| Apply the Command Sets to Network Resources in a Realm | Will apply the command set(s) to all network resources in the realm selected. |
| Apply the Command Sets to specific Network Resources | Will apply the command set(s) only to the specific network resources chosen. |
| Apply the Command Sets to the Network Resources retrieved from a Realm | Will apply the command set(s) to all network resources in the retrieved realm. |

5. The second part of **Scope of Application** window displays. Select the realm name/network resources as applicable to the choice made in the previous window. This filters devices based on their support level e.g, to display SmartModel only. Units of Work can also be filtered by Name or VTMOS filter as required. However, this is an optional step. Wildcards are in place by default to retrieve all possibilities. Click **Next** to proceed.
6. The **Configure Execution Options** dialog displays. Using the following table as a guide, please enter the appropriate information requested. Select **Next** to proceed.

*Table 12. Configure Execution Options dialog*

| Element | Description |
|---|---|
| **Execution Mode** | |

| *Table 12. Configure Execution Options dialog (continued)* | |
|---|---|
| **Element** | **Description** |
| Execute Mode | Applies command set to selected network resources. |
| Report Only Mode | Does not change resources, but produces a report detailing the changes that would be made to those resources if in execute mode. |
| Apply Device at a time | Applies all command sets to one individual device at a time. |
| Apply Command Set at a time | Applies one command set at a time to a resource. |
| **Failure Options** | |
| Ignore All Errors | Indicates that the UOW will continue processing, regardless of any failures that occur. If each command set is to be applied to each resource regardless of any errors, select the **Override** flag as well. |
| Fail After X Total Errors. | User has the ability to select how many errors can occur before total failure of process. |
| Fail After X Percent Errors | User has the ability to select the maximum percentage of failures that can occur before the UOW stops processing. |
| **Pre-Emptive Compliance Options**<br>**Note:** These options are only available if the user is a member of a group with Pre-Emptive compliance activities. Pre-emptive options are only available for Modeled Command Sets. | |
| Enable Pre-Emptive Compliance Checks | When in Execute mode all Pre-emptive modes are available. However if the user has selected Report Only execution mode, then report only pre-emptive mode is automatically selected. If the user has ‘Manage Work' rights they will be able to disable Pre-emptive Compliance checks by deselecting the check box. Users who do not have 'Manage Work' rights will not be able to modify pre-emptive settings. |
| Block Configuration Change if projected configuration contains compliance failures | Policy is run against the current and projected configuration to determine if a violation is present. If a violation is found, the configuration change is blocked. |

| *Table 12. Configure Execution Options dialog (continued)* | |
|---|---|
| **Element** | **Description** |
| Block Configuration Change if projected configuration contains new compliance failures only | If a compliance violation is found within the projected configuration and the current configuration has no violations then the configuration change will be blocked. If both projected and current configurations have failures then the configuration change will not be blocked and changes will be made to the device. |
| Report Compliance Failure(s) only (Configuration change will not be blocked) | Produces a report providing information on violations in both the current and projected configuration. Pre-Emptive failures are ignored and the command set continues to execute. |
| Command Sets | This lists the command sets that will be rolled back. |

**Note:** If Execute Mode has been chosen, the **Rollback Options** window will be displayed. Otherwise, the wizard skips ahead to the **Enter Parameters** window.

7. The **Rollback Options** window displays. A Rollback can be requested in the event that a command set fails. The Rollback can be carried out for a single command set, or multiple command sets. Using the following table as a guide, please enter the appropriate information requested. Select **Next** to proceed.

| *Table 13. Rollback Options fields* | |
|---|---|
| **Field** | **Definition** |
| **How should Rollbacks on Command Set failures be handled?** | |
| No Rollback | Select this to turn off the rollback option. |
| Use Modeled Rollback | This option will enable a rollback to a modeled configuration. |
| Reload the configuration and reboot the device | This option will load the original configuration and reboot the device. |
| Check here to have Rollbacks verified | Select this checkbox to enable rollback verification. |
| **How should Rollbacks be done for each Network Resource?** | |
| Rollback only the failed Command Set on the failed Network Resource | This option rolls back only that command set that failed. |
| Rollback all Command Sets on the failed Network Resources | This option rolls back all command sets on the failed resource. |

8. The **Enter Parameters** window displays. Using the following table as a guide, please enter the appropriate information requested. Select **Next** to proceed.

| *Table 14. Enter Parameters fields* | |
|---|---|
| **Field** | **Definition** |
| Manual | Used where the same parameter name is used in multiple command sets, but each different value can be defined depending on the command set. |
| Local | Uses the Command Set Editor to step through each command set, providing a value for each parameter. |

9. The **Password Override**window displays. Using the following table as a guide, please enter the appropriate information requested.

| *Table 15. Password Override fields* | |
|---|---|
| **Field** | **Definition** |
| Override ITNCM - Base Authentication | Select this check box to override the default authentication information. |
| Login Name | Provide the login name for the device you are accessing. |
| Password | Provide the password for the device you are accessing. |
| Enable Password | Provide the device enable password for the device you are accessing. |
| Only Use This Authentication | Select this check box if you will always use this authentication for your resource. |

10. The **Execution Priority** window displays. By default all UOWs are submitted with a priority of Medium. Select the priority required and click **Next** .
11. The **Schedule Work** window displays. If you select Immediate, the **Describe Work** window will be displayed. If you select Scheduled or Recurring Schedule, use the information in the following table to make the rest of your selections in the **Schedule Work** window.

| *Table 16. Schedule Work options* | |
|---|---|
| **Option** | **Definition** |
| Scheduled | The job will run at a specific time, based on the values entered for Scheduled Start and Scheduled End. |
| Hourly | Use this option to specify that the process should run each hour, or every n hours after the scheduled start time, for example, Every 3 hours after Scheduled Start. |
| Daily | Use this option to specify that the process should run every *n* days, for example, Every 5 days, or else every weekday (Monday - Friday). |

| *Table 16. Schedule Work options (continued)* | |
|---|---|
| **Option** | **Definition** |
| Weekly | Use this option to specify that the process should run every *n* weeks on a specific day of the week, for example, Every 3 weeks on a Monday. |
| Monthly | Use this option to specify that the process should run on a specific day of every *n* months, for example, Day 30 of every 6 months. Or, you can specify that the process runs on a relative day of every month, for example, The First Monday of every 3 months. |
| Yearly | Use this option to specify that the process runs on a specific day and month of every year, for example, Every January 1st. Or, you can specify that the process should run on a relative day of the week of a specific month, for example, The First Monday of January |
| Scheduled Start | Enter the scheduled start time and date. |
| Scheduled End | Enter the scheduled end time and date. |
| Next Execution | Enter the time and date for the next execution. |
| Window Size | Use the drop-down lists to indicate the window size. |
| Every n hours after Scheduled Start | Choose the number of hours from the drop-down list. |
| Every n days | Choose the number of days from the drop-down list. |
| Every Weekday | The job will run every weekday. |
| Recur every n weeks | Choose the number of weeks from the drop-down list and select the appropriate day. |
| Day n of every n months | Choose the number of days and months from the drop-down lists. |
| The specific day of every n month | Choose the specific day and month from the drop-down lists. |
| Every specific date | Choose the month and day from the drop-down lists. |
| The specific day of every n month | Choose the specific day and month from the drop-down lists. |

12. The **Resources per UOW** window is displayed if more than one network resource has been chosen to synchronize. Make the required selections or go to the next step if you only chose one resource. Click **Next** to proceed.

13. The **Describe Work** window displays. Enter a description for the UOW, and then click **Finish**.

The command set is now submitted as a UOW and will run when scheduled, as long as the proper approvals are granted. The number of approvals required for the UOW depends on the group policy.

**Related tasks**

Creating pre-emptive policies

Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device, allowing you to evaluate the impact of configuration changes against pre-defined compliance policies for a device. In order to run a pre-emptive compliance, you first create or modify existing policies to make them suitable for execution in a pre-emptive manner. You then create a compliance process to apply the pre-emptive policy to a device.

Applying native command sets (via wizard)

Native command sets are defined by your administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying native command sets** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager.

Applying modeled command sets (via wizard)

Modeled command sets are defined by an administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying modeled command sets** wizard. You access the wizard from either the Activity Viewer or from the Network View, Hop View and Path View in Network Manager.

## Using command set parameters

Using the full parameter functionality, a user can set up a command set with a parameter rather than a defined value. There are three different types of parameters: Manual, Local, and Global. The method to use depends on the number of command sets, the number of parameters, and whether you know which commands the parameters represent.

A parameter can be defined when using native command sets and modeled command sets. If any command sets in your UOW contain parameters, you must assign an actual value to each parameter before the UOW can be submitted.

The manual method of parameter entry is only applicable for modelled command sets.

1. The manual method of entering parameter values uses the Command Set Editor to step through each command set, providing a value for each parameter.
   a) Select the **Manual** option on the **Enter Parameters** window, and click **Next**. The second part of the **Enter Parameters** window is displayed.
   b) This dialog lists the command sets containing parameters. Notice that each contains unset parameters to allow values to be assigned to the parameters. Click the **Edit** button next to the command set to be edited. The command set chosen is opened in the Configuration Editor. Only the commands that require parameters to be filled in are shown.
   c) Enter the value required for each parameterized field (you may have to switch to Replace view) and then select **File** > **Save**. The window reverts back to the **Apply Command Set** wizard when this has been completed, and the text next to the first command set is Completed Parameters.
   d) Continue the same process for any additional command sets that need parameters defined. Click **Next** when done to continue with the **Apply Command Set** wizard.
2. The local parameter option uses the Command Set Editor to step through each command set, providing a value for each parameter. This option should be used if the same parameter name is used in multiple command sets, but you want to define each different value depending on the command set. The Local option is available regardless of the number of command sets in the UOW.
   a) Select the Local option on the **Enter Parameters** window, and click **Next** . The second part of the **Enter Parameters** window is displayed.
   b) Enter the value required for each parameterized field. This dialog shows a table with each command set and parameter name.

c) Select the parameter to set. Type the value in the box at the bottom of the dialog.

d) Click **Next** when done to continue with the **Apply Command Set** wizard.

The format for the creation of parameters is: **${parametername=default value}$** For example: **interface $fastEthernet=2/1/0$**

## Using CSV command sets

There are several different ways to apply a command set. You can select a command set and apply it to one or more network resources, or you can select one or more network resources and then apply a command set. You can also apply multiple command sets to multiple network resources. In addition, you can apply one or more command sets to a realm.

When applying a command set, the system verifies that the running and stored (candidate) configurations on each impacted resource are the same. If not the same, you will see a mismatch error. After a successful configuration change, the system writes the running configuration to the stored/candidate configuration on each resource, ensuring that all three configurations (current, running, stored) are in sync.

The main purpose of a CSV applied command set is to apply a large number of command sets to multiple devices. The CSV utility allows for the specifications of a set of parameters for a command set, or native command set using a CSV file rather than manual entry. This extends the functionality of performing bulk import operations.

**Note:** CSV command sets with large numbers of parameters are not viewable in the GUI. You must define the correct values in a CSV command set before importing it into Netcool Configuration Manager.

This task describes how to create a CSV file, apply a CSV command set, and open a CSV text editor, for example, Microsoft Excel.

1. To create the CSV file, invoke a CSV text editor, for example, Microsoft Excel.
2. Create the following column headings: **work-type, work-name, work-realm, work-device, device-realm, parameter**
3. Using the following table as a reference, enter values for the fields in the column headings as appropriate.

*Table 17. CSV column headings*

| CSV column heading | Description |
|---|---|
| work-type | Enter either CommandSet or NativeCommandSet. |
| work-name | Name given to the command set. |
| work-realm | Path to command set. Use / to indicate folder hierarchy. |
| work-device | Name given to network resource. |
| device-realm | Path to network resource. Use / to indicate folder hierarchy. |
| parameter (option 1...n) | Optional. You may have multiple parameters as required, but only if defined within the command set. |

The first five of the above headings are **mandatory**. Specify the optional parameter heading by creating a heading of *parametername*. For example, if `CommandSet1` has a parameter named `set_timezone`, then a column with the heading `set_timezone` is required in the CSV file. If a parameter has been declared within a command set, and it is not represented in the CSV file, an error will be displayed to the user.

4. Enter the sample data as shown in the following example:

```
CommandSet,ModelledTest,ROOT,10.216.1.44,ROOT,
```

5. When the data has been entered, save the file as a CSV file. This means that it can be imported into the editor.
6. In order to apply a command set, there are a number of stages which need to be completed. To assist in the process a wizard is used to collect information. Select Resource Browser from the navigation tree.
7. Navigate to the resource to which you want to apply a command set.
8. Select **Tools** > **Apply from CSV File** > **Apply from CSV File** > **(Native) Command Set**.
9. The **Csv - Apply Command Sets** wizard is displayed. You are required to select a file to import. Select Browse to search for the Import file location.
10. An **Open** dialog will be displayed. Browse to the location of the CSV file you want to import, and select Open. If there are any errors with the format of your CSV file, an error will be displayed. Errors must be corrected before proceeding with the file import. Erroneous CSV files cannot be imported. Once the error has been corrected, the user must browse and re-select the amended CSV file.
11. The file you select to import will be populated into the wizard. Click **Next**.
12. At the next stage of the wizard, you will be requested to Configure Execution Options. Using the following table as a guide, please configure the dialog according to your needs. Click Next.

*Table 18. Configure Execution Options dialog*

| **Element** | **Definition** |
|---|---|
| **Execution Mode** | |
| Execute Mode | Applies command set to selected network resources. |
| Report Only Mode | Does not change resources, but produces a report detailing the changes that would be made to those resources if in Execute Mode. |
| Apply Device at a time | Applies all command sets to one individual device at a time. |
| Apply Command Set at a time | Applies one command set at a time to a resource. |
| **Failure Options** | |
| Ignore All Errors | Indicates that the UOW will continue processing, regardless of any failures that occur. If each command set is to be applied to each resource regardless of any errors, select the Override flag as well. |
| Fail After X Total Errors | User has the ability to select how many errors can occur before total failure of the process. |
| Fail After X Percent Errors | User has the ability to select the maximum percentage of failures that can occur before the UOW stops processing. |
| **Pre-Emptive Compliance Options** | **These options are only available for modelled command sets and if the user is a member of a group with Pre-Emptive compliance activities.** |

| *Table 18. Configure Execution Options dialog (continued)* | |
|---|---|
| **Element** | **Definition** |
| Enable Pre-Emptive Compliance Checks | When in Execute mode all Pre-Emptive modes are available. However if the user has selected Report Only execution mode, then report only Pre-emptive mode is automatically selected. If the user has ‘Manage Work' rights they will be able to disable Pre-Emptive Compliance checks by deselecting the check box. Users who do not have 'Manage Work' rights will not be able to modify Pre-Emptive settings. |
| Block Configuration Change if projected configuration contains compliance failures | Policy is run against the current and projected configuration to determine if a violation is present. If a violation is found, the configuration change is blocked. |
| Block Configuration Change if projected configuration contains new compliance failures only | Policy is run against the projected configuration to determine if a violation is present. If a violation is found, the configuration change is blocked. |
| Report Compliance Failure(s) only (Configuration change will not be blocked) | Produces a report providing information on violations in both the current and projected configuration. Pre-Emptive failures are ignored and the command set continues to execute. |
| Command Sets | This lists the command sets that will be rolled back. |

13. Rollback Options in the event of a command set failure are requested. Using the following table as a guide, please configure the dialog according to your needs. Click **Next**.

| *Table 19. Rollback Options dialog* | |
|---|---|
| **Field** | **Definition** |
| **How should Rollbacks on Command Set failures be handled?** | |
| No Rollback | Select this to turn off the rollback option. |
| Use Modeled Rollback | This option will enable a rollback to a modeled configuration. |
| Use JUNOS based Rollback | This option rolls back XML commands. |
| Reload the configuration and reboot the device | This option will load the original configuration and reboot the device. |
| Check here to have Rollbacks verified | Select this checkbox to enable rollback verification. |
| **How should Rollbacks be done for each Network Resource?** | |
| Rollback only the failed Command Set on the failed Network Resource | This option rolls back only that command set that failed. |
| Rollback all Command Sets on the failed Network Resources | This option rolls back all command sets on the failed resource. |

14. The **Password Override** window will be displayed. This is an optional step, which means that Netcool Configuration Manager Authentication may be overridden if required. Using the following table as a guide, please configure this optional dialog according to your needs. Click Next.

*Table 20. Password Override dialog*

| **Field** | **Definition** |
|---|---|
| Override ITNCM Authentication | Select this check box to override the default ITNCM authentication information. |
| Login Name | Provide the login name for the device you are accessing. |
| Password | Provide the password for the device you are accessing. |
| Enable Password | Provide the device enable password for the device you are accessing. |
| Only Use This Authentication | Select this check box if you will always use this authentication for your resource. |

15. The **Execution Priority** window is displayed. The precedence of the task must be considered for this option. Select the appropriate priority required. Click **Next**.
16. The next window to be displayed is the **Schedule Work** window. You will need to select the scheduling preference. If Immediate is selected, the wizard skips forward to the **Describe Work** window. However, if you select Scheduled or recurring Schedule, the information in the following table should be used as a guide to complete the selections required. These are dependent on your needs.

*Table 21. Execution Priority options*

| **Option** | **Definition** |
|---|---|
| Scheduled | The job will run at a specific time, based on the values entered for Scheduled Start and Scheduled End. |
| Hourly | The job will run daily, based on the values entered for Next Execution, Window Size, Every n days, or Every Weekday. |
| Daily | The job will run daily, based on the values entered for Next Execution, Window Size, Every n days, or Every Weekday. |
| Weekly | The job will run weekly, based on the values entered for Next Execution, Window Size, and Recur every n weeks on day of the week. |
| Monthly | The job will run monthly, based on the values entered for Next Execution, Window Size, Day n of every n months, or The specific day of every month. |
| Yearly | The job will run yearly, based on the values entered for Next Execution, Window Size, Every month and day, or The specific date. |
| Scheduled Start | Enter the scheduled start time and date. |
| Scheduled End | Enter the scheduled end time and date. |
| Next Execution | Enter the time and date for the next execution. |

| *Table 21. Execution Priority options (continued)* | |
|---|---|
| **Option** | **Definition** |
| Window Size | Use the drop-down lists to indicate the window size. |
| Every n hours after Scheduled Start | Choose the number of hours from the drop-down list. |
| Every n days | Choose the number of days from the drop-down list. |
| Every Weekday | The job will run every weekday. |
| Recur every n weeks | Choose the number of weeks from the drop-down list and select the appropriate day. |
| Day n of every n months | Choose the number of days and months from the drop-down lists. |
| The specific day of every n month | Choose the specific day and month from the drop-down lists. |
| Every specific date | Choose the month and day from the drop-down lists. |
| The specific day of every n month | Choose the specific day and month from the drop-down lists. |

17. The **Resources per UOW** window is displayed only if it meets a specific condition. It will be displayed, only if the user has described in the CSV file that all network resources will apply the exact same group of command sets and associated parameter values. Using the following table as a guide, configure the options according to your needs. Click Next.

| *Table 22. Resources per UOW options* | |
|---|---|
| **Element** | **Definition** |
| Slider Bar | Move the slider bar to set the number of resources for each UOW. |
| Resources per UOW selection window | Type or click the arrows to select the resources per UOW. |
| Number of UOWs | Type or click the arrows to select the number of UOWs |

18. The **Describe Work** window is displayed. This gives you an opportunity to enter a description for the UOW. Click **Finish**.

The command set will run when scheduled, based on your approvals. The number of approvals required for the UOW depends on your group's policy.

## Defining command order

Network devices that are CLI based process commands in a sequential order. These CLI based commands have dependency requirements. With CLI ordering most command dependencies can be resolved. To be able to order the CLI correctly, these command dependencies are stored in a Native Command Generation Data file.

Command Generation Data enables you to define Key and KeyRef definitions for ordering commands during native command generation. For example, Command B refers to Command A. With such a dependency you cannot put in Command B unless Command A exists on the device. If you try to do this

the device will error out. Due to such dependency issues which the device does not handle automatically, Netcool Configuration Manager provides a way of handling CLI Ordering requirements.

This task describes how to define Key and KeyRef definitions for ordering commands during native command generation.

1. The following example is a snippet sample of a Command Generation Data XML document.
2. To edit a Command Generation Data resource, select the resource you want to edit.
3. Right Click and select Edit. The XML editor is displayed.
4. Nested keyrefs allow you to specify an ordering relationship between keyrefs. A nested keyref will appear in the output after its parent keyref.

   Consider the following the keyref pair:

```
<key-keyref-pair>
<key>/configuration/class-map/*/ARG.001</key>
<keyref>/configuration/policy-map/class/ARG.001</keyref>
<key-keyref-pair>
<key>/configuration/policy-map/class/bandwidth/ARG.001</key>
<keyref>/configuration/policy-map/class/random-detect</keyref>
<key-keyref-pair>
<key>/configuration/policy-map/class/random-detect/prec-based</key>
<keyref>/configuration/policy-map/class/random- detect/precedence</keyref>
</key-keyref-pair>
</key-keyref-pair>
</key-keyref-pair>
```

   This keyref pair will have its CLI output in the following order:

```
policy-map test-p
class test-c
bandwidth 20
policy-map test-p
class test-c
random-detect prec-based
policy-map test-p
class test-c
 random-detect precedence 0 1 2 3
```

The following example shows a configuration file that defines the Key and KeyRef definitions for ordering the commands during native command generation:

```
<?xml version="1.0" encoding="UTF-8"?>
 <!-- The purpose of this configuration file is to define the Key And
KeyRef definitions for Ordering the Commands during the native command
generation. -->
<data>
<nativeCommandGenerationData>
```

```
<key-keyref-pair>
<key>/configuration/interface/*/ARG.001;concat(name(..), string(.))</key>
<keyref>/configuration/ip//route</keyref>
</key-keyref-pair>
 <key-keyref-pair>
<key>/configuration/interface/FastEthernet/encapsulation/ARG.001</key>
<keyref>/configuration/interface/FastEthernet/ip/address</keyref>
</key-keyref-pair>
<key-keyref-pair>
<key>/configuration/interface/*/ARG.001;concat(name(..), string(.))</key>
<keyref>/configuration/ip//mroute/ARG.005</keyref>
 </key-keyref-pair>
<key-keyref-pair>
</nativeCommandOrderingData>
</nativeCommandGenerationData>
</data>
```

# Using command set groups

Command set groups are collections of device-specific command sets that all perform the same configuration change. You use command set groups when you want to apply the same change to devices of a different VTMOS.

## Command set groups overview

To change a device you need to deploy a command set specific to that device type. To apply the same change to a number of different device types, you can create a group of command sets that collects together those device-specific command sets.

The Command Set Advisor can suggest the command sets for you to add to the group in order to achieve full coverage for all your selected devices, thereby enabling a network operator to apply a configuration change to one or more network resources without specific network resource knowledge.

Command set groups can consist of native or modeled command sets, and are scheduled and submitted like any other unit of work (UOW).

Parameters in a command set group are shared by all command sets in the group, so that the values that are modified at run time are applied to all the devices covered. For example, a command set group can change the banner for a range of devices. When applying the group to the devices, an operator can supply the new banner name (the parameter), which is then inserted into each of the command sets in the group, and applied to each device.

**Remember:**

- The command sets in a command set group should all perform the same change.
- Together, all command sets in a group should cover all selected devices.
- Parameters in command set groups are shared by individual command sets.
- Devices must be in synch before applying command set groups.

**Command Set Advisor**
After you have selected the devices to be configured by the command set group, you use the Command Set Advisor to add command sets to the group until all devices are covered.

For example, a command set that changes the login banner for a router might be slightly different from one that does the same on a switch. Therefore if you create a command set group to change the login banners of a range of different devices, you need to select specific command sets that are capable of changing the banner of each of the devices.

**Coverage**
Each time you add a command set to a group the Command Set Advisor calculates the percentage of selected devices covered.

You add command sets to the group until all devices are covered, that is, until your coverage reaches 100%.

**Automatic coverage**
Automatic coverage occurs when the defined command set (or native command set) is deemed valid by the system for one or more devices.

**Note:** Empty modeled command sets will not be deemed valid for any device.

**Manual coverage**
Manual coverage occurs when the user overrides the system and sets a command set to be valid for one or more devices.

**Note:** When you add or remove a device for manual coverage the system determines which other devices will be affected by this, and then adds or removes these as well.

**Failures**
A failure occurs if there is no applicable command set for a selected device. If this happens the command set is not processed against the device and the error is logged.

If a native command set is applicable for a selected device and the UOW is run in 'report only' mode, a failure occurs and the error is logged.

**Multiple command set groups**
Multiple command set groups can be applied within the same UOW.

**Reevaluating command set groups after adding or removing drivers**
When adding or removing Netcool Configuration Manager drivers, you must reevaluate all existing command set groups.

Use the icosutil 'ReevaluateGroups' command to determine if the addition or deletion of drivers has an impact on the coverage of the command set groups, and to then update them accordingly. See the scripting chapter in the *IBM Tivoli Netcool Configuration Manager Reference Guide* for information on how to use the icosutil utility to run the 'ReevaluateGroups' command.

**Note:** In addition to running the icosutil 'ReevaluateGroups' command, you should also manually review the coverage of the command set groups after adding or removing drivers.

**Security sets**
Security sets do not apply to the command sets contained within a command set group.

**Related tasks**
Using command sets
Command sets are snippets of resource configurations that can be applied across multiple network resources. Command sets use standard configuration syntax and markup to identify the commands.

## Creating command set groups

This task describes how to create a command set group. Once created, you have to edit the command set group before it can be applied.

1. Navigate to the realm in the Resource Browser where you want to create a command set group.
2. Select **File** > **New** > **Command Set Group**.

3. When the **New Command Set Group** window displays, specify the name of the new command set group.

   **Note:** When creating a command set group, the list of VTMOS labels from which you can select when creating a modeled or native command set is set to */*/*/* and can not be edited. VTMOS are specific to individual command sets, not command set groups.
4. Select **OK** to complete.

This action creates the command set group in the Resource Browser under the current realm.

You can now edit the command set group.

## Editing command set groups

After you create a command set group, you must edit it. You can also rename an existing command set group, or move it to a different realm.

You must create a command set group before you can edit it

1. Navigate to the realm in the Resource Browser where you want to edit a command set group.
2. Highlight the command set group that you want to edit, and select **Edit** > **Edit** from the menu bar. Alternatively, you can select **Edit** from the right-click menu.

   The **Command Set Advisor** window is displayed.
3. Click **Select Coverage to Add Command Sets**.

   The **Select Coverage** window is displayed.
4. Select either **Device** or **Realm** from the **Selection Type** drop-down list, and then complete the following steps:

   **If Realm**
   Select the realm or realms to be covered by the command set group.

   Select the **Include Sub-Realms** checkbox to cover all sub-realms contained within the selected realm or realms.

   **If Device**
   Navigate through the realms and select a device.

   Click **Add** to add the selected device to the list of devices to be covered by the command set group.

   Add as many devices to the list of devices to be covered as required.

   **Tip:** You can select multiple realms or devices using **Ctrl** when selecting the realms or devices. You can select a range of realms or devices using **Shift** while selecting the top and bottom resource.
5. Click **OK** update the coverage data in the Command Set Advisor, and close the **Select Coverage** window.

   **Note:** Coverage is not saved. Each time you open the command set group you need to select coverage again.

   Information specific to the command set group is displayed in the Device Coverage and Command Sets tables:

   **Device Coverage**
   If coverage has been selected, coverage information is shown in the **Device Coverage** table in the following columns:

   **Total**
   The total number of devices to be covered by the command set group.

   **Covered**
   The total number of devices covered.

   **Not Covered**
   The total number of devices not covered.

**Manual**
The Manual checkbox is selected if there is any manual coverage in the command set group.

**Overlap**
The Overlap checkbox is selected if any device is covered by more than one command set.

If manual coverage has been defined, it may result in such an overlap, in which case you should ignore it. The manually assigned command set takes precedence and the automatic selection is ignored at run time.

If no manual coverage has been defined, the command sets within the group may have been defined incorrectly. An example would be if command sets with different functionality have been added to the command set group. Should this be the case, you must remedy this overlap before the command set group is applied.

**Remember:** Command set groups have been designed to perform the same configuration change on devices of different VTMOS, and not to perform different types of configuration changes.

**Coverage**
The device coverage achieved by the command sets in a group expressed as a percentage. The target is for a command set group to achieve 100% coverage of the selected devices. Note that native command sets have to be manually assigned in order to contribute to the coverage total.

**Restriction:** If the Overlap checkbox is selected this indicates that devices are covered by more than one command set. This may cause the total coverage percentage to be less than the sum of the individual command set coverage percentages.

**Command Sets**
If command sets have been saved in the group, command set information is shown in the **Command Sets** table in the following columns:

**Set**
The name of the command sets saved in the groups.

**Type**
The types of the command sets saved in the groups, which will be either 'modeled' or 'native'.

**Modified by**
The name of the user who has modified the command set.

**Modified at**
The date and time that the command set was modified.

**Covered**
The number of devices covered by the command set.

**Manual**
The Manual checkbox is selected if the command set has been set to manually cover any of the selected devices within the command set group.

**Coverage**
The device coverage achieved by the individual command set expressed as a percentage.

6. If the coverage is below 100%, you can now add new command sets. To add more command sets, click **Sets** > **Add Command Sets** and then select one of the following options:

**Next Suggested**
Based on the chosen list of devices and the calculated coverage, the advisor analyses the popular, and not automatically covered, list of devices, and then determines which variation of command set would achieve the highest increase in coverage.

**Modeled (Select Device)**
Creates a command set based on a selected device and adds it to the group. The devices offered for selection are those SmartModel devices that have not already been automatically assigned.

**Native (Select Device)**
Creates a native command set based on a selected device and adds it to the group. The devices offered for selection are those devices that have not already been automatically assigned.

**Note:** If you save an empty modeled command set, there will be no change in coverage.

7. Perform the following additional actions from the **Command Set Advisor** window. You access these options from the **Sets** menu on the navigation bar.

   **Refresh**
   Click **Refresh** to refresh the displayed data.

   **Open Command Set**
   Opens the Command Set Editor in view-only mode.

   This allows users without editing permission to view command sets.

   **Edit Command Set**
   Opens the Command Set Editor.

   See the command set chapter in the *IBM Tivoli Netcool Configuration Manager User Guide* for information on editing command sets.

   **Delete Command Set**
   Deletes all selected command sets.

   **Rename Command Set**
   Rename a command set in a command set group.

   **View Coverage**
   Lists the devices that the command set covers, if any.

   You can select multiple command sets and view the devices assigned to those that are selected.

   **Manual Coverage**
   Opens the **Manual Coverage** window for the selected resource.

   When a modeled command set is created it may apply to a range of devices that employ the same command structure. When such a command set is created for a group and saved, the coverage of devices is calculated and displayed. This range of devices can be considered the 'automatic' coverage. You can, however, choose to manually cover a device with a command set which takes precedence over automatic coverage.

   **Note:** When you add or remove a device for manual coverage the system determines which other devices will be affected by this, and then adds or removes these as well.

   The **Manual Coverage** window has the following tabs:

   **Add Devices**
   Manually adds devices to a command set.

   **Remove Devices**
   Manually removes devices from a command set.

   **Remove Drivers**
   Manually removes drivers from a command set.

   While device coverage is not saved, driver information is saved. You use this tab to remove manual coverage when devices are not selected.

8. To view the devices included in the command set group, click **Coverage** > **View All Coverage**.

   You can perform the following actions from the **View All Coverage** window:

   **Refresh**
   Refreshes the displayed data.

   **Reset Filter**
   Resets all filters.

   Filters filter the results in the table based on a user's entry under a table column (wildcards are supported).

   **View in Resource Browser**
   Selected devices are displayed in the Resource Browser as Search results

   **Select All**
   Selects all devices or realms.

**Clear Selection**
Deselects all selected devices or realms.

The command set group can now be applied.

**Related tasks**

Using command sets

Command sets are snippets of resource configurations that can be applied across multiple network resources. Command sets use standard configuration syntax and markup to identify the commands.

## Applying command set groups

You can apply a command set group in different ways. A command set group can be selected and applied to one or more network devices. One or more network devices can be selected, and then a command set group can be applied. Also multiple command set groups can be applied to multiple network devices. In addition, one or more command set groups can be applied to a realm.

You must create and edit a command set group before you can apply it. Devices must be in synch before applying command set groups.

A number of different steps and therefore different windows are presented when applying command set groups. The sequence of the windows are dependent on the type and composition of the command set group.

**Note:** Only one command set from a command set group will be applied to each device.

1. Navigate to the Resource Browser, and highlight the command set group from the listing of network resources.
2. From the menu bar, select **Tools** > **Apply Command Set Group**.
3. When the **Apply Command Set Groups** window is displayed, choose the command set groups required using the **Add/Remove** buttons in between the panels. The **Move Up** and **Move Down** buttons are used for prioritizing the order in which the command set groups are applied.
4. When you have selected all required command set groups, select **Next** to proceed.
5. The **Scope of Application** dialog displays. Using the following table as a guide, enter the appropriate information requested.

*Table 23. Scope of Application dialog*

| Selection | Description |
|---|---|
| Apply the Command Set Group(s) to Network Resources in a Realm | Will apply the command set group(s) to all network resources in the realm selected. |
| Apply the Command Set Group(s) to specific Network Resources | Will apply the command set group(s) only to the specific network resources chosen. |
| Apply the Command Set Group(s) to the Network Resources retrieved from a Realm | Will apply the command set group(s) to all network resources in the retrieved realm. |

6. When done, select **Next** to display the second part of the **Scope of Application** window. Select the realm name/network resources as applicable to the choice made in the previous window. This filters devices based on their support level, for example to display SmartModel only. Units of Work can also be filtered by Name or VTMOS as required. However, this is an optional step. Wildcards are in place by default to retrieve all possibilities. Click **Next** to proceed.
7. The **Configure Execution Options** dialog displays. Using the following table as a guide, please enter the appropriate information requested.

| *Table 24. Configure Execution Options dialog* | |
|---|---|
| **Element** | **Description** |
| **Execution Mode** | |
| Execute Mode | Applies command set group to selected network resources. |
| Report Only Mode | Does not change resources, but produces a report detailing the changes that would be made to those resources if in execute mode.<br>**Note:** The Report Only mode does not apply to native command sets. |
| Apply Device at a time | Applies all command set groups to one individual device at a time. |
| Apply Command Set Group at a time | Applies one command set group at a time to a resource. |
| **Pre-Emptive Compliance Options**<br>**Note:** These options are only available if the user is a member of a group with Pre-Emptive compliance activities. Pre-emptive options are only available for Modeled command sets. | |
| Enable Pre-Emptive Compliance Checks | When in Execute mode all Pre-emptive modes are available. However if the user has selected Report Only execution mode, then report only pre-emptive mode is automatically selected. If the user has ‘Manage Work' rights they will be able to disable Pre-emptive Compliance checks by deselecting the check box. Users who do not have 'Manage Work' rights will not be able to modify pre-emptive settings. |
| Block Configuration Change if projected configuration contains compliance failures | Policy is run against the current and projected configuration to determine if a violation is present. If a violation is found, the configuration change is blocked. |
| Block Configuration Change if projected configuration contains new compliance failures only | If a compliance violation is found within the projected configuration and the current configuration has no violations then the configuration change will be blocked. If both projected and current configurations have failures then the configuration change will not be blocked and changes will be made to the device. |
| Report Compliance Failure(s) only (Configuration change will not be blocked) | Produces a report providing information on violations in both the current and projected configuration. Pre-Emptive failures are ignored and the command set group continues to execute. |

| *Table 24. Configure Execution Options dialog (continued)* | |
|---|---|
| **Element** | **Description** |
| Command set groups | This lists the command set groups that will be rolled back. |

8. Select **Next** to proceed. If Execute Mode has been chosen, the **Rollback Options** window will be displayed. Otherwise, the wizard skips ahead to the **Enter Parameters** window.
9. If the **Rollback Options** window displays, use the following table as a guide to enter the appropriate information. A Rollback can be requested in the event that a command set group fails. The Rollback can be carried out for a single command set group, or multiple command set groups.

| *Table 25. Rollback Options fields* | |
|---|---|
| **Field** | **Definition** |
| **How should Rollbacks on command set group failures be handled?** | |
| No Rollback | Select this to turn off the rollback option. |
| Use Modeled Rollback | This option will enable a rollback to a modeled configuration. |
| Reload the configuration and reboot the device | This option will load the original configuration and reboot the device. |
| Check here to have Rollbacks verified | Select this checkbox to enable rollback verification. |
| **How should Rollbacks be done for each Network Resource?** | |
| Rollback only the failed command set group on the failed Network Resource | This option rolls back only that command set group that failed. |
| Rollback all command set groups on the failed Network Resources | This option rolls back all command set groups on the failed resource. |

10. When done, select **Next** to proceed.

    If parameters are detected in the command sets in the group, the **Enter Parameters** window is displayed.
11. If parameters are present, enter a value for each parameter.
12. When done, select **Next** to proceed.
13. The **Password Override** window displays. Using the following table as a guide, please enter the appropriate information requested.

| *Table 26. Password Override fields* | |
|---|---|
| **Field** | **Definition** |
| Override ITNCM Authentication | Select this check box to override the default authentication information. |
| Login Name | Provide the login name for the device you are accessing. |

| *Table 26. Password Override fields (continued)* | |
|---|---|
| **Field** | **Definition** |
| Password | Provide the password for the device you are accessing. |
| Enable Password | Provide the device enable password for the device you are accessing. |
| Only Use This Authentication | Select this check box if you will always use this authentication for your resource. |

14. The **Execution Priority** window displays. By default all UOWs are submitted with a priority of Medium. Select the priority required and click **Next** .
15. The **Schedule Work** window displays. If you select **Immediate**, the **Describe Work** window will be displayed. If you select **Scheduled** or **Recurring Schedule**, use the information in the following table to make the rest of your selections in the **Schedule Work** window.

| *Table 27. Schedule Work options* | |
|---|---|
| **Option** | **Definition** |
| Scheduled | The job will run at a specific time, based on the values entered for Scheduled Start and Scheduled End. |
| Hourly | Use this option to specify that the process should run each hour, or every n hours after the scheduled start time, for example, Every 3 hours after Scheduled Start. |
| Daily | Use this option to specify that the process should run every *n* days, for example, Every 5 days, or else every weekday (Monday - Friday). |
| Weekly | Use this option to specify that the process should run every *n* weeks on a specific day of the week, for example, Every 3 weeks on a Monday. |
| Monthly | Use this option to specify that the process should run on a specific day of every *n* months, for example, Day 30 of every 6 months. Or, you can specify that the process runs on a relative day of every month, for example, The First Monday of every 3 months. |
| Yearly | Use this option to specify that the process runs on a specific day and month of every year, for example, Every January 1st. Or, you can specify that the process should run on a relative day of the week of a specific month, for example, The First Monday of January |
| Scheduled Start | Enter the scheduled start time and date. |
| Scheduled End | Enter the scheduled end time and date. |

| *Table 27. Schedule Work options (continued)* | |
|---|---|
| **Option** | **Definition** |
| Next Execution | Enter the time and date for the next execution. |
| Window Size | Use the drop-down lists to indicate the window size. |
| Every n hours after Scheduled Start | Choose the number of hours from the drop-down list. |
| Every n days | Choose the number of days from the drop-down list. |
| Every Weekday | The job will run every weekday. |
| Recur every n weeks | Choose the number of weeks from the drop-down list and select the appropriate day. |
| Day n of every n months | Choose the number of days and months from the drop-down lists. |
| The specific day of every n month | Choose the specific day and month from the drop-down lists. |
| Every specific date | Choose the month and day from the drop-down lists. |
| The specific day of every n month | Choose the specific day and month from the drop-down lists. |

16. The **Describe Work** window displays. Enter a description for the UOW, and then click **Finish**.

The command set group is now submitted as a UOW and will run when scheduled, as long as the proper approvals are granted. The number of approvals required for the UOW depends on the group policy.

# Using security sets

Security sets implement view, add, modify, and delete rights inside a resource configuration.

## Overview of security sets

Security sets extend a SmartModel to include view, add, modify, and delete (VAMD) rights to commands inside a configuration. Once defined, you can reuse security sets for different SmartModels.

A security set is a tool that layers security on top of modeled configurations, thereby supporting security at the presentation layer. Security sets add view, add, modify, and delete permissions (that is, VAMD permissions) to the commands inside a configuration.

- You create security sets as resources in the IBM Tivoli Netcool Configuration Manager GUI.
- Security sets are applicable to any SmartModel, meaning that when you create one for one SmartModel, you can use it for any SmartModel.
- Security sets are schema-specific, but you can use them across devices with the same vendor and type.
- A security set must be in a realm where devices can resolve it.

### Mapping a native configuration to XML hierarchy

When mapping a native configuration to XML, a hierarchy of data is created consisting of parent-child relationships, which are based on the indentation used by the native configuration. Commands that are indented are sub-commands to their parent. Using this XML configuration format, you can overlay security set metadata onto the XML structure, by for example defining VAMD rights on configuration nodes, which are then inherited down the configuration hierarchy.

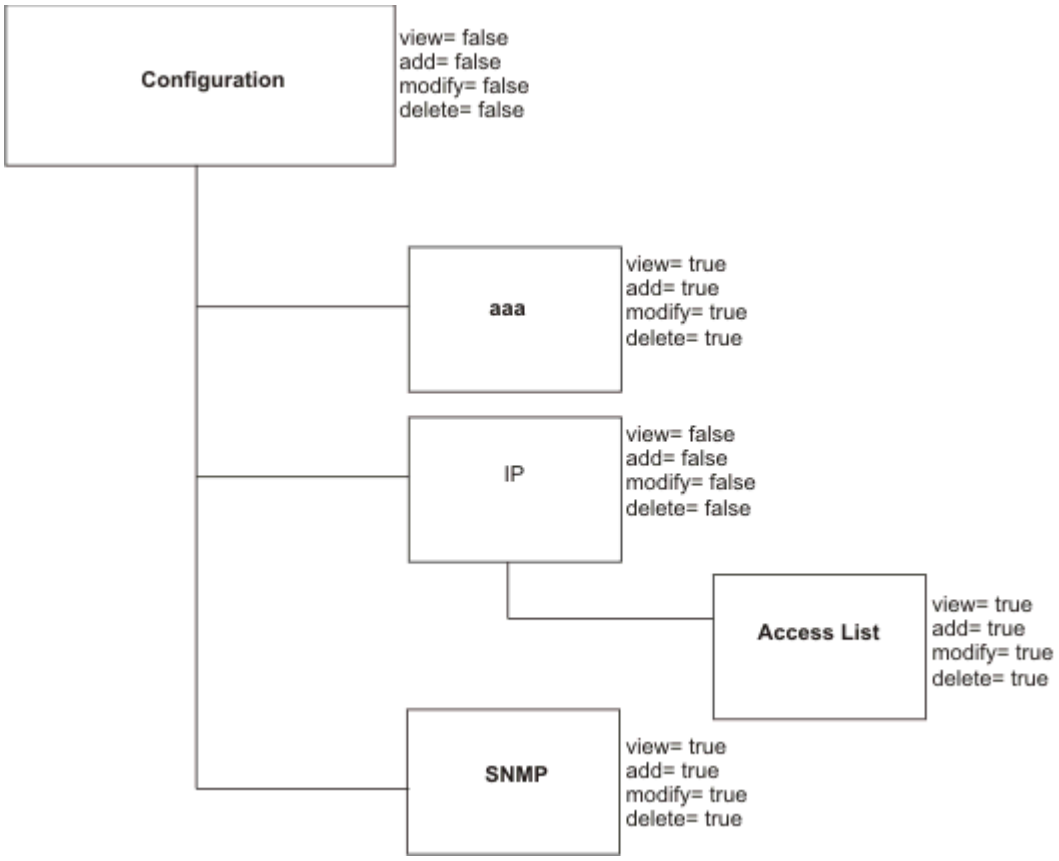


*Figure 1. Layering security sets onto a hierarchy example*

In this example, the base node of the XML configuration is 'Configuration'. VAMD rights are all set to false. If it is left this way and the security set is applied, the user sees nothing upon opening the configuration.

However, in subsequent nodes down the tree, the VAMD rights are modified. For example, the 'aaa' node of the configuration has all its VAMD rights set to true. If applied, the users see the 'aaa' node of the configuration.

The same is true for all the SNMP commands. VAMD rights are inherited down the configuration tree. For all other commands not shown in this example, their VAMD rights are all false.

In the 'IP' node of the configuration, the security set is designed so that users can see and modify any access lists under the 'IP' node of the tree. However, anything else under 'IP' is hidden.

## Creating security sets

You create security sets in the Resource Browser. While security sets are schema-specific, you can use them across devices with the same vendor and type. A security set must be in a realm where devices can resolve it.

This task describes how to create a security set. Once created, you edit the security set using XML. Instead of creating a new security set, you can copy and edit an existing security set.

**Tip:** You can use an external XML editor to create the required XML code, and then copy it into the security set.

1. Navigate to the realm in the Resource Browser where you want to create a security set.
2. Perform one of the following steps:
   - Select **File** > **New** > **Security Set**.
   - Select **Edit** > **Copy Security Set**.

   The **New Security Set** window is displayed.
3. Specify the name and VTMOS of the security set.
4. Click **OK** to complete.

This action creates the security set in the Resource Browser under the current realm.

- Placing the security set in the realm does not initially affect users. Group security applies the security sets to the configurations, when users in that group open the configuration editor.
- The security document is overlaid on a configuration, which means its node structure must align with the node structure of the configuration. Security sets are vendor-specific. You can often use them across devices with the same vendor and type. However, if the nodes do not align, the security sets have no effect.

Next, you edit the security set.

## Editing security sets

After you have created or copied a security set, you edit it in XML. You can use an external XML editor to create the security set XML, and then copy it into the security set.

1. Highlight the security set you want to edit, and select **Edit** > **Edit** from the menu bar.

   The security set is opened in a simple text editing window that allows you to enter XML, or copy it in from an external XML editor.
2. Edit the security set using the following example as a guide.

   This example security set hides everything about a configuration except its access control lists (ACLs). As this is a Cisco device example, ACLs can exist in two locations, as a series of base commands in the configuration, and as a series of commands under the IP node of the configuration.

   **Required base node with VAMD settings**

   All VAMD rights are disabled at the base 'configuration' node. This prevents any sub-nodes from automatically inheriting inappropriate view, add, modify or delete permissions.

   ```
   <configuration
       add="false"
       delete="false"
       modify="false"
       view="false"
       xmlns:securityMarkup="http://intelliden.com/securityMarkup">
   ```

   **Note:** The closing tag is >

   **Example access-list node (nested underneath 'configuration')**

   The VAMD rights are enabled for the ACLs.

   ```
       <access-list
           securityMarkup:add="true"
           securityMarkup:delete="true"
           securityMarkup:modify="true"
           securityMarkup:view="true"/>
   ```

   **Note:** The closing tag is />

**Example IP node (also nested underneath 'configuration'), with access-list underneath**

The IP node inherits VAMD access rights from its parent 'configuration' node. This prevents users from accessing all the sub-nodes under the IP node. In this Cisco device example, 'access-list' is a child of the IP node To enable VAMD rights for ACLs, you must set the them to 'true'.

```
    <ip >
        <access-list
            securityMarkup:add="true"
            securityMarkup:delete="true"
            securityMarkup:modify="true"
            securityMarkup:view="true"/>
    </ip>
</configuration>
```

**Note:** The IP closing tag is `</ip>`, followed by the configuration closing tag `</configuration>`

3. Once you have edited your security set, click **File** > **Save**.

To use a security set, you apply it to groups and realms.

## Applying security sets to a User Group and Realm

You apply a security set to groups and realms, thereby enabling it to control configuration security.

Only one security set per realm is supported. If you apply more than one security set to a device, you will receive a warning about having an empty configuration.

1. As a Netcool Configuration Manager system administrator, log into the **Account Management** page.
2. Select the user group you would like to apply the security set to.
3. Navigate to the **Security** tab, and select a realm from the **Realm** dropdown list.
4. Choose a security set and command filter, then click **Apply**.

   The security set is displayed in a table under the headings 'realm', 'resource', and 'resource type'.
5. Click **Save**.

   A locked padlock icon in the table next to a security set indicates that it has been saved to a group.

The security set is now submitted as a unit of work (UOW) and will run when scheduled, as long as the proper approvals are granted. The number of approvals required for the UOW depends on the group policy.

# Command filters

Command filters enable group administrators to restrict commands users can execute on network devices during an IDT session. Both administrators and users can create command filter resources and set the VTMOS for such.

In order to create or modify command filters, you need to have an understanding of how to configure network resources, and be familiar with the use of Java regular expressions. You must also understand each system's operating system, topology and resource naming conventions.

The administrator for a group assigns command filters to that group through the accounts administration page and any users that are members of that group will have the resource assigned to it. At this point they also select a realm to assign the command filter to and any devices contained in this realm and sub realms will have the command filter assigned to it subject to VTMOS.

During an IDT session to a device, the command filters that have been assigned to the users group(s) and to the devices realm are applied.

## Command filters overview

Command filters enable group administrators to restrict commands users can execute on network devices during an IDT session. Both administrators and users can create command filter resources and set the

VTMOS for such. Using IDT, network operators can initiate TELNET and SSH terminal sessions with devices in order to change the device configuration.

This allows administrators to control the specific changes operators can make to devices without restricting the type of direct access to a device that IDT provides. Command filters therefore provide a less reactive way of controlling and monitoring device changes than, for example, key stroke logs.

**Note:** Netcool Configuration Manager GUI and API users cannot modify or delete command filters assigned to their own user groups.

IDT displays device output in response to commands. Command filtering restricts the commands that can be sent to a device, but does not filter the output once a command begins to extract data from a device.

**Remember:** Key stroke logs provide a detailed audit trail of changes operators make to devices in the network.

## Command filter attributes

When adding or editing a Permit or Deny entry, you define specific attributes.

### Purpose

Command filter attributes are associated with Permit or Deny entries. Permit entries take precedence over Deny entries.

### Parameters

**`Position`**
Refers to the location where the current entry resides in the Permit or Deny list.

**`Expression`**
Contains the regular expression that the command will be checked against before being permitted or denied during an IDT session.

**`Match Criteria`**
This attribute can have one of two values:

- `Match Exactly:` — The command is checked for an exact match against the expression.
- `Contains:` — The command is checked to see if it contains the expression.

**`Match Case`**
This attribute can have one of three values:

- `Match As Is:` — The case of the command will remain as is (unchanged) when matched against the expression.
- `Convert to Upper:` — The case of the command entered will be converted to upper case before it is matched against the expression.
- `Convert to Lower:` — The case of the command entered will be converted to lower case before it is matched against the expression.

**`Trim`**
Select True or False to specify whether the command filter should remove leading and trailing whitespace before matching. The default value is True, which removes trailing and leading whitespace.

**`Ignore`**
Specify whether this filter is active (true) or inactive (false).

**`Description`**
Optionally, enter a description of a maximum of 30 characters.

## About working with command filters

Use this information to obtain an overview of the tasks that you can perform when working with command filters.

The following table identifies the tasks associated with command filters. The table contains the following columns:

- Task — Specifies the command filters task.
- Tool — Specifies the tool used to complete the command filters task.
- Stand alone — Specifies whether the command filters task applies to Netcool Configuration Manager when operating in a stand alone environment.
- Integrated — Specifies whether the command filters task applies to Netcool Configuration Manager when operating in an integrated environment, that is, with Network Manager and Tivoli Netcool/OMNIbus.

| Task | Tool | Stand alone | Integrated |
|---|---|---|---|
| Viewing command filters | Resource Browser | Yes | Yes |
| Creating command filters | Resource Browser or API | Yes | Yes |
| Modifying command filters | Resource Browser | Yes | Yes |
| Modifying command filter content | Resource Browser | Yes | Yes |
| Deleting command filters | Resource Browser | Yes | Yes |
| Testing command filters | Command Filter Test Tool (accessed through Resource Browser) | Yes | Yes |
| Assigning command filters to groups | Accounts Administration Homepage or API | Yes | Yes |

## Viewing command filters

You can view command filters and their content and properties in the Resource Browser.

You can view command filters for the Netcool Configuration Manager realms in which you have 'resource view' permissions.

By default, command filter resources will be displayed in the Resource Browser. You can select not to display command filters from **File** > **Preferences** > **Resource Browser**, by deselecting the command filter option from the 'Resources' list.

1. In the Resource Browser, select **File** > **Command Filter Properties** from the menu.
2. View the command filter properties.

## Creating command filters

You can create command filters using either the Resource Browser or API.

You can only create command filters for the Netcool Configuration Manager realms in which you have 'resource add' permissions.

- When you create a new command filter, it contains default examples for both Permit and Deny sets, which are disabled. These examples can be edited or deleted, and provide practical examples of commands an administrator may want to permit or deny.

- If a command does not match any entry in the Permit or Deny sets, the default behavior option, which can be set to 'Permit All Others' or 'Deny All Others', determines whether the command is permitted or denied.
- Command filter content is applied to individual lines of text entered into the IDT.
- Operators with access to the command filter can create a shortcut to the command filter.

1. In the Resource Browser, select **File** > **New** > **Command Filter** from the menu. Alternatively, import a command filter from a file by selecting **Tools** > **Import from File** > **Command Filter(s)** from the menu.
2. Enter a name for the command filter.

   Command filter names cannot be longer than 65 characters, must be unique within their realms, and must not contain any of the following special characters:

   ```
   \=+,<>?";*£$&!~^%#@/
   ```

3. Select a VTMOS for the command filter, or stay with the default wildcards */*/*/*.

**Note:** To create command filters through the API, refer to the *IBM Tivoli Netcool Configuration Manager API Guide*.

## Modifying command filters

You can modify command filters using the Resource Browser. Provided you have the required permissions, you can rename filters and move them between realms.

- You can only modify command filters for the Netcool Configuration Manager realms in which you have 'resource modify' permissions.
- You can only move command filters out of one domain or realm into another if you have 'resource delete' permissions for the source, and 'resource add' permissions for the destination.
- You can only move command filters or rename them if the domain or realm to which they are to belong does not already contain a filter with the same name.

Command filter content is applied to individual commands entered during an IDT session with a device.

1. In the Resource Browser, select the command filter, then select **File** > **Rename** from the menu. Alternatively, select the command filter in the resource list and then select the rename option from the right-click menu.
2. Move a command filter from one domain or realm into another using drag-and-drop.

## Modifying command filter content

You can modify command filter content using the Resource Browser. Provided you have the required permissions, you can add, edit, and delete Permit and Deny entries for a command filter.

You can only modify command filter content for the Netcool Configuration Manager realms for which you have 'resource modify' permissions.

The following list describes pertinent information about this task:

- Command filter content is applied to individual commands entered during an IDT session with a device.
- When adding or editing a Permit or Deny entry, Netcool Configuration Manager validates the expression attribute to ensure that the regular expression entered is valid. If it is not valid, a warning message is displayed and you must correct the entry before it can be saved.

  **Note:** When editing or adding Permit and Deny statements in a command filter, you can test what commands will be permitted and denied by launching the Command Filter Test Tool.

  For detailed information, see "Testing command filters" on page 93.

1. In the Resource Browser, select the command filter, then select **Edit** > **Edit Command Filter** from the menu to open the **Edit Command Filter** window. Alternatively, select the command filter in the resource list and use the right-click menu to open the **Edit Command Filter** window.

**Note:** The **Edit Command Filter** window contains two tabs, one for 'Permit' entries and one for 'Deny' entries.

2. You can modify command filter content by adding new content, editing existing content, or deleting existing content.
   a) To add a permit or deny entry, select the appropriate **Permit** or **Deny** tab, then select **Edit** > **Add** from the menu. Alternatively, right click and select **Add** from the right-click menu, or use the **Add** icon on the toolbar menu.
   b) To edit a permit or deny entry, select the appropriate **Permit** or **Deny** tab, then select **Edit** > **Edit** from the menu. Alternatively, right click and select **Edit** from the right-click menu, or use the **Edit** icon on the toolbar menu.
   c) To delete a permit or deny entry, select the appropriate **Permit** or **Deny** tab, then select **Edit** > **Delete** from the menu. Alternatively, right click and select **Delete** from the right-click menu, or use the **Delete** icon on the toolbar menu.

## Deleting command filters

You can delete command filters using the Resource Browser, provided you have the required permissions.

- You can only delete command filters for the Netcool Configuration Manager realms in which you have 'resource delete' permissions.
- You cannot delete command filters that are assigned to a group of which you are a member.

**DANGER:** Deleting command filters can affect many users, reducing the restrictions placed on their interaction with devices.

In the Resource Browser, select **Edit** > **Delete Command Filter** from the menu. Alternatively, select the command filter in the resource list and click **Delete Command Filter** on the right-click menu.

## Testing command filters

You can test the coverage of a command filter by using the Command Filter Test Tool. The Command Filter Test Tool checks that the user entered commands against the Permit entries, the Deny entries, and the default behavior defined in a command filter.

The Command Filter Test Tool is intended for use by administrators who want to test the coverage of existing command filters. One command is entered per line.

1. In the Resource Browser, select a command filter, then click **Run Test Tool** on the toolbar. The Command Filter Test Tool displays.
2. Type or paste commands into the text field.
3. Click **Test** to check the commands against the command filter. Commands that are permitted are displayed in the box labelled **Permitted**, and commands denied are displayed in the box labelled **Denied**.

## Assigning command filters to groups

Group administrators can assign command filters to user groups and Netcool Configuration Manager realms using either the Netcool Configuration Manager Accounts Administration Homepage or through the API.

Command Filters can only be assigned or unassigned to a group by an administrator for that group.

Command filters are assigned by Netcool Configuration Manager administrators using the Accounts Administration Homepage and applied by IDT during device sessions.

1. In the Netcool Configuration Manager Accounts Administration Homepage, select a group from the left hand side of the screen.
2. Select the **Security** tab, then the **Content** tab.
3. Select a realm from the **Realm** drop down list.

4. Select a command filter from the **Command Filter** drop down list.
5. Click **Add** to add the command filter to the table.
6. Click **Save**.

All users belonging to the user group have the assigned command filters applied to their IDT sessions provided the device being accessed resides in the realm or sub-realm where the command filter has been applied to, subject to VTMOS applicability.

# Device configuration in the Resource Browser

Use the Netcool Configuration Manager GUI (hereinafter referred to as the Resource Browser) to access, manage, and control multiple device configurations of multiple resources. You can use the Resource Browser to manage network devices manufactured by multiple vendors. Your window displays only those system resources for which you have authorization for display or control.

## Overview

The Resource Browser is a high level translation of native resource commands. The various drop down lists are dynamically generated based on the type of resource you are working with. Should you want to view the actual native resource commands for a configuration, you can do so. Your window will show only those system resources for which you have authorization for display or control.

You can display the following editable configurations for all device model types:

- Current resource configuration
- Previous configuration
- Previously saved draft configuration
- All configurations for a specific resource

### Configuration validation

The values you provide for the various configuration parameters must be valid for the appropriate VTMOS. The system does not validate configuration data for most fields.

### Disaster recovery

If a network resource becomes unmanageable for any reason, you often need to revert to a previous good configuration. You normally do so by applying a versioned configuration. When a versioned configuration is normally applied, Netcool Configuration Manager calculates the differences between the configuration currently running on the resource and the old (versioned) configuration. These changes are then applied to the network resource. If the device is unmanageable, you can instead select the disaster recovery mode when applying a versioned configuration. By doing so, you can push the entire versioned configuration to the device using the native CLI commands.

Note that this will require the device to be rebooted if it uses a startup and running configuration and should only be used as a last resort to recover the network device.

### Importing configurations

Netcool Configuration Manager allows both manual and automated initial input of your network resource information into the Netcool Configuration Manager database.

For information about the BulkLoader utility, see the *IBM Tivoli Netcool Configuration Manager Administration Guide*.

**Related tasks**

Applying versioned configurations
Use this procedure to apply an earlier configuration version to a network resource.

Importing resources

Use this procedure to manually import resources into the database.

Applying native command sets (via wizard)
Native command sets are defined by your administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying native command sets** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager.

Applying modeled command sets (via wizard)
Modeled command sets are defined by an administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying modeled command sets** wizard. You access the wizard from either the Activity Viewer or from the Network View, Hop View and Path View in Network Manager.

Synchronizing configurations (via wizard)
When the running and the stored (or candidate) configurations on a device are out of synch, you identify the correct configuration and use it to replace the incorrect one so that the two are synchronized. To do so you submit a synchronization request as you would any other unit of work (UOW). You access the Synchronization wizard from either the Activity Viewer or from the Network View in Network Manager IP Edition.

Applying configurations (via wizard)
You apply a configuration to a device using the Submit Configuration wizard, which you access from the Activity Viewer.

# Configuration states

The Netcool Configuration Manager database can store multiple versions of a configuration for a resource. These include current version; a future version that is either not complete, not approved, or in the queue to be implemented; and all previous versions. Saved configurations are identified by date and timestamp, along with the state of the configuration (current, draft, or versioned). Use this information to learn about the different states of configuration that can exist within Netcool Configuration Manager.

## Current configuration

The current configuration is the configuration that deems to be loaded on the network resource, and which is labeled as current in the Netcool Configuration Manager database. When you submit a configuration (creation or change), that configuration becomes the current configuration. You can create a configuration synchronization log (see “Synchronizing Configurations” on page 140) at anytime to see if there are any differences between the current configuration and the configuration running on the resource.

For information about synchronizing configurations, see “Synchronizing configurations” on page 103.

## Stale configuration

A Stale Configuration is defined as a device configuration which is older on Netcool Configuration Manager than the configuration held on the network resource. An example of a Stale Configuration is if the config setting 'update on change' has been unticked in the resource access document used by the device, and a draft config is submitted to the device.

## Draft configurations

The Netcool Configuration Manager supports draft configurations, which are modified configurations of existing resources waiting to be pushed to the resource. There can be multiple draft configuration per user per resource, but each must have a unique name. The system will alert you if you try to name a draft configuration the same as an existing draft.

### Versioned configuration

Versioned configurations are copies of previous current configurations. After a draft configuration is submitted and becomes the current configuration, the old current configuration is saved as a versioned configuration. Should you need to, you can always revert the resource to a previous version of the configuration by selecting and submitting an old version.

### Failed draft configurations

If a parent draft (a draft on which children drafts are based) fails to run for any reason, all child drafts are listed as being failed drafts. These drafts never got a chance to run because the parent draft on which they were based did not complete.

### Locked configurations

When searching or modifying configurations, you may see a configuration that is listed as being "locked." Locked configuration is a state that occurs while a draft configuration is waiting to be run, and also when a draft config is being applied to a device. Configurations remain locked after a successful execution, and will only be unlocked if they become either failed or expired.

You can view, but not edit, a locked configuration (though you can make changes to the locked configuration and save it as another name).

All configurations are stored in the Netcool Configuration Manager database. Each saved configuration includes the following information:

- Description
- Creator user name
- Creation date and time stamp
- Draft, versioned, or current flag

Each resource can have two different configurations: the running configuration and either a stored (CISCO) or a candidate (Juniper) configuration. The running configuration is just that: the configuration that is currently running on the resource. A stored configuration is a draft that is stored in non volatile RAM on a CISCO resource. A candidate is a draft that is stored on the file system of a Juniper resource.

When making a configuration change, Netcool Configuration Manager checks to be sure the current, running, and stored (or candidate) configurations are all the same. You will see a "mismatch" error message if any of the three configurations are different. The configuration synchronization function is useful for seeing what differences exist between the running and the current configurations, and for overwriting the selected configuration so they are back in sync.

For information about synchronizing configurations, see "Synchronizing configurations" on page 103.

## About working with device configurations

Use this information to obtain an overview of the tasks that you can perform when working with device configurations.

The following table identifies the tasks associated with device configurations. The table contains the following columns:

- Task — Specifies the device configuration task.
- Tool — Specifies the tool used to complete the device configuration task.
- Stand alone — Specifies whether the device configuration task applies to Netcool Configuration Manager when operating in a stand alone environment.
- Integrated — Specifies whether the device configuration task applies to Netcool Configuration Manager when operating in an integrated environment, that is, with Network Manager and Tivoli Netcool/OMNIbus.

| Task | Tool | Stand alone | Integrated |
|---|---|---|---|
| Creating partial configurations | **New Network Resource** dialog and Configuration Editor<br>**Note:** Access this dialog and the Configuration Editor from the Resource Browser. | Yes | Yes |
| Showing all configurations | Configuration Editor | Yes | Yes |
| Viewing a read-only configuration | Configuration Editor | Yes | Yes |
| Modifying configurations | Configuration Editor | Yes | Yes |
| Applying previous configurations | **Submit Configuration Change** wizard<br>**Note:** Access this wizard from the Resource Browser. | Yes | Yes |
| Viewing native commands | Resource Browser | Yes | No |
| Synchronizing configurations | **Configuration Synchronization** wizard<br>**Note:** Access this wizard from the Resource Browser. | Yes | No |
| Comparing native configurations | **Show Differences** wizard<br>**Note:** Access this wizard from the Resource Browser. | Yes | Yes |
| Comparing modeled configurations | **Show Differences** wizard<br>**Note:** Access this wizard from the Resource Browser. | Yes | Yes |
| Synchronizing configurationsnative command sets (via wizard) | **Synchronization** wizard<br>**Note:** Access this wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition. | No | Yes |

## Creating partial configurations

A partial configuration can be any configuration, or part of a configuration, that is not associated with an actual resource on your network. Partial configurations are useful for many tasks, such as serving as templates for new devices.

Within Netcool Configuration Manager, configurations are always associated with a resource, so in order to create a partial configuration, you first must create a “dummy” resource.

To create the "dummy resource, follow these steps.

1. Select the Resource Browser in the navigation tree.

   The Resource Browser displays.
2. Navigate to and highlight the desired realm in the folder tree.
3. Select **File** > **New** > **Network Resource**.

The **New Network Resource** dialog displays.

4. Complete the fields contained in the **New Network Resource** dialog:

| Field name | Description |
|---|---|
| Name | Enter a name for the new resource. This should be either a valid IP address or a hostname that resolves correctly using DNS. The resource name must be unique within the entire Netcool Configuration Manager database. This is a required field that can accept a maximum of 128 characters. Do not confuse the resource name with the configuration name. |
| Vendor | Select the vendor name from the drop down menu. Required field. |
| Type | Select the resource type from the drop down menu. Required field. |
| Model | Select the model from the drop down menu. The list of models is based on the vendor and resource type you selected. Required field. |
| OS | Select the correct OS version from the drop down menu. Required field. |

5. Click the **OK** button.

   The new network resource (that is, the "dummy" resource) is shown in the Network Resource listing.

6. Now that the “dummy” resource is created, highlight it and select **File** > **Edit**.

   A blank configuration catalog is opened in the Configuration Editor. The commands shown are based on the VTMOS you selected when creating the resource.

7. Begin adding the commands you want present in the partial configuration.
8. When finished, save the configuration.

## Showing all configurations

A single network resource can have numerous configurations (drafts and previous versions in addition to the current configuration) stored within the Netcool Configuration Manager database.

1. Select the Resource Browser in the navigation tree.
2. Select the **Configurations** tab.

   The available configurations are displayed in the **Configurations** tab.

## Viewing a read-only configuration

Use this procedure to open a read-only version of the of the configuration in the Configuration Editor. If you do not have modify rights for a resource, this is the only way you can view the configuration.

1. Select the Resource Browser in the navigation tree.

   The Resource Browser displays.

2. Search for the configuration you want to view.
3. Click to highlight and select the desired configuration.
4. Select **File** > **Show All Configurations**.

   The configuration details for the chosen configuration are displayed in the Configuration Editor. You can now view the configuration catalog of the resource or view the native commands.

## Modifying configurations

Use this procedure to edit a configuration that already exists within the Netcool Configuration Manager database.

When modifying an existing configuration, the system first verifies that the running and stored (candidate) configurations on the resource are the same. If not the same, you will see a mismatch error. You must resolve this mismatch before submitting any changes to the resource. After a successful configuration change, the system also writes the running configuration to the stored/candidate configuration on the resource, ensuring that all three configurations (current, running, and stored) are in sync.

For information about mismatch errors, see "Synchronizing configurations" on page 103.

1. Select the Resource Browser in the navigation tree.

   The Resource Browser displays.
2. Click the Search icon.

   The **Search Resources** form displays.
3. Search for the configuration you want to edit. This could be either the current configuration, or an existing draft configuration.
4. Click to highlight and select the desired configuration.
5. Select the **Configuration** tab.

   To edit the configuration, right click on the configuration and select **Edit**.
6. Click **Save** or **Submit** to save or submitr the changed configuration.
   For more information, see "Viewing native commands in the Resource Browser" on page 102.

## Applying versioned configurations

Use this procedure to apply an earlier configuration version to a network resource.

Within Netcool Configuration Manager all previous current configurations for a given resource are saved as 'versioned' configurations, enabling you to reapply one of these earlier configurations to a resource if needed.

When applying a versioned configuration, the system also writes the running configuration to the stored/candidate configuration on the resource, ensuring that all three configurations (current, running, and stored) are back in sync.

**Note:** If the access values for a resource have been changed, applying an older versioned configuration (one with different access information) back to the device will result in Netcool Configuration Manager not being able to communicate with the device.

**Tip:** Before you apply an earlier configuration version to a network resource, you can use the report-only option, which returns information informing you what results would have been caused by the configuration change.

1. Select the **Resource Browser** in the navigation tree.
2. Select or Search for the resource to which you want to apply a versioned configuration.
3. Select the **Configurations** tab.

   The available configurations are displayed in the Configurations Tab.
4. Select a configuration, then right-click, and select **Submit** from the context menu.

   The **Submit Configuration Change** wizard displays the Configure Execution Options dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

| *Table 28. Configure Execution Options dialog* | |
|---|---|
| **Element** | **Description** |
| **Execution Mode** | |
| Execute Mode | Applies Config Change to the selected network resources. |
| Report Only Mode | Does not change resources but will run Compliance Checks only. |
| **Pre-Emptive Compliance Options**<br>**Note:** These options are only available if the user is a member of a group with Pre-Emptive compliance activities. | |
| Enable Pre-Emptive Compliance Checks | This option allows the user to disable Pre-Emptive validations only if the user's group has the 'Manage Work' activity. Users who do have this activity will not be able to change this setting. |
| Block Configuration Change if projected configuration contains compliance failures | If a compliance violation is found within the projected configuration then the configuration change will be blocked. |
| Block Configuration Change if projected configuration contains new compliance failures only | If a compliance violation is found within the projected configuration and the current configuration has no violations then the configuration change will be blocked. If both projected and current configurations have failures then the configuration change will not be blocked and changes will be made to the device. |
| Report Compliance Failure(s) only (Configuration change will not be blocked) | In execution mode 'execute' any compliance failure will be ignored and the changes will be applied to the device. In report only execution mode only the compliance checks will be run - the UOW finish after Pre-Emptive checks. |

5. The **Submit Configuration Change** wizard displays the Password Override dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

| *Table 29. Password Override dialog* | |
|---|---|
| **Field** | **Definition** |
| Override ITNCM Authentication | Select this check box to override the default authentication information. |
| Login Name | Provide the login name for the device you are accessing. |
| Password | Provide the password for the device you are accessing. |

| *Table 29. Password Override dialog (continued)* | |
|---|---|
| **Field** | **Definition** |
| Enable Password | Provide the device enable password for the device you are accessing. |
| Only Use This Authentication | Select this check box if you will always use this authentication for your resource. |

6. The **Submit Configuration Change** wizard displays the Config Change dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

| *Table 30. Configuration Change (page 1 of 2) dialog* | |
|---|---|
| **Field** | **Definition** |
| Force Directory Override | Make this selection to force the changes and override the database. |
| Disaster Recovery; Use Raw CLI | Provide the login name for the device you are accessing. |

7. Only when submitting a draft configuration, the **Submit Configuration Change** wizard displays a second Config Change dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

| *Table 31. Configuration Change (page 2 of 2) dialog* | |
|---|---|
| **Field** | **Definition** |
| Merge | Adds the config settings you have made to those currently on this network resource. Any settings currently on the Network Resource will remain intact. |
| Replace | Applies the changes required to make the configuration on the Network Resource the same as the configuration being submitted. Please be careful with this option as it may remove items off the Network Resource that are necessary for it to communicate. |

8. The **Submit Configuration Change** wizard displays the Execution Priority dialog. By default, all UOWs are submitted with a priority of Medium. Select the appropriate radio button for the required execution priority and then click **Next**.
9. The **Submit Configuration Change** wizard displays the Rollback Options dialog. A Rollback can be requested in the event that applying a configuration fails. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next** to proceed.

| *Table 32. Rollback Options dialog* | |
|---|---|
| **Field** | **Definition** |
| **How should Rollbacks on configuration change failure be handled ?** | |
| No Rollback | Select this to turn off the Rollback option. |
| Rollback | Select this to turn on the Rollback option. |

| *Table 32. Rollback Options dialog (continued)* | |
|---|---|
| **Field** | **Definition** |
| Use Modelled Rollback | This option will enable a Rollback to a modeled configuration. |
| Reload the configuration and reboot the device | This option will load the original configuration and reboot the device. |
| Check here to have Rollbacks verified | Select this checkbox to enable Rollback verification. |

10. The **Submit Configuration Change** wizard displays the Schedule Work dialog. Select either immediate or scheduled execution. If you select scheduled execution, additional fields are displayed asking for the execution window. Provide the start date and time, and the end date and time for executing the work. From this dialog you can also specify a recurring schedule for the UOW.

    After making your selections, click **Next**.
11. The **Submit Configuration Change** wizard displays the Describe Work dialog. Type a description for your work and click **Finish**.

**Related concepts**

Overview

The Resource Browser is a high level translation of native resource commands. The various drop down lists are dynamically generated based on the type of resource you are working with. Should you want to view the actual native resource commands for a configuration, you can do so. Your window will show only those system resources for which you have authorization for display or control.

**Related tasks**

Creating pre-emptive policies

Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device, allowing you to evaluate the impact of configuration changes against pre-defined compliance policies for a device. In order to run a pre-emptive compliance, you first create or modify existing policies to make them suitable for execution in a pre-emptive manner. You then create a compliance process to apply the pre-emptive policy to a device.

Applying configurations (via wizard)

You apply a configuration to a device using the Submit Configuration wizard, which you access from the Activity Viewer.

## Viewing native commands in the Resource Browser

Use this procedure to view the native commands for a selected configuration, and depending on the resource vendor, view the configuration in either XML or CLI format.

Follow these steps to view the native commands for a selected configuration.

1. Select the Resource Browser in the navigation tree.

   The Resource Browser displays.
2. Search for the configuration you want to view.
3. Go to the **Configuration** tab, and right click on the selected configuration. Then select **View Native Commands**.

   A pop up window showing the native commands for the selected configuration is displayed. This may take several minutes. From this window, you can print the commands or save them. If no native commands are available, the option will be greyed out.

## Synchronizing configurations

Use this procedure to either synchronize a single resource, or synchronize all resources of a certain VTMOS at the realm level.

When synchronizing from the resource to Netcool Configuration Manager, a new version of the configuration is created and stored in the database regardless if changes are found. It is faster to do the synchronization in this way, rather than first checking for differences and then copying the configuration.

A configuration synchronization identifies differences between the configuration stored in the Netcool Configuration Manager database (called the current configuration) and the running configuration on the corresponding physical resource. If differences are found, you can choose to update either the configuration information in the Netcool Configuration Manager database or on the resource, bringing the two back into synchronization. Regardless of the direction of synchronization you choose, the stored/candidate configuration on the resource is also updated so that it too is in sync. After you make all selections, the configuration synchronization is submitted just like any other unit of work.

Configuration synchronization requires you to understand the following:

- Configuration mismatch errors — Each resource can have two different configurations: the running configuration and either a stored (CISCO/IOS type resources) or a candidate (Juniper/XML type resources) configuration. The running configuration is just that: the configuration that is currently running on the resource. A stored configuration is a draft that is stored in nonvolatile RAM on an IOS resource. A candidate is a draft that is stored on the file system of a Juniper/XML-based resource. In the case of a reboot, the resource will come up running either the stored or candidate configuration. For this reason, it is important to keep the stored or candidate configuration up to date with the running configuration.
- Viewing of mismatch error logs — When you perform a configuration change or apply a command set, Netcool Configuration Manager ensures all three configurations are the same. When you try to import a resource, Netcool Configuration Manager ensures that the running and stored configurations are the same. If any differences are found, your import or config change will fail and the description will specify: “The running and stored/candidate configurations on Resource do not match.”
- Resolving mismatch errors — Whenever you perform a configuration synchronization, regardless of the direction of change, both the running and stored (candidate) configurations are brought into synchronization with each other as well as with the current configuration.

1. Choose the network resource required for synchronization.
2. Right click and select **Synchronize**.

   The Configuration Synchronization wizard displays the **Select Network Resources** dialog.
3. Add the required device or devices from the left hand pane using the navigation buttons in the middle of the screen and then click **Next**.
4. The Configuration Synchronization wizard displays the Configure Failure Options dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

*Table 33. Configure Failure Options dialog*

| **Field** | **Definition** |
|---|---|
| Ignore All Errors | Indicates that the UOW is not to stop processing, regardless of how many failures occur. |
| Fail After X Total Errors | Choose the maximum number of failures that should occur before the UOW stops processing. |

| *Table 33. Configure Failure Options dialog (continued)* | |
|---|---|
| **Field** | **Definition** |
| Fail After X Percent Errors | Choose the maximum percentage of failures that should occur before the UOW stops processing.<br>Select the maximum percentage of failures you want to occur before the UOW stops processing. This option is useful when there are a large number of command sets being applied to a large number of resources. For example, if 51% is chosen, and there are two command sets and five resources, the formula is as follows:<br>`Max # of failures: (51/100) x (2x5) = 5.1 = 5` |
| Enable Password | Provide the device enable password for the device you are accessing. |
| Only Use This Authentication | Select this check box if you will always use this authentication for your resource. |

5. The Configuration Synchronization wizard displays the Password Override dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information or accepting the default, click **Next**.

| *Table 34. Password Override dialog* | |
|---|---|
| **Field** | **Definition** |
| Override ITNCM Authentication | Select this check box to override the default authentication information. |
| Only Use This Authentication | Select this check box if you will always use this authentication for your resource. |

6. The Configuration Synchronization wizard displays the Execution Priority dialog. By default, all UOWs are submitted with a priority of Medium. Select the appropriate radio button for the required execution priority and then click **Next**.
7. The Configuration Synchronization wizard displays the Configuration Synchronization Options dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

| *Table 35. Configuration Synchronization Options dialog* | |
|---|---|
| **Field** | **Definition** |
| Report Only Mode | This enables you to view differences in configurations. It also provides a work log with any differences between the managed and running configurations. |
| Synchronize from Network Resource to ITNCM | This enables you to update Netcool Configuration Manager to the Network Device configuration. |

| *Table 35. Configuration Synchronization Options dialog (continued)* | |
|---|---|
| **Field** | **Definition** |
| Synchronize from ITNCM to Network Resource | This enables you to update your Network Device to match the Netcool Configuration Manager configuration. This option is greyed out if a device is not SmartModel. |

8. The Configuration Synchronization wizard displays the Schedule dialog. Select either immediate or scheduled execution and type a description for the work. If you select scheduled execution, additional fields are displayed asking for the execution window. Provide the start date and time, and the end date and time for executing the work. From this page you can also specify a recurring schedule for the UOW.

   After entering the requested information, click **Next**.
9. The Configuration Synchronization wizard displays the Describe Work dialog. Write a description of the work completed and click **Finish**.
10. To view or save an existing Config Sync log, right-click any Config Sync UOW from the Work Finished List in the Queue Manager.

    **Note:** A status of Successful for a Config Sync simply means that the UOW ran and one or more of the attempted updates succeeded. The log will show information about any errors.
11. Select **ShowLog**.

    If the log file is very large, you are asked if you want to view the log or save the log to your computer as a file.
12. Select either **View** or **Save**.

    If you selected to view the log, it is displayed in a dialog box. If you choose to save the log to disk, you are prompted for a file name and location.
13. To correct any mismatch error condition, decide which configuration you want to treat as the correct, (either the current Netcool Configuration Manager database configuration, or the running configuration on the resource).
14. If you want the current configuration in the Netcool Configuration Manager database to be used as the correct version of the configuration, simply perform a Configuration Synchronization and select the “Sync to the Device” option.

    This option takes the current configuration and uses it to overwrite the running and the stored/candidate configurations on the resource. All three configurations are now the same, reflecting the values of the current configuration.

    OR

    If you want the running configuration on the resource to be used as the golden version of the configuration, perform a Configuration Synchronization and select the “Sync to ITNCM - Base” option.

    All three configurations are now the same, reflecting the values of the running configuration.

If you are synchronizing at the realm level, the specific resources that will be included are determined at execution time rather than submittal time. For example, if you pick an entire realm and a new resource is imported within that realm between submission and execution of the configuration synchronization, that new resource will be included in the UOW.

Depending on the policy in place, the newly created UOW may require approval before executing.

After the UOW containing the config sync has been approved and finishes, you can also view, print, or save the log to your client's hard drive.

**Related tasks**

Applying native command sets (via wizard)

Native command sets are defined by your administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying native command sets** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager.

Applying modeled command sets (via wizard)
Modeled command sets are defined by an administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying modeled command sets** wizard. You access the wizard from either the Activity Viewer or from the Network View, Hop View and Path View in Network Manager.

Synchronizing configurations (via wizard)
When the running and the stored (or candidate) configurations on a device are out of synch, you identify the correct configuration and use it to replace the incorrect one so that the two are synchronized. To do so you submit a synchronization request as you would any other unit of work (UOW). You access the Synchronization wizard from either the Activity Viewer or from the Network View in Network Manager IP Edition.

## Comparing native configurations

Use this procedure to compare and view the differences between native configurations. The native configurations being compared can be any that exist in the Netcool Configuration Manager database, regardless of whether these configurations have been obtained from an actual network resource or simply entered by a user as a “draft” configuration.

**Access rights**
Your access rights are determined by group membership, and they dictate the commands for which you can view any differences.

For example, if you do not have view rights for 'ntp server', you would not see any differences for the ntp server command.

**Comparing native configurations for head end devices**
With VmWare there is no concept of native commands. The driver communicates with the target using a VmWare supplied SOAP interface, the results of which are mapping to XML. Only modelled comparisons are supported for head end devices. For more information about comparing modeled configurations, see “Comparing modeled configurations” on page 107.

**Juniper devices**
The 'show diff' functionality is only available for Juniper devices that are using SmartModel drivers.

Generating a list of configuration differences allows you to quickly view any differences in command values between one native configuration (or a part of that native configuration) and another. You can also compare network resources to each other. Netcool Configuration Manager simply compares the current native configuration of each network resource. If no current native configuration exists, Netcool Configuration Manager uses the default draft (partial configuration).

To compare and view the differences between native configurations, follow these steps.

1. Select the Resource Browser in the navigation tree.

   The Resource Browser displays.
2. Search for the resources or configurations that you want to compare.
3. Click to highlight the selected configurations.

   **Note:** The Ctrl key may be used to select more than one configuration.
4. Right click and select **Show Differences**.

   **Remember:** The 'show diff' functionality is only available for Juniper devices that are using SmartModel drivers.
5. If you chose one configuration, the **Show Differences** wizard displays the **Select Master and Compared** dialog.

Select which configuration you want to consider the master and click **Next**. You can change your selections, and even choose different configurations at this point. Deciding which configuration to use as the master is important if you decide to leave the **Show All Differences** check box unchecked. You can click the Switch icon to change your master and compared selections. Click **Next** to continue.

6. If you chose multiple configurations or devices, the **Show Differences** wizard displays the **Select View of Report** dialog. If the support level of the device/configuration is SmartModel, there are options for a Modeled view and a Native View.

   To view compare and view native configurations:

   a) Select the **Native View** radio button.

   b) Click **Finish**.

      The Configuration Differences report begins executing immediately. When finished executing, the report displays in a new dialog box. The following table provides descriptions of the items that the Configuration Differences report displays:

| Report item | Description |
|---|---|
| File | Select **File** > **Close** to exit the report. |
| Edit | Select to access options on finding information within the report. |
| Tools | From this option you can view the next or previous set of differences. |
| Left Pane | Displays each command found on the master configuration. |
| Right Pane | Displays each command that differed from the value found on the master configuration. |

## Comparing modeled configurations

Use this procedure to compare and view the differences between modeled configurations on a device. The modeled configurations being compared can be any that exist in the Netcool Configuration Manager database, regardless of whether these configurations have been obtained from an actual network resource or simply entered by a user as a “draft” configuration.

**Access rights**

Your access rights are determined by group membership, and they dictate the commands for which you can view any differences.

For example, if you do not have view rights for 'ntp server', you would not see any differences for the ntp server command.

**Juniper devices**

The 'show diff' functionality is only available for Juniper devices that are using SmartModel drivers.

Generating a list of configuration differences allows you to quickly view any differences in command values between one modeled configuration (or a part of that modeled configuration) and another.

To compare and view the differences between modeled configurations, follow these steps.

1. Select the Resource Browser in the navigation tree.

   The Resource Browser displays.

2. Search for the resources or configurations that you want to compare.
3. Click to highlight the selected devices.

   **Note:** The Ctrl key may be used to select more than one device. Selected devices must have the same device model in order to compare.

4. Right click and select **Show Differences**.

**Remember:** The 'show diff' functionality is only available for Juniper devices that are using SmartModel drivers.

5. If you chose one device, the **Show Differences** wizard displays the **Select Master and Compared** dialog.

   Select which device you want to consider the master and click **Next**. You can change your selections, and even choose different devices at this point. In addition, you must choose the same model devices for comparison. Deciding which device to use as the master is important if you decide to leave the **Show All Differences** check box unchecked. You can click the Switch icon to change your master and compared selections. Click **Next** to continue.

6. If you chose multiple devices, the **Show Differences** wizard displays the **Select View of Report** dialog. If the support level of the device/configuration is SmartModel, there are options for a Modeled view and a Native View.

   To compare and view modeled device configurations:

   a) Select the **Modeled View** radio button. If you want to view all differences, check the **Show All Differences** check box.

      Information is displayed according to the following scenarios:

| Scenario | Show All Differences radio button is selected | Show All Differences radio button is unselected |
|---|---|---|
| Command is in the Master config, but not in the Compared config. | Command shown in report. | Command shown in report. |
| Command is in Compared config, but not in Master config. | Command shown in report | Command not shown in report. |
| Command is in both configs. | Command shown in report | Command shown in report |

   b) Click **Finish**.

      The Configuration Differences report begins executing immediately. When finished executing, the report displays in a new dialog box. The following table provides descriptions of the items that the Configuration Differences report displays:

| Report item | Description |
|---|---|
| File | Select **File** > **Close** to exit the report. |
| Edit | Select to access options on finding information within the report. |
| Tools | From this option you can view the next or previous set of differences. |
| Left Pane | Displays each command found on the master configuration. |
| Right Pane | Displays each command that differed from the value found on the master configuration. |

## Managing golden configurations

Fix Pack 1 A 'golden' configuration is a configuration version that you can use in compliance management as a known valid master version to compare device SmartModel configurations against. You use a golden configuration to generate compliance evaluation XPaths (by associating the configuration's device with a compliance definition) for running against a target device's configuration.

## Before you start

You must have 'Golden Configuration Management' user authority in order to create a golden configuration.

## About golden configurations

A 'golden' configuration is a configuration version used in compliance management as an ideal configuration against which configurations from similar devices can be compared. Any differences found are by default recorded as compliance evaluation failures. You can use this feature to quickly compare many thousands of details without having to manually create any evaluations.

**Note:** Golden configurations used for compliance purposes can only be for devices that have SmartModel drivers.

Fix Pack 2 You can mark a device configuration as one of two types:

**Globally available golden configurations**
A Golden Configuration that is globally available to all devices, and can be used for compliance-checking the configurations of other devices.

**Device-specific golden configurations**
A Golden Configuration that is locally available (to its own devices only), and restricted to compliance-checking against its own devices' current configuration.

## Globally available golden configurations (option 1)

Fix Pack 2

Golden configurations that are globally available for compliance checking are typically used where an ideal device configuration has been verified, and can then be used to compliance-check other target device configurations in the network. This ideal device configuration can be modified with regular expressions in order to allow for expected differences between the golden and target configurations. The modified golden configuration can be loaded into Netcool Configuration Manager using the file-based access method in the Resource Access Document.

With this option, you create a golden configuration compliance definition, which points to a device with a golden configuration. Compliance evaluations are then automatically created based on the commands specified in the golden configuration. These evaluations can be run against other devices by including the compliance definition in compliance rules, policies or processes.

In cases where a range of values is acceptable, you can edit the golden configuration to provide a regular expression, and evaluations are treated as failures only if the values found in the compared configurations do not satisfy the regular expression in the golden configuration.

If an imported configuration contains regex, it has an initial status of 'false'. If it does not contain regex, it has an initial status of 'has regex'.

**Example scenario**
You start with a text file of native configuration settings derived from multiple real device configurations with similar VTMOS.

You then add regular expressions to make the text file more generic.

Next, you create a virtual VTMOS-based device, edit the device's RAD to specify that configuration imports will be file-based, and import the configuration.

Once imported, you define the configuration as 'golden'.

You subsequently use the Netcool Configuration Manager - Compliance UI to use the feature.

**Restriction:**

The only supported mechanism for creating/updating configurations containing golden configuration regular expressions is to add the regular expressions to the golden configuration outside Netcool

Configuration Manager, before importing the configurations using the 'file based access' method delivered in the Drivers 20 release. See the Drivers 20 documentation for more information.

Currently 'file based access' method does not support Alcatel OLT devices.

Only Alcatel and Cisco devices are supported for golden configurations with the regex syntax outlined below. Juniper JUNOS supports the older syntax. See the note below for more information.

With Alcatel routers and switches, the content of fields with regular expressions must be surrounded by double quotes.

The 'golden configuration' feature depends on the presence of SmartModel configurations.

- Only a SmartModel configuration can be marked as a golden configuration.
- Only target devices with SmartModel configurations can be validated using a golden configuration.
- *(Even though the regular expression mark-up shown in the examples here can be defined in the native configuration, the evaluations generated are SmartModel-based).*

**Restriction:**

Configurations that contain regular expressions are subject to the following restrictions:

- – SmartModel-related right-click actions, such as for 'Edit' of configuration, are disabled, both at the configuration and network resource level (if it is the current configuration).
  - Showing 'Modelled View' differences is not supported.
  - Command Set Application is not supported.
  - The 'Re-discover' action is not available.
  - The 'Trigger Config Backup' action is not available.

**Tip:** Separately validate a golden configuration before using it for compliance checking.

You can annotate textual command argument values in the native configuration with specific regular expression (regex) mark-up in order to affect the compliance evaluation XPaths that are generated.

**Keywords**

**regex content**
A valid regular expression syntax

**valid value**
An example valid value for the argument.

This is used to support applying the regex syntax to argument values of any type, such as text, integer, and others. It ensures that the argument is constructed correctly on the SmartModel configuration, and compliance evaluation XPath.

The surrounding parenthesis are part of the syntax.

The translated smartmodel XML will not show the valid value in the regex markup, unless the translation results in the markup being placed in an ARG.999 element.

The following mark-up is available:

**@@@(valid value)@<regex content>@@@**
The compliance evaluation XPath generated matches a single occurrence of the same command in the target configuration, where the target command's argument values satisfy the regular expression supplied in `regex content`.

In the following example, an evaluation is created that matches a single occurrence of interface `Tunnel 64` where the argument value satisfies the regex `172.\d{2}.0.\d{2,3}`. The example valid value is `172.25.0.34`

```
!
interface Tunnel64
tunnel destination @@@(172.25.0.34)@172.\d{2}.0.\d{2,3}@@@
```

Below shows the SmartModel configuration XML that will be generated for the above. The example `valid value` is removed during the XML generation process.

```
<Tunnel>
   <ARG.001>64</ARG.001>
   <tunnel>
      <destination>
         <ARG.001>@@@172.\d{2}.0.\d{2,3}@@@</ARG.001>
      </destination>
   </tunnel>
</Tunnel>
```

**@@@(valid value).@regex content@@@(non Juniper JUNOS-based network devices)**

The compliance evaluation XPath generated matches multiple occurrences of the same command in the target configuration where the target command's argument values satisfy the regular expression supplied in `regex content`. When a match is found it also validates that any children in the golden configuration under the command with the regex are the same in the target configuration.

In the following example, an evaluation is created to confirm that all snmp-server hosts in the target configuration with a value starting with 'myhost' also have a udp-port value of '1620'. The example `valid value` is `myhost123`

```
snmp-server host 123.123.123.123 @@@(myhost123).@myhost.*@@@ udp-port 1620
```

The following example illustrates the dependency on SmartModels and what the resulting evaluation XPath would look like in compliance. The '@@@(valid value).@' regex markup would result in a contextual evaluation containing the following two SmartModel Xpath parts:

- Context XPath : /configuration/snmp-server/host[matches(ARG.003,'myhost.*')]
- Defined XPath : udp-port[ARG.001='1620']

  **Note:** The '123.123.123.123' value is not included in the XPath as explained in more detail below. The 'ARG' values are part of the SmartModel configuration, for example:

```
<snmp-server>
    <host>
        <ARG.001>123.123.123.123</ARG.001>
        <ARG.003>@@@.@myhost.*@@@</ARG.003>
        <udp-port>
            <ARG.001>1620</ARG.001>
        </udp-port>
    </host>
    <snmp-server>
```

  The example valid value is removed during the XML generation process.

**@@@(valid value)P@<regex content>@@@**

The compliance evaluation XPath generated matches multiple occurrences of the same command in the target configuration where the target command's argument values satisfy the regular expression supplied in `regex content`, such as `@@@(uplink)@P@uplink.*@@@` to match a text value starting with 'uplink'. When a match is found it will also validate that any siblings in the golden configuration structure under the **parent** of the command with the regex are the same in the target configuration.

In the following example, evaluations are created to confirm that all xe interfaces with a description starting with ‘uplink’ in the target configuration also have the following VLAN values.

```
<interface>
    <name junos:key="key">xe-0/0/0</name>
    <description>@@@(uplink)@P@uplink.*@@@</description>
    <mtu>9192</mtu>
    <unit>
        <name junos:key="key">0</name>
        <family>
            <ethernet-switching>
                <port-mode>trunk</port-mode>
                <vlan>
                    <members junos:key="key">1234</members>
                </vlan>
            </ethernet-switching>
        </family>
```

```
    </unit>
</interface>
```

For the two multiple occurrence regex items described above, any non regex argument values at the same or higher level in a command (relative to the argument with the regex) will be ignored when generating an evaluation; that is, the regex will be the only filter. For example, in the '@@@(valid value)P@' mark-up configuration example, the '0/0/0' argument on the xe interfaces will be ignored when creating an evaluation filtering on the description field starting with 'uplink'. The example `valid value` is removed during the XML generation process.

**Tip:** For a description of 'Defined XPath (single occurrence) and 'Context XPath' (multiple occurrence), see 'Creating compliance definitions using Golden Configuration'.

For Juniper JUNOS golden configurations

- The 'P@' mark-up will behave the same as the '.@' mark-up does for non-Juniper JUNOS configurations. This is to allow for differences in how Juniper JUNOS arguments are modeled.
- See the note below for more information.

If none of the above regex mark-up is supplied at any level down to a command element in a golden configuration, then the compliance evaluation XPath generated will check for a single exact match, that is, a 'Defined XPath', for the element between the golden and target configuration.

**Notice:** The new regex format above is not supported for:

- Multi-line textual fields, such as ‘banner motd’ argument values
- Juniper JUNOS golden configurations

For these, the older format, which only supports textual arguments that have no special format validation, should still be used.
The older format options are:

- @@@regex content@@@
- @@@.@regex content@@@,
- @@@P@regex content@@@)

In all other cases the new '@@@(valid value)...' format outlined above should be used to ensure that the argument is constructed correctly on the SmartModel configuration.

## Device-specific golden configurations (option 2)

Fix Pack 2

Device-specific golden configurations are locally available and restricted to own devices. They would typically be used where a particular configuration version for a device contains the set of commands for the device that are not expected to be altered.

Compliance checks between the device-specific configuration and the current configuration for a device can be configured by marking a configuration version as ‘device-specific’, and including its device in the scope of a compliance process that contains one of two new ‘device-specific’ pre-defined compliance definitions. (See “Creating compliance definitions using a 'device-specific' golden configuration” on page 282).

Device-specific compliance definitions do not specify any evaluations. Evaluations are generated when compliance process or policy is running (based on the current and device golden configurations of the target device). There are fields with a configuration that would be expected to be different between configuration versions (such as a timestamp or password value). These types of fields are identified in the Driver schema for the device (the field will have a ‘NonComparable’ attribute). A new XML file is now delivered with the Drivers in order to support the ‘NonComparable’ checking, If the file is not present then an updated driver will have to be installed.

## To set a configuration

You set a selected configuration as 'golden' or 'device-specific'.

**Important:** Before starting this task, add the Golden column to the columns displayed in the configurations tab. Due to Linux 'thick client' limitations, this must be done in Windows.

Any configuration containing the '@@@'' mark-up initially has a value of 'has regex' in the Golden column after import. This value can be modified by the actions below and once it has been set to one of the states below it will not subsequently revert at any stage to 'has regex'.

1. Select the **Resource Browser** in the navigation tree.
2. Search for the SmartModel device you want to view.
3. Click the **Configuration** tab, then right-click the selected configuration.
4. Select the **Make Golden** option. A window opens displaying the details for the selected configuration, and a radio button to select one of the following compliance execution scopes for the configuration:
   - Configuration is available to other devices
   - Configuration is restricted to this device (device-specific)

   If a configuration is already golden, the **Make Golden** option is disabled.

   Fix Pack 6 You can type a description of the change in the **Configuration description** field. The maximum number of characters is 1,000. The description is shown in the **Description** column of the Summary table. The **Description** column is not displayed by default.
5. Click **Finish** to complete the procedure.

The selected configuration is now marked as golden by displaying one of the following statuses:

**golden without regex**
If the scope is available to other devices and the configuration does not contain regex.

**golden**
If the scope is available to other devices and the configuration contains regex.

**device-specific without regex**
If the scope is restricted to this device and the configuration does not contain regex.

**device-specific**
If the scope is restricted to this device and the configuration contains regex.

Also, the configuration icon will have a gold mark in the top right corner. If another configuration for the device was already marked with one of the above four states, then that configuration is now unmarked, and has one of the following values in the Golden column:

**previous golden without regex**
If the scope is available to other devices and the configuration does not contain regex.

**previous golden**
If the scope is available to other devices and the configuration contains regex.

**previous device-specific without regex**
If the scope is restricted to this device and the configuration does not contain regex.

**previous device-specific**
If the scope is restricted to this device and the configuration contains regex.

## To remove a golden configuration

You can remove the 'golden' status from a configuration, unless the associated device is included in a compliance golden definition.

**Important:** Before starting this task, add the Golden column to the columns displayed in the configurations tab. Due to Linux 'thick client' limitations, this must be done in Windows.

**Note:** If the configuration is marked Golden and the associated device is included in a compliance golden definition, it will not be possible to undo the Golden status until the device is removed from the compliance golden definition.

1. Select the **Resource Browser** in the navigation tree.
2. Search for the device you want to view.
3. Click the **Configuration** tab, then right-click the selected configuration. It will have the status of 'golden' or 'golden without regex' in the Golden column, and the configuration icon will have a gold mark in the top right corner.
4. Select the **Undo Golden** option. A window displays the details for the selected configuration.
5. Click **Finish** to complete the procedure.

The selected configuration is now unmarked as golden and displays one of the following values: 'previous golden', 'previous golden without regex', 'previous device-specific', or 'previous device-specific without regex' in the Golden column.

### Possible values for the Golden state

Fix Pack 6

The following table shows all allowed values for the Golden state. A configuration cannot move from one column to another. States can only change within the same column.

For configurations that have one of the states in the 'Configuration contains regex' column, the following restrictions apply:

- – SmartModel-related right-click actions, such as for 'Edit' of configuration, are disabled, both at the configuration and network resource level (if it is the current configuration).
  – Showing 'Modelled View' differences is not supported.
  – Command Set Application is not supported.
  – The 'Re-discover' action is not available.
  – The 'Trigger Config Backup' action is not available.

It will still be possible to view the XML Configuration of a device in text format in the Compliance GUI. The '@@@...' mark-up is not supported for use with 'device-specific' or 'previous device-specific' configurations.

| Action | Configuration contains regex | Configuration does not contain regex |
|---|---|---|
| Initial import | has regex | false |
| Mark golden | golden | golden without regex |
| Unmark golden | previous golden | previous golden without regex |
| Mark device specific | device specific | device specific without regex |
| Unmark device specific | previous device specific | previous device specific without regex |

## Backing up and restoring configurations

You can back up and restore configurations of devices that are managed by an EMS.

Netcool Configuration Manager can send commands to an Element Management System (EMS) to instruct the EMS to back up or restore the configuration of a device that it manages.

The commands are sent by using a SOAP call.

Device configurations are usually stored on the EMS, but this can be configured in the EMS.

To back up or restore a device configuration, complete the following steps:

1. To back up a configuration, right-click on a device and select **Trigger Config Backup** .
2. To restore a configuration, right-click on a device and select **Trigger Config Restore**.

# Configurations and command sets in the Configuration Editor

Use this information about the Configuration Editor to view and edit configurations and command sets.

**Related concepts**

Managing extractions

Extractions are Netcool Configuration Manager resources that you can create much like configurations or command sets. They are defined on a specific VTMOS, and, once created, are visible in the Resource Browser. Instead of defining only specific values, extractions can be parameterized so that some values can be modified at run time. You can also export and import extractions.

**Related tasks**

Editing extractions

After you have created an extraction, you edit it using the Extraction Editor.

## Overview of the Configuration Editor

The Configuration Editor is an applet used for viewing and editing configurations and command sets.

Each configuration or command set, regardless of the vendor/type/ model/operating system (VTMOS), is displayed as a configuration catalog for ease of use. The following topics promote an understanding of the Configuration Editor and how you can use it to effectively view and edit configurations and command sets:

- Understanding configuration catalogs
- Understanding Configuration Editor features
- Importing configurations and command sets
- Working with configurations
- Working with command sets

### Understanding configuration catalogs

Configuration catalogs are the graphical folder trees that Netcool Configuration Manager uses to represent resource configurations and command sets. The configuration catalog is similar to a typical Windows list of folders and files, except some of the folders also contain data. When you click any element/object name from the catalog, the right pane of the application page shows that command and allows you to make edits.

### Understanding some Configuration Editor features

Text at the bottom of the Configuration Editor changes to “Configuration” or “command set” depending on what is currently being edited. Text is also displayed both in the title bar and at the bottom of the screen to indicate that there is changed/unsaved data in a configuration or command set.

The top of the Configuration Editor includes tool bar icons to make your editing tasks easier. Depending on whether a configuration or command set is opened, the title bar at the top of the screen shows the resource name, configuration name, and VTMOS, or it shows the command set name and VTMOS.

The Configuration Editor also shows the exact VTMOS found on the resource, if that information is available, regardless of what was entered when the resource was created.

You can have multiple Configuration Editor/Command Set Editor sessions open at the same time. After opening a command set or configuration, simply click back on the Resource Browser and search for another command set or configuration to open. You can open any combination of command sets and configurations at the same time.

## Importing configurations and command sets

You can use the Configuration Editor to import an existing configuration or command set into the configuration or command set currently being edited. This feature is useful if you want to "seed" a configuration with another configuration that is being treated as a template, or default configuration. It can also be helpful before applying a command set to see exactly what the effect of the command set will be on a given configuration by importing the command set into a configuration.

The VT of the configuration or command set being imported must match the VT of the current configuration or command set.

The following table summarizes the result of each of the possible import scenarios.

| Importing a ... | Into a ... | Result |
|---|---|---|
| Command set | Command set | The imported command set is appended to the command set being edited. In the case where both command sets contain data for the same node/argument, both will be shown in the combined command set. |
| Command set | Configuration | The imported command set is applied to the configuration. If any parameterized values are included in the command set, they must also include a default value in order to be imported. This would be the way to apply a default configuration (stored as a command set) to a resource. |
| Configuration | Configuration | The two configurations are merged together. Any commands present in only one of the configurations are kept. If a command exists in both configurations but with different values, the values of the configuration you are importing are kept. |
| Configuration | Command set | The configuration information within the command set is entirely replaced with the data from the configuration. There is now no markup (add, modify, or delete symbols) within the command set, so you must provide the mark-up before applying this command set to any configurations. |

**Note:** After opening a configuration, if you make any changes to the configuration, the **Import** option will be disabled.

Use the following procedure to import a configuration or command set into another command set or configuration.

1. With a command set or configuration opened in the Configuration Editor, select **File** > **Import**.

   The Import dialog box displays. This dialog box shows all configurations and command sets of the same Vendor and Type as the configuration or command set you are currently editing. The configurations and command set are arranged by realm, and different icons distinguish command sets from configurations. If a network resource has multiple configurations, all are displayed.
2. Highlight the desired command set or configuration and click Import.

   The import occurs, using the rules described in the previous table.

## Working with configurations

Use the Configuration Editor to edit configurations. Regardless of the VTMOS of a configuration, the usage of the catalog is the same.

The following list identifies some of the configuration related tasks that you can perform using the Configuration Editor:

- Adding an element on an unbounded command
- Viewing specific configuration data

- Using CLI text boxes for configurations
- Viewing native commands
- Calculating native command changes
- Editing managed resources
- Managing roll ups

### Working with command sets

Use the Configuration Editor to edit command sets. Regardless of the VTMOS of a command set, the usage of the Configuration Editor is the same.

**Note:** Subsequent topics describe how to navigate the Command Set/Configuration Editor and add mark up tags indicating the desired changes. The supported functionality varies depending on VTMOS, and even within a single VTMOS not all functionality is supported for every element or argument.

Unlike configurations in which you simply make changes to a given command, when working with command sets you must use markup to specify what you want to happen when the command set is applied. If you want to add a command, you must mark it to be added; if you want to delete a command, you must mark it to be deleted. A command set containing data but no markup will have no effect on a network resource when applied.

The following list identifies some of the command set related tasks that you can perform using the Configuration Editor:

- Marking commands to be added, modified, or deleted
- Using wild cards
- Using parameters
- Applying command sets with parameters
- Specifying sibling values as dependencies
- Specifying order on list commands
- Switching between match and replace values
- Using CLI text boxes for command sets
- Managing access control lists

**Related tasks**

Editing modeled command sets
After you have created or copied a command set, you use the Command Set Editor to add commands and logic to each command set.

Deleting resources
Use this procedure to delete the following categories of resources: network, general, realm, and search set.

Synchronizing configurations (via wizard)
When the running and the stored (or candidate) configurations on a device are out of synch, you identify the correct configuration and use it to replace the incorrect one so that the two are synchronized. To do so you submit a synchronization request as you would any other unit of work (UOW). You access the Synchronization wizard from either the Activity Viewer or from the Network View in Network Manager IP Edition.

Applying configurations (via wizard)
You apply a configuration to a device using the Submit Configuration wizard, which you access from the Activity Viewer.

## Configuration catalogs

Within the Configuration Editor, configuration information for both full configurations and command sets are displayed using configuration catalogs. Configuration catalogs are graphical folder trees similar to a

typical Windows list of folders and files, except some of the folders also contain data. They represent resource configurations.

## Purpose

When you click any element/object name from the configuration catalog, the right pane of the application page shows that command and allows you to make edits. Regardless of the vendor/type/model/operating system (VTMOS) of a network resource, the usage for the configuration catalog is the same.

## Catalog elements

Every label (file or folder) used in a configuration catalog is an actual resource command. Whether a command is shown as a folder or as a label depends on command complexity and whether the command contains sub-commands.

There can be two types of folders within a catalog, along with file labels. Both folders and file labels represent actual commands on the network resource.

**Note:** For consistency, a CISCO 26xx router is used for the examples in the following procedures, but the procedures would be the same for any supported VTMOS.

## Catalog icons

The following table describes the icons used in the configuration catalog to show what changes have been made to the commands of a configuration or command set.

*Table 36. Catalog Icons*

| Icon | Description |
|---|---|
|  | Signifies that this command contains data. |
|  | Signifies that this command has been added. |
|  | Signifies that this command has been deleted or disabled. This icon is displayed only when viewing “Old Values.” |
|  | Signifies that a command (or a child of the command) has been modified. |

## Object groupings

Folders with no icons are called object groupings. Object groupings are used to group variations of the command, and to contain sub-commands.

**Note:** The object groupings in the folder contain no attributes.

## Object creators

Folders with icons are called object creators. Object creators can contain attributes and other folders.

## Nested commands

When a folder is contained within a folder, it represents a nested command, or sub-command.

In this example, the interfaces command has an unbounded sub-command called interface.

## CLI text boxes

The label “CLI text box” in the folder tree indicates that a command (for example, Ethernet/FastEthernet) has non-modeled sub-commands.

While the system does not provide the normal user interface widgets (check boxes, lists, and so forth) for these non-modeled sub-commands, the CLI text box option allows you to still use the sub-command by entering the appropriate native command language syntax. For more information, see “Using CLI text boxes for configurations” on page 121.

## Right pane elements

Within the Configuration Editor, the configuration catalog occupies the left pane. When you click a folder or text label representing a command, the right pane is populated with an editable form, which varies depending on the selected command.

## Collapse and expand

To save space in the right pane, all commands include **Collapse All** and **Expand All** options. By default, all commands are displayed collapsed.

Click the **Expand All** icon or the **Collapse All** icon to toggle between expanded and collapsed.

## Bounded versus unbounded commands

Commands to which you can add siblings are said to be unbounded. Commands to which you cannot add siblings are considered to be bounded. As an example, on a CISCO 26xx router, the hostname command is bounded while the interface/FastEthernet command is unbounded. All unbounded elements include an **Add** button in the right pane. For information on how to add elements on an unbounded command, see “Adding commands” on page 122.

## Required fields

Red asterisks are used to indicate required fields. You will not be able to save a command set or configuration without providing data for any required fields within the command you are editing.

## Data validation

Many fields show the required format of data (for example, a field label might indicate that 0-15 are the valid values). If you enter a value that is not valid for a field, the field turns red when you try to exit that field.

## Tool bar functions

This section describes the usage of the various tool bar icons found at the top of the Configuration Editor. Although the Configuration Editor is used to edit both configurations and command sets, the available icons vary depending on which is being edited.

The following list describes the use of the Configuration Editor tool bar:

- Pages back through the commands that you have opened and viewed.
- Saves command set or configuration. Use **File** > **Save As** if you wish to save the command set or configuration with a new name.
- Views native commands.
- Expands all roll-ups for the current command.
- Collapses all roll-ups for the current command.
- Moves a roll-up up the list.
- Moves a roll-up down the list.

- Duplicates a roll-up.
- Deletes a roll-up.
- Marks the command as disabled. Use this icon to enable/disable such commands as cdp/enable or interface/shutdown.
- Toggles all fields between old values (baseline) and new values (changes).
- For command sets, marks the current command as being added.
- For command sets, marks the current command as being deleted or disabled.
- For command sets, marks the current command as being modified.
- For command sets, indicates that the value of the current command must be found in a configuration in order for your other modifications on the command's siblings to happen.
- When modifying a command within a command set, allows you to signify that you want the command to be changed regardless of the old (match) value. The wildcard is a full wildcard; it will match the command as long as there is any value (not null).
- For command sets, marks the current command as being a parameter. This means that the user applying the command set can determine its value at that time. You can also supply a default value for a parameterized field.
- When modifying a text field in a command set, allows you to switch between the value to match and the new (replaced) value that should be applied.

## Adding an element on an unbounded command

Use the Configuration Editor to add an element on an unbounded command.

To add an element on an unbounded command, follow these steps.

1. Click an unbounded element (represented by an object creator) in the configuration catalog.

   The right pane shows the editable parameters of the command, including an Add button.
2. Click the Add button.

   The right pane expands to show the new element field.
3. Enter the values for the new element and then press <F5> to refresh the configuration catalog.

The added element displays in the configuration catalog.

## Viewing specific configuration data

Configurations can become quite large, and so it is often helpful to view only the parts of the configuration that have data, or even just the parts that you have changed (edited).

When the Configuration Editor first displays a configuration, the “Show Entire Tree” option is selected. Even when viewing the entire tree, you can easily see which commands contain data. Any command with a “paper” icon next to it contains data. Using the Configuration Editor, you can selectively view specific configuration data.

Use this procedure to view specific configuration data.

1. Select the “Show Only Data” option from the drop down list on the menu bar to limit your view to the parts of the configuration that contain data.

   a) Click on any command to see the data (value) for that command.
2. Select the “Show Only Changes” option from the drop down list to view the changes that have been made to the draft in relation to the configuration on which it was based (changes that you have made in the current editing session, plus any other changes made to the draft in previous editing sessions).
3. Select the "Show Mandatory" option from the drop down list view to filter the tree, and show only nodes marked with the **Mandatory** icon. If you have mandatory nodes in any part of the configuration which are incomplete, a dialog appears when saving to indicate that this is mandatory and must be completed.

4. As you are editing a configuration, if you want to see what the old value for a changed field was, simply click the binocular icon to toggle back and forth between the old (baseline) and new (changed) values.

   **Note:** The bottom of the screen always identifies which value you are viewing.

## Using CLI text boxes for configurations

The label “CLI text box” in the folder tree indicates that a command has non-modeled sub-commands.

While the system does not provide the normal user interface “widgets” (check boxes, lists, and so forth.) for these non-modeled sub-commands, the CLI text box option allows you to still use the subcommand by entering the appropriate native command language syntax.

**Note:** CLI text boxes allow you to enter and edit commands that are not modelled. CLI text boxes are included throughout the configuration catalog. Be sure to use a text box in the proper location/level of the catalog for the command you want to edit.

Use the following procedure to add commands using CLI text boxes.

1. Click a CLI text box label in the configuration catalog.

   The right pane shows information about the command, and an Add button.
2. Click the Add icon (plus sign).

   The right pane expands to show a text entry field.
3. Enter a valid native command language entry.

   For any free text fields, such as banners, descriptions, login prompts, or password prompts, you must use delimiting characters where appropriate. Consult the help for the IOS you are using for specific rules.
4. Click Add again to create a new text box for a new line of code. Each line of code (command) must be entered in a separate text entry box.
5. To view all commands for a configuration that includes information added via CLI text boxes, use the View Native Commands function.

After a configuration change containing values entered using CLI text boxes is successfully pushed out to the network resource, the changes are applied to the running configuration just like any other configuration changes.

The next time the new configuration is edited, the values will be displayed in the same CLI text boxes (same hierarchical level) as they were originally added, unless you added a modelled command to the CLI text box. In this case, the data you added will be displayed with the modelled command.

To view all commands for a configuration that includes information added via CLI text boxes, use the View Native Commands function.

For instructions on how to view native commands, see “Viewing native commands in the Configuration Editor” on page 121.

## Viewing native commands in the Configuration Editor

Use the Configuration Editor to view native commands for a specific configuration.

Use this procedure to view the native commands for a configuration that is loaded into the Configuration Editor.

Select **Tools** > **View Native Commands**.

A new window displays that contains the native commands for this configuration.

## Calculating native command changes

Use the Configuration Editor to view the actual commands that will be sent to the network resource.

Use this procedure to view the actual commands that will be sent to the network resource.

Select **Tools** > **Calculate Native Command Changes**.

## Editing managed resources

Use the Configuration Editor to edit managed resources.

When viewing the network resources in the database, you cannot tell the difference between a managed and modeled resource. However, after opening a configuration for a managed resource to edit, you will see that the entire configuration is shown as CLI commands in one large CLI text box.

Use this procedure to make a configuration change to a managed resource.

1. In the CLI text box editing area (right pane), clear out the existing configuration information.
2. Enter the CLI commands you want to send to the network resource. Enter the commands just as if you were connected directly to the device in a Telnet session.
3. Select **File** > **Save** when done editing.
4. Submit the new draft configuration.

For information on submitting a new draft configuration, see "Viewing native commands in the Configuration Editor" on page 121.

## Managing rollups

Use the Configuration Editor to manage rollups.

Using the Configuration Editor, you can collapse all rollups, expand all rollups, move rollups, and duplicate rollups. By default, all commands display as collapsed.

Use this procedure to collapse all rollups, expand all rollups, move rollups, and duplicate rollups.

1. Use the Configuration Editor to toggle between expanded and collapsed commands by clicking the Expand All icon or the Collapse All icon.
2. Use the Configuration Editor to arrange unbounded list items, for example access control list entries. To do this:
   a) Highlight an access control list command.
   b) Then click either the Move Down button or the Move Up button to arrange the items as needed.
3. Use the Configuration Editor to speed up the process of adding new roll-ups by duplicating an existing roll-up. Often, an existing roll-up already has some of the values you need to add to your new rollup. To create a new roll-up, follow this step:
   a) Highlight the roll-up you want to copy and click the Duplicate icon.

      The Configuration Editor adds the new roll-up to the bottom of the list of roll-ups.

## Deleting commands and rollups

Use the Configuration Editor to delete commands and rollups.

Use this procedure to delete commands and rollups.

Highlight the desired roll-up and click the<Delete> key or click the Trash icon.

## Adding commands

Use the Configuration Editor to add commands.

Use this procedure to add commands.

1. From the Configuration Editor, select a command that you want to add.

   The command is displayed in the right pane of the Configuration Editor.
2. Click the Plus icon next to Add.

   The Configuration Editor expands the command.

3. Click the Plus icon (the one next to the “exec” with the gray background).

   The Configuration Editor displays the data fields for the command.
4. Complete all the necessary fields for the new command.

After adding the command, a Plus sign icon is added to the command in the configuration catalog.

## Marking a command as disabled

Use the Configuration Editor to mark a command as disabled within a configuration.

Use this procedure to mark a command as disabled within a configuration.

1. From the Configuration Editor, select a command that you want to mark as disabled.
2. Click the Disabled icon.

   The Configuration Editor adds a Disabled icon next to the command.
3. To ensure the correct command is going to be sent to the resource, select **Tools** > **View Native Commands**.

## Working in list view

Use the settings in Configuration Editor to list commands in what is called "list view".

In normal view, each list command is shown and you can expand any or all of the commands. You can change the Configuration Editor settings to see a specific number of lines without scrolling, as in the following example:

```
Lines to trigger list: 20
Lines shown in list: 10
```

These settings allow you to see only 10 lines without scrolling (the value specified in the `Lines shown in list:`) because there are more than 20 items in the list (the value in `Lines to trigger list:`).

Use this procedure to view and work with a command that is shown in list view.

1. Double-click the Details icon.

   The Configuration Editor expands the command.
2. To go back to the list view of the entire list command, click the back icon on the tool bar.

## Command sets usage tips

Use this information to learn about general usage tips for creating command sets.

### Match/replace: determining siblings

When using the match/replace feature within command sets, it is important to know which commands are at the same level (siblings), because match/replace works only on such commands. For example, you cannot create a command set that matches on a particular host-name, and if found, adds an SNMP Server contact; those commands are not siblings. You can, however, match on “permit 2.2.2.2” within an access-list, and if found, add “log.”

The edit pane of the Configuration Editor provides visual clues to help you determine which commands are siblings. Much like Windows Explorer, dashed lines are used to show each command's relative position in the hierarchy.

For example, consider a situation where there are numerous siblings directly beneath a “tcp” command. You could set up a match/replace operation using any pair of these siblings that are connected by the dashed line.

On some complex commands, such as interfaces, the command is split into several pages for easier editing. This does make it harder, however, to figure out what commands are at the same level (siblings).

### Errors

The most common error you will see when attempting to set up a match/replace condition in a command set is “a match must have a replace action at same level.” For best results, and to cut down on such validation errors when editing, you should mark your “match” conditions after marking the corresponding “replace.”

### Bounded versus unbounded commands

Commands on network resources can be either bounded (only 1 such command allowed) or unbounded (more than 1 allowed). Banner/motd is an example of a bounded command, while an access-list deny statement is unbounded. This difference is key when considering the effects of a command set that attempts to add a comma.

If the command you are trying to add is bounded, it will be added only if the command does not already exist. For example, if a resource contains “banner/motd/old” and you add “banner/motd/new,” no change will be made to the router. If a bounded command already exists, and you want to change its value, you must modify the command.

If you are adding an unbounded command, the presence of the command alone does not prevent a new one from being added, unless the value you are trying to add already exists (a resource can have multiple “access-list” commands, for example, but only 1 “access-list 1.”

### Testing command sets

After creating a command set (but before applying it to an actual network resource), there are a few ways you can test the command set to be sure it is marked up correctly and will achieve the desired results.

First, visually inspect the markup of each command in the editing window (the right part of the Configuration Editor) and verify that all commands/values have an icon indicating markup.

An unmarked command is ambiguous. Unmarked commands require additional markup to specify the command set operation.

### Importing

Before applying a command set, you can use the Configuration Editor to see exactly what the effect of the command set will be on a given configuration by importing the command set into a configuration.

The VT (Vendor and Type) of the command set being imported must match the VT of the test configuration.

## Marking commands to be added, modified, or deleted

Use the Configuration Editor to mark commands to be added, modified, or deleted.

Unlike configurations in which you simply make changes to a given command, when working with command sets you must use markup to specify what you want to happen when the command set is applied. If you want to add a command, you must mark it to be added; if you want to delete a command, you must mark it to be deleted. A command set containing data but no markup will have no effect on a network resource when applied.

In order to modify a command value using a command set, you need to identify the old value for the command (or a wildcard to indicate that you do not care what the old value was) and the new value for the command (or a parameter indicating you want to be able to decide the new value at apply time).

**Note:** The user interface does not support match/replace modifications for elements (usually shown as pick lists). You can, however, mark up the command set manually to do so, or you can perform a delete/add combination instead of a match/replace modification.

When modifying a command, the system will only modify the command if the command already exists. If you want the command to be added if it does not already exist, you must add the command rather than modify it. This may mean you need to create two different command sets in order to end up with the

desired results (one command set that modifies the command if present and another command set that adds the command if not present).

You can use a command set to delete a specific command that has a specific value as its current (Match) value. You can also specify a wildcard as the Match value if you wish to delete the command regardless of the current value.

To mark a command to be added, modified, or deleted, follow these steps.

1. Click the command in the configuration catalog.

   The command displays in the right pane.
2. To mark the command to be added:
   a) Click the command check box in the right pane.

      Depending on the command, a text box, drop down menu, or some other widget is displayed.
   b) After checking that the bottom of the Configuration Editor says “Replace,” type or select the value or text that you want to be applied to the command. This will be the new value of the added command.
   c) Click the Add icon to mark this command as being added.

      An Add icon is added next to the command.

      When applied, this command set will add the marked command if that command does not already exist.

      If the command you are trying to add is bounded and already exists in a configuration, the “add” does not change the existing value to the new value.
3. To mark the command to be modified:
   a) Click the command check box in the right pane.

      Depending on the command, a text box, drop down menu, or some other widget is displayed.
   b) After checking that the bottom of the Configuration Editor says “Replace,” type or select the value or text that you want to be applied to the command. This will be the new value.
   c) Click the Modify icon to mark this command as being modified.

      A Modify icon is added next to the command.
   d) Click the Match/Replace icon to switch to old values (the value you want to match).

      The bottom of the Configuration Editor should now say “Match.”
   e) Type or select the value that you want to match on for this command. If you select or type a specific value, remember that the command will only be modified to the new value if that old value exists. If you want the command value to be changed to your new value regardless of the existing value, click the Wildcard icon.

      For more information, see “Using wildcards” on page 126.

      When applied, this command set will modify the marked command if that command exists.
4. To mark the command to be deleted:
   a) Click the command check box in the right pane.

      Depending on the command, a text box, drop-down menu, or some other widget is displayed.

      After checking that the bottom of the Configuration Editor says “Match,” enter an existing value for the command; this value must exist for the command in order for the command set to delete the command.

      Alternatively, you can insert the Wildcard icon to mark the field as a wildcard.
   b) Switch to “Replace” view and click the Delete icon to mark this command as being deleted.

      A Delete icon is added next to the command.

When applied, this command set will delete the marked command if that command exists and has the specified value.

## Using wildcards

Use wildcards in the Configuration Editor when you want to modify an existing command regardless of its value.

Wildcards are useful when you want to modify an existing command regardless of its value (full wildcard), or modify a command that matches a partial wildcard value. When matching on a command, you can either modify that same command or any other command within the configuration.

**Note:** When using a full wildcard, the command will be matched as long as there is any value (not null).

To use wildcards, follow these steps.

1. Click the command in the configuration catalog.

   The command displays in the right pane.
2. Click the command check box in the right pane.
3. Place your cursor in the field you are trying to change.
4. Click the Match/Replace icon to switch to old values (the value you want to match) if necessary.

   Be sure the bottom of your screen says “Match.”
5. Click the Wildcard icon to mark the field as a wildcard.

   The text field will now show an asterisk. If you want to match on a full wild card (any value for the field), simply leave the asterisk as is and continue with the next step.

   If you want to use a regular expression to represent a partial wildcard, place your cursor in the text field, delete the asterisk, and type a regular expression.

   For more information, see “Glob regular expressions” on page 126.
6. Click the Match/Replace icon to switch back to the Replace mode (new values) and then enter the new value for the field.

When this command set is applied, the field will be changed if the current value matches the wildcard expression you entered.

### Glob regular expressions

Use Glob regular expressions in the Configuration Editor to define a partial match.

#### Purpose

When defining a partial match (not a full match which is denoted by a single asterisk and nothing more) in the Configuration Editor, you must use Glob regular expressions.

#### Glob Expressions

**?**
Matches any one character. For example:

“1?3” would match “123” and “133,” but not “12.”

*****
Matches as many characters as possible, but can match 0. For example:

“12*” would match “12” and “123,” but not “1.”

**12.*.5.??**
Combines the ? (match one character) and * (match as many characters as possible) expressions. For example:

"12.*.5.??" would match "12.3.5.67" and "12.33.5.67" but not "12.3.5.6."

**[XYZ]**
Matches any of the characters between the brackets. For example:

"[123]" would match "1" and "3," but not "123."

**[XYZ][ABC]**
Matches any of the characters between each pair of brackets, but nothing more. For example:

"[123][789]" would match "17" and "38," but not "171" or "12."

**[XYZ][ABC]**
Matches any of the characters between each pair of brackets, but nothing more. For example:

"[123][789]" would match "17" and "38," but not "171" or "12."

**[XYZ]***
Matches any of the characters between the brackets, plus any other additional characters. For example:

"[123]*" would match "1" and "1999."

**[!XYZ]**
Matches any character but ones between the brackets. For example:

"[!123]" would match "4," and "8," but not "3."

A dash (-) indicates a range, unless it is the first or last character. For example:

"[1-3]" would match "2," but not "4."

## Using parameters

Use the Configuration Editor to specify parameters.

Parameters allow you to reuse a command set because each time the command set is applied, you can specify what you want the value of a parameterized value to be. Parameters can be used for both the value you are trying to match and the value you are using to replace.

The user applying the command set is prompted to provide values for any parameterized fields.

**Note:** Parameters can be applied only to text fields and editable combo boxes. You can also enter a default value for any parameterized field.

To specify parameters, follow these steps.

1. Starting in "Replace" mode, click the command in the configuration catalog.

   The command is shown in the right pane.
2. Click the command check box in the right pane.
3. Place your cursor in the field you are trying to add, delete, or change.
4. Enter a default value if desired (optional), then click the Parameter icon to mark the command as being a parameter.

   The Parameter Name dialog box displays.
5. Type a name for this parameter. A name is particularly useful if you will be using the command set from the API.

   The parameter icon is added to the command in the configuration catalog on the left side of the Configuration Editor.
6. If you are modifying a text field, and you wish to use a parameter for the value being matched, click the Match/Replace icon to switch to old values (the value you want to match).
7. Enter a default value if desired (optional), then click the Parameter icon to mark the command as being a parameter.

When this command set is applied, the user will be prompted to provide a value for the parameterized field or fields.

## Applying command sets with parameters

Use the Configuration Editor to apply a command set with parameters.

When you apply a command set containing parameters, the Configuration Editor opens the command with the view restricted to “Show Parameters Only.”

To apply a command set with parameters, follow these steps.

1. Supply a specific value for the parameterized fields, or simply accept the default value (if one exists).
2. Select **File Submit**.

   The Task Scheduling dialog box displays.
3. Select either immediate or scheduled execution and type a description for the work. If you select scheduled execution, additional fields are displayed asking for the execution window. Provide the start date and time, and the end date and time for executing the work.
4. Click Submit.

The Configuration Editor creates a UOW that will run as scheduled, as long as it is approved by the required number of approvers.

**Related tasks**

Applying native command sets (via wizard)
Native command sets are defined by your administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying native command sets** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager.

Applying modeled command sets (via wizard)
Modeled command sets are defined by an administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying modeled command sets** wizard. You access the wizard from either the Activity Viewer or from the Network View, Hop View and Path View in Network Manager.

## Specifying sibling values as dependencies

Use the Configuration Editor to specify sibling values as dependencies.

You can use the equals icon to indicate that the value of the current command must be found in a configuration in order for your other modifications on the command's siblings to happen.

**Note:** It is best to mark the “replace” action prior to marking the “match” condition.

To specify sibling values as dependencies, follow these steps.

1. Select and open the command for which you want to specify sibling values as dependencies.
2. While in Replace view (switch if necessary by using the Match/Replace icon), mark the commands that you want to be added, modified, or deleted.
3. Switch to Match view and select the command that must exist and click the equals icon.

   The equals symbol is displayed next to the command, and if applicable, next to the argument field as well.
4. If the command has an argument field, enter the desired value.

When the Configuration Editor applies the command set, the changes you marked in Replace view will happen only if the value you specified as a match is found in the baseline configuration.

## Specifying order on list commands

Use the Configuration Editor to specify order on list commands.

On list commands, you can use the equals icon to specify the location at which you want a new command added.

**Note:** If you choose not to use the match icon, any newly added list commands are appended to the end of the command.

To specify order on list commands, follow these steps.

1. Select and open the command you wish to edit.
2. While in Match view, select the command that must exist and click the equals icon.
3. Switch to Replace view (by using the Match/Replace icon.
4. Add the command you want to be inserted, and using the up and down arrows if necessary, move the newly added commands to the proper place in relation to the matched command.

Consider the following command set specified in the Configuration Editor:

```
match:permit host 2.2.2.2
add: permit host 1.1.1.1 before 2.2.2.2
add:permit host 3.3.3.3 after 2.2.2.2
add:permit host 4.4.4.4 after 3.3.3.3
```

If this command set is applied to the following base-line configuration:

```
permit host 0.0.1.1
permit host 2.2.2.2 <---- changes will occur due to this match
permit host 5.5.5.5
deny ip any any log
```

The configuration will look as follows after the command set is applied:

```
permit host 0.0.1.1
permit host 1.1.1.1
permit host 2.2.2.2
permit host 3.3.3.3
permit host 4.4.4.4
permit host 5.5.5.5
deny ip any any log
```

## Switching between "match" and "replace" values

Use the Configuration Editor to specify between "match" and "replace" values.

When modifying the value of a text command using a command set, the Match/Replace icon allows you to switch between the value to match and the new (replaced) value that should be applied.

To specify between "match" and "replace" values, follow these steps.

1. Start in “Replace” mode.
2. Click the command in the configuration catalog.

   The command is shown in the right pane.
3. Click the command check box in the right pane.
4. Place your cursor in the field you are trying to modify.
5. Mark the command as being modified.
6. Enter the value to which you want the command changed.
7. Click the Match/Replace icon to switch to old values (the value you want to match).

   Be sure the bottom of your screen says “Match.”
8. Enter the value you want to match in the existing configuration.

9. Before finishing with the command, toggle back and forth to be sure you have correctly entered the old and new values.

## Using CLI text boxes for command sets

Use the Configuration Editor to specify command sets in the "CLI text box".

The label “CLI text box” in the folder tree allows you to enter commands that are not modeled into your command sets for application to network resources. Simply enter the appropriate native command language syntax into the CLI text box, and then mark the command as being added, deleted, or modified.

**Note:** CLI text boxes allow you to enter and edit commands that are not modelled. CLI text boxes are included throughout the configuration catalog. Be sure to use a text box in the proper location/level of the catalog for the command you want to edit.

To specify command sets in the "CLI text box", follow these steps.

1. Click a CLI text box label in the configuration catalog.
2. Click the Add icon (plus sign).

   The right pane expands to show a text entry field.
3. Enter a valid native command language entry.

   For any free text fields, such as banners, descriptions, login prompts, or password prompts, you must use delimiting characters where appropriate. Consult the help for the IOS you are using for specific rules.
4. Click Add again to create a new text box for a new line of code. Each line of code (command) must be entered in a separate text entry box.

After a command set containing values entered using CLI text boxes is successfully applied to a network resource, the changes are applied to the running configuration just like any other configuration change.

The next time that configuration is edited, the values will be displayed in the same CLI text boxes (same hierarchical level) as they were originally added within the command set, unless you added a modelled command to the CLI text box. In this case, the data you added will be displayed with the modeled command.

## Managing access control lists

Use the Configuration Editor to manage access control lists (ACLs).

Because ACLs can be long and confusing, this procedure addresses how to use command sets to make the following typical ACL-related changes.

- Add a new ACL to a command set
- Add a new deny statement to an existing ACL
- Delete an ACL
- Use match and replace on an ACL

When adding list commands (such as ACL permit statements), any newly added command is automatically appended to the end of the current list unless you specify otherwise. Use the equals icon to specify the location at which you want a new command added.

The following procedure shows how to match `access-list 1 permit host 2.2.2.2` and then add one new permit statement before and two more new permit statements after.

1. Switch to Match mode (if necessary) and select the type of access-list you are modifying from the drop down lists.
2. Enter the number of the existing access-list, and then use the Equals icon to indicate you are matching on 1.
3. Add a `permit host 2.2.2.2` to the ACL.

4. While in Match view, select the command that must exist (`permit host 2.2.2.2`) and click the equals icon.

   The Configuration Editor should now show the Plus (match) icon next to the number of the ACL (1) as well as the permit statement.
5. Switch to Replace view and add the new permit statements you wish to be inserted.
6. Mark each of the new permits as Adds.
7. Using the up and down arrows if necessary, move the newly added commands to the proper place in relation to the matched command.

   The Modify icon at the top level (ACL) indicates that an existing ACL is being modified. The Equals icons show what must exist for the change to take place (as well as the relative position of the new permit statements). And the Plus icons show what will be added.

Use this procedure to manage ACLs.

1. Regardless of whether you are adding, modifying, or deleting an ACL, you must start by adding one to your command set.
   a) Click access-list in the configuration catalog.

      The Add access-list prompt is shown.
   b) Click the Plus icon to add.

      A blank access-list is added.
   c) Click the top-most Plus icon to expand the blank access-list.

      A drop-down list is displayed.
2. To add a new ACL:
   a) After switching to Replace mode (if necessary), select the type of access-list you are adding from the drop down lists.
   b) Enter the number of the new access-list.
   c) Click the Plus icon next to either deny, permit, or remark.
   d) Expand the new statement and complete, at minimum, the required fields. For example, if you specified deny, then expand the deny statement and complete the required fields.
   e) Select the outer most access-list box by clicking the “access-list 1 deny” title (in this example where the deny statement was chosen).

      The title bar should turn blue.
   f) Click the Add icon to mark this new access-list as being added.

      Add icons are added at each level of the ACL, signifying that the entire ACL is an add. A Plus icon is displayed next to each command, indicating that a new ACL is being added.

      When applied, this command set will add the following ACL to each resource (as long as there is not already an access-list 1):

      ```
      access-list 1 deny 1.1.1.1
      ```
3. To add to an existing ACL, follow these steps. The example shows how to add a new deny statement to an existing ACL.
   a) After switching to Match mode (if necessary), select the type of access-list to which you are adding from the drop down lists.
   b) Enter the number of the existing access-list, and then use the Equals icon to mark it as match.
   c) Switch to Replace mode and click the Plus icon next to deny.
   d) Expand the new deny statement and complete, at minimum, the required fields.
   e) Select the “deny” box by clicking the “deny” title.

      The title bar should turn blue.

f) Click the Add icon to mark this new deny statement as being added to the ACL.

Add icons are shown at the deny level, while modify icons are shown higher up at the ACL level, signifying that the ACL is being modified by adding a new deny statement.

When applied, this command set will add “deny 1.1.1.1” to “access-list 1” on each resource that has one. If a resource does not contain an “access-list 1,” no changes will be made.

4. To delete a specific ACL, follow these steps.

**Note:** You could also specify a wildcard as the Match value if you wanted to delete all current ACLs.

a) After switching to Match mode (if necessary), select the type of access-list you are deleting from the drop down lists.

b) Enter the number of the access-list.

This value must exist for the ACL in order for the command set to delete the ACL.

c) Switch to “Replace” view, select the access-list title, and click the Delete icon to mark this command as being deleted.

A Delete icon is added next to the top-level ACL command, as well as the ACL number (1) indicating that the entire ACL will be deleted.

When applied, this command set will search for an access-list 1 and delete the entire ACL, regardless of what deny and permit statements it may have.

-OR-

While still in Match mode, enter a specific deny or permit value to further narrow the match criteria. Switch to “Replace” view, select the access-list title, and click the Delete icon to mark this command as being deleted.

A Delete icon is added next to the command.

When applied, this command set will search for an access-list 1 with the specific permit or deny value you entered, and delete the entire ACL if found.

5. To use match and replace on a specific ACL, follow these steps.

**Note:** In general, you can perform a match/replace as long as both commands are siblings, or at the same level. The command set in the following procedure is designed to add a log statement if an “access-list deny 1.1.1.1” command is found.

a) Switch to Replace mode (if necessary), and begin entering the values for the commands you will be changing.

b) Enter the number of the existing access-list (1 in this example).

c) Click to add a deny statement, and enter the address.

d) Select the type of access-list you are modifying from the drop down lists.

e) Select Log, and mark it as being added.

f) Switch to Match mode.

g) Select the access-list 1 and use the Equals icon to indicate you are matching on 1.

h) Select the deny statement and use the Equals icon to mark the address as a match.

The Modify icon at the top level (ACL) indicates that an existing ACL is being modified. The Equals icons show what must exist for

## Managing extractions

Extractions are Netcool Configuration Manager resources that you can create much like configurations or command sets. They are defined on a specific VTMOS, and, once created, are visible in the Resource Browser. Instead of defining only specific values, extractions can be parameterized so that some values can be modified at run time. You can also export and import extractions.

An extraction is the retrieval of information from a specific device configuration. Once retrieved, this information can then be reused. Typically, an advanced user such as an administrator would define an extraction, which is then used by other users, such as operators. Extractions can be imported and exported.

**Important:** Extractions consult the current configuration for a device as stored in Netcool Configuration Manager, not the device itself, so it is important that the two are kept in sync.

Extractions can only be deployed against devices with modeled configurations, and not against devices using standard drivers. They are applied as a unit of work (UOW), and therefore can be scheduled and approved. The result of an extraction is recorded in the UOW log.

You have two options when extracting information from a device configuration:

**Branch**
The entire branch can be extracted from a devices configuration in the command tree, for example, an ethernet port and all its attributes.

**Parameter**
A single value can be extracted from a devices configuration in the command tree, for example, the name of an ethernet port.

Additionally, you can use a match ('=') to narrow the selection, for example, the speed of the first ethernet port on the device. To offer flexibility at runtime, the match operation can be controlled by a parameter, set by the user when the extraction is applied.

**Related tasks**
Configurations and command sets in the Configuration Editor
Use this information about the Configuration Editor to view and edit configurations and command sets.

## Creating extractions

You create extractions in the Netcool Configuration Manager Resource Browser. Once created, you edit them in the Extraction Editor.

1. In the Netcool Configuration Manager - Base UI, navigate to the realm in the Resource Browser where you want to create an extraction.
2. Select **File** > **New** > **Extraction**.
   The **New Extraction** window is displayed.
3. Specify the extraction VTMOS (vendor, type, model and operating system).

   **Note:** When creating an extraction, the list of VTMOS labels from which you can select has been filtered to only display the labels for Smart Model drivers. Standard driver VTMOS are excluded.
4. Select **OK** to create the extraction.

This action creates the extraction in the Resource Browser under the current realm.

Next, you edit the extraction in the Extraction Editor.

## Editing extractions

After you have created an extraction, you edit it using the Extraction Editor.

Before you edit an extraction, you must create it.

In the Extraction Editor, configuration information is displayed in configuration catalogs in the left pane. Configuration catalogs are graphical folder trees that are similar in appearance to a typical list of folders and files, except some of the folders also contain data. You can filter them to display all entities, or an edited list.

Every label (file or folder) displayed in a configuration catalog represents a managed entity within a device configuration. Whether an entity is shown as a folder or as a label depends on its complexity, and whether it contains other sub-entities. When you click a folder or text label, the right pane is populated with an editable form, which varies depending on the selected entity.

Regardless of the VTMOS of a network resource, the usage for the configuration catalog is the same.

1. Navigate to the appropriate realm in the Resource Browser.
2. Highlight the extraction you want to edit, and select **Edit** > **Edit** from the menu bar.
   Alternatively, you can highlight the extraction, then select **Edit** from the context menu.

   The extraction is opened in the Extraction Editor, which you use much like the command set or configuration editors.
3. Edit the extraction using the following information as guidance:
   a) Click a managed entity in the entity tree to import it into the right pane.
   b) Select the entity and click **Extraction** on the toolbar to mark it as an extraction.
   c) Define the extraction details:
      - Select whether the extraction is to use the branch or parameter extraction method.
      - To mark the selected extraction as a match, click **=** on the toolbar.
      - To add a parameter field to the extraction, click **P** on the toolbar.
        Define a default value for the parameter. When the extraction is applied, users can change this value as required.
   d) Select **File** > **Save** when done.

The extraction can now be applied from within the Resource Browser. If you have defined a parameter, users can change the parameter value before applying the extraction.

**Related tasks**

Configurations and command sets in the Configuration Editor
Use this information about the Configuration Editor to view and edit configurations and command sets.

## Applying extractions

When applying an extraction, a UOW is created and submitted. You apply extractions from within the Resource Browser.

1. Navigate to the Resource Browser realm, and highlight the extraction required from the list of network resources.
2. From the menu bar, select **Tools** > **Apply** > **Extraction**.
3. When the **Select Extraction** window is displayed, choose the extractions required using the **Add>** or **<Remove** buttons. Use the **Move Up** and **Move Down** icons for prioritizing the order in which the extractions are applied.
4. Click **Next** to display the **Scope of Application** dialog.
5. Select one of the following options, then click **Next**.
   - **Apply the Extraction to Network Resources in a Realm**
   - **Apply the Extraction to specific Network Resources**
   - **Apply the Extraction to the Network Resources retrieved from a Realm**
6. To filter UOWs by name or VTMOS filter, define the realm name or VTMOS filter details as determined by the choice made in the previous step, then click **Next** to proceed.

   The **Enter Parameters** window is displayed.
7. Select one of the following options, then select **Next** to proceed:

   **Manual**
   Used where the same parameter name is used in multiple extractions, but each different value can be defined depending on the extraction.

   **Local**
   Steps through each extraction.

   You must provide a value for each parameter.
8. Enter the values for the defined parameters, then click **Next**.

The **Execution Priority** window is displayed.

9. Select the priority with which the extraction UOW is to be submitted, then click **Next** .

   The **Schedule Work** window is displayed.

10. Select one of the following options, then click **Next** to display the **Describe Work** window.

    **Immediate**
    Select **Immediate** to submit the UOW immediately.

    **Scheduled**
    Define values for the **Scheduled Start** and **Scheduled End** options.

    **Recurring Schedule**
    Enter a start date and time.

    Define the period for which the recurring schedule applies.

    Define the hourly, daily, weekly, monthly or yearly intervals after the start date during which the extraction should be applied.

11. Enter a description for the UOW, and then click **Next** to view a confirmation screen containing a summary of the extraction about to be applied.
12. Click **Finish**.

The extraction is now submitted as a UOW and will run when scheduled, as long as the proper approvals are granted. The number of approvals required for the UOW depends on the group policy.

## Exporting extractions

You export extractions from the Netcool Configuration Manager Resource Browser, and then save them as a text file.

1. In the Netcool Configuration Manager - Base UI, navigate to the realm in the Resource Browser from where you want to export an extraction.
2. Select one or more extractions in the Resource Browser for export.
3. Select **Tools** > **Export to File** > **Extraction(s)**.

   **Tip:** If you have selected a resource that is not an extraction, the **Extraction(s)** menu item is unavailable.

   A **Save** window is displayed.
4. Specify the location and name for the extraction(s) to be exported, and click **Save**.

This action exports the extraction and creates a txt file containing extraction information, similar to the following example.

```
FileType=Extraction
Name=ExtractionTest
Vendor=Cisco
Type=Router
Model=100*
Os=*12.0*
Detail=<?xml version="1.0" encoding="utf-8"?><configuration
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cmdSetMarkup="http://www.intelliden.com/ns/cmdSetMarkup"
xmlns:deltaxml="http://www.deltaxml.com/ns/well-formed-delta-v1"
xmlns:extr="http://ibm.com/extractionMarkup"
xmlns:deviceMarkup="http://www.intelliden.com/deviceMarkup"></configuration>
```

## Importing extractions

You import extractions from the Netcool Configuration Manager Resource Browser.

1. In the Netcool Configuration Manager - Base UI, navigate to the realm in the Resource Browser to where you want to import an extraction.
2. Select **Tools** > **Import from File** > **Extraction**.

A **Browse** window is displayed.

3. Browse to the location where the extraction to be imported is located.
4. Select the extraction text file, and click **Open**.

This extraction is imported and displayed in the Resource Browser.

# Using queues

The Queue Manager enables you to view and manage your queue of approval tickets and units of work (UOW). Depending on your rights, you can approve or reject work, reschedule work, or cancel work from the Queue Manager.

In order to approve or reject work in the Queue Manager, the approving user must have membership to a group with the "Manage Work" privilege.

## Overview

You use the Queue Manager to manage the queues of approval tickets and Units of Work (UOWs). A UOW is any item of work or task that a user requests.

The Queue Manager processes each UOW with its own priority, type, and approval state. UOWs can be scheduled for immediate or future execution. Depending on the level of access granted to the user, a UOW can approve or reject work, reschedule work, or cancel work from the Queue Manager.

### Security

A user submitting a UOW with a policy set of 0 (zero) does not need to provide approval. The UOW status automatically goes to "Executing" (if it has been scheduled for immediate execution). If the UOW is scheduled, its status changes to "Ready for Execution". A user submitting a UOW with a policy set of 1 or more needs to provide approval, and the UOW goes into the "Work Pending Approval" queue. Some UOWs which appear in the "Work Pending Approval" listing may have been submitted by users who have membership to other groups. A user may only approve/reject those tickets that list your group in the Approval column.

Please note however, if the "Manage Work" privilege is removed from a group which previously had the activity, that groups' users will retain the ability to approve work without having the "Manage Work" permission. This condition is true for all UOWs created during the time that the user previously had this activity. The reason being - once the UOW has been passed on for approval, it will stay in the Work Pending Approval queue to be approved/rejected. However, any subsequent UOWs created after the removal of this activity, can NOT be approved by the user without "Manage Work".

### Display

The Queue Manager environment consists of a number of fields, providing a range of UOW information. The following table details the information available:

*Table 37. UOW information*

| **Information** | **Description** |
|---|---|
| Type | Either UOW, recurring UOW or Approval. |
| UOW ID | When a UOW is submitted, a UOW ID is generated thus providing unique identification. |
| Submitter | This is the login name of the user who submitted the UOW. |
| WINDOW START/WINDOW END | The window start/end is a timestamp indicative of the start/end time of UOW execution. The window start/end represents the period of time for which the UOW is valid. |

| *Table 37. UOW information (continued)* | |
|---|---|
| **Information** | **Description** |
| Request Type | Each UOW has a request type, which indicates the type of action created in the UOW. |

The Request Types are outlined in the following table:

| *Table 38. Request types* | |
|---|---|
| **Request Type** | **Description** |
| Apply Search Sets | Refers to the ability to search network resource configurations for specific command criteria |
| Autodiscovery | Refers to the ability to use the Auto-Discovery feature to discover the VTMOS of a network resource, when only the IP address is known |
| Command Set | Refers to a configuration change executed using a command set |
| Command Set (Report Only) | Refers to a configuration change executed using a command set in report only mode i.e. no changes will be applied to the device |
| CommandSetCollection | Refers to a configuration change executed using a command set group |
| Configuration Change | Refers to a change of configuration |
| Configuration Synchronization (ITNCM to Device) | Refers to the synchronization of a configuration from Netcool Configuration Manager to resource |
| Configuration Synchronization (Device to ITNCM) | Refers to the synchronization of a configuration from resource to Netcool Configuration Manager |
| Configuration Synchronization (Report Only) | Refers to the logging of any differences between the managed and running configurations |
| Extraction | Refers to an extraction of commands performed on a network resource configuration |
| Import Configuration | Refers to a configuration that is being imported via the GUI or the API. This request type is also used for Bulk Imports |
| Native Command Set | Refers to the application of native command sets against a resource |
| OS Upgrade | Refers to the application of an OS image to a network resource |
| Remove Network Resource | Refers to a resource that has been deleted from Netcool Configuration Manager |
| Service | Refers to a service that has been executed via NSM |
| Update Configuration | Refers to updating the operating system of one or more network resources |

**WORK STATE** Each UOW in the Queue Manager has a work state, which describes the status of UOW. Searches may be conducted on the basis of any, or all of these states. The information in the following table describes the UOW Work states available.

| *Table 39. UOW work states* | |
|---|---|
| **Approval State** | **Description** |
| Cancelled | UOW was either dequeued or removed from the queue manager before execution began. |
| Expired | The scheduled execution window for the UOW has expired before it could be approved or rejected. |
| Ready for Execution | UOW has not began executing because a) the worker server has not picked the UOW up, or b) if it is scheduled, the execution time is in the future. |
| Pending Approval | UOW is awaiting approval. |
| Finished | Indicates the request made to the UOW was completed successfully. |
| Executing | UOW is currently executing the request. |

**EXECUTION STATUS** When a UOW executes and reaches completion it is assigned an execution status, which reflects how the UOW reached completion. The information in the following table describes the different Execution states available.

| *Table 40. Execution states* | |
|---|---|
| **Status** | **Description** |
| Success | UOW completed successfully. The UOW can be shown as a success even if some of the individual changes failed. The description will show how many individual work components succeeded, and the total number of components. Successful simply means the UOW ran without errors. |
| Failure | UOW was approved and executed. However, one or more errors occurred. See the Log file for details. |
| Approved | UOW has been approved. |
| Rejected | UOW was rejected, and did not execute. UOW will be in the "Finished" queue. |
| Expired | The scheduled execution window for the UOW has expired before it could be approved or rejected. If a UOW expires while the system is paused, the UOW stays in its current state until the system is resumed, at which time the UOW is moved to the Expired state. |
| Dequeued | UOW was removed from the Queue Manager before it began to execute. A UOW can be dequeued while it is executing. If you cancel a UOW that is executing, it will not process any more tasks within the UOW; however it will finish processing all the tasks it is currently executing. |

**DESCRIPTION** The description field is a short narrative entered by the user to explain the UOW. The description field shows a condensed version of the description. To view the full description properly, click the 'View Description' button in the Tab.

**PRIORITY** Each UOW is assigned a priority which, alongside the scheduled execution time determines when the UOW is processed. If two or more UOWs are scheduled for execution at the same time, the one with the highest priority shall be executed first. By default, all UOWs have a priority of Low when submitted. The priority may be altered at execution time if necessary.

**FAILURE CATEGORIES** When a UOW fails to execute successfully it is assigned failure category, which reflects how the UOW failed to reach completion.

**RESOURCES** This specifies the hostname or IP address of the resource that the UOW was run against. If the UOW was applied against multiple devices, the text "Multiple Devices" will be displayed under this

column. A complete listing of device names is not provided when there is more than one device due to performance. However, a full list of device names and their status can be found by selecting the Resource tab.

**APPROVALS REQUIRED** This indicates the number of approvals a UOW requires in order to commence execution. This is directly linked to Policy Set security, and operates on the basis of 0-3 approvals. When a UOW is approved, the "Approvals required" figure is readjusted accordingly.

### Color Coding

Color coding is employed in the UOW search results and filters to indicate the status of the various UOWs in the Queue Manager.

The following table explains what each color represents.

*Table 41. Color coding in UOW search results*

| Color | Description |
|---|---|
| Green | Successful. Indicates that the UOW successfully ran as scheduled. |
| Red | Failure. Indicates that the UOW was approved, but did not run as scheduled. |
| Black | UOW Executing. Indicates that the UOW was approved and is currently running. |
| Grey | Pending approval. Indicates that the UOW has been submitted for approval. |
| Purple | Indicates that the UOW has been approved and is waiting for its scheduled execution window to run. |
| Yellow | Partial Success. Indicates a mixture of failed and successful resources in the UOW. |

## Searching queues

Use the Queue Manager to search for UOWs or approval tickets using default filters, or by creating your own filters.

To search within the Queue Manager, select **Queue Manager**, or a **Queue Manager** sub-set from the navigation tree. Then select the search icon. Your search options are displayed in the left pane.

You can search by using the following options: Search by state, date, association, failure categories, and attributes.

- **Search by state**: As units of work (UOWs) and approval tickets move through the system, their states change. It is sometimes useful to filter the data shown in the Queue Manager based on one or more of these states.
- **Search by date**: This drop-down enables you to search queue manager for UOWs by explicitly set dates, or relative to current time.
- **Search by association**: Using the **Search by Association** form, the user can choose to view work submitted by them, or work for which they are the approver. Note if the user is a member of a group with the “View All Work” activity assigned to them, they have the ability to view all results for ALL groups - regardless of whether they are a member of the group.
- **Search by failure categories**: You can search by failure category. This can help you search for UOWs based on why they may have failed.
- **Search by attribute**: You can search by the following UOW attributes: priority, type, ID, submitter, and description.
- **Search by recurring sequence:** You can display all UOWs in a recurring sequence.

1. SEARCHING BY STATE (UOW)
   a) Select **Search by State**. The **Search by State** menu expands.
   b) Select **Units of Work**. The **Units of Work** selections display. Select from the following:

| *Table 42. Units of Work elements* | |
|---|---|
| **Element** | **Definition** |
| **Pending Approval** | Shows a list of tickets waiting for approval and for which your group(s) have approval rights. From this list, you can view or remove an approval ticket, as long as you have the appropriate permissions. |
| **Ready to Execute** | Shows a scrollable list of work that has been approved and is waiting to execute. |
| **Locked** | This returns all work that is locked. |
| **Executing** | This returns all work that is in an executing state. |
| **Finished** | This returns a list of work that has been completed. Each completed work item includes a column showing the type of request. Each completed UOW also includes information specifying its status. Clicking any UOW will populate the associated Queue Manager information |
| **Cancelled** | This returns all work that has been cancelled. |
| **Expired** | This returns all work that expired before it was completed. |

   c) Click **Search**. Your results display in the main window.
2. SEARCHING BY STATE (APPROVAL TICKETS)
   a) Select **Search by State**. The **Search by State** menu expands.
   b) Select **Approval Tickets**. The approval ticket selections display. Select from the following.

| *Table 43. Select Approval Tickets elements* | |
|---|---|
| **Element** | **Definition** |
| **Pending** | This returns all tickets pending. |
| **Approved** | This returns all tickets approved. |
| **Rejected** | This returns all rejected tickets. |
| **Expired** | This returns all expired tickets. |
| | This returns all historical tickets. |

   c) Click **Search**. Your results display in the main window.
3. SHOW ALL DATES SEARCH
   a) This search returns all results.
4. SEARCHING BY EXPLICITLY SET DATES
   a) You can filter the data shown in the Queue Manager by using the Date Range search. The significance of the date and time you select varies, depending on the type of data you are searching for. For completed UOWs (finished, cancelled, or expired) the work stop time is used. For all other UOWs (pending, waiting for execution, locked, and executing) the scheduled start time is used. For

work scheduled to execute immediately, the submission time is used. For recurring UOWs, the next execution time is used. For approval tickets, the UOW associated with the approval ticket is used, so the same rules apply.

b) Select **Search by Date** from the menu. The **Search by Date** menu expands.

c) Select **Explicitly Set Dates**. Type a from and to date and time for the tickets or work you are searching.

d) Click Search. Your results are displayed in the main window.

5. SEARCHING RELATIVE TO THE CURRENT TIME

a) You can filter the data shown in the Queue Manager by using the Date Range search. The significance of the date and time you select varies depending on the type of data you are searching for. For completed UOWs (finished, cancelled, or expired) the work stop time is used. For all other UOWs (pending, waiting for execution, locked, and executing) the scheduled start time is used. For work scheduled to execute immediately, the submission time is used. For recurring UOWs, the next execution time is used. For approval tickets, the UOW associated with the approval ticket is used, so the same rules apply. The following process enables you to search Queue Manager Relative to the Current Time. This process enables you to search for information generated during as well as before and after the time selected.

b) Select Search by Date from the menu. The Search by Date menu expands.

c) Select Relative to Current Time.

d) Select from the drop-down the time value for which you want to search Before your work was generated. Your choices are as follows: Hours, Days, Weeks, Months, Years. Select a number for the value you selected.

e) Repeat step 3 and 4 for the After value.

f) Click Search. Your results are displayed in the main window.

6. SEARCHING BY ASSOCIATION

a) Using the Search by Association form, you can choose to view work submitted by you, or work for which you are the approver. The following process enables you to search Queue Manager by Association.

b) Select Search by Association. The Search by Association menu expands. Select from the following.

*Table 44. Search by association descriptions*

| **Association** | **Description** |
|---|---|
| Submitter | Shows work you submitted, or approval tickets for work you submitted. |
| Group | Shows work submitted by any user in any group in which you have membership, or approval tickets for such work. |
| Approver | Shows work, or approval tickets, for which you are an approver. When searching for approval tickets, this search also shows the tickets generated for other groups for the work that you can approve. |

Please note if the user is a member of a group with the “View All Work” activity assigned to them, they have the ability to view all results for ALL groups - regardless of whether they are a member of the group.

c) Click Search. Your selections are displayed in the main window.

7. SEARCHING BY FAILURE CATEGORIES

a) This process enables you to search by one or more error categories. This can help you search for UOWs based on why they may have failed.

b) Select Search by Failure Categories. The Search by Failure Categories menu expands. Select from the following.

*Table 45. Search by Failure Categories elements*

| Element | Definition |
|---|---|
| Authentication | This displays results based on Authentication errors. |
| Commands Out of Sequence | This displays results based on commands being out of sequence. |
| Connection refused | |
| Connection Timed Out | |
| Device Error | This displays results based on device errors. |
| Device out of Sync | This displays results based on failures due to devices being out of sync. |
| Device Revised | |
| Discovery | This displays results based on discovery errors. |
| Host Unreachable | This displays results based on IP hosts being unreachable. |
| Import Failed | This displays results based on failed imports.p |
| Internal Error | |
| Invalid VTMOS | This displays results based on an invalid VTMOS given. |
| Locked Resource | This displays results based on failures because resources were in a locked state. |
| Name Not Unique | This displays results based on names for servers not being unique.` |
| Not Attempted - Previous Error | This displays results based on work not attempted because they previously failed. |
| Rollback Failed | This displays results based on rollbacks that failed. |
| Staged Device | This displays results based on staged devices. |
| Uncategorized | This displays results based on uncategorized changes. |
| Unknown Host | This displays results based on unknown hosts. |

c) Click Search. Your results are displayed in the main window.

8. SEARCHING BY ATTRIBUTE

a) Select **Search by Attribute**. The **Search by Attribute** menu expands.

b) Select from the following attributes:

*Table 46. Select attribute*

| Attribute | Definition |
|---|---|
| **UOW ID** | Use this attribute to search for a specific UOW for which you know the ID. |

| *Table 46. Select attribute (continued)* | |
|---|---|
| **Attribute** | **Definition** |
| **Priority** | Use this attribute to search for only the UOWs of a certain priority, such as 'high', 'medium' or 'low'. |
| **Type** | Use this attribute to search for only the UOWs of a specific type. For a list of UOW types, see Table 38 on page 137. |
| **Submitter** | Use this attribute to search for UOWs that were submitted by a specific user. |
| **Description** | Use this attribute to search for UOW for which you know the description. This field is wild-carded, so you can enter only part of the description. |

c) Click **Search**. Your results display in the main window.

9. DISPLAYING RELATED UOWS
   a) Right-click a recurring UOW and select **Show Recurring Sequence** from the drop-down menu.
   All the UOWs in the recurring sequence are displayed.

## Creating custom search filters

In addition to the canned filters, you can create your own Queue Manager filters. These filters can be created to house information based on the search criteria you provide.

Creating a search into Queue Manager is a two step process where you first create the search by saving it, and then adding that search to the list in Queue Manager.

1. Select Queue Manager from the left menu. See the previous sections for more information.
2. Select your Queue Manager search options.
3. Click File | Save Search. The **Save Queue Manager Search** dialog is displayed.
4. Type a name for your search. Select the realm in which you want to save your search results.
5. Click OK. Your search is saved and placed in the realm you selected.
6. Once you have created a search queue, you can the add it to the list of filters in the Queue Manager.
7. Select Queue Manager from the left menu tree. Click File | Add Search. The Add Search to **Queue Manager Searches** dialog is displayed.
8. Select the realm in which you saved your search. Highlight the search you want placed in the Queue Manager tree and click OK. The search is added to the tree.

## Moving or deleting search filters

You have the ability to move filters within Queue Manager, helping you to organize your work, and filter criteria. You can also remove any un-needed search filters.

This task describes how to move or remove Queue Manager searches.

1. To move a Select a filter within Queue Manger. Click Edit | Move to place the filter in the desired location within Queue Manager.
2. If you wish to remove the search, select the filter you want to remove within Queue Manager. Click Edit | Delete Search. The file is removed from Queue Manager. However the Generalized Resource is still located in the realm where it was created.

## Viewing units of work (UOWs)

The Queue Manager provides a tabbed environment for displaying information specific to any UOW selected. The tabs available are dependent upon the UOW Request Type of that particular UOW. For

example, the **Command Set** tab will only be shown in the Details section if the UOW chosen had a Command Set applied against it.

The UOW detail available within the Queue Manager presents the information using the following categories:

- Summary
- Results
- Resources
- Approvals
- Schedule
- Details

To view UOW Details for a UOW, simply select the UOW required and the tabbed information regarding that particular UOW will populate into the lower section of the screen. All six tabs available are all types of UOWs. However, the **Details** tab will contain different sub-tabs, if any, dependent on the type of UOW selected.

UOW attributes can only be provided for one UOW at a time. Please note that UOW log information can also be viewed in the Resources tab. There are numerous icons which can be used to extend functionality within the UOW Details section. The user also has the ability to expose further information through the use of sub-tabs on the **Details** tab.

This task describes how to view UOW.

1. Navigate to the Queue Manager.
2. Select a UOW, and use the tabs in the lower part of the screen to view the UOW information.

## Queue Manager: UOW details

The Queue Manager's **Unit of work** window presents UOW information on Summary, Results, Resources, Approvals, Schedule and Details tabs. Only tabs relevant to the type of UOW are displayed.

**SUMMARY TAB:**

The Summary tab of the UOW Details section provides an overview of information about a particular UOW. You can select one of the following:

| Field | Definition |
|---|---|
| Type | Either UOW, recurring UOW or Approval. |
| UOW ID | When a UOW is submitted, a UOW ID is generated thus providing unique identification. |
| Submitter | Login name of the user who submitted the UOW. |
| Window Start | The Window start time is a timestamp indicative of the start time of UOW execution. |
| Window End | The Window end time is a timestamp indicative of the end time of UOW execution. |
| Request Type | Each UOW has a request type, which indicates the type of action created by the UOW e.g. import configuration, configuration change |
| Work State | Describes the status of UOW, e.g Executing, Finished, Pending Approval. |
| Started At | Timestamp indicative of the starting time of execution of the UOW. |

| Field | Definition |
|---|---|
| Finished At | Timestamp indicative of the finishing time of execution of the UOW. |
| Execution Status | Status of UOW execution, e.g Success, Failure, Partial Success. |
| Description | The description field is a short narrative entered by the user to explain the UOW. |
| Priority | Each UOW is assigned a priority which, alongside the scheduled execution time determines when the UOW is processed. By default, all UOWs have a priority of Low when submitted. The priority may be altered at execution time if necessary. |
| Failure Categories | When a UOW fails to execute successfully it is assigned failure category, which reflects how the UOW failed to reach completion, e.g. Device Error, Discovery. |
| Resources | This specifies the hostname or IP address of the resource that the UOW was run against. If the UOW was applied against multiple devices, the text "Multiple Devices" will be displayed. |
| Approvals required | This indicates the number of approvals a UOW requires in order to commence execution. |

**RESULTS TAB:**

The Results tab is used to display all related results information pertaining to that particular UOW. The user can select one of the following:

| Field | Definition |
|---|---|
| Resource Status | Reflects the Execution status of the resource within the UOW. |
| Number | Number of devices with the Resource Status shown, against the total number of devices the UOW was executed against. |
| Percent | Devices with the Resource Status shown, as a percentage of the total number of devices the UOW was executed against. |

**RESOURCE(S) TAB:**

The Resource tab is used to display information about the device against which the UOW was ran against. In the case of "Run Autodiscovery" request type, the Resources information is also in the Details tab.

The summary information for each device includes Name, Realm, Status(Execution status), Failure(Failure Category) and Server. Each of these fields may be filtered using the filtering options at the bottom of the dialog. The Name, Realm and Server filters all support wildcards (*) where partial information may be supplied. The Status and Failure filters provide all the possibilities for those fields in a drop down format. These filters may be used in conjunction with one another in the event of a large number of devices. If no devices are found with the combination of filters selected, the device listing will simply be blank. When a device is selected, the event log is populated for that particular device on the right hand side of the screen.

**APPROVALS TAB:**

The Approvals tab displays any approval information that may have been required during UOW creation The user can select one of the following:

| Field | Definition |
|---|---|
| UOW ID | Unique identification for UOW. |

| Field | Definition |
|---|---|
| Submitter | Displays the user who created the UOW. |
| Request Type | Indicates type of action created in the UOW. |
| Date | Date and time in which the UOW was approved. |
| Approval Group | Group in which the user who created the UOW has membership to. |
| Approval | Displays whether the approvals have been approved, rejected or pending. |
| Approver | User who approved the UOW. |

**SCHEDULE TAB:**

The Schedule tab is used to display the schedule indicated by the user in the schedule created during UOW creation. The user can select one of the following :

| Field | Definition |
|---|---|
| Single Schedule | Either immediate or scheduled execution. If scheduled execution is chosen, additional fields are displayed for the execution window. |
| Recurring Schedule | Recurring selections can be based on hourly, daily, weekly, monthly, or yearly changes. |

**DETAILS TAB:**

The Details tab consists of a series of sub-tabs, each providing a further level of information specific to the selected UOW. The Details sub-tabs are: Synchronize, Command Set, Native Command Set, Rollback Options, Sets/Resources, Conflicts, Config Change, Search Sets and Selected Configurations. Each of these sub-tabs is described in the following :

**SYNCHRONIZE TAB** The Synchronize tab provides the Configuration Synchronization options available.

| Field | Definition |
|---|---|
| Report Only Mode | Displays if this change was to only report what would happen if it were actually applied. |
| Synchronize from Network Resource to ITNCM | Displays that the synchronization was made with the Network Resource changing the config within Netcool Configuration Manager. |
| Synchronize from Netcool Configuration Manager to Network Resource | Displays that the synchronization was made with Netcool Configuration Manager changing the config on the Network Resource. |

**COMMAND SET TAB** The Command Set tabbed information is used for viewing details of any Command Sets that were applied against the network resource.

| Element | Definition |
|---|---|
| **Execution Mode** | |
| Execute Mode | Displays whether changes were attempted. |

| Element | Definition |
|---|---|
| Report Only Mode | Displays if this change was to only report what would happen if it were actually applied. |
| Apply Device at a time | Displays whether all command sets to each individual device were applied at a time. All sets were applied to one device, then the second, then the third, etc. |
| Apply Command Set at a time | This option applies one command set at a time to a resource. To apply one command set to all the resources then apply the second to all the resources. |
| **Failure Options** | |
| Ignore All Errors | This indicates that you didn't want the UOW to stop processing, regardless of how many failures occurred. The command set will be applied to each resource regardless of any errors. |
| Fail After Total Errors | This option shows the number of errors you wanted passed before the process failed. |
| Fail After Percent Errors | This option shows the maximum percentage of failures you wanted to occur before the UOW stopped processing. This option is useful when there are a large number of command sets being applied to a large number of resources. If your desired percentage does not equal a whole number, the number of failures necessary to cause termination is rounded up. For example, if you select 51% and there are two command sets and five resources, the formula is as follows: Max# of failures: (51/100) x (2x5) = 5.1 = 5 |
| **Command Sets** | |
| Realm | Displays the realm where the Command Set exists. |
| Name | Displays the name of the Command Set. |
| VTMOS | Displays the VTMOS of the Command Set. |

**NATIVE COMMAND SET TAB** The Native Command Set tab is used for viewing details of any Native Command Sets that were applied against the network resource.

| Element | Definition |
|---|---|
| Apply Device at a time | Displays whether all command sets to each individual device were applied at a time. All sets were applied to one device, then the second, then the third, etc. |
| Apply Command Set at a time | This option applies one command set at a time to a resource. To apply one command set to all the resources then apply the second to all the resources. |
| **Failure Options** | |

| Element | Definition |
|---|---|
| Ignore All Errors | This indicates that you didn't want the UOW to stop processing, regardless of how many failures occurred. The command set will be applied to each resource regardless of any errors. |
| Fail After Total Errors | This option shows the number of errors you wanted passed before the process failed. |
| Fail After Percent Errors | This option shows the maximum percentage of failures you wanted to occur before the UOW stopped processing. This option is useful when there are a large number of command sets being applied to a large number of resources. If your desired percentage does not equal a whole number, the number of failures necessary to cause termination is rounded up. For example, if you select 51% and there are two command sets and five resources, the formula is as follows: Max# of failures: (51/100) x (2x5) = 5.1 = 5 |
| **Native Command Sets** | |
| Realm | Displays the realm where the Command Set exists. |
| Name | Displays the name of the Command Set. |
| VTMOS | Displays the VTMOS of the Command Set. |

**ROLLBACK OPTIONS TAB** The Rollback Options tab presents the options available for handling rollbacks on Command Set failures.

| Element | Definition |
|---|---|
| **How Rollbacks on Command Set failures are handled** | |
| No Rollback | Selected if you selected not to perform a possible rollback on changes. |
| **Rollback** | |
| Use Modeled Rollback | If a rollback was selected during the creation of the command set, this option will enable a rollback to a modelled configuration. |
| Reload the configuration and reboot the device | This option will load the original configuration and restart the device. |
| Perform Rollback Verification | This is selected if rollbacks were to be verified. |
| **How Rollbacks are done for each Network Resource** | |
| Rollback only the failed Command Set on the failed Network Resource | Selected only if you wanted the failed Command Set rolled back from the failed Network Resource. |

| Element | Definition |
|---|---|
| Rollback all Command Sets on the failed Network Resources | This rolls back all failed Command Sets on the failed Network Resource. |

**SETS/RESOURCES TAB** The Sets/Resources tab is displayed for any Command Set, Native Command Set or Search Sets created.

| Element | Definition |
|---|---|
| Set Name | Displays the set name used during creation. |
| Resource Realm | Displays the realm for the device. |
| Resource | Displays the hostname for the device. |
| Last Modified | Displays the date and time the device was last modified. |
| Status | Displays the status for the change. Possibilities are Successful, Failure, and Not Attempted. |
| Failure Categories | Displays the reason for any possible failure. |
| **View Native** button | Opens a dialog that displays the native commands to be generated when the command set is applied to the device.<br>You can see potential changes the command set will make to a device, including the commands it sends to the device, before approving the UoW. |

**CONFIG CHANGE TAB** The Config Change tab is shown in the event that changes to the device configuration were made.

| Element | Definition |
|---|---|
| Network Resource | Displays the hostname for the network resource on which the config was applied. |
| Realm | Displays the realm in which the network resource resides. |
| Configuration | Displays the name of the configuration. |
| View Configuration | Click to view the configuration within in the Resource Browser. |
| Force Directory Override | This is selected if the user performing the change chose to force an override of the directory. |
| Disaster Recovery; Use Raw CLI | This is selected if Raw CLI was used to enable change for disaster recovery. |

**SEARCH SETS TAB** The Search Sets tab is available for any Search Set that have been created on a device.

| Element | Definition |
|---|---|
| Realm | Displays the realm in which the Search Set resides. |

| Element | Definition |
|---|---|
| Name | Displays the name for the Search Set. |
| VTMOS | Displays the VTMOS of the Search Set. |

## Submitting units of work (UOWs)

The UOW submission wizard is displayed when a user submits a UOW.

The wizard consists of a series of dialog windows. Each dialog window requests information from the user. Since the parameters required for each UOW type vary, the dialog window sequences differ.

This task describes the UOW Submit Wizard.

1. Users have the ability to configure the dialog windows displayed in the UOW submit wizard, regardless of the UOW type. Any dialog window can be hidden from view, and the system defaults for those dialog windows are used instead. The UOW Submit Wizard can be configured to hide dialog windows from the display sequence using the **Wizard Panels** tab in User Preferences.
2. To hide any dialog window or windows from view in the UOW Submit wizard, the default value held in System Properties can be modified to suit the users' needs.
3. Please see the following table for system defaults for each dialog window:

*Table 47. System defaults*

| Dialog window Name | Default Value |
|---|---|
| Configure Failure Options | Ignore all errors. |
| Password Override | “Override ITNCM” flag is NOT checked. |
| Execution Priority | For Synchronization and Import UOW the default is Low. For all other UOW types, the default is Medium. |
| Configuration Synch | “Synchronize from network resource to ITNCM” flag is checked |
| Config Change | Requires settings only if a draft config based on a versioned config is re-applied to a device. In this case the new config is merged with the current config. |
| Configuration Execution Options | Command is executed in Execute Mode, Apply Device at a Time and Ignore All Errors both selected. |
| Rollback Options | Default setting for this step can be set in the RAD used for a specific device or group of devices. |
| Schedule Work | Single Schedule -Immediate. |
| Resources per UOW | Create a single UOW. |
| Schedule Workflow Options | Synchronize device pre OS Upgrade, Resource check pre OS Upgrade, Delete file or erase the file system then download the image to the device, Reload device, Synchronize device post OS Upgrade. |

4. All the System Property names relevant to the UOW Submit Wizard have a prefix of "Wizard", for example, Wizard-Config change Pane Visible.

**Related tasks**

Dequeueing units of work (UOWs)
The Queue Manager provides the ability to stop work, and remove it from the queue. The removal of a UOW is referred to as Dequeueing

Requeueing units of work (UOWs)
The Queue Manager provides the option to requeue work in the event that a UOW needs to be resubmitted.

Approving or rejecting units of work (UOWs)
When a UOW is submitted, it is subject to approval depending on the security privileges of the user.

Importing and making changes to resources in a single UOW
Use this procedure to manually import the current configuration for a resource into the database and make changes to it in a single unit of work (UOW).

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Requeueing units of work (UOWs)

The Queue Manager provides the option to requeue work in the event that a UOW needs to be resubmitted.

Not all UOW types are requeueable. The following table provides information on which work types can be requeued, and how the result of a previous submission can have an effect on requeueing the UOWs.

*Table 48. Work types that can be requeued*

| Work Type | Requeue on Success | Requeue on Failure |
|---|---|---|
| Autodiscovery | Yes | Yes |
| Command Set | Yes | Yes |
| Configuration Change | Yes | Yes |
| Configuration Housekeeping | No | No |
| Configuration Synchronization | Yes | Yes |
| Import Configuration | Yes | Yes |
| Native Command Set | Yes | Yes |
| OS Upgrade | No | Yes |
| Remove Network Resource | No | Yes |
| Search Set | Yes | Yes |
| Work Housekeeping | No | No |

There are many reasons why a UOW might be requeued, for example, UOW failure due to a network problem, or a failure in submission of individual network resources. UOWs can be requeued on a one-off, or recurring basis. UOWs with an execution status of Success, Finished, Cancelled, or Expired may all be requeued. The following procedure describes the steps to be taken to requeue a UOW

1. Within Queue Manager, right click on the UOW(s) required and choose Requeue, or alternatively select **Tools** > **Requeue** from the menu bar.
2. The Requeue Work wizard displays Page 1 of 2 **Filter Resources** window. These are the options available for requeueing the selected UOW against the network resources.

3. The Requeue Work wizard displays Page 2 of 2 **Filter Resources** window. Select the appropriate Failure category.
4. The **Configure Failure Options** window is displayed. Using the following table as a guide, enter the appropriate information requested and click Next.

*Table 49. Configure Failure Options fields*

| Field | Definition |
|---|---|
| Ignore All Errors | Indicates that the UOW is not to stop processing, regardless of how many failures occur |
| Fail After X Total Errors | Choose the maximum number of failures that should occur before the UOW stops processing |
| Fail After X Percent Errors | Choose the maximum percentage of failures that should over before the UOW stops processing Select the maximum percentage of failures you want to occur before the UOW stops processing. This option is useful when there are a large number of command sets being applied to a large number of resources. For example, if 51% is chosen, and there are two command sets and five resources, the formula is as follows: **Max # of failures: (51/100) x (2x5) = 5.1 = 5** |

5. The **Password Override** window is displayed. To override the Netcool Configuration Manager authentication, provide a login name and password. Click Next to continue to the next window.
6. The**Execution Priority** window is displayed. By default, all UOWs are submitted with a priority of Medium. Please select the appropriate execution priority and select Next to continue.
7. The **Schedule Work** window is displayed. Select either immediate or scheduled execution. If scheduled execution is chosen, additional fields are displayed prompting for the execution window. Provide the start date/time, and end date/time for executing the work. From this dialog, a recurring schedule can be specified for the UOW. The recurring schedule is offered on a yearly/monthly/weekly/daily/hourly basis. Click Next when this is complete.
8. The **Describe Work** window is displayed. Enter a description to identify the UOW, and click Next to finish.

The sequence of windows displayed for requeueing of Work can vary depending on the request type. For example the request type “Run Autodiscovery” has a reduced number of windows as some are not applicable.

**Related tasks**

Dequeueing units of work (UOWs)
The Queue Manager provides the ability to stop work, and remove it from the queue. The removal of a UOW is referred to as Dequeueing

Approving or rejecting units of work (UOWs)
When a UOW is submitted, it is subject to approval depending on the security privileges of the user.

Submitting units of work (UOWs)
The UOW submission wizard is displayed when a user submits a UOW.

## Dequeueing units of work (UOWs)

The Queue Manager provides the ability to stop work, and remove it from the queue. The removal of a UOW is referred to as Dequeueing

To dequeue a UOW another user submitted "Manage Work" permissions must be granted. In addition rights to view the realm and resource that the UOW affects are required. A UOW may be dequeued even if it has been approved, or if the work is already executing. If you cancel a UOW that is executing, it will

not process any more tasks within the UOW; however, it will finish processing all the tasks it is currently executing.

The following procedure describes the steps that need to be taken to dequeue a UOW. The procedure for dequeuing single or multiple tickets is the same.

1. Select the UOW or UOWs to be removed and select Tools | Dequeue or right click on it and dequeue.
2. The **Dequeue** dialog is displayed. Type a description of why the UOW is being stopped in the dialog presented. Click Dequeue.i
3. The UOW is removed from the queue (Pending Approval, Work Waiting to Execute, or Work Currently Executing) and moved to Work that is Finished list with an execution status of dequeued and a work state of Cancelled.

**Related tasks**

Approving or rejecting units of work (UOWs)
When a UOW is submitted, it is subject to approval depending on the security privileges of the user.

Requeueing units of work (UOWs)
The Queue Manager provides the option to requeue work in the event that a UOW needs to be resubmitted.

Submitting units of work (UOWs)
The UOW submission wizard is displayed when a user submits a UOW.

## Approving or rejecting units of work (UOWs)

When a UOW is submitted, it is subject to approval depending on the security privileges of the user.

If a UOW is approved, it is Ready to Execute and the work will be applied to the resource. If a UOW is rejected, it means the approver has rejected the commencement of work, and it will not execute. However in this case, the UOW may be modified and requeued.

The following procedure outlines how to Approve or Reject a UOW. Please note that the procedure for approving/rejecting either single or multiple tickets is the same.

1. Select Pending Approval Tickets from the Queue Manager tree. A listing of all UOWs that require approval is displayed.
2. Highlight the ticket(s) to be approved, and then right click to select Approve/Reject OR choose **Tools** > **Approve/ Reject** from the menu bar. Alternatively, approvals can also be approved in the Approvals tab in the lower section of the screen.
3. The **Approval Ticket** dialog box is displayed with information about the selected approval ticket. Enter a reason for the approval or rejection, and then click on the approve / reject button to process the ticket. If this was the last approval required for the ticket, the UOW should change state to either "work waiting to execute", if it is scheduled for the future, or to "Executing" if it was scheduled for immediate execution. If the ticket still requires additional approvals, it will stay in the "Pending Approval" state. Regardless of how many more approvals were required for the work to run, the rejected UOW is displayed in the Completed Work list with a status of Rejected.

**Related tasks**

Dequeueing units of work (UOWs)
The Queue Manager provides the ability to stop work, and remove it from the queue. The removal of a UOW is referred to as Dequeueing

Requeueing units of work (UOWs)
The Queue Manager provides the option to requeue work in the event that a UOW needs to be resubmitted.

Submitting units of work (UOWs)
The UOW submission wizard is displayed when a user submits a UOW.

Creating pre-emptive policies
Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device, allowing you to evaluate the impact of configuration

changes against pre-defined compliance policies for a device. In order to run a pre-emptive compliance, you first create or modify existing policies to make them suitable for execution in a pre-emptive manner. You then create a compliance process to apply the pre-emptive policy to a device.

## Viewing UOW logs

A UOW log file is generated to record the sequence of events which take place during the submission of a UOW. A log file is created regardless of the outcome of the UOW. This is useful to determine the reason for a UOW failure.

A UOW log file can be viewed for UOW in any state - except for Pending Approval Tickets, Work Waiting to Execute or Expired. In which case the log will display "Log Unavailable". Only the log file for a single UOW can be viewed at any one time.

The UOW log file consists of a listing of each device that was run against that UOW on the left hand side of the screen. When one of these devices is highlighted, the event log is populated on the right hand side of the screen.

1. Select the UOW you wish to view the log file for, and select **Tools** > **Log** or right click on it and Log. The **Resource Logs** dialog is displayed.
2. The UOW log file displays all devices associated with that particular UOW. The summary information for each device includes Name, Realm, Status (Execution status), Failure (Failure Category) and Server. Each of these fields may be filtered using the filtering options at the bottom of the dialog. The Name, Realm and Server filters all support wildcards (*) where partial information may be supplied. The Status and Failure filters provide all the possibilities for those fields in a drop down format. These filters may be used in conjunction with one another in the event of a large number of devices. If no devices are found with the combination of filters selected, the device listing will simply be blank. When a device is selected, the event log is populated for that particular device on the right hand side of the screen. This UOW log can be saved, printed, searched, text copied and pasted elsewhere, and an auto update and refresh can also be performed. The UOW Log Type setting in User Preferences also affects log size. Please make sure to set the Type to "debug" to view all log information.
3. At the centre of all Queue Manager screens is a paging function, which provides the user with the ability to view all UOW at once, or to customize the number of UOW they see on the screen at a time.
4. The number of records shown on the screen at any one time may be configured using the "Page Size" drop down selection. The options available are 100, 250, 500, 1000, 2500, 5000, 10000 or show all records. The user can add/remove entries to and from the Page Size dropdown in the User Preferences dialog. Users have the ability to navigate through each report page, or skip to a particular page of the report. The arrow keys can be used to navigate to the first page of the report, the previous page, the next page or the final page of the report. The user may also choose the page they wish to navigate to from the drop down list at the centre of the arrow keys. The figure shown on the right hand side of the paging functionality eg 1-100 (173), is indicative of how many records are currently being shown out of the total number of records.

   **Note:** In the event of a filed Auto-Discovery, there are no devices listed in the Device listing since Auto-Discovery did not find a resource. If the user wants to locate the resource they were attempting to discover, they can either look in the Details Tab, or click on the View Log Summary button in the Summary Tab.

# Managing resources

Use this information to learn how to manage and configure network resources.

Some of the tasks associated with managing and configuring network resources include:

- Creating resources
- Deleting resources
- Discovering resources
- Editing resources
- Importing resources

- Moving resources
- Renaming resources
- Viewing resource properties
- Searching for resources
- Exporting binary config to file

# Overview

Use the Resource Browser to view and work with all the different resource types used by Netcool Configuration Manager. You can access, manage, and control multiple configurations of multiple resources manufactured by multiple vendors from the Netcool Configuration Manager user interface. Your window will show only those system resources for which you have authorization for display or control.

The Netcool Configuration Manager user interface is a high level translation of native resource commands. The various dropdown lists are dynamically generated based on the type of resource you are working with. Should you want to view the actual native resource commands for a configuration, you can do so.

## Driver types

Netcool Configuration Manager supports the following types of drivers:

- Standard Mode Driver — Specifies a driver that IBM creates and delivers to customers. A Standard Mode Driver uses a generic schema and device-specific metadata.
- SmartModel Mode Driver — Specifies a driver that IBM creates and delivers to customers. A SmartModel Mode Driver uses a device-specific schema and device-specific metadata. When a SmartModel driver is first installed it starts off in Standard mode and behaves as a Standard driver. A SmartModel upgrade script is then used to put it into SmartModel mode.
- Custom Driver — Specifies a driver that a customer creates on site using a generic schema and generic metadata.

Typically, you import device resources using one of the previously listed driver types.

## Resource states for devices

Netcool Configuration Manager supports two states for device resources: managed and staged.

- Staged — A staged device resource is one that has been created, but whose configuration has yet to be imported into the database.
- Managed device resource — A managed device resource is one whose configuration has been imported into the database using one of the driver types.

The following table describes the characteristics of managed device resources, depending on which driver is used in the import resource task.

For instructions on how to import a managed device resource, see “Importing resources” on page 171.

| Driver used when importing a managed device resource | Description |
|---|---|
| Standard Mode Driver and Custom Driver | Managed device resources whose configurations are imported into the database using a Custom Driver or a Standard Mode Driver have the following characteristics:<br>• Because these managed device resources have not been translated into XML, their configurations cannot be viewed as hierarchical command trees from the Configuration Editor. |

| Driver used when importing a managed device resource | Description |
|---|---|
| | • The configurations of these managed device resources remain in native (CLI) format.<br>• When working with these managed resources, you have a more limited set of functionality than when working with SmartModel devices (described in the following table item.) Making configuration changes to these managed device resources is possible by using CLI commands, rather than by using the GUI widgets that are available with managed device resources imported using the SmartModel Mode Driver.<br>• You can create and apply native command sets to these managed device resources.<br>**Note:** These managed device resources are sometimes referred to as non-modelled devices because their configurations have not been translated into XML. Contrast the term non-modelled devices with the terms SmartModel or modelled devices in the following table item. |
| SmartModel Mode Driver | Managed device resources whose configurations are imported into the database using a SmartModel Mode Driver have the following characteristics:<br>• Because these managed device resources have been translated into XML, the Configuration Editor can present the configuration as a hierarchical command tree. For each command, you can make changes using a simple GUI widget, for example, by selecting a valid value from a dropdown menu.<br>• When working with these managed device resources, you can make use of all Netcool Configuration Manager functionality.<br>**Note:** These managed device resources are sometimes referred to as SmartModel or modelled devices because their configurations have been translated into XML. Contrast the term SmartModel or modelled devices with the term non-modelled devices described in the previous table item. |

## Resource support level for devices

Netcool Configuration Manager has a support level for each device which is displayed in the Resource Browser.

| Support level | Description |
|---|---|
| Null | This is the value applied to a staged device, that has not yet been imported. |
| Limited | Device import has been attempted, and failed. The device is unknown, as a generic unknown driver is in use. The device has not been modeled using the Netcool Configuration Manager modeling process. |
| Standard | The device has not been modeled using the Netcool Configuration Manager modeling process. This is CLI device support. |
| SmartModel | The device has been modeled using the Netcool Configuration Manager modeling process. This is Graphical device support. |

**Note:** The functionality available is dependent on the support level. If the device does not have the required support level, some menu options will be greyed out. The following functionality is only available if the support level is SmartModel; otherwise it is greyed out:

- **Tools** > **Apply Command Set**
- **Tools** > **Apply Search Set**
- **Tools** > **Apply from CSV File** > **Command Set**
- Right click functionality on a device in the Resource Browser panel to **Open** or **Edit** a device.
- Right click functionality on a configuration in the Configurations tab to **Open** , **Edit** or **Submit** a configuration.

  **Note:** You cannot open or edit configurations for standard support levels.

### Device Communication

In order to perform any kind of configuration management (import, config synchronization, command set, configuration change, and so forth), Netcool Configuration Manager must be able to establish a connection with the resource.

**Related tasks**

Importing resources
Use this procedure to manually import resources into the database.

## Resource types

Use this information to understand the available resource types on which Netcool Configuration Manager operates.

### Purpose

The resources described here require a VTMOS. The resources described here are also referred to as general resources.

### Parameters

**`Command Set`**
Allows the user to apply resource configuration changes to multiple network resources.

**Note:** When creating a modeled command set, the list of VTMOS labels from which you can select has been filtered to only display the labels for Smart Model drivers. Standard driver VTMOS are excluded.

**`Native Command Set`**
Allows the user to send native commands (CLI) to more than one resource at a time.

**`Network Resource`**
Creates a network resource based on the available VTMOS.

**`Shortcut`**
Creates a shortcut to any other type of general resource.

**`Authentication`**
Allows the user to specify user login credentials, as well as SNMP device login community strings.

**`Command Generation Data`**
Enables the user to define Key and KeyRef definitions for ordering commands during native command generation.

**`Device Script`**
Allows the user to amend and configure any of the default values in the device script.

**`File Transfer`**
Allows the user to specify an FTP server to use when transferring configurations.

**OS Registry**
Creates a database of compatible OS image files that have been approved for a particular VTMOS.

**OS Specification**
Allows the user to detail the specification which must be used for that particular image file.

**OS Upgrade Device Script**
Allows the user to make modifications to a device script.

**Realm**
Creates a new realm for managing resources. Realms are helpful in organizing the resources and other information with the application. For example, you can have a realm named Shortcut, where you house all the shortcuts within the application.

Realms provide a logical way to better manage large networks with many resources. Often, realms are based on geographic divisions.

By default, Netcool Configuration Manager is set up with a root realm (the default is ITNCM). Additional realms should be set up, and used to define scope for groups/users.

Any user who has access to a realm also has access to the contents of this realm, including any sub-realms.

It is not possible to rename, move, or delete realms that were created at installation time.

**Resource Access**
Allows the user to create an XML document that Netcool Configuration Manager uses to communicate with devices on the network.

**Search Set**
Creates a search set allowing the user to search resource configurations for specific command criteria.

Search sets allow you to search network resource configurations for specific command criteria which can be data from the configuration itself or from configuration tag data.

For example, using a search set you could quickly determine which CISCO routers in a particular realm have at least one “ntp server” with the “prefer” option.

Another powerful use of search sets is to query a set of resources for the current values of certain elements, and then plug those values into one or more command sets.

Search Sets can be parameterized so that some values can be modified at run time.

**Note:** When creating a modeled command set, the list of VTMOS labels from which you can select has been filtered to only display the labels for Smart Model drivers. Standard driver VTMOS are excluded.

**Security Set**
Allows the user to control which nodes are visible on the Configuration tree.

**Note:** When creating a modeled command set, the list of VTMOS labels from which you can select has been filtered to only display the labels for Smart Model drivers. Standard driver VTMOS are excluded.

**Work Server**
Allows the user to specify which work servers are allowed to process work for the realm.

## XPath Criteria

Within a search set, you must use XPath notation to specify which part of the configuration you are searching. Similar to an SQL “select” statement with a “where” clause, the XPath language allows you to specify which nodes should be selected based upon the existence of other criteria in the XML (the “where” clauses are called predicates).

For example, an XPath statement to find all “ntp server” commands with the “prefer” option would look like the following:

```
/configuration/ntp/server[prefer]
```

An XPath statement to find a configuration tag with the value of “acme” on any interface, regardless of type, would look like the following:

```
/config/interface/*[idm:tag/idm:name=”acme”]
```

An XPath statement to find all commands with any banner/login command (regardless of the value) would look like the following:

```
/banner/login[arg.001=”*”]
```

An XPath statement to find all commands with a banner/login command of “foo” would look like the following:

```
/banner/login[arg.001=”foo”]
```

Only one XPath statement is allowed per search set. The XPath statement is required.

For more information on XPaths, refer to this URL: http://www.w3.org/TR/xpath.

## Annotations

Annotations allow you to specify that certain values from a configuration are returned as key value pairs that can then be plugged into a command set or another search set. The following two types of annotations are available:

- elementNameKey — Used to return the name of an element.
- textValueKey — Used to return the value of an argument.

Each search set can contain multiple annotations. Annotations are optional.

### Search Set Example

The following search set example shows the proper XML syntax to use for specifying an XPath and annotations.

```
<searchSet xmlns:ssm="http://www.example.com/ns/searchSetMarkup">
<xpath>/configuration/interface/*</xpath>
<annotation ssm:elementNameKey="INTERFACE_TYPE">
<xpath>/configuration/interface/*</xpath>
</annotation>
<annotation ssm:textValueKey="INTERFACE_NUMBER">
<xpath>/configuration/interface/*/ARG.001</xpath>
</annotation>
</searchSet>
```

In this example, the XPath notation specifies that the configurations with any type of interface should be searched and returned. For each configuration snippet that is returned, the annotations specify that two key/value pairs also be returned: the interface type and the interface number.

The following results indicate that one configuration was found, with an interface type of “Tunnel” and a value of “5.”

```
<configuration xmlns:ssm="http://www.example.com/ns/searchSetMarkup">
<interface>
<Tunnel ssm:elementNameKey="INTERFACE_TYPE">
<ARG.001 ssm:textValueKey="INTERFACE_NUMBER">5</ARG.001>
</Tunnel>
</interface>
</configuration>
```

**Related concepts**

Resource Browser search options

You can search the Resource Browser by Type, Realm, Name, Native Config, Stale Config, VTMOS, Custom Fields, Driver, and State.

**Related tasks**

Applying search sets
Search sets enable you to search network resource configurations for specific command criteria. For example, using a search set you can quickly determine which CISCO routers in a particular realm have at least one `ntp server` with the `prefer` option. Another powerful use of search sets is to query a set of resources for the current values of certain elements, and then plug those values into one or more command sets. Use this procedure to specify how to apply a specified search set.

Applying the search set to network resources in a realm
Use this procedure to apply a search set to network resources in a realm.

Applying the search set to network resources retrieved from a realm
Use this procedure to apply a search set to network resources retrieved from a realm.

Applying the search set to specific network resources
Use this procedure to apply a search set to specific network resources.

Creating resources
Use this procedure to create the following categories of resources from the Resource Browser: network, general, realm, and search set.

Deleting resources
Use this procedure to delete the following categories of resources: network, general, realm, and search set.

Discovering resources
Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

Editing resources
Use this procedure to edit resources.

Editing resource XML
Use the XML editor to make it easier to edit XML files.

Importing and making changes to resources in a single UOW
Use this procedure to manually import the current configuration for a resource into the database and make changes to it in a single unit of work (UOW).

Importing resources
Use this procedure to manually import resources into the database.

Moving resources
Use this procedure to move the following categories of resources: network, general, realm, and search set.

Renaming resources
Use this procedure to rename the following categories of resources: network, general, realm, and search set.

Searching for resources
Use this procedure to invoke the Resource Browser and use the Search icon to search for resources.

Submitting units of work (UOWs)
The UOW submission wizard is displayed when a user submits a UOW.

Using configuration tags
Configuration tags are a way of attaching an extra description to any node within the configuration of a network resource.

Viewing hardware properties for a resource
Use this procedure to select the **Hardware Tab** to view hardware inventory.

Viewing related work for a resource

Use this procedure to find and view all related work for a selected resource from the Resource Browser.

Viewing resource properties
Use this procedure to view resource properties.

## About working with resources

Use this information to obtain an overview of the tasks that you can perform when working with resources.

The following table identifies the tasks associated with resources. The table contains the following columns:

- Task — Specifies the resource task.
- Tool — Specifies the tool used to complete the resource task.
- Stand alone — Specifies whether the resource task applies to Netcool Configuration Manager when operating in a stand alone environment.
- Integrated — Specifies whether the resource task applies to Netcool Configuration Manager when operating in an integrated environment, that is, with Network Manager and Tivoli Netcool/OMNIbus.

| Task | Tool | Stand alone | Integrated |
|---|---|---|---|
| Searching for resources | Resource Browser | Yes | Yes |
| Viewing post-compliance results | Resource Browser | Yes | Yes |
| Viewing related work for a resource | Resource Browser | Yes | Yes |
| Viewing hardware properties for a resource | Resource Browser | Yes | Yes |
| Creating resources | Resource Browser | Yes | Yes |
| Importing resources | Resource Browser | Yes | Yes |
| Importing and making changes to resources in a single UOW | Resource Browser | Yes | Yes |
| (VMware environment only) Importing a certificate for VMware | certificate tool (launched from VMware vSphere) | No | Yes |
| Discovering resources | Auto-Discovery<br>**Note:** The Auto-Discovery tool does not support the importing of head end devices. | Yes | Yes |
| Editing resources | Configuration Editor (accessed through the Resource Browser) | Yes | Yes |
| Editing resource XML | XML editor | Yes | Yes |
| Applying search sets | Resource Browser | Yes | Yes |
| Moving resources | Resource Browser | Yes | Yes |
| Renaming resources | Resource Browser | Yes | Yes |

| Task | Tool | Stand alone | Integrated |
|---|---|---|---|
| Deleting resources | Resource Browser | Yes | Yes |

## Searching for resources

Use this procedure to invoke the Resource Browser and use the Search icon to search for resources.

Read the following information before beginning this procedure:

- General information
  - You should understand the meaning of the different types of resources that Netcool Configuration Manager manipulates.
  - When importing a network resource into the database using the user interface, it is recommended that you make any changes to the resource as a separate unit of work. If you import and make changes within the same UOW, the network resource cannot be rolled back correctly if an error occurs.
  - When simply importing (rather than importing and making changes), you can import any number of resources together. Multiple imports can appear under one UOW. After creating one or more new resources, use the following procedure to import the current configuration of each into the database.
- Resource Browser information
  - The Resource Browser shows a list of all network resources currently being managed by Netcool Configuration Manager. Netcool Configuration Manager maintains a complete configuration audit trail of each device. This is a particularly valuable resource for users who wish to view a history of what has been configured on each of the devices.
  - Users can use the Resource Browser to search by Type, Realm, Name, Native Config, Stale Config, VTMOS, Custom Fields, Driver, and State.
  - For a head end device resource, users can click on the Search icon on the toolbar to invoke the searching mechanism. Also, users can right click on the head end device and select **Search by Associated**.
  - For a head end device resource, the column **associated** displays the string `Multiple` even if there is only one vswitch on the system.
  - Users can specify more than one search criteria. For example, a user can search the root realm for an optimal driver, with the matched results appearing in the Search Results pane.
  - Users can only see those devices and realms for which they have the appropriate permissions to view.

Follow these steps to invoke the Resource Browser and use the Search icon to search for resources.

1. Select the Resource Browser in the navigation pane.

   The Resource Browser displays all realms setup in Netcool Configuration Manager. The realms shown can be navigated to locate various devices that have been imported.
2. Click the Search icon on the toolbar to invoke the searching mechanism.

   The searching pane displays on the left hand side of the Resource Browser.
3. Select the desired search option from the searching pane using the following table as a guide:

| Search option | Description |
|---|---|
| **Search by Type** | Click this option to search by a particular UOW type. |
| **Search by Associated** | Click this option to search by a particular head end device. |
| **Search by Realm** | Click this option to limit your search to a particular realm. |

| Search option | Description |
|---|---|
| **Search by Name** | Click this option to search network resources by name. |
| **Search by Native Config** | Click this option to search resources based on the contents of the native configuration. |
| **Search by Stale Config** | Click this option to search resources based on the contents of the previous configuration. |
| **Search by VTMOS** | Click this option to search resources by VTMOS. |
| **Search by Custom Field** | Click this option to search on user defined custom labels. This option shall only appear if a custom label is mandatory, and has a value assigned to it. |
| **Search by Driver** | Click this option to search resources by Optimal or Non-Optimal Driver. |
| **Search by State** | As units of work (UOWs) and approval tickets move through the system, their states change. Click this option to search on the current state. If the **Search by Type** option is not specified in conjunction with the **Search by State** option, it shall default to Network Resource accordingly. |
| **Search** | Click this option to initiate your search. |
| **Reset** | Click this option to reset your search and remove your search criteria. |

For more information on these search options, see "Resource Browser search options" on page 164.

All matched results are presented in the Search Results pane, replacing the previous Resource Browser listing. If no results are found to match the criteria, the message "No Items Found" will appear in the Search Results pane.

You can perform any of the following tasks if you want to manipulate the Search results while they are in the Search Results pane:

| Search result task | Steps |
|---|---|
| **Export list of devices to a CSV or TXT file** | To export a list of devices to a CSV or TXT file, follow this step:<br>1. **Select Tools** > **Export to File** > **Selected Device(s)**<br>The CSV file will contain all Resource Browser device attributes regardless of attributes chosen for the filter, and shown on screen. The results are saved in the required format to a user defined location. |
| **Review current config of NW resource results** | To review the current configuration of any of the devices that were matched against the search criteria, follow this step:<br>1. Right click on the device and select **View Native Commands**.<br>The configuration opens in native mode. |
| **Apply standard ITNCM - Base operations** | To perform standard Netcool Configuration Manager operations (such as, Viewing Configurations, Synchronizing Configurations, or applying a Command Set) against search results, follow this step:<br>1. Right click on the device and select the appropriate Netcool Configuration Manager operation or use the Tools menu. |

| Search result task | Steps |
| --- | --- |
| **Paging functionality** | The paging feature situated in the center of the screen, provides you with the ability to view all results at once, or to customize the number of results visible on a screen at a time. |

**Related concepts**

Resource Browser search options
You can search the Resource Browser by Type, Realm, Name, Native Config, Stale Config, VTMOS, Custom Fields, Driver, and State.

**Related tasks**

Creating resources
Use this procedure to create the following categories of resources from the Resource Browser: network, general, realm, and search set.

Discovering resources
Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

Importing resources
Use this procedure to manually import resources into the database.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Resource Browser search options

You can search the Resource Browser by Type, Realm, Name, Native Config, Stale Config, VTMOS, Custom Fields, Driver, and State.

You can perform the following searches:

**By type**
The Search by Type option allows you to perform a search based on the resource type, for example Command Set or Configuration. The **Search by Type** dropdown list can be expanded to enable the user to select the appropriate resource type to search. The user chooses the required resource type, and then selects Search to filter all resources to match the desired criteria.

**By associated**
The Search by Associated option allows you to perform a search for head end devices.

**By realm**
The Search by Realm option allows you to perform a search for network resources in the Netcool Configuration Manager realms. This search can be extended to filtering on sub-realms, simply by selecting the Search Subrealms checkbox.

**By name**
The Search by Name option enables you to search by the resource name. This search is driven by a user defined search string in a text box. Wild cards (denoted by an asterisk (*)) can be used in the search string if required. For example, the search string `10.216*` returns all device names beginning with `10.216`.

Enter the required search string in the text box, making use of wild cards if appropriate, and then select Search to filter all resources in Netcool Configuration Manager to match the desired criteria.

**By native config**

The Search by Native Config option provides an enhanced search, which allows you to search for resources based on the contents of the Native Config. Because the search will only return matches found in the current native configuration of a device, staged devices and blank configurations are automatically excluded from the search. This search option is accessible only when searching by Configuration and Network Resource Types.

Searching by native config is resource-intensive. To avoid performance issues with searches, constrain the search space by using additional options. Use **Search By Realm** to reduce the number of devices searched, and the **Search by VTMOS** option to further reduce the search space.

This search is driven by a user defined search string in a text box that searches through native configurations. The text box is large enough to specify large regular expressions, and searches for multiple configuration lines (as a block). Wild cards (denoted by an asterisk (*)) are not supported in the native configuration search, as they conflict with regular expression searches. All native configuration searches are case insensitive.

Regular expression logic can also be used as part of the search criteria. Regular expression provides the flexibility to execute complex searches. For example, `[a]{2,3}` will find every instance where the letter a occurs at least two or three times.

Enter the required search string, making use of regular expressions where appropriate, and then select Search to filter all resources in Netcool Configuration Manager that fulfil the desired search criteria.

**By stale config**

The Search by Stale Config option allows you to search resources that have a Stale config. A Stale Config is defined as a device configuration which is older on Netcool Configuration Manager than the configuration held on the network resource. The search options are Stale and Not Stale.

Enter the Stale Config search option required, and then select Search to filter all resources in Netcool Configuration Manager to match the desired criteria.

**By VTMOS**

The Search by VTMOS option allows you to search by the resource VTMOS. The search options for the four VTMOS selections are all wild cards (denoted by an asterisk (*)) by default. The dropdown menus present a listing of all VTMOS options available in Netcool Configuration Manager. Since wild cards are employed here, you do not need to enter the entire VTMOS for the resource. For example, if you choose CISCO as the Vendor, and leave the other selections as `*`, all CISCO devices regardless of Type, Model, and Operating System will be returned.

Enter the required VTMOS search options, making use of wild cards if appropriate, and then select Search to filter all resources in Netcool Configuration Manager to match the desired criteria.

**By custom fields**

The Search by Custom Fields option allows you to perform a search for network resources by user defined Custom labels. This option only appears if a Custom label is Mandatory, and has a value assigned to it.

Choose the required Label Options, and then select Search to filter all resources in Netcool Configuration Manager to match the desired criteria.

**By driver**

The Search by Driver option allows you to perform a search for network resources which have a particular driver installed. This search option is accessible only when searching by Configuration and Network Resource Types. The search options are based on an Optimal driver or a Non-Optimal driver. An Optimal driver is where the `optimalDriver- Loader.sh` script has been run against the latest version of the driver. A Non-Optimal driver on the other hand, is not the latest version of the driver installed. Non-Optimal drivers are further broken up into Compatible and Incompatible. Compatible places an orange arrow beside the driver icon, and represents a driver of the same VTMOS, but not the latest version. Incompatible places a red arrow beside the driver icon, and represents a driver of a different VTMOS, which is neither the latest version. Drivers that have been made inactive will appear as Incompatible in this search.

Choose the Driver Option, and then select Search to filter all resources in Netcool Configuration Manager to match the desired criteria.

**By state**

The Search by State option allows you to search resources by State. The search options are Managed and Staged. Managed defines any resource that was imported into Netcool Configuration Manager, while Staged defines any resource that was created within Netcool Configuration Manager.

Choose the required State, and then select Search to filter all resources in Netcool Configuration Manager to match the desired criteria.

**Related tasks**

Searching for resources
Use this procedure to invoke the Resource Browser and use the Search icon to search for resources.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Viewing resource properties

Use this procedure to view resource properties.

Read the following information before beginning this procedure:

- You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
- Each Generalized Resource is provided with a set of properties you can view. The property information is populated when you create the Generalized Resource.

Follow these steps to view resource properties:

1. Select the Generalized Resource for which you want to view property information, then choose **File** > **Properties**.

   The Properties dialog box displays for the resource that you selected.
2. Select one of the following properties tabs:

| Properties tab | Description |
|---|---|
| **General** | Provides general information such as the resource name, realm, type, who created the resource, and its current state. |
| **Type** | Provides the VTMOS for the resource and its data type. |

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Viewing post-compliance results

Use this procedure to view the current post-compliance results from the Resource Browser.

Follow these steps to view the current post-compliance results.

1. In the Resource Browser, right-click a device to select it.
2. Click the **Compliance** tab.

   This lists the current compliance status of a particular device against a set of policies.
3. Drill down into the Validation detail by double-clicking on the individual policy, or by selecting the **Policy** row and then clicking **View Policy Result Detail**.

## Viewing related work for a resource

Use this procedure to find and view all related work for a selected resource from the Resource Browser.

Read the following information before beginning this procedure:

- You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.

Follow these steps to find and view all related work for a selected resource.

1. In the Resource Browser, select or Search for the resource for which you want to review related work.
2. Highlight the resource, and then select the **Work** tab from the bottom pane. All related work for that network resource displays.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Viewing hardware properties for a resource

Use this procedure to select the **Hardware Tab** to view hardware inventory.

Read the following information before beginning this procedure:

- You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
- When a resource is imported into the database, Netcool Configuration Manager not only imports the running configuration of the resource, but it also runs several show commands so that the current hardware information of the resource can be imported.
- The information shown on the **Hardware Tab** reflects the hardware on the device the last time the show commands were run by Netcool Configuration Manager. The show commands are run and the hardware information is updated each time a device is imported (or re-imported). In addition, you can configure the system so that the information is also updated when a configuration change or configuration synchronization is performed.

Follow this step to view hardware inventory.

Highlight the resource, and then select the **Hardware Tab** from the bottom pane.

All related work for that resource displays.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Creating resources

Use this procedure to create the following categories of resources from the Resource Browser: network, general, realm, and search set.

Read the following information before beginning this procedure:

- General information
  - You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
  - Within a realm, each resource must have a unique name, regardless of the type of resource.
  - Creating a resource is synonymous with adding a resource.
- About creating realms
  - Realms are helpful in organizing the resources and other information with the application. For example, you can have a realm named Shortcut, where you house all the shortcuts within the application.
  - Netcool Configuration Manager is installed with a default, top-level realm. Additional realms may then be added to organize the network resources.

- About creating shortcuts
  - Shortcuts are helpful when you have resources you need to access often, and it is easier than navigating the different realms you created.
  - Because a shortcut is a general resource, you must have the same security rights as those required for activities on an actual resource (view, move, rename, delete, and so forth).
  - View rights are required on the actual resource in order to create a shortcut to that resource. Add rights are required for the realm in which you are creating the shortcut.
  - In any case where the shortcut is de-referenced and used (UOWs for example), you must posses the required rights on both the shortcut and the actual resource.
- About creating network resources
  - You can create a network resource in any realm for which you have rights, but you should avoid putting resources into the top-level realm created as part of the Netcool Configuration Manager installation process.
  - Creating a network resource creates a placeholder in the database. You then need to either import the configuration or create a new configuration to later submit to the resource.
  - Regardless of what VTMOS you specify when you create a resource, after it is imported, Netcool Configuration Manager will show the exact VTMOS found on the resource.
- About defining custom labels
  - A user has the ability to define additional device "labels". These labels are fields, which can be used to capture additional device information, for example, Device ID. The custom labels must first be configured within the system properties function.

    For information on how to configure the custom labels within the system properties function, see the *IBM Tivoli Netcool Configuration Manager Administration Guide*.
  - These labels are available in the Resource Browser and the **Device Summary** tab, and may be searched for using the **Search by Custom Fields** option.

You use the Resource Browser to create all categories of resources in a similar manner. Follow these steps to create the following:

- General resource with a VTMOS
- Shortcut
- Network resource
- Custom label
- Realm
- Search set

1. Most resources require the designation of a VTMOS. To create a general resource with a VTMOS, follow these steps:
   a) Click **File** > **New** and select from the list of general resources. The following table describes each of the general resources:

| General resource | Description |
|---|---|
| Command Set | Allows the user to apply resource configuration changes to multiple network resources. |
| Native Command Set | Allows the user to send native commands (CLI) to more than one resource at a time. |
| Network Resource | Creates a network resource based on the available VTMOS. |
| Shortcut | Creates a shortcut to any other type of general resource. |

| General resource | Description |
|---|---|
| Authentication | Allows the user to specify user login credentials, as well as SNMP device login community strings. |
| Command Generation Data | Enables the user to define Key and KeyRef definitions for ordering commands during native command generation. |
| Device Script | Allows the user to amend and configure any of the default values in the device script. |
| File Transfer | Allows the user to specify an FTP server to use when transferring configurations. |
| OS Registry | Creates a database of compatible OS image files that have been approved for a particular VTMOS. |
| OS Specification | Allows the user to detail the specification which must be used for that particular image file. |
| OS Upgrade Device Script | Allows the user to make modifications to a device script. |
| Realm | Create a new realm for managing resources. |
| Resource Access | Allows the user to create an XML document which Netcool Configuration Manager uses to communicate with devices on the network. |
| Search Set | Creates a search set allowing the user to search resource configs for specific command criteria. |
| Security Set | Allows the user to control which nodes are visible on the configuration tree. |
| Work Server | Allows the user to specify which work servers are allowed to process work for the realm. |

When you select **File** > **New**, the **New Network Resource** dialog box displays.

b) Specify values for the **New Network Resource** dialog box using the following table as a guide:

| Element | Description |
|---|---|
| **Name** | Type a name for the resource that you are creating. |
| **Vendor** | Type the vendor name for the resource you are creating. |
| **Type** | Type a type name for the resource you are creating. |
| **Model** | Select an available model from the drop down list for the resource you are creating. Some models allow you to use wild cards. |
| **OS** | Select an available operating system from the drop down list for the resource you are creating. Some operating systems can be specified by using a wildcard. |

c) Click **OK**.

The general resource that you specified is created.

2. To create a shortcut, follow these steps:
   a) Select the resource for which you want a shortcut.
   b) Click **File** > **New** > **Shortcut**.

      The shortcut is created in the realm in which your selected resource resides.
   c) Click to select and then drag the resource to the realm in which you have your shortcuts located.
3. To create a network resource, follow these steps.
   a) Select the Resource Browser in the navigation tree.

      The Resource Browser displays.
   b) Select **File** > **New** > **Network Resource** from the menu bar.

      The **New Network Resource** dialog box displays.
   c) Specify values for the **New Network Resource** dialog box using the following table as a guide:

| Element | Description |
|---|---|
| **Name** | Type a name for the resource that you are creating. |
| **Vendor** | Type the vendor name for the resource you are creating. |
| **Type** | Type a type name for the resource you are creating. |
| **Model** | Select an available model from the drop down list for the resource you are creating. Some models allow you to use wild cards. |
| **OS** | Select an available operating system from the drop down list for the resource you are creating. Some operating systems can be specified by using a wildcard. |

4. If custom labels have been defined in system properties and the label state is set to 'mandatory', they are displayed when a new resource is created. Enter a custom label in the field or fields provided.
5. To create a realm, follow these steps:
   a) Navigate to the Resource Browser, where you want to add realms.
   b) Select **File** > **New** > **Realm**.

      The **New Realm** dialog box displays.
   c) Enter a name for the new realm, and the click **OK**.

      **Note:** The name must be unique within the given realm.

      The new realm then appears in the navigation pane.
6. To create a search set, follow these steps:
   a) Navigate to the Resource Browser.
   b) Select **FileNewSearch Set**.

      The **New Search Set** dialog box displays.
   c) Enter a name for the new Search Set and the required VTMOS, and then click **OK**.

      **Note:** Smart model drivers: When creating a search set, the list of VTMOS labels from which you can select has been filtered to only display the labels for Smart Model drivers. Standard driver VTMOS are excluded.

You can create another resource by following the instructions in this procedure.

**Related tasks**
Discovering resources

Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

Importing resources
Use this procedure to manually import resources into the database.

Deleting resources
Use this procedure to delete the following categories of resources: network, general, realm, and search set.

Importing and making changes to resources in a single UOW
Use this procedure to manually import the current configuration for a resource into the database and make changes to it in a single unit of work (UOW).

Moving resources
Use this procedure to move the following categories of resources: network, general, realm, and search set.

Renaming resources
Use this procedure to rename the following categories of resources: network, general, realm, and search set.

Searching for resources
Use this procedure to invoke the Resource Browser and use the Search icon to search for resources.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

# Importing resources

Use this procedure to manually import resources into the database.

Read the following information before beginning this procedure:

- General information
  - You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
  - Netcool Configuration Manager allows both manual and automated initial input of your network resource information into the database.

    **Note:** If you have many resources to import, there is a separate command line BulkLoader utility available. This utility provides a way to automate the import of resources.

    For information on the BulkLoader utility, see the *IBM Tivoli Netcool Configuration Manager Administration Guide*.
  - When importing an existing resource into the database, the system also writes the running configuration to the stored/candidate configuration on the resource, ensuring that all three configurations (current, running, stored) are in sync.
  - When importing a network resource into the database using the Resource Browser, it is recommended that you make any changes to the resource as a separate unit of work. If you import or make changes within the same UOW, the network resource cannot be rolled back correctly if an error occurs.
  - When simply importing (rather than importing and making changes), you can import any number of resources together. Multiple imports can appear under one UOW. After creating one or more new resources, use the following procedure to import the current configuration of each into the database.
  - You can import resources into the database using the Netcool Configuration Manager API.
- About importing head end devices and its associated managed devices (vswitches)
  - (VMware environment only) Before importing a head end device in a VMware environment, you must run the certificate tool to import a certificate for VMware. Otherwise, the import of the head end device will fail.

For more information, see "(VMware environment only) Importing a certificate for VMware" on page 177.

- Importing a head end device on its own renders its associated vswitch (the managed device) stale.

- About importing head end managed devices (vswitches)
  - By default, head end managed devices are imported into their own realm. This is configurable in the RAD can be turned on or off.
  - Netcool Configuration Manager displays an error indicating that the operation failed when you attempt to do the following:
    - Specify the **Report differences between running and stored** RAD option in a RAD configuration for a head end device (vswitch)
    - Import the head end device (vswitch)

    The reason for the error is that the VmWare server has no concept of a stored configuration, so this driver does not support retrieval of a stored configuration for head end devices. Thus, the **Report differences between running and stored** RAD option is not meaningful for head end devices.

**Note:** If the VmWare hypervisor is moved to a new realm and the vswitch is added to the actual config, on next import or sync of hypervisor the new vswitch is created in the new vswitch sub-realm.

Follow these steps to manually import resources into the database.

1. Select the Resource Browser in the navigation tree.

   Your resources display.
2. Select or Search for the network resources you want to import.
3. Click to highlight the desired resource, and then right click and select **Import**. (Use `Ctrl-click` to select multiple resources.)

   The **Import Network Resource** wizard displays.

   Any resources that you selected in the Resource Browser are preselected here. You can add more resources and adjust the order on this panel. Use the buttons in the middle of the panel to add, remove, and rearrange resources to be imported.
4. Click **Next**.

   The **Configure Failure Options** wizard displays.
5. Select one of the fields from the **Configure Failure Options** wizard using the following table as a guide, and then click **Next**.

| Field | Description |
|---|---|
| **Ignore All Errors** | Indicates that you do not want the UOW to stop processing, regardless of how many failures occur. |
| **Fail After Total Errors** | Select the maximum number of failures you want to occur before the UOW stops processing. |
| **Fail After Percent Errors** | Select the maximum percentage of failures you want to occur before the UOW stops processing. This option is useful when there are a large number of command sets being applied to a large number of resources. If your desired percentage does not equal a whole number, the number of failures necessary to cause termination is rounded up. For example, if you select 51% and there are 2 command sets and 5 resources, the formula is as follows:<br>`Max # of failures: (51/100) x (2x5) = 5.1 = 5` |

   The **Password Override** wizard displays.

6. Select one of the fields from the **Password Override** wizard using the following table as a guide, and then click **Next**.

| Field | Description |
|---|---|
| **Override ITNCM Authentication** | Select this check box to override the default Netcool Configuration Manager authentication information. |
| **Login Name** | Provide the login name for the device you are accessing. |
| **Password** | Provide the password for the device you are accessing. |
| **Enable Password** | Provide the device enable password for the device you are accessing. |
| | Select this check box if you will always use this authentication for your resource. |

   The **Execution Priority** wizard displays.
7. The default execution priority is Medium. Choose the appropriate priority and click **Next**.

   The **Schedule Work** wizard displays.
8. Select either immediate or scheduled execution. If you select scheduled execution, additional fields are displayed asking for the execution window. Provide the start date and time, and the end date and time for executing the work. From this dialog you can also specify a recurring schedule for the UOW. Click **Next** when complete.

   The **Describe Work** wizard displays.
9. Type a description and click **Finish**.

**Related concepts**

Overview
The Resource Browser is a high level translation of native resource commands. The various drop down lists are dynamically generated based on the type of resource you are working with. Should you want to view the actual native resource commands for a configuration, you can do so. Your window will show only those system resources for which you have authorization for display or control.

Overview
Use the Resource Browser to view and work with all the different resource types used by Netcool Configuration Manager. You can access, manage, and control multiple configurations of multiple resources manufactured by multiple vendors from the Netcool Configuration Manager user interface. Your window will show only those system resources for which you have authorization for display or control.

**Related tasks**

Creating resources
Use this procedure to create the following categories of resources from the Resource Browser: network, general, realm, and search set.

Deleting resources
Use this procedure to delete the following categories of resources: network, general, realm, and search set.

Discovering resources
Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

Importing and making changes to resources in a single UOW
Use this procedure to manually import the current configuration for a resource into the database and make changes to it in a single unit of work (UOW).

(VMware environment only) Importing a certificate for VMware
Use this procedure to import a certificate for VMware.

Moving resources

Use this procedure to move the following categories of resources: network, general, realm, and search set.

Renaming resources
Use this procedure to rename the following categories of resources: network, general, realm, and search set.

Searching for resources
Use this procedure to invoke the Resource Browser and use the Search icon to search for resources.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Importing and making changes to resources in a single UOW

Use this procedure to manually import the current configuration for a resource into the database and make changes to it in a single unit of work (UOW).

Read the following information before beginning this procedure:

- General information
  - You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
  - The Netcool Configuration Manager allows both manual and automated initial input of your network resource information into the database.

    **Note:** If you have many resources to import, there is a separate command line BulkLoader utility available. This utility provides a way to automate the import of resources.

    For information on the BulkLoader utility, see the *IBM Tivoli Netcool Configuration Manager Administration Guide*.
  - The resource that you are importing and making changes to should have a state of staged, indicating that it has not yet been imported into the Netcool Configuration Manager database.
  - If you import and make changes within the same UOW, the network resource cannot be rolled back correctly if an error occurs.
- About importing and making changes to head end devices
  - Importing a head end device on its own renders its associated vswitch (the managed device) stale. Thus, when importing an entire realm that contains head end devices and vswitches (managed devices), make sure to set the VTMOS filter in the **Import Network Resource** wizard.

    First, import the head end device. Then import the vswitches. This sequence assures that all configurations are current.

Follow these steps to manually import a resource into the database and make changes to the resource in a single UOW.

1. Select the Resource Browser in the navigation tree.

   Your resources display.
2. Select or Search for the network resources you want to import.

   **Note:** The resource should have a state of “staged,” indicating that it has not yet been imported into the Netcool Configuration Manager database.
3. Click to highlight the desired resource, and then select **Edit** > **Edit** , or alternatively right click on the resource and select **Edit**.

   The Configuration Editor displays a blank configuration.
4. Add the configuration information you want to be applied to the resource.
5. Save the new configuration (**File** > **Save**).

6. From the Configuration Editor, select **File** > **Submit**.

   A dialog displays giving you several choices of how to handle the combined import/configuration change.
7. The **Submit Configuration Change** wizard displays the Configure Execution Options dialog, only if the support level of the configuration is SmartModel. If the support level is Standard, this dialog is not available. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

*Table 50. Configure Execution Options dialog*

| Element | Description |
|---|---|
| **Execution Mode** | |
| Execute Mode | Applies Config Change to the selected network resources. |
| Report Only Mode | Does not change resources but will run Compliance Checks only. |
| **Pre-Emptive Compliance Options**<br>**Note:** These options are only available if the user is a member of a group with Pre-Emptive compliance activities. | |
| Enable Pre-Emptive Compliance Checks | This option allows the user to disable Pre-Emptive validations only if the user's group has the 'Manage Work' activity. Users who do have this activity will not be able to change this setting. |
| Block Configuration Change if projected configuration contains compliance failures | If a compliance violation is found within the projected configuration then the configuration change will be blocked. |
| Block Configuration Change if projected configuration contains new compliance failures only | If a compliance violation is found within the projected configuration and the current configuration has no violations then the configuration change will be blocked. If both projected and current configurations have failures then the configuration change will not be blocked and changes will be made to the device. |
| Report Compliance Failure(s) only (Configuration change will not be blocked) | In execution mode 'execute' any compliance failure will be ignored and the changes will be applied to the device. In report only execution mode only the compliance checks will be run - the UOW finish after Pre-Emptive checks. |

8. The **Submit Configuration Change** wizard displays the Password Override dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

| *Table 51. Password Override dialog* | |
|---|---|
| **Field** | **Definition** |
| Override ITNCM Authentication | Select this check box to override the default authentication information. |
| Login Name | Provide the login name for the device you are accessing. |
| Password | Provide the password for the device you are accessing. |
| Enable Password | Provide the device enable password for the device you are accessing. |
| Only Use This Authentication | Select this check box if you will always use this authentication for your resource. |

9. The **Submit Configuration Change** wizard displays the Config Change dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

| *Table 52. Config Change dialog* | |
|---|---|
| **Field** | **Definition** |
| Force Directory Override | Make this selection to force the changes and override the database. |
| Disaster Recovery; Use Raw CLI | Provide the login name for the device you are accessing.<br>**Note:** If you are submitting a standard config, this field must be selected in order to proceed. Until it is selected, the **Next** button is greyed out. |

10. Only when submitting a draft configuration, the **Submit Configuration Change** wizard displays a second Config Change dialog. Use the following table as a guide to entering the appropriate information. After entering the requested information, click **Next**.

| *Table 53. Config Change (page 2 of 2) dialog* | |
|---|---|
| **Field** | **Definition** |
| Merge | Adds the config settings you have made to those currently on this network resource. Any settings currently on the Network Resource will remain intact. |
| Replace | Applies the changes required to make the configuration on the Network Resource the same as the configuration being submitted. Please be careful with this option as it may remove items off the Network Resource that are necessary for it to communicate. |

11. The **Submit Configuration Change** wizard displays the Execution Priority dialog. By default, all UOWs are submitted with a priority of Medium. Select the appropriate radio button for the required execution priority and then click **Next**.

12. The **Rollback Options** window displays, only if the support level of the configuration is SmartModel. If the support level is Standard, this dialog is not available. A Rollback can be requested in the event of a configuration change failure. The Rollback can be carried out for a single configuration change, or multiple configuration change. Using the following table as a guide, please enter the appropriate information requested. Select **Next** to proceed.

*Table 54. Rollback Options fields*

| Field | Definition |
|---|---|
| **How should Rollback on configuration change failure be handled?** | |
| No Rollback | Select this to turn off the rollback option. |
| Rollback | Select this to activate the rollback option. |
| Reload the configuration and reboot the device | This option will load the original configuration and reboot the device. |
| Use Modeled Rollback | This option will enable a rollback to a modeled configuration. |
| Click here to have Rollbacks verified | Select this checkbox to enable rollback verification. |

13. The **Submit Configuration Change** wizard displays the Schedule Work dialog. Select either immediate or scheduled execution. If you select scheduled execution, additional fields are displayed asking for the execution window. Provide the start date and time, and the end date and time for executing the work. From this dialog you can also specify a recurring schedule for the UOW.

    After making your selections, click **Next**.
14. The **Submit Configuration Change** wizard displays the Describe Work dialog. Type a description for your work and click **Finish**.

**Related tasks**

Creating resources
Use this procedure to create the following categories of resources from the Resource Browser: network, general, realm, and search set.

Discovering resources
Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

Importing resources
Use this procedure to manually import resources into the database.

Submitting units of work (UOWs)
The UOW submission wizard is displayed when a user submits a UOW.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## (VMware environment only) Importing a certificate for VMware

Use this procedure to import a certificate for VMware.

Read the following information before beginning this procedure:

- Perform this procedure only if you are running ESX devices in a VMware environment.
- It is necessary to run the certificate tool to import a certificate for VMware. Otherwise, the import of the head end device will fail.

Follow these steps to import a certificate for VMware into the database.

1. Select the certificate tool by launching VMware vSphere and connect to *IPaddress*/*hostname*.

   Where:

   - *IPaddress* — Specifies the IP address of the VMware client.
   - *hostname* — Specifies the name of the host computer on which the VMware client is running.
2. Select to login.

   A certificate window displays.
3. View and download the certificate.
4. Copy the certificate to the following directory:

   ```
   ncm-install-dir/cert
   ```

   Where:

   - *ncm-install-dir* — Specifies the directory on which you installed Netcool Configuration Manager.
5. Change to the following directory on the Netcool Configuration Manager server:

   ```
   cd install-dir/jre/bin
   ```

   Where:

   - *install-dir* — Specifies the directory on which you installed the JRE (Java runtime environment).Netcool Configuration Manager.
6. Using the downloaded certificate, execute the following command on the Netcool Configuration Manager server:

   ```
   ./keytool -import -file ncm-install-dir/cert/bfovm05again.cer
   -keystore install-dir/cert/vmware.keystore -alias qa
   ```

   Where:

   - *ncm-install-dir* — Specifies the directory on which you installed Netcool Configuration Manager.
   - `bfovm05again.cer` — Specifies the name of the certificate. Your name will most likely be different than the one shown here.
   - qa — Specifies the alias for the certificate. The alias must be different for each certificate that is installed.
7. Enter the password when prompted.
8. Restart Netcool Configuration Manager.

You can now import any head end devices.

**Related tasks**

Importing resources
Use this procedure to manually import resources into the database.

## Discovering resources

Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

Read the following information before beginning this procedure:

- General information
  - Management of the network using Netcool Configuration Manager requires network resources to be imported. Often, the VTMOS for a resource is unknown.
  - The Auto-Discovery tool in Netcool Configuration Manager "discovers" the VTMOS of each network resource, allowing the import to take place without prior knowledge of the VTMOS credentials. Either the IP address or the DNS name of the resource is used instead.

  - A rediscover option is also available. For more information, see “Rediscovering resources” on page 180.
- About discovering head end devices
  - The Auto-Discovery tool does not support the importing of head end devices.

    To import head end devices, see “Importing resources” on page 171.

Follow these steps to invoke the Auto-Discovery tool to import a resource into the database.

1. Select the Resource Browser in the navigation tree.
2. Navigate to the realm where you want to import the new resource.
3. Select **Tools** > **Discover**.

   The Network Resource Discovery wizard displays.
4. Select one of the fields from the **Password Override** wizard using the following table as a guide, and then click **Next**.

| Field | Description |
|---|---|
| **Override ITNCM Authentication** | Select this check box to override the default Netcool Configuration Manager authentication information. |
| **Login Name** | Provide the login name for the device you are accessing. |
| **Password** | Provide the password for the device you are accessing. |
| **Enable Password** | Provide the device enable password for the device you are accessing. |
| | Select this check box if you will always use this authentication for your resource. |

   The **Execution Priority** wizard displays. By default, all UOWs are submitted with an execution priority of Medium.
5. Choose the appropriate execution priority or leave the default selection, and click **Next**.

   The **Schedule Work** wizard displays.
6. Select the type of execution required, then click **Next**.

   **Immediate execution**
   Immediate execution invokes the execution instantaneously.

   **Scheduled execution**
   Scheduled execution allows the user to choose when execution takes place.

   Additional fields are displayed requesting start/end date and time for executing the work.

   The **Describe Work** wizard displays.
7. Enter a description for the UOW, so that it can be easily identified when it is revisited.
8. Click **Finish** when complete.

**Related tasks**

Creating resources
Use this procedure to create the following categories of resources from the Resource Browser: network, general, realm, and search set.

Deleting resources
Use this procedure to delete the following categories of resources: network, general, realm, and search set.

Rediscovering resources

Use this procedure to invoke the Auto-Discovery tool to import a resource into the database that has previously been discovered.

Importing resources
Use this procedure to manually import resources into the database.

Importing and making changes to resources in a single UOW
Use this procedure to manually import the current configuration for a resource into the database and make changes to it in a single unit of work (UOW).

Moving resources
Use this procedure to move the following categories of resources: network, general, realm, and search set.

Renaming resources
Use this procedure to rename the following categories of resources: network, general, realm, and search set.

Searching for resources
Use this procedure to invoke the Resource Browser and use the Search icon to search for resources.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Rediscovering resources

Use this procedure to invoke the Auto-Discovery tool to import a resource into the database that has previously been discovered.

Read the following information before beginning this procedure:

- General information
  - Management of the network using Netcool Configuration Manager requires network resources to be imported. Often, the VTMOS for a resource is unknown.
  - The Auto-Discovery tool in Netcool Configuration Manager 'discovers' the VTMOS of each network resource, allowing the import to take place without prior knowledge of the VTMOS credentials. Either the IP address or the DNS name of the resource is used instead.
  - If a network device previously fails to discover correctly, re-discover can be used to update the VTMOS information for that device.
  - If re-discover is used against an already successfully discovered device an import UOW is created.
- About discovering head end devices
  - The Auto-Discovery tool does not support the importing of head end devices.

    To import head end devices, see “Importing resources” on page 171.

Follow these steps to invoke the Auto-Discovery tool to import a resource into the database.

1. Select the Resource Browser in the navigation tree.
2. Navigate to the realm where the resource exists.
3. Select **Tools** > **Rediscover**.

   A warning message is displayed if the device has already successfully been discovered, stating that it will not change the VTMOS, but will generate an import UOW.
   The Network Resource Discovery wizard displays.
4. Select any additional network resources you would like to rediscover, and click **Next**.

   The Password Override wizard displays.
5. Opionally, select one of the fields from the **Password Override** wizard using the following table as a guide, and then click **Next**.

| Field | Description |
|---|---|
| **Override ITNCM Authentication** | Select this check box to override the default Netcool Configuration Manager authentication information. |
| **Login Name** | Provide the login name for the device you are accessing. |
| **Password** | Provide the password for the device you are accessing. |
| **Enable Password** | Provide the device enable password for the device you are accessing. |
| | Select this check box if you will always use this authentication for your resource. |

The **Execution Priority** wizard displays. By default, all rediscover UOWs are submitted with an execution priority of 'Low'.

6. Choose the appropriate execution priority, or leave the default selection, and click **Next**.

   The **Schedule Work** wizard displays.

7. Select the type of execution required, and click **Next**.

   **Immediate execution**
   Immediate execution invokes the execution instantaneously.

   **Scheduled execution**
   Scheduled execution allows the user to choose when execution takes place.

   Additional fields are displayed requesting start/end date and time for executing the work.

   The **Describe Work** wizard displays.

8. Enter a description for the UOW, so that it can be easily identified when it is revisited.
9. Click **Finish** when complete.

**Related tasks**

Discovering resources
Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

## Editing resources

Use this procedure to edit resources.

Read the following information before beginning this procedure:

- General information
  - You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
- About editing a resource
  - When you edit a resource, you are in fact editing the current configuration for that resource. The procedure described in this task is for editing the current configuration. This procedure eliminates the need to search for a resource, show all configurations for the resource, and then pick the current configuration to edit for the resource.
  - If a resource has no current configuration (that is, it serves as a placeholder and thus has never been imported into the database), the Configuration Editor displays an empty configuration.
- About editing a shortcut
  - As with any other resource, you can move, delete, or rename a shortcut, as long as you have the necessary security rights.

  - When you edit a shortcut, you actually edit the current configuration for the resource to which the shortcut points.
  - Before editing a shortcut, be sure to consider the ramifications for other users (as they may also have shortcuts pointing to the same resource).
- About editing realm properties
  - Each user can specify through Resource Browser Preferences which types of realms are shown. Thus, even if you change the properties of a realm to be “hidden,” users whose Resource Browser Preferences are set to view hidden realms will still be able to see the realm.
- About editing an SNMP device script
  - Standard Mode is also supported. In standard mode, a CLI text box (instead of the **Device Script** window) displays the SNMP device script information, for example, a list of the OIDs and their associated values.

Follow these steps to edit the following:

- Current configuration for a resource
- Current configuration for a shortcut
- Realm properties
- Newly created search set
- Existing search set
- Existing search set definition
- SNMP device script
- Native command sets for SNMP drivers
- Native command sets for non-SNMP drivers
- Change VTMOS on an unknown device

1. To edit the current configuration for a resource, follow these steps:
   a) Select the Resource Browser in the navigation tree.

      The Resource Browser displays.

   b) Search for the network resource you want to edit.
   c) Highlight the desired resource and select **Edit** > **Edit**, or alternatively right click on the resource and select **Edit**.

      The Configuration Editor displays the current configuration for the selected resource.
2. To edit the current configuration for a shortcut, follow these steps:
   a) Select the Resource Browser in the navigation tree.

      The Resource Browser displays.

   b) Highlight the desired shortcut and select **Edit** > **Edit**, or alternatively right click on the shortcut and select **Edit**.

      The Configuration Editor displays the current configuration for the resource to which the selected shortcut points.
3. To edit realm properties, follow these steps:
   a) Select the realm you want to modify.
   b) Select **File** > **Properties**.

      The **Realm Properties** dialog box displays. The **General** tab shows information about the realm, such as who created the realm and when the realm was last modified.

   c) Select the **Realm** tab.

      The **Realm** tab shows security information that applies specifically to the current user logged in. If you belong to multiple groups, the intersection of rights from each group is shown.

d) To change the visibility of the realm, select the appropriate radio button and then click **Apply**.

4. To edit a newly created search set, follow these steps:
   a) Highlight the new search set and right click and select **Edit**. Alternatively, select **File** > **Edit** from the menu bar.

      The new search set is opened in the XML editor window. A sample search set (commented out) is automatically added to each new search set to show you the proper syntax.

      This same editing window is used for editing security sets, access properties, and authentication resources.

   b) Make changes to the sample search set and remove the comment tags.
   c) Select **File** > **Save** and then close the XML editor.
5. To edit an existing search set, follow these steps:
   a) Select the Resource Browser in the navigation tree.

      The Resource Browser displays.

   b) Click the **Search** icon on the tool bar.

      The **Search Resources** form displays on the left side of the page.

   c) Search for the search set you want to edit.
   d) Rename, move, or delete the desired search set using the appropriate procedure.
6. To edit an existing search set definition, follow these steps:
   a) Select **File** > **Edit** from the menu bar.

      The existing search set is opened in the XML editor window.

   b) Make changes to the search set using the information in the Example section.
   c) Select **File** > **Save** and then close the XML editor.
7. To edit an SNMP device script, follow these steps:
   a) Select **Edit** > **Edit** from the Menu bar, or alternatively right click on the SNMP device script and select **Edit**.

      The **Device Script** window displays.

   b) Fill in the fields on the **Device Script** window using the following table as a guide.

| Field name | Description |
|---|---|
| **Object Name** | Specifies the replica of the configuration hierarchy. |
| **Object ID** | Specifies the OID associated with that object. The user must define which OID returns the device model, and which returns the device OS. |
| **Configuration** | When checked, this object will appear in the configuration. |
| **Hardware Inventory** | Specifies the parts of the MIB to appear in the hardware inventory. |
| **Ignore for Compare** | When performing a configuration compare, you can choose to omit certain objects from the comparison. Select this option to ignore MIBs on a configuration synchronization operation. |

8. To edit native command sets for SNMP drivers, follow these steps:
   a) Ensure that the selected driver is in SNMP mode.
   b) Use the following syntax to instruct the selected SNMP driver to set the `sysContact` attribute:

```
1.3.6.1.2.1.1.4.0=admin
sysContact.0=admin
sysContact=admin
```

c) Use the following syntax to instruct the selected SNMP driver to get the `sysContact` attribute in interrogation mode:

```
1.3.6.1.2.1.1.4.0
```

9. To edit native command sets for non-SNMP drivers, follow these steps:
   a) Ensure that the SNMP access type is enabled within the RAD, and the port element is set to 161.
   b) Access the XML format for the RAD, and add the following lines at the beginning of the SNMP access-type.

```
<snmp-version>2c</snmp-version>
<snmp-getbulk-max-reps>10</snmp-getbulk-max-reps>
<snmp-allow-oids-out-of-order>false</snmp-allow-oids-out-of-order>
```

   c) Use the following syntax to instruct the selected non-SNMP driver to set the `sysContact` attribute:

```
#snmpset 1.3.6.1.2.1.1.4.0 s=admin
```

   The SNMP datatype can be one of the following:

| SNMP datatype | Description |
|---|---|
| s | String |
| i | Integer |
| a | IP address |
| t | Time ticks |
| u | Unsigned integer |

   d) Use the following syntax to instruct the selected non-SNMP driver to get the `sysContact` attribute in interrogation mode:

```
#snmpget 1.3.6.1.2.1.1.4.0
```

10. To edit the VTMOS for an unknown device, follow these steps:
    a) The VTMOS for an unknown device will be displayed as *Unknown/Unknown/Unknown/Unknown*. Highlight the device in the Resource Browser.
    b) Then select **Edit** > **Modify Network Resource** from the menu bar.

       The network resource VTMOS is opened in the **Modify Network Resource** window.
    c) Make changes to the VTMOS as required.
    d) Select **OK** to save the changes you have made.

The following search set example shows the proper XML syntax to use for specifying an XPath and annotations:

```
<searchSet xmlns:ssm="http://www.example.com/ns/searchSetMarkup">
<xpath>/configuration/interface/*</xpath>
<annotation ssm:elementNameKey="INTERFACE_TYPE">
<xpath>/configuration/interface/*</xpath>
</annotation>
<annotation ssm:textValueKey="INTERFACE_NUMBER">
<xpath>/configuration/interface/*/ARG.001</xpath>
```

```
</annotation>
</searchSet>
```

In this example, the XPath notation specifies that the configurations with any type of interface should be searched and returned. For each configuration snippet that is returned, the annotations specify that two key/value pairs also be returned: the interface type and the interface number.

The following results indicate that one configuration was found, with an interface type of `Tunnel` and a value of 5:

```
<configuration xmlns:ssm="http://www.example.com/ns/searchSetMarkup">
<interface>
<Tunnel ssm:elementNameKey="INTERFACE_TYPE">
<ARG.001 ssm:textValueKey="INTERFACE_NUMBER">5</ARG.001>
</Tunnel>
</interface>
</configuration>
```

**Related tasks**

Editing resource XML
Use the XML editor to make it easier to edit XML files.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

# Editing resource XML

Use the XML editor to make it easier to edit XML files.

Read the following information before beginning this procedure:

- Much of the data used within Netcool Configuration Manager is in XML format. When working with the Resource Browser, you do not need to worry about the XML that forms resource configurations and command sets because the Configuration Editor translates the XML into easily editable GUI objects such as lists, fields, and check boxes.
- To create or edit security sets, authentication resources, and network resource access properties, however, you must work with the actual XML. To make working with the XML easier, a simple XML editor is used.

Follow these steps to use the XML editor to edit an XML file.

1. To view XML, right click on the resource and select **Resource Access** from the drop down menu.

   The XML editor displays the XML code associated with the selected resource.
2. Use breaks and spaces (tabs) to make the data in the XML file easier to read.

   **Note:** When working with XML, spaces and line breaks do not matter.
3. Check for errors.

   The simple XML editor checks for errors (for example, missing angle brackets). The XML editor provides the line number where the error occurs along with a brief description of the issue. The editor checks for well-formed XML only. You still need to ensure that all attribute names are correct.

   When you view an Authentication general resource (GR) that has a password or enable password making use of special characters (for example, the ampersand (&) in the Preview screen (**File** > **Preview**) or in XML format, the character will be displayed in its escaped form, that is, `&amp`.
4. When finished creating or editing an XML document, select **File** > **Save**.

The following example shows the XML code for a resource access general resource:

```
<?xml version="1.0" encoding="UTF-8"?><resource-access-data>
    <access-order>
        <name>telnet</name>
    </access-order>
```

```
    <rollback-options>
        <option name="NO_ROLLBACK">
            <description>No rollback</description>
            <required>false</required>
            <recommended>false</recommended>
        </option>
        <option name="MODELLED_ROLLBACK">
            <description>Use modelled rollback</description>
            <required>false</required>
            <recommended>true</recommended>
        </option>
        <option name="REBOOT_ROLLBACK">
            <description>Reload the configuration and reboot the device.
                    </description>
            <required>false</required>
            <recommended>false</recommended>
        </option>
    </rollback-options>
    <access-types>
        <access-type name="ssh">
            <script-id>ssh</script-id>
            <ssh-type>ssh1</ssh-type>
            <streaming-put-flag>false</streaming-put-flag>
            <streaming-get-flag>true</streaming-get-flag>
            <native-compare-flag>false</native-compare-flag>
            <import-prewrite-flag>true</import-prewrite-flag>
            <sync-prewrite-flag>true</sync-prewrite-flag>
            <import-report-diffs-flag>false</import-report-diffs-flag>
            <configDataType>CLI</configDataType>
            <reboot-on-config-load>true</reboot-on-config-load>
            <import-char-streaming-flag>false</import-char-streaming-flag>
            <import-char-streaming-time-interval>0
            </import-char-streaming-time-interval>
            <lbl-mode-flag-forncs>true</lbl-mode-flag-forncs>
            <user/>
            <password/>
            <enable-password/>
            <prev-user/>
            <alt-user/>
            <prev-password/>
            <alt-password/>
            <prev-enable-password/>
            <alt-enable-password/>
            <hostname/>
            <port>22</port>
            <ssh1>
                <cipher>des</cipher>
            </ssh1>
            <ssh2>
                <cipher>blowfish</cipher>
            </ssh2>
            <connectResponseTimeout/>
            <connectRetryDelay/>
            <maxResponseTimeout/>
            <ResponseTimeout/>
            <socketConnectTimeout/>
            <additional-errors/>
            <compareDeviceAndIntelliden>true
            </compareDeviceAndIntelliden>
            <finalConfigCompare>false</finalConfigCompare>
            <multipleConfigCompare/>
            <disableConfigChecksOnChanges>false
            </disableConfigChecksOnChanges>
            <retry-errors/>
            <retry-error-delay/>
            <max-error-retries/>
            <useOsUpgradeDefaultMethod>true</useOsUpgradeDefaultMethod>
        </access-type>
        <access-type name="telnet">
            <script-id>default</script-id>
            <ssh-type>none</ssh-type>
            <streaming-put-flag>false</streaming-put-flag>
            <streaming-get-flag>true</streaming-get-flag>
            <native-compare-flag>false</native-compare-flag>
            <import-prewrite-flag>true</import-prewrite-flag>
            <sync-prewrite-flag>true</sync-prewrite-flag>
            <import-report-diffs-flag>false</import-report-diffs-flag>
            <configDataType>CLI</configDataType>
            <reboot-on-config-load>true</reboot-on-config-load>
            <import-char-streaming-flag>false</import-char-streaming-flag>
            <import-char-streaming-time-interval>0
            </import-char-streaming-time-interval>
            <lbl-mode-flag-forncs>true</lbl-mode-flag-forncs>
            <user/>
            <password/>
            <enable-password/>
            <prev-user/>
            <alt-user/>
            <prev-password/>
            <alt-password/>
            <prev-enable-password/>
            <alt-enable-password/>
            <hostname/>
```

```
            <port>23</port>
            <ssh1>
                <cipher>des</cipher>
            </ssh1>
            <ssh2>
                <cipher>blowfish</cipher>
            </ssh2>
            <connectResponseTimeout/>
            <connectRetryDelay/>
            <maxResponseTimeout/>
            <ResponseTimeout/>
            <socketConnectTimeout/>
            <additional-errors/>
            <compareDeviceAndIntelliden>true
            </compareDeviceAndIntelliden>
            <finalConfigCompare>false</finalConfigCompare>
            <multipleConfigCompare/>
            <disableConfigChecksOnChanges>false
            </disableConfigChecksOnChanges>
            <retry-errors/>
            <retry-error-delay/>
            <max-error-retries/>
            <useOsUpgradeDefaultMethod>true</useOsUpgradeDefaultMethod>
        </access-type>
        <access-type name="snmp">
            <snmp-version>2c</snmp-version>
            <snmp-getbulk-max-reps>10</snmp-getbulk-max-reps>
            <snmp-allow-oids-out-of-order>false
            </snmp-allow-oids-out-of-order>
            <script-id>snmp</script-id>
            <ssh-type>none</ssh-type>
            <streaming-put-flag>false</streaming-put-flag>
            <streaming-get-flag>true</streaming-get-flag>
            <native-compare-flag>false</native-compare-flag>
            <import-prewrite-flag>true</import-prewrite-flag>
            <sync-prewrite-flag>true</sync-prewrite-flag>
            <import-report-diffs-flag>false</import-report-diffs-flag>
            <configDataType/>
            <reboot-on-config-load>true</reboot-on-config-load>
            <import-char-streaming-flag>false
            </import-char-streaming-flag>
            <import-char-streaming-time-interval>0
            </import-char-streaming-time-interval>
            <lbl-mode-flag-forncs>true</lbl-mode-flag-forncs>
            <user/>
            <password/>
            <enable-password/>
            <prev-user/>
            <alt-user/>
            <prev-password/>
            <alt-password/>
            <prev-enable-password/>
            <alt-enable-password/>
            <hostname/>
            <port>161</port>
            <ssh1>
                <cipher>des</cipher>
            </ssh1>
            <ssh2>
                <cipher>blowfish</cipher>
            </ssh2>
            <connectResponseTimeout/>
            <connectRetryDelay/>
            <maxResponseTimeout/>
            <ResponseTimeout/>
            <socketConnectTimeout/>
            <additional-errors/>
            <compareDeviceAndIntelliden>true
            </compareDeviceAndIntelliden>
            <finalConfigCompare>false</finalConfigCompare>
            <multipleConfigCompare/>
            <disableConfigChecksOnChanges>false
            </disableConfigChecksOnChanges>
            <retry-errors/>
            <retry-error-delay/>
            <max-error-retries/>
            <useOsUpgradeDefaultMethod>true
            </useOsUpgradeDefaultMethod>
        </access-type>
        <access-type name="alt-telnet">
            <script-id>alt-telnet</script-id>
            <ssh-type>none</ssh-type>
            <streaming-put-flag>false</streaming-put-flag>
            <streaming-get-flag>true</streaming-get-flag>
            <native-compare-flag>false</native-compare-flag>
            <import-prewrite-flag>true</import-prewrite-flag>
            <sync-prewrite-flag>true</sync-prewrite-flag>
            <import-report-diffs-flag>false</import-report-diffs-flag>
            <configDataType/>
            <reboot-on-config-load>true</reboot-on-config-load>
            <import-char-streaming-flag>false
            </import-char-streaming-flag>
            <import-char-streaming-time-interval>0
```

```
            </import-char-streaming-time-interval>
            <lbl-mode-flag-forncs>true</lbl-mode-flag-forncs>
            <user/>
            <password/>
            <enable-password/>
            <prev-user/>
            <alt-user/>
            <prev-password/>
            <alt-password/>
            <prev-enable-password/>
            <alt-enable-password/>
            <hostname>10.216.1.254</hostname>
            <port>2034</port>
            <ssh1>
                <cipher>des</cipher>
            </ssh1>
            <ssh2>
                <cipher>blowfish</cipher>
            </ssh2>
            <connectResponseTimeout/>
            <connectRetryDelay/>
            <maxResponseTimeout/>
            <ResponseTimeout/>
            <socketConnectTimeout/>
            <additional-errors/>
            <compareDeviceAndIntelliden>true
            </compareDeviceAndIntelliden>
            <finalConfigCompare>false</finalConfigCompare>
            <multipleConfigCompare/>
            <disableConfigChecksOnChanges>false
            </disableConfigChecksOnChanges>
            <retry-errors/>
            <retry-error-delay/>
            <max-error-retries/>
            <useOsUpgradeDefaultMethod>true
            </useOsUpgradeDefaultMethod>
        </access-type>
    </access-types>
    <scripts>
<script name="example-script"><![CDATA[ ### Defaults for sending commands.
Errors must be separated by , not spaces default.prompt=enable)
default.error=Error,Usage,Unknown command,Failed,must be in the range,
Cannot add,Invalid,must be less than,Feature not supported,Bad mod,
Unknown host,failed,VLAN number must be in the range,VLAN name and
state may be set default.errorResponse=Error sending command
### Connection Global # if connect.* is not present use connect.all.properties
connect.errorResponse=Unable to connect to router connect.01.if=name:
connect.02.then=send=$connect_username$ connect.03.elseIf=ogin:
connect.04.then=send=$connect_username$ connect.05.endIf
connect.06.wait=assword: connect.07.send=$connect_password$
connect.08.send=en connect.09.if=:
connect.10.then=send=$enable_password$
connect.11.endIf connect.12.wait=enable) connect.13.send=set
length 0 connect.14.wait=enable)  ### Get configuration
config.errorResponse=ciscoCat Configuration Error
# Info diag.01.send=show version diag.02.wait=enable)
diag.03.send=show module diag.end=enable)
# Model model.send=show version model.end=enable)
model.FIND-BEGIN=Model:  model.FIND-END=Serial # check for
Running config and stored config values multipleConfigs or
SingleConfig config.check.end=singleConfig
# copy Running config to stored copyRunning.01.send=
# Running config config.running.send=show config all config.running.end=
end config.running.FIND-BEGIN=#version  config.running.FIND-END=end
# Stored config config.stored.send=show config all config.stored.end=
end config.stored.FIND-BEGIN=#version  config.stored.FIND-END=end
# Version config.version.send=show version config.version.end=enable)
config.version.FIND-BEGIN=NmpSW:  config.version.FIND-END=
# Signals start of config config.start=!  # Signals end of config
config.end=end  # Identifies error retreiving config.
Errors must be separated by ,
not spaces config.fail=Error,Usage,Unknown command,Failed,must be in
the range,must be less than,Feature not supported
### Disconnect disconnect.errorResponse=Error disconnecting from device.
### Ftp file ftp.01.send=copy tftp config ftp.02.wait=?
ftp.03.send=$ftp_hostname$ ftp.04.wait=? ftp.05.send=$ftp_filename$
ftp.06.wait=? ftp.07.send=y ftp.08.wait=enable)  ### stream file
streamFile.01.sendData=$stream_input$ streamFile.02.wait=enable)
### Notify logged on users notify.message.send=$message$
### Directory dir.01.send=dir $dir_input$ dir.02.wait=)
### del del.01.send=del $del_input$ del.02.if=? del.03.then=send=y
del.04.endIf del.05.wait=enable)  ### Change directory cd.01.send=cd
$cd_input$: cd.02.wait=#  ### Squeeze directory squeeze.01.send=squeeze
$squeeze_input$: squeeze.02.wait=? squeeze.03.send=y squeeze.04.wait=?
squeeze.05.send=y squeeze.06.wait=enable)  ### Copy copyDown.01.send=copy
tftp flash copyDown.02.wait=? copyDown.03.send=$ftp_althostname$
copyDown.04.wait=? copyDown.05.send=$copy_input1$ copyDown.06.if=[bootflash]?
copyDown.07.then=send= copyDown.08.endIf copyDown.09.if=copy
to [ copyDown.10.then=send= copyDown.11.endIf copyDown.12.wait=?
copyDown.13.send=y copyDown.14.wait=enable) copyDown.15.sleep=5000
copyDown.16.send=verify $copy_input1$ copyDown.17.wait=enable)
### Erase erase.01.send=erase $erase_input$: erase.02.wait=?
erase.03.send=y erase.04.wait=#  ### reload reload.01.send=reset
```

```
reload.02.wait=? reload.03.send=y reload.04.sleep=240000]]&gt;</script>
    </scripts>
</resource-access-data>
```

You can edit another XML file by using this procedure.

**Related tasks**

Editing resources
Use this procedure to edit resources.

Using parameters in search sets
Use this procedure to specify parameters in a search set.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Applying search sets

Search sets enable you to search network resource configurations for specific command criteria. For example, using a search set you can quickly determine which CISCO routers in a particular realm have at least one `ntp server` with the `prefer` option. Another powerful use of search sets is to query a set of resources for the current values of certain elements, and then plug those values into one or more command sets. Use this procedure to specify how to apply a specified search set.

Read the following information before beginning this procedure:

- You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.

Follow these steps to specify how to apply the selected search set.

1. Select the Resource Browser in the navigation tree.

   Your resources display.
2. Select or search for a resource to which you want to apply a search set.
3. Select **Tools** > **Apply Search Set**.

   The **Select Search Sets** window of the **Apply Search Set** window displays.
4. Select the search set to apply and click **Next**.

   The **Select the Scope of Application** (Page 1 of 2) window displays. This filters devices based on their support level e.g, Standard, SmartModel.
5. Select how you want to apply the search set by selecting one of the radio buttons on the **Select the Scope of Application** (Page 1 of 2) window.

| If | Then |
|---|---|
| You selected **Apply the Search Sets to Network Resources in a Realm**. | Click **Next** and go to “Applying the search set to network resources in a realm” on page 190. |
| You selected **Apply the Search Sets to specific Network Resources**. | Click **Next** and go to “Applying the search set to specific network resources” on page 191. |
| You selected **Apply the Search Sets to the Network Resources retrieved from a Realm**. | Click **Next** and go to “Applying the search set to network resources retrieved from a realm” on page 193. |

**Related tasks**

Using parameters in search sets

Use this procedure to specify parameters in a search set.

**Related reference**

Resource types

Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Applying the search set to network resources in a realm

Use this procedure to apply a search set to network resources in a realm.

Read the following information before beginning this procedure:

- After you select the **Apply the Search Sets to Network Resources in a Realm** radio button, the **Select the Scope of Application** (Page 2 of 2) window displays.
- You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.

Follow these steps to apply the selected search set to network resources in a realm.

1. The **Select the Scope of Application** (Page 2 of 2) dialog displays. This filters devices based on their support level e.g, to display SmartModel only. Specify values for the fields displayed in the **Select the Scope of Application** (Page 2 of 2) window, using the following table as a guide:

| Field | Description |
|---|---|
| **Realm** | Select the Realm with any Name/VTMOS Filters for this Unit of Work. |
| **Include Sub-Realms** | Select this box to search all sub-realms. |
| **Name Filter** | Enter the name of the command set (maximum of 128 characters) for which you are searching. Trailing wild cards (*) are acceptable. Leave blank to search for all names. |
| **Vendor** | Select the vendor from the dropdown list. |
| **Type** | Select the resource type from the dropdown list. |
| **Model** | Select the model from the dropdown list. |
| **OS** | Select the OS version from the dropdown list. |

2. Click **Next**.

   The **Configure Failure Options** window displays.

3. Specify values for the radio buttons displayed in the **Configure Failure Options** window, using the following table as a guide:

| Radio button | Description |
|---|---|
| **Ignore All Errors** | Indicates that you do not want the UOW to stop processing, regardless of how many failures occur. |
| **Fail After Total Errors** | Select the maximum number of failures you want to occur before the UOW stops processing. |
| **Fail After Percent Errors** | Select the maximum percentage of failures you want to occur before the UOW stops processing. This option is useful when there are a large number of command sets being applied to a large number of resources. If your desired |

| Radio button | Description |
|---|---|
| | percentage does not equal a whole number, the number of failures necessary to cause termination is rounded up. For example, if you select 51% and there are two command sets and five resources, the formula is as follows:<br>`Max # of failures: (51/100) x (2x5) = 5.1 = 5` |

4. Click **Next**.

   The **Execution Priority** window displays. By default, all UOWs are submitted with a priority of medium.
5. Select the appropriate radio button for the priority needed and click **Next**.

   The **Schedule Work** window displays.
6. Select either immediate or scheduled execution. If you select scheduled execution, additional fields are displayed asking for the execution window. Provide the start date and time, and the end date and time for executing the work. From this dialog you can also specify a recurring schedule for the UOW.
7. Click **Next**.

   The **Describe Work** window displays.
8. Type a description for the unit of work and then click **Finish**.

You have completed the task of applying a search set to network resources in a realm.

**Related tasks**

Applying the search set to network resources retrieved from a realm
Use this procedure to apply a search set to network resources retrieved from a realm.

Applying the search set to specific network resources
Use this procedure to apply a search set to specific network resources.

Using parameters in search sets
Use this procedure to specify parameters in a search set.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Applying the search set to specific network resources

Use this procedure to apply a search set to specific network resources.

Read the following information before beginning this procedure:

- After you select the **Apply the Search Sets to specific Network Resources** radio button, the **Select the Scope of Application** (Page 2 of 2) window displays.
- You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.

Follow these steps to apply the selected search set to specific network resources.

1. The **Select the Scope of Application** (Page 2 of 2) dialog displays. This filters devices based on their support level e.g, to display SmartModel only. Specify values for the fields displayed in the **Select the Scope of Application** (Page 2 of 2) window, using the following table as a guide:

| Field | Description |
|---|---|
| **Realm** | Select the Realm with any Name/VTMOS Filters for this Unit of Work. |
| **Include Sub-Realms** | Select this box to search all sub-realms. |

| Field | Description |
|---|---|
| **Name Filter** | Enter the name of the command set (maximum of 128 characters) for which you are searching. Trailing wild cards (*) are acceptable. Leave blank to search for all names. |
| **Vendor** | Select the vendor from the dropdown list. |
| **Type** | Select the resource type from the dropdown list. |
| **Model** | Select the model from the dropdown list. |
| **OS** | Select the OS version from the dropdown list. |

2. Click **Next**.

   The **Configure Failure Options** window displays.
3. Specify values for the radio buttons displayed in the **Configure Failure Options** window, using the following table as a guide:

| Radio button | Description |
|---|---|
| **Ignore All Errors** | Indicates that you do not want the UOW to stop processing, regardless of how many failures occur. |
| **Fail After Total Errors** | Select the maximum number of failures you want to occur before the UOW stops processing. |
| **Fail After Percent Errors** | Select the maximum percentage of failures you want to occur before the UOW stops processing. This option is useful when there are a large number of command sets being applied to a large number of resources. If your desired percentage does not equal a whole number, the number of failures necessary to cause termination is rounded up. For example, if you select 51% and there are two command sets and five resources, the formula is as follows:<br>`Max # of failures: (51/100) x (2x5) = 5.1 = 5` |

4. Click **Next**.

   The **Execution Priority** window displays. By default, all UOWs are submitted with a priority of medium.
5. Select the appropriate radio button for the priority needed and click **Next**.

   The **Schedule Work** window displays.
6. Select either immediate or scheduled execution. If you select scheduled execution, additional fields are displayed asking for the execution window. Provide the start date and time, and the end date and time for executing the work. From this dialog you can also specify a recurring schedule for the UOW.
7. Click **Next**.

   The **Describe Work** window displays.
8. Type a description for the unit of work and then click **Finish**.

You have completed the task of applying a search set to specific network resources.

**Related tasks**

Applying the search set to network resources in a realm
Use this procedure to apply a search set to network resources in a realm.

Applying the search set to network resources retrieved from a realm

Use this procedure to apply a search set to network resources retrieved from a realm.

Using parameters in search sets
Use this procedure to specify parameters in a search set.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Applying the search set to network resources retrieved from a realm

Use this procedure to apply a search set to network resources retrieved from a realm.

Read the following information before beginning this procedure:

- After you select the **Apply the Search Sets to the Network Resources retrieved from a Realm** radio button, the **Select the Scope of Application** (Page 2 of 2) window displays.
- You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.

Follow these steps to apply the selected search set to network resources retrieved from a realm.

1. The **Select the Scope of Application** (Page 2 of 2) dialog displays. This filters devices based on their support level e.g, to display SmartModel only. Specify values for the fields displayed in the **Select the Scope of Application** (Page 2 of 2) window, using the following table as a guide:

| Field | Description |
|---|---|
| **Realm** | Select the Realm with any Name/VTMOS Filters for this Unit of Work. |
| **Include Sub-Realms** | Select this box to search all sub-realms. |
| **Name Filter** | Enter the name of the command set (maximum of 128 characters) for which you are searching. Trailing wild cards (*) are acceptable. Leave blank to search for all names. |
| **Vendor** | Select the vendor from the dropdown list. |
| **Type** | Select the resource type from the dropdown list. |
| **Model** | Select the model from the dropdown list. |
| **OS** | Select the OS version from the dropdown list. |

2. Click **Next**.

   The **Configure Failure Options** window displays.

3. Specify values for the radio buttons displayed in the **Configure Failure Options** window, using the following table as a guide:

| Radio button | Description |
|---|---|
| **Ignore All Errors** | Indicates that you do not want the UOW to stop processing, regardless of how many failures occur. |
| **Fail After Total Errors** | Select the maximum number of failures you want to occur before the UOW stops processing. |

| Radio button | Description |
|---|---|
| **Fail After Percent Errors** | Select the maximum percentage of failures you want to occur before the UOW stops processing. This option is useful when there are a large number of command sets being applied to a large number of resources. If your desired percentage does not equal a whole number, the number of failures necessary to cause termination is rounded up. For example, if you select 51% and there are two command sets and five resources, the formula is as follows:<br>`Max # of failures: (51/100) x (2x5)`<br>`= 5.1 = 5` |

4. Click **Next**.

   The **Execution Priority** window displays. By default, all UOWs are submitted with a priority of medium.
5. Select the appropriate radio button for the priority needed and click **Next**.

   The **Schedule Work** window displays.
6. Select either immediate or scheduled execution. If you select scheduled execution, additional fields are displayed asking for the execution window. Provide the start date and time, and the end date and time for executing the work. From this dialog you can also specify a recurring schedule for the UOW.
7. Click **Next**.

   The **Describe Work** window displays.
8. Type a description for the unit of work and then click **Finish**.

You have completed the task of applying a search set to network resources retrieved from a realm.

**Related tasks**

Applying the search set to network resources in a realm
Use this procedure to apply a search set to network resources in a realm.

Applying the search set to specific network resources
Use this procedure to apply a search set to specific network resources.

Using parameters in search sets
Use this procedure to specify parameters in a search set.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Using parameters in search sets

Use this procedure to specify parameters in a search set.

You need to understand the following format for specifying parameters in search sets:

```
${parametername=default value}$
```

For example:

```
“$SERVER_IP_ARG_NAME$”
```

Netcool Configuration Manager supports the use of parameters in Search Sets. Using the full parameter functionality, a user can set up a Search Set with a parameter rather than a defined value.

If any Search sets in your UOW contain parameters, you must assign an actual value to each parameter before the UOW can be submitted.

Follow these steps to specify parameters in a search set.

1. The global parameter option uses the XML editor to provide a value for each parameter. When a parameterized value has been entered in the editor, the wizard displays the **Global Parameters** window.
2. Select the parameter to set.
3. Type the value in the box at the bottom of the dialog.
4. Click **Next** when done to continue with the **Apply Search Set** wizard.

You have completed the task of specifying parameters in a search set.

**Related tasks**

Applying search sets
Search sets enable you to search network resource configurations for specific command criteria. For example, using a search set you can quickly determine which CISCO routers in a particular realm have at least one `ntp server` with the `prefer` option. Another powerful use of search sets is to query a set of resources for the current values of certain elements, and then plug those values into one or more command sets. Use this procedure to specify how to apply a specified search set.

Applying the search set to network resources in a realm
Use this procedure to apply a search set to network resources in a realm.

Applying the search set to network resources retrieved from a realm
Use this procedure to apply a search set to network resources retrieved from a realm.

Applying the search set to specific network resources
Use this procedure to apply a search set to specific network resources.

Editing resource XML
Use the XML editor to make it easier to edit XML files.

## Using configuration tags

Configuration tags are a way of attaching an extra description to any node within the configuration of a network resource.

Read the following information before beginning this procedure:

- You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
- A configuration tag is not an actual part of the configuration and is not stored on the network resource; it is only stored in the Netcool Configuration Manager database.
- Simply changing a configuration tag does not create a new version of the configuration.

It is a common practice for network engineers to place one or more identification keywords (or tags) within device configuration interface description fields for later reference. These tags can be used to associate the interface with a particular customer, or to refer to other commands within the configuration. Unfortunately, only one description field is available per interface, so tags must be stored in the same field. Furthermore, the majority of commands (at least for CISCO IOS) do not have any description field at all, so there is no way to assign tags to them.

Through the use of configuration tags, you can associate as many description tags as necessary to any element within a device configuration. The real power of configuration tags is that once they are attached to a device configuration, they can be referred to during configuration changes, command sets, search sets, and conformance checking. Please consult with the IBM Tivoli support staff for help in leveraging configuration tags; their use within search sets, command sets, and configuration changes is exposed only through the API.

**Related reference**

Resource types

Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Moving resources

Use this procedure to move the following categories of resources: network, general, realm, and search set.

Read the following information before beginning this procedure:

- General information
  - You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
- About moving a resource
  - Moving a resource implies that it already exists in the Netcool Configuration Manager database.
  - Moving a resource means moving it from one realm to another realm within the Netcool Configuration Manager database. All configurations associated with the resource are also moved.
  - You can move a resource only if you have the appropriate rights for each realm, and no work is currently scheduled for the resource.
  - Moving a resource causes no changes to be made to the actual resource.
- About moving a head end device
  - Moving a head end device does not result in a move of the associated head end managed devices (vswitches).

You use the Resource Browser to move all categories of resources in a similar manner. Follow these steps to move a resource.

1. Select the Resource Browser in the navigation tree.

   The Resource Browser displays.
2. Click the **Search** icon on the menu bar.

   The **Search Resources** form displays on the left side of the window.
3. Search for the resource you want to move.
4. Click to select and highlight the desired resource.

   **Note:** If the resource you want to move is a search set, use `<Ctrl> + Click` to select multiple search sets.
5. Select **Edit** > **Move** from the menu bar. Alternatively, right click on the resource and select **Move**.

   The **Move** dialog box displays.
6. Select the new location (realm) to which you want to move the resource, and then click **Move**.

   The resource and all its associated configurations are moved to the new realm.

You can move another resource by following the instructions in this procedure.

**Related tasks**

Creating resources
Use this procedure to create the following categories of resources from the Resource Browser: network, general, realm, and search set.

Discovering resources
Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

Importing resources
Use this procedure to manually import resources into the database.

**Related reference**

Resource types

Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Renaming resources

Use this procedure to rename the following categories of resources: network, general, realm, and search set.

Read the following information before beginning this procedure:

- General information
  - You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
  - Renaming a resource implies that it already exists in the Netcool Configuration Manager database.
- About renaming vswitches
  - Renaming a vswitch can be done using the Resource Browser and does not affect work flows. The renaming operation does not affect the real virtual device because Netcool Configuration Manager does not connect to the head end device and instruct it to rename the vswitch device internally. To rename a vswitch internally requires a configuration change on the head end device through a command set or a configuration edit.
  - It is possible to create a command set that renames a vswitch that is managed by some head end device. However, Netcool Configuration Manager prevents the vswitch from being renamed.
- About renaming realms
  - The realm is renamed, along with any realm paths that include the renamed realm. The following table shows an example of the impact of renaming a realm from `test/east` to `test/west`.

| Old name | New name |
|---|---|
| `test/east` | `test/west` |
| `test/east/core` | `test/west/core` |
| `test/east/edge` | `test/west/edge` |

  - The new realm name must be a unique name within the realm.

Follow these steps to rename a resource.

1. Select the Resource Browser in the navigation tree.

   The Resource Browser displays.
2. Click the **Search** icon on the menu bar.

   The **Search Resources** form displays on the left side of the window.
3. Search for the resource you want to rename.
4. Click to select and highlight the desired resource.
5. Select **Edit** > **Rename** from the menu bar. Alternatively, right click on the resource and select **Rename**.

   Your cursor is now active within the name field of the resource.
6. Type the new name for the resource and then click **Enter**.

   The name of the resource is changed.

You can rename another resource by following the instructions in this procedure.

**Related tasks**
Creating resources

Use this procedure to create the following categories of resources from the Resource Browser: network, general, realm, and search set.

Discovering resources
Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

Importing resources
Use this procedure to manually import resources into the database.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Deleting resources

Use this procedure to delete the following categories of resources: network, general, realm, and search set.

Read the following information before beginning this procedure:

- General information
  - You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
  - Deleting a resource implies that it already exists in the Netcool Configuration Manager database.
  - By removing a resource from the Netcool Configuration Managerdatabase, you move the resource and all its configurations to decommissioned status within the database. The resource is still part of your network, but you can no longer manage it with Netcool Configuration Manager.
  - You cannot remove a resource if there are any units of work for the resource pending in the system.
- About deleting realms
  - It is possible to delete a realm that contains another realm or network.
- About deleting head end managed devices
  - You cannot use this procedure to delete head end managed devices. Instead, you delete head end managed devices by using the Configuration Editor to edit the configuration of the head end device.
  - Deleting a head end managed device in the Configuration Editor deletes the specified head end managed device. The actual head end configuration is not affected and can be imported again at any time. The import operation recreates the deleted head end managed device.
- About deleting head end devices
  - Deleting a head end device causes all its head end managed devices (vswitches) to also be deleted. The actual head end configuration is not affected and can be imported again at any time.

You use the Resource Browser to delete all categories of resources in a similar manner. Follow these steps to delete a resource.

1. Select the Resource Browser in the navigation tree.

   The Resource Browser displays.
2. Click the **Search** icon on the menu bar.

   The **Search Resources** form displays on the left side of the window.
3. Search for the resource you want to rename.
4. Click to select and highlight the desired resource. You can use `<Ctrl> + Click` to select multiple resources.
5. Select **Edit** > **Delete** from the menu bar. Alternatively, right click on the resource and select **Delete**.

   The **Delete** dialog box displays.
6. Verify that the correct resource is shown, and click **Next**.

The **Describe Work** window displays.

7. Type a description for the UOW (unit of work) and click **Finish**.

   The specified resource is deleted.

You can delete another resource by following the instructions in this procedure.

**Related concepts**

Overview of the Configuration Editor
The Configuration Editor is an applet used for viewing and editing configurations and command sets.

**Related tasks**

Creating resources
Use this procedure to create the following categories of resources from the Resource Browser: network, general, realm, and search set.

Discovering resources
Use this procedure to invoke the Auto-Discovery tool to import a resource into the database.

Importing resources
Use this procedure to manually import resources into the database.

**Related reference**

Resource types
Use this information to understand the available resource types on which Netcool Configuration Manager operates.

## Deleting resources

Use this procedure to delete the following categories of resources: network, general, realm, and search set.

Read the following information before beginning this procedure:

- General information
  - You should understand the meaning of the different categories of resources that Netcool Configuration Manager manipulates.
  - Deleting a resource implies that it already exists in the Netcool Configuration Manager database.
  - By removing a resource from the Netcool Configuration Managerdatabase, you move the resource and all its configurations to decommissioned status within the database. The resource is still part of your network, but you can no longer manage it with Netcool Configuration Manager.
  - You cannot remove a resource if there are any units of work for the resource pending in the system.
- About deleting realms
  - It is possible to delete a realm that contains another realm or network.
- About deleting head end managed devices
  - You cannot use this procedure to delete head end managed devices. Instead, you delete head end managed devices by using the Configuration Editor to edit the configuration of the head end device.
  - Deleting a head end managed device in the Configuration Editor deletes the specified head end managed device. The actual head end configuration is not affected and can be imported again at any time. The import operation recreates the deleted head end managed device.
- About deleting head end devices
  - Deleting a head end device causes all its head end managed devices (vswitches) to also be deleted. The actual head end configuration is not affected and can be imported again at any time.

You use the Resource Browser to delete all categories of resources in a similar manner. Follow these steps to delete a resource.

1. Select the Resource Browser in the navigation tree.

The Resource Browser displays.

2. Click the **Search** icon on the menu bar.

   The **Search Resources** form displays on the left side of the window.
3. Search for the resource you want to rename.
4. Click to select and highlight the desired resource. You can use `<Ctrl> + Click` to select multiple resources.
5. Select **Edit** > **Delete** from the menu bar. Alternatively, right click on the resource and select **Delete**.

   The **Delete** dialog box displays.
6. Verify that the correct resource is shown, and click **Next**.

   The **Describe Work** window displays.
7. Type a description for the UOW (unit of work) and click **Finish**.

   The specified resource is deleted.

You can delete another resource by following the instructions in this procedure.

# Chapter 4. Managing network compliance

Use this information about Netcool Configuration Manager to perform network compliance management tasks.

## Compliance overview

Netcool Configuration Manager compliance management functionality focuses on the early detection and remediation of network vulnerabilities associated with compliance violations.

### Total network compliance

Compliance management provides a flexible application framework to ensure network compliance for regulatory, security and operational requirements. Network device configuration is continuously monitored against a set of predefined network policies to highlight devices that are violating compliance configuration rules.

### Completing the compliance life cycle

Netcool Configuration Manager's compliance management functionality completes the compliance process loop by defining compliance policy, running validations on the active network configuration, and automating the remediation activities of compliance violations. The solution captures device configuration changes as they occur and automatically initiates device level compliance checks to instantly detect compliance violations, which can then trigger remedial actions to bring devices back into compliance.

### Linking business and IT

Compliance management allows users to aggregate the network level implementation of a compliance policy to an easy-to understand graphical representation of the business rule that is supported. This capability allows organizations to create a bridge between the business requirements driven by Service Level Agreements and regulatory frameworks on one side to the implementation of these requirements via the network configuration. The application also contains a set of reports targeted at the various interested parties that provide each of these user communities with the relevant compliance information at the appropriate level of detail.

### Compliance management benefits

Netcool Configuration Manager's compliance management solution provides several unique benefits to network-driven organizations. It provides a unified solution for managing total network compliance needs. It provides an important bridge between business groups-who require the network to be compliant with mandates and service level agreements-and the network group, which is responsible for implementing the necessary compliance policies. It also provides a flexible and intelligent way to regain control in a complex network environment. It eliminates configuration errors that cause network disruptions thereby enhancing network stability, reliability, and availability. It improves operational efficiency by eliminating costly time-consuming and error prone manual processes. It speeds up the discovery and resolution of configuration-related vulnerabilities, improving network security. And finally, its continuous monitoring and enforcement approach mitigates the risk of non-compliance.

### System Architecture

The compliance management functionality is provided as a component of Netcool Configuration Manager. It can be deployed on a separate server to optimize performance, allowing customer deployment of Netcool Configuration Manager to be scaled independently to meet specific usage and network size requirements.

**Related tasks**

Applying policies (via wizard)
Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

## Compliance entities

Compliance Administration refers to the management of compliance entities which require configuration in order for the Netcool Configuration Manager compliance functionality to execute correctly. In addition Compliance Administration describes the relationship between each of these entities. Compliance entities encompass the compliance process, compliance policy, compliance definition, compliance rule, and the corrective action.

Each compliance entity has an important role to play in the compliance validation process:

**Event**
An event triggers a compliance validation process to run.

**Compliance Process**
A compliance process coordinates the execution of all regularly scheduled compliance validations, and can also be used for the ad-hoc validation of a group of policies. A ompliance process can be triggered by a number of different events.

**Compliance Policy**
A compliance policy specifies conditions that the devices must adhere to. A compliance policy describes the validation process in English rather than configuration lines.

**Compliance Definition**
Compliance definition captures the actual device configuration expected on the device.

**Compliance Rule**
A compliance rule allows the user to combine multiple compliance definitions to build the full validation, to which a device must adhere in order to pass a compliance test.

**Compliance Extraction**
A compliance extraction has the ability to extract chunks of data from a native/modelled configuration or a show command.

**Corrective Action**
A corrective action may be defined for a policy or rule, and specifies the action to be taken if a specific device violates the policy.

**Policy Exemption**
A policy exemption is available in the event that a device or a number of devices should temporarily be excluded from the execution of a policy.

All of the compliance entities can be maintained in the same way using the Administration Panel, which is available by right-clicking on any entity type. A drag-and-drop functionality is also available to speed up the process of moving a compliance entity from one folder to another.

**Related tasks**

Applying policies (via wizard)
Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

## Launching the Compliance UI

The Compliance UI can be launched using Java WebStart or the DASH.

1. Launch the Compliance UI using one of the following procedures:
   - Launch the Compliance UI using Java Web Start.

Use the following syntax: `http://IP of server ITNCM-Compliance installed on:port`. A working example may look like : `http://192.168.20.83:16310/`

- Launch the Compliance UI from the DASH.
  Click **Configuration Management** > **Client Portal** > **Compliance**.

The login screen is displayed.

2. Enter the following information:
   - Login name
   - Password.
   - Compliance server IP address
   - Web server HTTP port
3. Optional: If you want to use SSL to login, select the `Secure` checkbox.

# Compliance UI

The Compliance UI displays a series of icons at the top of the screen.

## General Compliance UI fields and icons

The following list describes the general Compliance UI fields and icons. The icons that are visible depend on which tab is currently being viewed. For procedures describing the tasks performed here, see the related links.

**Search**
Click to search policies.

**Help**
Click to display the User Assistance.

**Refresh**
Click to refresh page.

**Back**
Click to go back one screen.

**Forward**
Click to go forward one screen.

**Up one directory level**
Click to go up one directory level.

**Table preferences**
Click to set table preferences.

**Calendar**
Click to set the date.

**Device Tree View**
Click to display greater results details.

**Show/Hide the navigation tree**
Click to show or hide the navigation tree.

**Show/Hide the VTMOS tree**
Click to show or hide the VTMOS tree.

**Create New Policy Definition**
Click to create new policy definition.

**Disable Policy Definition**
Click to disable selected policy definition.

**Delete Policy Definitions** 
Click to delete selected policy definition.

**Policy Exemptions** 
Click to display the policy exemption wizard.

**Policy Definitions** 
Click to display a drop down menu with compliance entities to choose from.

**Results finished** 
Click to display only finished results.

**Results running** 
Click to display only running results.

**Results scheduled** 
Click to display only scheduled results.

**Result Panel View** 
Click to display a drop down menu with various views of results.

## Table preferences

The Table Preferences option allows for modifications to the table currently being viewed. The tables can be adjusted in terms of content display and column size.

When selected, the table preferences option populates the field names of the table currently in view. Fields can be hidden or displayed depending on your preference. The column size is adjusted when a field is hidden or displayed. The Reset Sizes, Reset View and Reset All options all retrieve the default view.

## Invalid characters

There are several characters that are not allowed for certain data fields within Netcool Configuration Manager - Compliance. If you try to include one of these characters in a field that does not allow the characters, an error dialog box is displayed and your data will not be saved. The following list identifies that are not allowed for certain data fields:

- “ (double quote)
- |(pipe)
- \ (back slash)
- / (forward slash)
- < (less than)
- > (greater than)
- % (percent sign)
- & (ampersand)
- = (equals)

## Required fields

Throughout the Netcool Configuration Manager - Compliance user interface, mandatory fields are indicated by an asterisk (*) at the end of the field name. Progression to the next screen is not permitted if a mandatory field is not completed.

## Shortcut keys

Within the user interface there are a number of short cut keys which can be used to save time to access certain modules.

The following table describes some of the main shortcuts available through the user interface.

*Table 55. Main shortcuts*

| Short Cut | Description |
|---|---|
| F1 | Invokes on line help |
| Alt + F | Opens the File menu |
| Alt + C | Opens the Create menu |
| Alt + T | Opens the Parameter menu |
| Alt + A | Opens the Admin menu |
| Alt + H | Opens the Help menu |

## Closing the Compliance UI

There are two options for closing the Netcool Configuration Manager - Compliance UI. The user may logout or quit.

This task describes how to close out the Netcool Configuration Manager - Compliance UI.

1. To log out of the Netcool Configuration Manager - Compliance application, simply select File | Logout. This will log the current user out of Netcool Configuration Manager - Compliance, and will present the login screen again. This may be used when another Netcool Configuration Manager - Compliance user wishes to login on the same machine. Alternatively, this may be used when security settings have been modified and the current user wishes to enforce the new security privileges on the account.
2. The user also has the option to terminate Netcool Configuration Manager - Compliance, which will fully close down the Netcool Configuration Manager - Compliance application and all it's associated programs/processes. This can be achieved by selecting File | Quit.

# Compliance searches

The search function provides the ability to locate compliance entities and network resources using a criterion-based user interface. This can be used for a single device search or multiple devices using the same search criterion. This is particularly useful when there are a large number of compliance entities or resources on the network.

If the search is submitted successfully, the search results are visible in the foreground. A count of the results returned is also available at the bottom left hand corner of the screen in the information bar. This also indicates is the search was unsuccessful, and displays `No Results Found`.

There are a number of searches that can be conducted on devices, policy definitions and executions.

## Searching for devices

Searches may be performed on column names which appear in the devices tab. The devices search is invoked by clicking on the search icon. The Search By Column screen appears on the left hand side of the user interface.

The following procedure outlines how to search for devices

1. There are drop-down menus beside each column name. To search for a particular value, you must first choose the column you wish to conduct a search on.
2. Enter the value you wish to search for, e.g to retrieve all Cisco devices, you would enter "Cisco" in the Vendor column. Alternatively, select the asterisk (*) to return all database entries for that particular column.
3. Then select the "Search" icon at the bottom of the screen.

4. The drop-down list does not populate values already in the column. However, once a value has been searched for, that value will auto-populate into the appropriate column so that it can be searched for again.
5. Combinations of search criteria may be used. This type of search is particularly useful where there are a large number of network resources, as it helps to refine the criteria being searched for.

**Related tasks**

Creating a compliance process
Use this procedure to define a new Compliance Process. Defining a new Compliance Process requires access to the User Interface wizard.

Editing a compliance process
Use this procedure to modify an existing Compliance Process. Modifying a new Compliance Process requires access to the User Interface wizard.

## Searching for policy definitions

Searches may be performed on all Compliance Entities created. The Policy Definitions search is invoked by clicking on the search icon. The Search By Entity screen appears on the left hand side of the user interface.

A search on Process and Policy entity is available. Please note that the field listing you may search on differs with each Entity selection.

The following procedure outlines how to search for definitions.

1. To search for a particular value, you must first choose the field you wish to conduct a search on.
2. Enter the value you wish to search for, e.g to retrieve all Cisco devices, you would enter "Cisco" in the Vendor field. Alternatively, select the asterisk (*) to return all database entries for that particular field.
3. Then select "Search" icon at the bottom of the screen.
4. The drop-down list does not populate values already in the field. However, once a value has been searched for, that value will auto-populate into the appropriate field so that it can be searched for again.
5. Combinations of search criteria may also be used. This type of search is particularly useful where there are a large number of network resources, as it helps to refine the criteria being searched for.

## Searching for executions

Searches may be performed on all columns which appear in the Execution tab. The Execution search is invoked by clicking on the search icon. The Search By Column screen appears on the left hand side of the user interface

A search on Process and Device view are available. Please note that the field listing you may search on differs with each Entity selection.

The following procedure outlines how to search for executions

1. To search for a particular value, you must first choose the column you wish to conduct a search on.
2. Enter the value you wish to search for, e.g to retrieve all Cisco devices, you would enter "Cisco" in the Vendor column. Alternatively, select the asterisk (*) to return all database entries for that particular column.
3. Then select "Search" icon at the bottom of the screen.
4. The drop-down list does not populate values already in the column. However, once a value has been searched for, that value will auto-populate into the appropriate column so that it can be searched for again.

## Searching for device configurations

Searches can also be conducted on device configurations: Search using native CLI configuration lines, Search using native commands and Search using device models.

This task describes how to search for device configurations.

**Search using native CLI configuration lines:** CLI can be used alongside evaluation criteria to match CLI configuration lines against the device configuration stored in Netcool Configuration Manager - Compliance. The evaluation criteria can be used to determine whether all, any, one or none of these CLI configuration lines are present in the configuration., e.g no cdp run, no ip bootp server. Please refer to: Managing Compliance Definitions for further information on executing show commands.

**Search using native commands:** The device settings can be evaluated and searched by executing native (show) commands against the device. A show command can be executed against the device to retrieve specific information, e.g. show version, show config. Show commands are executed via Netcool Configuration Manager - Base, and the feedback read intoNetcool Configuration Manager - Compliance. Please refer to: Managing Compliance Definitions for further information on executing show commands.

**Search using device models:** Device settings can be searched for specific lines or fragments of device configuration using device models. Modelled definitions are based on XPaths. An XPath is a search mechanism used in XML. Please refer to: Managing Compliance Definitions for further information on executing show commands.

**Related tasks**

Creating compliance definitions using native CLI configuration lines
A compliance definition may contain one or more native command lines (CLI) and use evaluation criteria to match these CLI lines against the device configuration stored in ITNCM-Compliance, which are automatically synchronized from ITNCM - Base each time the configuration changes. Use this procedure to create compliance definitions using native CLI configuration lines.

Creating compliance definitions using native commands
Compliance definitions may contain a native (show) command that can be issued against the device to retrieve specific information from the device that is not available in the configuration itself. These definitions contain not only the native command that must be issued to the device, but also define the results that should (or should not) be present in the information returned from the device. Use this procedure to create compliance definitions using native commands.

Creating compliance definitions using device models
Modeled definitions are based on modeled device configurations. Modeled definitions are all based on XPaths. An XPath is a search mechanism used in XML, and models an XML document as a tree of nodes. Use this procedure to create Compliance Definitions using device models.

# Viewing device configurations

There are a number of options available for viewing device configurations. They can be viewed as Native Commands, Stored 'Show' Commands, or Modelled Configurations (for smart model devices).

This task describes how to view device configurations. These options are available by performing a right click operation on the required device(s).

- **Display Native Commands** Native Commands display the entire configuration for this device, and may be useful in creating rules or definitions. This displays the entire device configuration. Note, that configurations with more than 10,000 lines will be presented through pages with up to 10,000 configuration lines each.
- **Display Stored “Show” Commands** The Stored “Show” Commands option allows the user to view stored ‘show' commands retrieved from the device on the last configuration change, such as, for example, show version.
- **Display Modelled Config** The Modelled Configuration option gives the user the ability to display the modelled config.

  **Note:** Modelled configurations with more than 10,000 lines will be not be displayed.

**Note:** The 'Display modelled config' option will be enabled only for smart model devices.

**Related tasks**

Viewing results
Netcool Configuration Manager - Compliance will run the validation of devices against policies and generate the validation results. All results across all validations will be stored in the Netcool Configuration Manager - Compliance database, and are available for review by the user until they are removed through house keeping.

Viewing detailed results
The Results page gives the user access to compliance validation results based on their level of security. There are a number of different views in the Results tab, where validation results can be viewed and analyzed.

# Exporting devices

The user has the ability to export devices to a user defined location in csv format.

This task describes how to export devices into csv format.

1. Right click on the required device(s).
2. Choose ‘Export All' or ‘Export Selected' devices into csv format. These options provide the user with the ability to export the devices to a pre-defined location in csv format.

**Related tasks**

Exporting policy results
You can export single or multiple policies results and save them as a CSV file.

# Viewing pre-emptive policies and results

Use the pre-emptive compliance functionality to check proposed configuration changes to a device against predefined compliance policies for that device. Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device. The capability is intended to enable customers to evaluate the impact of configuration changes against predefined compliance policies for a device.

It can be useful to quickly view which pre-emptive policies are linked to a particular device. To view pre-emptive policies, you must first configure them and set up device associations.

You can view the pre-emptive policies that have been defined for a device from the Devices tab of the Netcool Configuration Manager - Compliance user interface. You can also access pre-emptive compliance results from both the Queue Manager and the Resource Browser.

1. To view the pre-emptive policies that have been defined for a device on the Netcool Configuration Manager - Compliance Devices tab, perform the following actions:
   a) Right-click the device to select it.
   b) Select **View Pre-emptive Policies for device**.

   A dialog displays a list of the applicable pre-emptive policies.
2. To view pre-emptive policy results form the Queue Manager, perform the following actions:
   a) Select the unit of work (UOW) in the Queue Manager from either the 'Work That is Finished' or the 'Work Pending Approval' column (if approvals are enabled).
   b) Select the Resources tab, and choose a device from the Resource list.

   The pre-emptive compliance policy results are displayed on the following two tabs:

   **Work log**
   The Work log shows the pre-emptive compliance result for both the current configuration and the projected configuration.

   **Pre-emptive Compliance**
   Shows the pre-emptive compliance results.

3. To view pre-emptive policy results form the Resource Browser, perform the following actions:
   a) Right-click the device to select it.
   b) Select the UOW from the Work tab.

   The pre-emptive compliance policy results are displayed on the following two tabs:

   **Audit log**
   The Audit log displays the pre-emptive compliance result for both the current configuration and the projected configuration.

   **Pre-emptive Compliance**
   Shows the pre-emptive compliance results for ‘Apply Command set' and ‘Submit configuration work types'.

   You can drill down into the Validation detail by double-clicking on the individual policy, or by selecting the **Policy** row and then clicking **View Policy Result Detail**.

**Related tasks**

Creating pre-emptive policies
Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device, allowing you to evaluate the impact of configuration changes against pre-defined compliance policies for a device. In order to run a pre-emptive compliance, you first create or modify existing policies to make them suitable for execution in a pre-emptive manner. You then create a compliance process to apply the pre-emptive policy to a device.

Viewing results
Netcool Configuration Manager - Compliance will run the validation of devices against policies and generate the validation results. All results across all validations will be stored in the Netcool Configuration Manager - Compliance database, and are available for review by the user until they are removed through house keeping.

Viewing detailed results
The Results page gives the user access to compliance validation results based on their level of security. There are a number of different views in the Results tab, where validation results can be viewed and analyzed.

Applying policies (via wizard)
Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

# Defining network compliance policies

You create compliance policies and define how they are applied using the Netcool Configuration Manager user interface.

## Compliance policies overview

Use this information to obtain an overview of the Compliance Administration section of the Netcool Configuration Manager - Compliance UI. The overview provides the relationships between the compliance entities.

### Entities interaction and process flow

Compliance Administration refers to the management of compliance entities that require configuration in order for the Netcool Configuration Manager compliance functionality to execute correctly. In addition, Compliance Administration describes the relationship between each of the following compliance entities:

- Compliance process
- Compliance policy
- Compliance definition

- Compliance rule
- Compliance action

Each of the compliance entities has an important role to play in the compliance validation process:

- An event triggers a compliance validation process to run.
- A compliance process coordinates the execution of all regularly scheduled compliance validations, and can also be used for the ad-hoc validation of a group of policies. A compliance process can be triggered by a number of different events.
- A compliance policy specifies conditions that the devices must adhere to. A compliance policy describes the validation process in English rather than configuration lines.
- A compliance definition captures the actual device configuration expected on the device.
- A compliance rule allows the user to combine multiple compliance definitions to build the full validation, to which a device must adhere in order to pass a compliance test.
- A compliance extraction has the ability to extract chunks of data from a native/modelled configuration or a show command.
- A corrective action may be defined for a policy or rule, and specifies the action to be taken if a specific device violates the policy.
- A policy exemption is available in the event that a device or a number of devices should temporarily be excluded from the execution of a policy.

All of the compliance entities can be maintained in the same way using the **Administration** window, which is available by right-clicking on any entity type. A selection of folders is displayed for each entity type. For example, right-clicking the compliance policy entity displays the following folders:

- Open Policy
- Edit Policy
- Rename Policy
- Copy Policy
- Move Policy
- Exemptions
- Disable Policy
- Delete Policy

A-drag-and-drop functionality is also available to speed up the process of moving a compliance entity from one folder to another.

## Compliance process

Compliance processes are a key element of compliance management. Processes are the execution vehicle for all regularly scheduled compliance validations, and can also be used for the ad-hoc validation of a group of policies. A compliance process can contain one or more compliance policies, and can be triggered by a number of different events:

**On-demand initiation by a user**
An example of this trigger occurs when a user selects a process in the execution tabs and clicks the **Execute** icon .

**Scheduled initiation at a predefined one-off or recurring time**
An example of this trigger occurs when a user schedules a process to run all security policies every morning at 5 AM.

**Automatic initiation after synchronization**
Automatic initiation after a new device configuration has been synchronized.

You can perform the following tasks associated with a compliance process:

**Create a compliance process**
For more information, see “Creating a compliance process” on page 9

**Edit a compliance process**
For more information, see “Editing a compliance process” on page 217

## Compliance policy

A compliance policy stipulates conditions that the devices must adhere to. A compliance policy contains compliance rules and can be configured to send a notification or an email action in the event that a policy fails. Compliance policies can cover all devices in an entire network, a subset of devices or a specific device. A compliance policy describes the validation process in English rather than configuration lines.

You can perform the following tasks associated with a compliance policy:

**Create a compliance policy**
For more information, see “Creating a compliance policy” on page 219.

**Edit a compliance policy**
For more information, see “Editing a compliance policy” on page 221.

**Create a compliance policy exemption**
For more information, see “Creating a compliance policy exemption” on page 223.

**Create a preemptive policy**
For more information, see “Creating pre-emptive policies” on page 224.

## Compliance definition

Compliance definitions capture the device characteristics that must be validated as part of a specific policy. The device settings can be evaluated using the stored device configuration (both CLI and XML configuration representations can be used), or by executing show commands against the device The scope of a compliance definition may range from a single configuration line that must evaluated to a complex evaluation of multiple configuration snippets with regular expression logic and parameters.

There are four different compliance definition formats to choose from:

**Compliance definition using native CLI configuration lines**
A compliance definition may contain one or more native command lines (CLI) and use evaluation criteria to match these CLI lines against the device configuration stored in the compliance database, which are automatically synchronized each time the configuration changes. The evaluation criteria set as part of this type of a compliance definition define whether the CLI lines are or are not expected to be present in the device configuration. When multiple configuration snippets have been defined, the evaluation criteria can also be used to define whether all, any, one or none of these snippets must be present in the configuration. Examples of evaluations which could be used are: no cdp run, no ip bootp server.

**Compliance definition using native commands**
Compliance definitions may contain a native (show) command that can be issued against the device to retrieve specific information from the device that is not available in the configuration itself. These definitions contain not only the native command that must be issued to the device, but also define the results that should (or should not) be present in the information returned from the device. The show commands are executed against the device(s) via Netcool Configuration Manager - Base, and the response read into Netcool Configuration Manager - Compliance. Using the evaluation criteria as described before, the response from the show command is evaluated against the expected results defined in the definition.

**Note:** Compliance definitions that contain native CLI can be used only to compare against the running configuration.

**Compliance definition using a device model**
Modeled definitions are based on modeled device configurations. Modeled definitions are all based on XPaths. An XPath is a search mechanism used in XML, and models an XML document as a tree of nodes. There are different types of nodes, including element nodes, attribute nodes and text nodes.

Direct XPaths and Contextual XPaths are supported in definitions. A Direct XPath is used in a simple definition, where only one entity is being searched for. A Contextual XPath should be used in more complex compliance policies, for example to loop through all FastEthernet interfaces defined on a device.

**Compliance definition using a script**

Compliance definitions can be created using JavaScript. Script-based definitions allow the user to compose their own validation logic and hence are in full control of what they are trying to validate.

For more information on using scripts, see “Compliance definitions scripting” on page 245.

## Compliance rules

Compliance rules enable the user to combine multiple compliance definitions to build the full validation to which a device must adhere in order to pass a compliance test. Each compliance definition in a rule constitutes a Boolean logic validation with a 'True' or 'False' outcome. By connecting different definitions a user can define 'And' and 'Or' logic between those definitions. A compliance Rule also defines the device applicability of the rule and its underlying compliance definition components, as well as the remedial action that must be executed when a device is found that violates the rule. The entire rule logic of a compliance Rule can be viewed at a glance. Therefore, it is easy to determine how the Rule works, how to isolate problems, and identify areas for improvement or expansion. The triggering event, decision points and the end point of the procedure can all be defined using the drag and drop graphical user interface (GUI) environment. The GUI environment consists of a work pane where the compliance Rule is built, and resource pane from where the user can select the steps and decision points required.

The rule begins with the "Start" node, and then moves on to the "Definition" node. At this point the outcome of the definition chosen may be either T (True) or F (False). If the result of this definition is T, the device is deemed to be compliant. Else, it is considered to be noncompliant, and may then be associated with a corrective action to bring back into compliance.

## Compliance action

Netcool Configuration Manager - Compliance simplifies the task of ensuring policy compliance, by enabling users to improve the detection of network vulnerabilities. When a compliance violation has been identified, remedial action processes may be used to correct device configurations or informational actions can be used to alert the appropriate personnel of the compliance violation. A compliance violation is an infringement of the policy that applies to a specific device. A corrective action can be declared for a policy, and specifies which action should be taken if a device violates the policy. When a compliance violation has been identified, a corrective action is applied.

## Compliance violation

A compliance violation is an infringement of the policy that has been declared for a device. Details of a compliance violation can be viewed by selecting the appropriate policy on the home page or results page and clicking the 'Details" function, or by performing a results search, which is also executed from the **Results** tab. A compliance violation is identified as a FAIL result. Following the identification of a compliance violation a corrective action may be applied if it has been specified and if it is applicable.

## Compliance extractions

Compliance extractions are a compliance component whereby specific chunks of data can be extracted from the native or modelled configuration or a show command. Compliance extractions are currently only used in conjunction with compliance definitions. An extraction is used within a definition where you want to use the extracted data as part of the definition. There is no restriction on the type of extraction you can use, for example, a native extraction can be used within a modelled definition. From within the definition wizard select the **Parameter Type** combo box, and then click **Extraction**. A list of available extractions will appear and once an extraction is selected, select 'Insert' to insert into the evaluation box. Only one extraction per evaluation is permitted.

There are three compliance extraction types to choose from:

**Compliance extraction using native CLI configuration lines**
A compliance extraction is very similar to a native definition. However, in the case of an extraction using native CLI configuration lines, a specific piece of data can be extracted from the matching CLI line or lines as specified in the extraction criteria.

**Compliance extraction using native commands**
In the compliance extraction using native commands option, a specific piece of data can be extracted from the matching native (show) commands as specified in the extraction criteria. The native commands are used for the search data and not the native configuration.

**Compliance extraction using a device model**
Modeled extractions are based on modeled device configurations. Modeled extractions use XPaths. An extraction XPath can be constructed to extract a certain piece of data from the modelled configuration.

## Corrective action

It is possible to associate multiple actions to a policy in the event of a violation. A corrective action can be classified as follows:

**Compliance policy level actions**
A compliance policy level action is an informational action that applies to all rules in a policy and is therefore selected at the policy level. A user can define two types of informational actions: email and notification. A user can associate an informational action to a policy during the initial definition or modification of a policy. To make it easier to create an email or notification action, use the following templates:

- Email template:
  An email message can be constructed using the template provided by Netcool Configuration Manager - Compliance. Recipients shall receive a comprehensive message detailing the cause of compliance violation and which devices were affected by it. The email template consists of an email header and an email body. The email header includes the fields To, Cc, Bcc, and Subject as a normal email would contain. The email body is free-text and can be used to add any comments as required. By default, the body of the email will also include the name of the policy that was violated, name of Process that is affected and the user who executed the policy. This will then be followed by a complete listing of all devices that caused the compliance violation.
  The following is an example of an email message:

```
From: ComplianceManager@BFSSUN12
[mailto:ComplianceManager@BFSSUN12]
Sent: 01 January 2019 15:11
To: Emma Thompson
Subject: test
test
Policy name: tester Process name: AdHoc_2019-01-01 15:09:36
Executed by: ComplianceManager
IBM/6506erma.IBM.test
IBM/emu2_001
IBM/emu2_002
IBM/emu2_003
IBM/emu2_004
IBM/emu2_005
IBM/emu2_006
IBM/emu2_007
IBM/emu2_008
IBM/emu2_009
```

- Notification template

**Compliance rule level actions**
A compliance rule level action is a remedial action that is specific to one or more device types and is therefore implemented at the rule level. A user defines a remedial action by using a command set. A user can also choose to define a remedial action with a no action taken in the event of a compliance violation. A user can associate an informational action to a policy during the initial definition or modification of a policy.

- Defines a remedial action by using a command set and associating the remedial action to a specific rule in a policy
- Choose to define a remedial action with no action taken in the event of a compliance violation
- Associate a remedial action to a rule during the initial definition or modification of a rule

### Remedial action

A remedial action is a procedure specified in the event that a device violates a policy. A remedial action executes a command set against device configurations, and brings the device back into compliance. A remedial action defined in Netcool Configuration Manager - Compliance creates a UOW in Netcool Configuration Manager - Base, which executes the specified command set against the violating device. This alters the device configuration so that the violation is removed.

The command set used in a remedial action can be native or modeled, and must be set up in Netcool Configuration Manager - Base first. From here they will be synchronized automatically to the Netcool Configuration Manager - Compliance application.

Therefore, to manage command sets the appropriate permissions must be given in the Netcool Configuration Manager - Base application. In complete lockstep with the command set that they invoke in Netcool Configuration Manager - Base, remedial actions are specific to a defined set of VTMOS combinations and are therefore selected as part of a compliance rule. The remedial action required can be selected from a list of command sets (native or modeled) that have been synchronized from Netcool Configuration Manager - Base.

**Note:** Parameters can be used to pass information from a policy to a remedial action. However, in order for this capability to function properly the user must ensure that parameter names are identical between policy and command set.

**Note:** Before a corrective action can be created in Netcool Configuration Manager - Compliance, the command set must have been created in Netcool Configuration Manager - Base, and have synchronized with the Netcool Configuration Manager - Compliance application.

**Note:** You can elect that no action is to be taken in the event of a compliance violation.

## Creating a compliance process

Use this procedure to define a new Compliance Process. Defining a new Compliance Process requires access to the User Interface wizard.

In defining Compliance Processes, a user must specify against which devices the process must run. For example, it is possible to run a process against all devices that must adhere to the set of policies that are included in the process. But it is also possible to set up a process that runs against only a sub-set of these devices, for example all devices in a part of the network that share the same NTP server. It is simple for a user to copy an existing Process, and modify some its components in order to create a new Process.

You can define the process parameters during the creation of the Compliance Process or later.

Follow the steps outlined under 'Procedure' to create a Compliance Process.

1. Select **CreateProcess**.

   The **Name and Description** window displays. Mandatory fields are denoted by an * (asterisk). Policy selection is also required at this stage.
2. Use the following descriptions as a guide to entering the appropriate information in the **Name and Description** window.

   **Name**
   Specifies the name used to identify the process. This field takes a maximum of 255 characters. This is a mandatory field.

   **Description**
   Specifies a brief narrative attached to the Policy whose purpose is to explain its function or use. This field takes a maximum of 4000 characters.

**Revision**
Specifies an automatically generated number that is given an initial value of one. Each time the Policy is edited, the revision number is incremented by one. This is for versioning control.

**Enable process for automatic validations**
When selected this option indicates that the policies selected within this process may be used by automatic processes.

**Policy Selection**
Policies to be included in the validation procedure should be selected here. Select the Policy/ Policies required from the navigation pane, and select using the arrows in the middle of the panel. A new Policy may be created at this stage using the **Create new** icon; this invokes the **Create a Policy** window.

3. Click Next on the **Name and Description** window.

   The **Pre-Emptive Options** window displays.

4. Use the following descriptions as a guide to entering the appropriate information in the **Pre-Emptive Options** window.

   **Enable Pre-Emptive Compliance Options for this Process**
   Specifies a check box that enables or disables the specified Compliance Process for pre-emptive compliance.

   **Policy Name**
   Specifies a list of Policies to be included. Policies that are not enabled for pre-emptive compliance appear in the list, but are greyed out. The user does not have the ability to enable them for pre-emptive compliance.

5. Click Next on the **Pre-Emptive Options** window.

   The **Select Devices** window displays.

6. Use the following descriptions as a guide to entering the appropriate information in or to making use of the icons at the bottom of the **Select Devices** window.

   **Retrieve Realms Button**
   Populates realms created

   **Device/Realm Selection drop-down menu**
   Options to view devices, realms, VTMOS device and VTMOS realm.

   **Check Device Coverage Button**
   Checks if Policies cover all devices selected.

   **Note:** The Check Device Coverage button will inform if all devices in the selection are covered by the policies, which will allow the user to continue to the next step in creating a Compliance Process. If there is a problem with the device coverage, the **Policy Coverage Check** window screen will be displayed. This window displays a reason such as: Policy not applicable or No rule applicable.

   **Search for Devices**
   Conduct a search on devices based on Name, Realm, Status, Synced at, and VTMOS.

   If sub-realms are employed in your realm structure, and you want to include these sub-realms in your selection, you must check the **Include Subrealms** checkbox. By default this is checked.

   The Devices/Realms that are required to execute the Process against should be selected. Using the navigation tree in the Device pane, select the necessary devices or realms.

7. Click **Next** on the **Select Devices** window.

   The **Parameters** window displays.

   You cannot add any new parameters here, but if you edit an existing parameter when creating a new policy that will create a process parameter in the 'Process Parameter' tab in the Process Administration GUI.

8. Select an existing parameter that exists in one of the included definitions, and then click **View** > **Edit**. Use the following descriptions as a guide, and note that not all of the following fields are editable:

**Name**
Specifies the name of the parameter. Parameters that have already been created in any of the Compliance definitions or through parameter administration display in this window.

**Type**
Specifies the type of the parameter, either LOCAL or GLOBAL.

**Description**
Specifies a description for the parameter.

**Current Value**
Specifies the current value for the parameter.

**Default Value**
Specifies the default value for the parameter.

**Realm**
Specifies the realm.

9. Click Next on the **Parameters** window.

   The **Process Schedule** window displays.
10. Use the following descriptions as a guide to entering the appropriate information in the **Process Schedule** window.

    **Unscheduled**
    Specifies a radio button used to specify an unscheduled execution of a Compliance Process.

    **Scheduled**
    Specifies a radio button used to specify a scheduled execution of a Compliance Process.

    **Recurring Schedule**
    Specifies radio buttons used to specify a scheduled or recurring execution of a Compliance Process. The recurring schedule is offered on an hourly, daily, weekly, monthly, or yearly basis.

    **Server Time:**
    Specifies the user's preference for date and time on the UI.

    **Scheduled Monthly**
    Specifies radio buttons used to specify the day and month if the Monthly radio button is selected.
11. Click Next on the **Process Schedule** window.
12. The **Choose a Save Location** window displays.
13. Navigate through the tree structure, and choose the location where you want to save the newly created Compliance Process. Otherwise, it is possible to create a new folder from here if required.
14. Click Finish on the **Choose a Save Location** window to complete the creation of the Compliance Process.

You can create another Compliance Process by following these instructions.

**Related tasks**

Editing process parameters
Use this procedure to edit process parameters.

Searching for devices
Searches may be performed on column names which appear in the devices tab. The devices search is invoked by clicking on the search icon. The Search By Column screen appears on the left hand side of the user interface.

Creating pre-emptive policies
Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device, allowing you to evaluate the impact of configuration changes against pre-defined compliance policies for a device. In order to run a pre-emptive compliance, you first create or modify existing policies to make them suitable for execution in a pre-emptive manner. You then create a compliance process to apply the pre-emptive policy to a device.

## Editing a compliance process

Use this procedure to modify an existing Compliance Process. Modifying a new Compliance Process requires access to the User Interface wizard.

An existing Compliance Process may be modified at any time. When all changes have been saved, the user can activate the Process as a new version. The previous version becomes inactive and the new version of the process will be used the next time the Compliance Process runs.

Follow these steps to modify an existing Compliance Process.

1. Access the Policy Definitions tab, and select Processes.
2. Right click on the Compliance Process you want to edit, and select "Edit Process". Alternatively, select the Compliance Process and click the Edit Process icon on the toolbar.

   The **Name and Description** window displays.
3. Use the following descriptions as a guide to modifying information in the **Name and Description** window.

   **Name**
   Specifies the name used to identify the process. This field takes a maximum of 255 characters. This is a mandatory field.

   **Description**
   Specifies a brief narrative attached to the Policy whose purpose is to explain its function or use. This field takes a maximum of 4000 characters.

   **Revision**
   Specifies an automatically generated number that is given an initial value of one. Each time the Policy is edited, the revision number is incremented by one. This is for versioning control.

   **Enable process for automatic validations**
   When selected this option indicates that the policies selected within this process may be used by automatic processes.

   **Policy Selection**
   Policies to be included in the validation procedure should be selected here. Select the Policy/ Policies required from the navigation pane, and select using the arrows in the middle of the panel. A new Policy may be created at this stage using the **Create new** icon; this invokes the **Create a Policy** window.
4. Click Next on the **Name and Description** window.

   The **Pre-Emptive Options** window displays.
5. Use the following descriptions as a guide to modifying information in the **Pre-Emptive Options** window.

   **Enable Pre-Emptive Compliance Options for this Process**
   Specifies a check box that enables or disables the specified Compliance Process for pre-emptive compliance.

   **Policy Name**
   Specifies a list of Policies to be included. Policies that are not enabled for pre-emptive compliance appear in the list, but are greyed out. The user does not have the ability to enable them for pre-emptive compliance.
6. Click Next on the **Pre-Emptive Options** window.

   The **Select Devices** window displays.
7. Use the following descriptions as a guide to entering the appropriate information in or to making use of the icons at the bottom of the **Select Devices** window.

   **Retrieve Realms Button**
   Populates realms created

   **Device/Realm Selection drop-down menu**
   Options to view devices, realms, VTMOS device and VTMOS realm.

**Check Device Coverage Button**
Checks if Policies cover all devices selected.

**Note:** The Check Device Coverage button will inform if all devices in the selection are covered by the policies, which will allow the user to continue to the next step in creating a Compliance Process. If there is a problem with the device coverage, the **Policy Coverage Check** window screen will be displayed. This window displays a reason such as: Policy not applicable or No rule applicable.

**Search for Devices**
Conduct a search on devices based on Name, Realm, Status, Synced at, and VTMOS.

If sub-realms are employed in your realm structure, and you want to include these sub-realms in your selection, you must check the **Include Subrealms** checkbox. By default this is checked.

The Devices/Realms that are required to execute the Process against should be selected. Using the navigation tree in the Device pane, select the necessary devices or realms.

8. Click Next on the **Select Devices** window.

   The **Parameters** window displays.
9. Use the following descriptions as a guide to modifying information in the **Parameters** window.

   **Name**
   Specifies the name of the parameter. Parameters that have already been created in any of the Compliance definitions or through parameter administration display in this window.

   **Type**
   Specifies the type of the parameter, either LOCAL or GLOBAL.

   **Description**
   Specifies a description for the parameter.

   **Current Value**
   Specifies the current value for the parameter.

   **Default Value**
   Specifies the default value for the parameter.

   **Realm**
   Specifies the realm.
10. Click Next on the **Parameters** window.

    The **Process Schedule** window displays.
11. Use the following descriptions as a guide to modifying information in the **Process Schedule** window.

    **Unscheduled**
    Specifies a radio button used to specify an unscheduled execution of a Compliance Process.

    **Scheduled**
    Specifies a radio button used to specify a scheduled execution of a Compliance Process.

    **Recurring Schedule**
    Specifies radio buttons used to specify a scheduled or recurring execution of a Compliance Process. The recurring schedule is offered on an hourly, daily, weekly, monthly, or yearly basis.

    **Server Time:**
    Specifies the user's preference for date and time on the UI.

    **Scheduled Monthly**
    Specifies radio buttons used to specify the day and month if the Monthly radio button is selected.
12. Click Next on the **Process Schedule** window.
13. The **Choose a Save Location** window displays.
14. Navigate through the tree structure, and choose the location where you want to save the modified Compliance Process. Otherwise, it is possible to create a new folder from here if required.
15. Click Finish on the **Choose a Save Location** window to save the modified Compliance Process.

**Note:** The modified Compliance Process is created as revision number 2 and can now be activated.

You can modify another existing Compliance Process by following these instructions.

You can also create a new Compliance Process by following the instructions in "Creating a compliance process" on page 9.

**Related tasks**

Editing process parameters
Use this procedure to edit process parameters.

Searching for devices
Searches may be performed on column names which appear in the devices tab. The devices search is invoked by clicking on the search icon. The Search By Column screen appears on the left hand side of the user interface.

## Creating a compliance policy

A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Use this procedure to create a compliance policy.

To define new Compliance Policies or edit existing Policies, access to the User Interface wizard is required. In defining Compliance Policies, a user must specify to which devices the Policy applies. It is simple for a user to copy an existing Policy, and modify some of its components in order to create a new Policy.

You can an informational action (e-mail) during the creation of the policy or later.

Follow these steps to create a Compliance Policy.

1. Select **Create** > **Policy**.

   The **Create a Policy** window displays. Mandatory fields are denoted by an * (asterisk). Rules to be included are also required at this stage.
2. Use the following descriptions as a guide to entering the appropriate information in the **Create a Policy** window.

   **Name:**
   Specifies the name used to identify the policy. This field takes a maximum of 255 characters. This is a mandatory field.

   **Description:**
   Specifies a brief narrative attached to the policy whose purpose is to explain its function or use. This field takes a maximum of 4000 characters.

   **Revision No:**
   Specifies an automatically generated number that is given an initial value of 1. Each time the policy is edited, the revision number is incremented by 1. This is for versioning control.

   **Impact:**
   Specifies a brief narrative to complement the Severity and Weight fields. This field takes a maximum of 255 characters.

   **Severity:**
   Specifies the severity of the error, in the event the policy is violated. The user can select one of the following severity values:

| Severity value | Severity |
|---|---|
| 1 | Critical |
| 2 | Major |
| 3 | Minor |

| Severity value | Severity |
|---|---|
| 4 | Warning |
| 5 | Indeterminate |

**Weight**
Specifies a "weight" that a user can assign to each policy using a sliding scale. The weight score can be between 1 and 100, with the default score being 25. This weight is used to calculate the compliance score that is shown in the Policy Compliance Score & Summary reports.

**Send Trap**
When this option is selected the policy will generate a compliance event upon execution. If Netcool Configuration Manager is integrated with Network Manager and Tivoli Netcool/OMNIbus, please be aware of the number of events that are being generated and passed to Network Manager. Users can safeguard by not selecting the “Send Trap” checkbox for those Policies which do not require traps. SNMP traps (Send trap checkbox) are enabled by default.

**Preemptive**
When this option is selected the policy can be used for pre-emptive validations.

**Note:** A pre-emptive policy can only contain modelled definitions and modelled extractions.

**Applicable Device Filter**
This filter allows the ability to select which device VTMOS applies to this policy. As well as drop down selection for VTMOS, a regular expression is supported for all filters.

**Note:** The selected value entered in the Model Filter will be checked against both 'Model' and 'Actual Model' fields (as in the Device Viewer).

**Rules Included**
Select the Rule(s) required from the navigation pane, and select using the arrows in the middle of the panel. A new Rule may be created at this stage using the "Create new" icon; this invokes the **Create a Rule** window.

**Note:** Please be aware of the following default properties in `/opt/ IBM/tivoli/netcool/ncm/compliance/config/properties/WorkFlowManager.properties`.

- `sendComplianceEvents=true` — Set this property to false if no events need to be sent.
- `sendRepeatComplianceEvents=false` — Set this property to true if repeat pass events need to be sent where the `sendComplianceEvent` property is set to true.

3. Click **Next** to progress.

   The **Select Actions** window displays. This window provides Action Types available in the event the Compliance Policy is violated.
4. Use the following descriptions as a guide to entering the appropriate information in the **Select Actions** window.

   **No Action**
   Specifies that no action will be taken.

   **Email**
   Specifies that an e-mail will be sent to an elected individual or application, and the content of the e-mail will explain the violation. All devices violating a specific policy will be included automatically in the body of the e-mail.
5. Click **Next** to continue.

   The **Choose a Save Location** window displays.
6. Navigate through the tree structure, and choose the location where you wish to save to. Otherwise, it is possible to create a new folder from here if required.
7. Click **Finish** to complete the creation of the Compliance Policy.

The new or updated Compliance Policy can be validated using the test function that can be invoked using the test icon. The test function allows the user to run an ad-hoc validation of a policy, but without adding the validation results to the overall network compliance status.

**Related tasks**

Creating an e-mail action
Compliance actions can be remedial (invoking a commandset in ITNCM - Base) or informational (e-mail) by nature. Use this procedure to create an e-mail compliance action.

Defining advanced VTMOS filters
The Advanced VTMOS filter provides a way to choose multiple options when filtering on devices. Use this procedure to create device filters from multiple options.

Creating pre-emptive policies
Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device, allowing you to evaluate the impact of configuration changes against pre-defined compliance policies for a device. In order to run a pre-emptive compliance, you first create or modify existing policies to make them suitable for execution in a pre-emptive manner. You then create a compliance process to apply the pre-emptive policy to a device.

## Editing a compliance policy

Users have the option of editing an existing Compliance Policy at any time. When all changes have been saved and the user has validated that the new version of the policy works correctly, the user can activate the Policy as a new version. Any previous active version becomes inactive.

To define new Compliance Policies or edit existing Policies, access to the User Interface wizard is required. In defining Compliance Policies, a user must specify to which devices the Policy applies. It is simple for a user to copy an existing Policy, and modify some of its components in order to create a new Policy.

You can create an informational action (e-mail) during the creation of the policy or later.

Follow these steps to edit a Compliance Policy.

1. Access the Policy Definitions tab, and select Policies.
2. Right click on the Policy you want to edit, and select **Edit Policy**. Alternatively, select the Policy and click the **Edit Policy** icon on the toolbar.

   The **Edit Policy** window displays.
3. Use the following descriptions as a guide to editing any of the information in the **Edit Policy** window.

   **Name:**
   Specifies the name used to identify the policy. This field takes a maximum of 255 characters. This is a mandatory field.

   **Description:**
   Specifies a brief narrative attached to the policy whose purpose is to explain its function or use. This field takes a maximum of 4000 characters.

   **Revision No:**
   Specifies an automatically generated number that is given an initial value of 1. Each time the policy is edited, the revision number is incremented by 1. This is for versioning control.

   **Impact:**
   Specifies a brief narrative to complement the Severity and Weight fields. This field takes a maximum of 255 characters.

   **Severity:**
   Specifies the severity of the error, in the event the policy is violated. The user can select one of the following severity values:

| Severity value | Severity |
|---|---|
| 1 | Critical |

| Severity value | Severity |
|---|---|
| 2 | Major |
| 3 | Minor |
| 4 | Warning |
| 5 | Indeterminate |

**Weight**
Specifies a "weight" that a user can assign to each policy using a sliding scale. The weight score can be between 1 and 100, with the default score being 25. This weight is used to calculate the compliance score that is shown in the Policy Compliance Score & Summary reports.

**Send Trap**
When this option is selected the policy will generate a compliance event upon execution. If Netcool Configuration Manager is integrated with Network Manager and Tivoli Netcool/OMNIbus, please be aware of the number of events that are being generated and passed to Network Manager. Users can safeguard by not selecting the “Send Trap” checkbox for those Policies which do not require traps. SNMP traps (Send trap checkbox) are enabled by default.

**Preemptive**
When this option is selected the policy can be used for pre-emptive validations.

**Note:** A pre-emptive policy can only contain modelled definitions and modelled extractions.

**Applicable Device Filter**
This filter allows the ability to select which device VTMOS applies to this policy. As well as drop down selection for VTMOS, a regular expression is supported for all filters.

**Note:** The selected value entered in the Model Filter will be checked against both 'Model' and 'Actual Model' fields (as in the Device Viewer).

**Rules Included**
Select the Rule(s) required from the navigation pane, and select using the arrows in the middle of the panel. A new Rule may be created at this stage using the "Create new" icon; this invokes the **Create a Rule** window.

**Note:** Please be aware of the following default properties in `/opt/ IBM/tivoli/netcool/ncm/compliance/config/properties/WorkFlowManager.properties`.

- `sendComplianceEvents=true` — Set this property to false if no events need to be sent.
- `sendRepeatComplianceEvents=false` — Set this property to true if repeat pass events need to be sent where the `sendComplianceEvent` property is set to true.

4. Click Finish to complete the modifications.

The Revision Number on the modified Policy will have been incremented by 1, and the Policy can now be activated. The previously active policy version will automatically become inactive. All subsequent validations will use the new policy version.

It is not necessarily the Policy with the highest Revision Number that is active, as the user may return to a previous version and activate.

**Related tasks**

Creating an e-mail action
Compliance actions can be remedial (invoking a commandset in ITNCM - Base) or informational (e-mail) by nature. Use this procedure to create an e-mail compliance action.

Defining advanced VTMOS filters

The Advanced VTMOS filter provides a way to choose multiple options when filtering on devices. Use this procedure to create device filters from multiple options.

## Creating a compliance policy exemption

Use this procedure to define a new Compliance Policy Exemption. Defining a new Compliance Policy Exemption requires access to the User Interface wizard.

Compliance Policy Exemptions are available in the event that a device or a number of devices should be excluded from the execution of a Policy. Effectively, a Policy exemption means that those devices selected shall be excluded when validation occurs. Devices exempt from a policy will be listed in the validation results of that policy though, but with a result value of "Exempt".

Follow these steps to create a Compliance Policy Exemption.

1. Access the Policy Definitions tab, and select Policies.
2. Choose the Policy to which you want to apply an exemption. Right click on the Policy, and select Exemptions. Alternatively, select the policy and then click the Exemption icon.

   The **Exemptions for Policy:** *Policy name* window displays.
3. Use the following descriptions as a guide to entering the appropriate information in the **Exemptions for Policy:** *Policy name* window.

   **Choose Devices/Realms**
   This field allows you to select the devices/realms for exemption. Using the navigation tree in the Devices pane, select the required devices using the arrows in the middle of the panel.

   **View by VTMOS**
   Displays folders in VTMOS hierarchy.

   **View Devices in Tree**
   Displays individual devices in VTMOS hierarchy.

   **Search for Devices**
   Conduct a search on devices based on Name, Realm, Status, Synced at, and VTMOS.

   **Refresh**
   Refresh displayed information.

   **Move up**
   Move up one directory level.

   **Search**
   If sub-realms are employed in your realm structure, and you want to include these sub-realms in your selection, you must check the **Include Subrealms** checkbox. By default this is checked.
4. The **Exemption Details** window displays. Use the following descriptions as a guide to entering the appropriate information in the **Exemption Details** window.

   **Start Time**
   Start date/time at which the exemption will come into effect. The date/time can be adjusted using the arrows on the right. A calendar is available, by selecting the icon.

   **End Time**
   End time at which the exemption will cease to take effect. The date/time can be adjusted using the arrows on the right. A calendar is available, also by selecting the icon.

   **Description**
   Brief narrative attached to the Policy Exemption created to explain its function/use.

   **Note:** The Exemption Details section at the bottom of the **Exemptions for Policy:** *Policy name* window should be used for verification of Exemption choice. It populates the exemption information selected. This may be edited if required, by selecting the Edit button.
5. Click Finish to complete the creation of the Compliance Policy Exemption.

The count of exemptions can be viewed on the Home tab, under the Current Policy Validation Summary. The field name under which these counts will appear is Exempt. Refer to Homepage for further information.

You can create another Compliance Policy Exemption by following these instructions.

## Creating pre-emptive policies

Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device, allowing you to evaluate the impact of configuration changes against pre-defined compliance policies for a device. In order to run a pre-emptive compliance, you first create or modify existing policies to make them suitable for execution in a pre-emptive manner. You then create a compliance process to apply the pre-emptive policy to a device.

Pre-emptive compliance can only be applied to 'Apply Commandset' and 'Submit Configuration' workflows, as it can only be applied to a modelled configuration. Pre-emptive compliance can only be applied to devices which have smart model driver support. By using the smart model we can project what the device configuration will look like if the changes were applied, and hence we can run compliance checks against this projected configuration.

**Note:** Any policy that contains native command line checks will be rejected, and result in a status of 'Not Assessed'.

All policy configurations are implemented through the Netcool Configuration Manager - Compliance UI.

1. Create a pre-emptive compliance policy, or edit an existing compliance policy, to be pre-emptive.
   See “Creating a compliance policy” on page 219 for more information.
2. Create a Compliance Process to apply the pre-emptive policy to a device.
   A process is an existing compliance entity normally used as the execution vehicle for compliance checks. See “Creating a compliance process” on page 9 for more information.
   When a pre-emptive execution is initiated from the Netcool Configuration Manager workflow, it queries any potential association, and locates which policies need to be applied. Since pre-emptive compliance can only be applied to a modelled configuration, only the 'Apply Commandset' and 'Submit Configuration' workflows are affected. See “Applying command sets” on page 65 and “Applying versioned configurations” on page 99 for more information.
3. Optional: To view the pre-emptive policies that have been defined for a device, perform the following actions:
   a) On the Netcool Configuration Manager - Compliance Devices tab, right-click a device to select it.
   b) Select **View Pre-emptive Policies for device**.
   A dialog displays a list of the applicable pre-emptive policies.
4. Optional: To view pre-emptive policy results from the Queue Manager, perform the following actions:
   a) Select the unit of work (UOW) in the Queue Manager from either the 'Work That is Finished' or the 'Work Pending Approval' column (if approvals are enabled).
   b) Select the Resources tab, and choose a device from the Resource list.
   The pre-emptive compliance policy results are displayed on the following two tabs:

   **Work log**
   The Work log shows the pre-emptive compliance result for both the current configuration and the projected configuration.

   **Pre-emptive Compliance**
   Shows the pre-emptive compliance results.
5. Optional: To view pre-emptive policy results form the Resource Browser, perform the following actions:
   a) Right-click the device to select it.
   b) Select the UOW from the Work tab.
   The pre-emptive compliance policy results are displayed on the following two tabs:

**Audit log**
The Audit log displays the pre-emptive compliance result for both the current configuration and the projected configuration.

**Pre-emptive Compliance**
Shows the pre-emptive compliance results for ‘Apply Command set' and ‘Submit configuration work types'.

You can drill down into the Validation detail by double-clicking on the individual policy, or by selecting the **Policy** row and then clicking **View Policy Result Detail**.

If the user submitting the work requires approval, the work will execute pre-emptive checks first before pushing the work into the Approval queue. The approver of the work can then view the pre-emptive results before approving or rejecting the work. Once approved the work will be applied to the device without running pre-emptive checks. For more information on approvals, see “Approving or rejecting units of work (UOWs)” on page 153.

**Note:**

Please be aware of the following default properties in `/opt/ IBM/tivoli/netcool/ncm/compliance/config/properties/WorkFlowManager.properties`.

`WorkFlowManager/usePolicyCache=false` - This can be set so that policies may be cached to enable faster execution. This is off by default.

`WorkFlowManager/clearPolicyCacheAfter=1800` - Cache is cleared after the specified number of seconds.

`Compliance/policies.find.mode=all` - Search mode can be all, xpath or name. “All” is a search conducted regardless of xpath or name, “xpath” will only run on xpath matches, “name” searches when a policy has the same name as the config being applied.

**Related tasks**

Viewing pre-emptive policies and results
Use the pre-emptive compliance functionality to check proposed configuration changes to a device against predefined compliance policies for that device. Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device. The capability is intended to enable customers to evaluate the impact of configuration changes against predefined compliance policies for a device.

Creating a compliance policy
A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Use this procedure to create a compliance policy.

Creating a compliance process
Use this procedure to define a new Compliance Process. Defining a new Compliance Process requires access to the User Interface wizard.

Applying command sets
When applying a command set, the system verifies that the running and stored (candidate) configurations on each impacted resource are the same. If these are not the same, a mismatch error will be presented. This mismatch must be resolved before submitting any changes to the resource. After a successful configuration change, the system writes the running configuration to the stored/candidate configuration on each resource, ensuring that all three configurations (current, running, stored) are in synch.

Applying versioned configurations
Use this procedure to apply an earlier configuration version to a network resource.

Approving or rejecting units of work (UOWs)

When a UOW is submitted, it is subject to approval depending on the security privileges of the user.

## Creating compliance definitions using native CLI configuration lines

A compliance definition may contain one or more native command lines (CLI) and use evaluation criteria to match these CLI lines against the device configuration stored in ITNCM-Compliance, which are automatically synchronized from ITNCM - Base each time the configuration changes. Use this procedure to create compliance definitions using native CLI configuration lines.

It is simple for a user to copy an existing definition, and modify some of its components to create a new definition.

Use the **Create a Definition** window of the User Interface to create a new compliance definition using native CLI configuration lines.

Follow these steps to create a compliance definition using native CLI configuration lines.

1. Select **Create->Compliance Definition**.

   The **Create a Definition** window displays.
2. Use the following descriptions as a guide to entering the appropriate information in the **Create a Definition** window.

   **Name**
   Name chosen to identify the compliance definition. The maximum number of characters for the name is 255. This is a mandatory field.

   **Description**
   Brief narrative attached to the compliance definition to be created that explains its function and use. The maximum number of characters is 4000.

   **Revision**
   This number is automatically assigned and initially given a value of 1. Each time the compliance definition is edited, the revision number increments by 1. This is for versioning control. The revision changes only if the entity is active.

   **Select Definition Type**
   Radio buttons that allow you to create the following types of compliance definitions:

| Radio button | Description |
|---|---|
| **Create compliance definition using CLI configuration lines** | Select this definition type if you want to define a Compliance Definition with a native definition that uses a stored configuration. Selecting this option causes the **Enter Native Definition Details** (CLI configuration lines) window to display. |
| **Create compliance definition using Native Commands** | Select this definition type if you want to define a Compliance Definition with Native Commands. Selecting this option causes the **Enter Native Definition Details** (Native Commands) window to display. |
| **Create compliance definition using a Device Model** | Select this definition type if you want to define a Compliance Definition with a modeled definition. Selecting this option causes the **Enter Modeled Definition Details** window to display. |
| **Create compliance definition using a Script** | Select this definition type if you want to define a Compliance Definition with a script. Selecting this option causes the **Enter Script-Based Definition Details** window to display. |
| **Create compliance definition using a Golden Configuration** | Select this definition type if you want to define a Compliance Definition using a device's golden configuration as a template for automatically generating evaluations. Selecting this option causes the **Select a Golden Device** window to display. |

**Prev**
Go to the previous selection.

**Next**
Go to the next selection.

**Finish**
Complete process.

**Cancel**
Cancel activities.

3. Select the **Create compliance definition using CLI configuration lines** radio button, and then click Next.

   The **Enter Native Definition Details** (CLI configuration lines) window displays.

4. Use the following descriptions as a guide to entering the appropriate information in the **Enter Native Definition Details** (CLI configuration lines) window.

   **Evaluation Line**
   The value or expression on which you want to search.

   **Parameters**
   This is an optional field. This field provides a drop down list for the type of parameter you want. There is also an **Insert Parameter** button used to insert the parameter.

   **Note:** Placing a parameter inside another parameter is not supported.

   **Match Criteria**
   Specifies a drop down list for the criteria used to match the device configuration. The following table describes the options in the drop down list:

| Match option | Description |
|---|---|
| **Match All** | Matches all evaluations added to the Compliance Definition. |
| **Match Any** | Matches any of the evaluations added to the Compliance Definition. |
| **Match None** | Matches none of the evaluations added must be found in the Device Configuration. |
| **Match One** | Matches only one of the evaluations added to the Compliance Definition. If more than one of the evaluations are matched, the match fails. |
| **Match Exactly** | Find and match all evaluations, and only these evaluations. If any found outside this criteria, the test result will Fail. |
| **Match Specific Number** | Matches a specific number of evaluations as defined by the user. For example, Match 2 out of the 6 evaluations listed. This choice activates an integer field called Specific Number. |

   **Number**
   This is activated when the Match Specific Number option is chosen. An integer must be entered here.

   **Evaluation Result if Context not found**
   You can opt to choose the result you wish to receive if the context is not found. The options are: Fail, Pass, Not Assessed, Not Applicable.

   If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.

**Evaluation List Criteria**

Used to match evaluations shown in the list.

See Match Criteria (for Group/Extraction Parameter values) above for explanation of choices available.

**Regex Tool**

You use the regex tool to test native definition regular expressions against a device configuration or a snippet of CLI. The regex tool is available for both definitions using native CLI configuration lines, and using native commands. You can either create your regex in the tool, or edit it using the text in the evaluation field.

| **Regex Tool window elements** | **Description** |
|---|---|
| **Tabs** | You can add as many tabs as your memory allows. The regex in the **Regex Pattern** field is applied to each tab and the matches are highlighted.<br>• To create a new tab, click the green plus (+).<br>• To delete a tab, click the red X.<br>• To rename a tab, double-click the name.<br>**Note:** The test tabs are only available when the wizard is open. |
| **Regex Test Data** evaluation field | Configurations are displayed here, as are any matches when the regex is run.<br>Matches are alternately highlighted in yellow and blue. |
|  | The Import Device icon is displayed under the first tab. Using this, you can import a configuration from a device into the **Regex Test Data** field.<br>When you click this option, the **Device Select** dialog opens. Drill down into the device realms and select a device. Click **OK** to populate the **Regex Test Data** field |
|  | This icon is displayed next to the Device tree icon. Using this, you can import a configuration from a text file into the **Regex Test Data** field.<br>When you click this option, a standard file selection dialog opens. Drill down into your folders and select a file.<br>**Note:** You can only select a text file.<br>Click **Open** to populate the **Regex Test Data** field with the contents of the selected text file. |
|  <br>  | These icons are displayed next to the Import File icon.<br>Once you have obtained matches, the arrow icons are enabled and you can use them to move from match to match.<br>Matches in the evaluation window are alternately highlighted in yellow and blue.<br>Currently selected matches are highlighted in grey.<br>These are enabled if there are matches on the selected tab. Up arrow highlights the previous match, down arrow highlights the next match. Current highlight matches are highlighted in grey |

| Regex Tool window elements | Description |
|---|---|
| **Regex Pattern** field | Enter the regular expression for testing into the **Regex Pattern** field. |
| **Match** | Execute the test against all open tabs, and highlight the matches in each tab with a count of the number of matches returned on each tab. |
| **Clear Matches** | Clear the matches highlighted, as well as the Match count on each tab. |
| **OK** | Move the regular expression in the Regex Pattern field into the **Regex Test Data** field. |
| **Cancel** | Closes the **Regex Tool** window. |
| Menu bar | All options described are also available from the menu bar (File, Edit, Regex, Tabs):<br>**Edit**<br>In addition to the button options, you can access the cut, copy and paste functionality from the Edit menu.<br>**Regex**<br>In addition to the Regex button options, you can access a History dropdown from the Regex menu.<br>The last ten successful matches are stored as history, with the most recent one at the top.<br>**Note:** If the regex is over a certain length, the History dropdown list displays a truncated version of it. |

**Add**
Adds another selection.

**Update**
Updates screen.

**Edit**
Edits current selection.

**Delete**
Deletes current selection.

**Test**
The definition test button is enabled when editing or creating a definition, but not when opening a definition. Also, it is only available for modeled and native definitions (not scripts).

You use the definition test functionality to execute a definition against all open tabs, and view the results.

You can test definitions using native CLI configuration lines, native commands or device models. You can view results in the evaluation list either in detail, or as a summary.

| Definition Test window elements | Description |
|---|---|
| **Definition Test** window | When you click **Test**, the **Definition Test** window is displayed (it resembles the **Regex Tool** window). |

| Definition Test window elements | Description |
|---|---|
| | When you import definitions from a device, the type of definition you are creating determines what content is imported from the device:<br>**For modeled definitions**<br>Imports the xml configuration from the device.<br>**For native CLI definitions**<br>Imports the CLI configuration for the device.<br>**For native commands definitions**<br>Imports the show commands from the device into the text area in the tab.<br>  **Warning:** Importing a text file from a file with an xml extension may result in an error when you execute the test. |
| **Tabs** | You can add as many tabs as your memory allows. The definition is applied to each tab and the results are flagged on the tabs.<br>**Green flag**<br>Passed<br>**Red flag**<br>Failed<br>**Yellow flag**<br>Not assessed |
| **Evaluation list** | Results are displayed in the **Evaluation list** under a number of columns.<br>**Evaluation**<br>532: Is the same as XPath<br>533: Is the same as Evaluation Line<br>534: Is the same as Evaluation Line<br>This is the search criteria for the Definition or the XPath to search for in the case of Device Models<br>**Match Criteria**<br>The criteria used to match the device configuration: Match All, Match Any, None, One, Exactly, Specific Number<br>**Match Criteria Argument**<br>532: Is the same as Number<br>533: Is the same as Number<br>534: Is the same as Number<br>Only available on group parameters and extractions. Same as Match Specific Number.<br>**Default Result**<br>The default result is the value defined in the **Evaluation Result if Context not found** option, that is, one of Fail, Pass, Not Assessed, and Not Applicable.<br>**Note:** If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass. |

| Definition Test window elements | Description |
|---|---|
| | User can opt to choose the result they wish to receive if the context is not found. The options are: Fail, Pass, Not Assessed, Not Applicable.<br>If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.<br>**Result**<br>Green text = Pass, Red text = Fail, Yellow text = Not Assessed/Not Applicable, Blue text =Error<br>**Restriction:** Script parameters and extractions are not supported. If any are found in the evaluation they will not be assessed during the test, and the overall definition result will be not assessed. |
| **Details mode** | You can toggle between Details and Summary mode to select the level of detail displayed in the test results. When in Summary mode, you can click on each evaluation to display detailed results. |
| **Clear all** | Clears the results from the Evaluation List and tabs. |
| **Test** | Click to run the test |
| **Close** | Closes the **Definition Test** window.<br>**Note:** The test tabs are only available when the window is open. |
| Menu bar | All options described are also available from the menu bar (File, Edit, Mode, Tabs). |

When an Evaluation is added to the list, it will appear in the lower section of the window. The **Choose a Save Location** window displays.

5. Navigate through the tree structure, and choose the location to which you want to save the Compliance Definition. Otherwise, it is possible to create a new folder from here if required.
6. Click Finish to complete the creation of the compliance definition.

You can create another compliance definition using Native Commands by following the instructions in this procedure.

**Related tasks**

Searching for device configurations
Searches can also be conducted on device configurations: Search using native CLI configuration lines, Search using native commands and Search using device models.

## Creating compliance definitions using native commands

Compliance definitions may contain a native (show) command that can be issued against the device to retrieve specific information from the device that is not available in the configuration itself. These definitions contain not only the native command that must be issued to the device, but also define the results that should (or should not) be present in the information returned from the device. Use this procedure to create compliance definitions using native commands.

It is simple for a user to copy an existing definition, and modify some of its components to create a new definition.

Use the **Create a Definition** window of the User Interface to create a new compliance definition using native commands.

Follow these steps to create a compliance definition using native commands.

1. Select **Create->Compliance Definition**.

   The **Create a Definition** window displays.
2. Use the following descriptions as a guide to entering the appropriate information in the **Create a Definition** window.

   **Name**
   Name chosen to identify the compliance definition. The maximum number of characters for the name is 255. This is a mandatory field.

   **Description**
   Brief narrative attached to the compliance definition to be created that explains its function and use. The maximum number of characters is 4000.

   **Revision**
   This number is automatically assigned and initially given a value of 1. Each time the compliance definition is edited, the revision number increments by 1. This is for versioning control. The revision changes only if the entity is active.

   **Select Definition Type**
   Radio buttons that allow you to create the following types of compliance definitions:

| Radio button | Description |
|---|---|
| **Create compliance definition using CLI configuration lines** | Select this definition type if you want to define a Compliance Definition with a native definition that uses a stored configuration. Selecting this option causes the **Enter Native Definition Details** (CLI configuration lines) window to display. |
| **Create compliance definition using Native Commands** | Select this definition type if you want to define a Compliance Definition with Native Commands. Selecting this option causes the **Enter Native Definition Details** (Native Commands) window to display. |
| **Create compliance definition using a Device Model** | Select this definition type if you want to define a Compliance Definition with a modeled definition. Selecting this option causes the **Enter Modeled Definition Details** window to display. |
| **Create compliance definition using a Script** | Select this definition type if you want to define a Compliance Definition with a script. Selecting this option causes the **Enter Script-Based Definition Details** window to display. |
| **Create compliance definition using a Golden Configuration** | Select this definition type if you want to define a Compliance Definition using a device's golden configuration as a template for automatically generating evaluations. Selecting this option causes the **Select a Golden Device** window to display. |

   **Prev**
   Go to the previous selection.

   **Next**
   Go to the next selection.

   **Finish**
   Complete process.

   **Cancel**
   Cancel activities.
3. Select the **Create compliance definition using Native Commands** radio button, and then click Next.

   The **Enter Native Definition Details** (Native Commands) window displays.
4. Use the following descriptions as a guide to entering the appropriate information in the **Enter Native Definition Details** (Native Commands) window.

**Native Commands**
Native Commands must be entered to indicate the Evaluation Source. Any type of show command may be entered in the Native command(s) criteria, for example, show version, show config.

**Use cached show command response**
This option may be used to speed up response time, if previous show commands have been executed.

**Evaluation Line**
The value/expression you wish to search on

**Parameters**
This is an optional field. This field provides a drop down list for the type of parameter you want. There is also an **Insert Parameter** button used to insert the parameter.

**Note:** Placing a parameter inside another parameter is not supported.

**Match Criteria**
Specifies a drop down list for the criteria used to match the device configuration. The following table describes the options in the drop down list:

| Match option | Description |
|---|---|
| **Match All** | Matches all evaluations added to the Compliance Definition. |
| **Match Any** | Matches any of the evaluations added to the Compliance Definition. |
| **Match None** | Matches none of the evaluations added must be found in the Device Configuration. |
| **Match One** | Matches only one of the evaluations added to the Compliance Definition. If more than one of the evaluations are matched, the match fails. |
| **Match Exactly** | Find and match all evaluations, and only these evaluations. If any found outside this criteria, the test result will Fail. |
| **Match Specific Number** | Matches a specific number of evaluations as defined by the user. For example, Match 2 out of the 6 evaluations listed. This choice activates an integer field called Specific Number. |

**Number**
This is activated when the Match Specific Number is chosen. An integer must be entered here.

**Evaluation Result if Context not found**
User can opt to choose the result they wish to receive if the context is not found. The options are: Fail, Pass, Not Assessed, Not Applicable.

If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.

**Match List Criteria**
Used to match evaluations shown in the listing.

See Match Criteria for Group/Extraction Parameter values above for explanation of choices available.

**Regex Tool**
You use the regex rool to test native definition regular expressions against a device configuration or a snippet of CLI. The regex tool is available for both definitions using native CLI configuration lines, and using native commands. You can either create your regex in the tool, or edit it using the text in the evaluation field.

| Regex Tool window elements | Description |
|---|---|
| **Tabs** | You can add as many tabs as your memory allows. The regex in the **Regex Pattern** field is applied to each tab and the matches are highlighted.<br>• To create a new tab, click the green plus (+).<br>• To delete a tab, click the red X.<br>• To rename a tab, double-click the name.<br>**Note:** The test tabs are only available when the wizard is open. |
| **Regex Test Data** evaluation field | Configurations are displayed here, as are any matches when the regex is run.<br>Matches are alternately highlighted in yellow and blue. |
|  | The Import Device icon is displayed under the first tab. Using this, you can import a configuration from a device into the **Regex Test Data** field.<br>When you click this option, the **Device Select** dialog opens. Drill down into the device realms and select a device. Click **OK** to populate the **Regex Test Data** field |
|  | This icon is displayed next to the Device tree icon. Using this, you can import a configuration from a text file into the **Regex Test Data** field.<br>When you click this option, a standard file selection dialog opens. Drill down into your folders and select a file.<br>**Note:** You can only select a text file.<br>Click **Open** to populate the **Regex Test Data** field with the contents of the selected text file. |
|  <br>  | These icons are displayed next to the Import File icon.<br>Once you have obtained matches, the arrow icons are enabled and you can use them to move from match to match.<br>Matches in the evaluation window are alternately highlighted in yellow and blue.<br>Currently selected matches are highlighted in grey.<br>These are enabled if there are matches on the selected tab. Up arrow highlights the previous match, down arrow highlights the next match. Current highlight matches are highlighted in grey |
| **Regex Pattern** field | Enter the regular expression for testing into the **Regex Pattern** field. |
| **Match** | Execute the test against all open tabs, and highlight the matches in each tab with a count of the number of matches returned on each tab. |
| **Clear Matches** | Clear the matches highlighted, as well as the Match count on each tab. |
| **OK** | Move the regular expression in the Regex Pattern field into the **Regex Test Data** field. |

| Regex Tool window elements | Description |
|---|---|
| **Cancel** | Closes the **Regex Tool** window. |
| Menu bar | All options described are also available from the menu bar (File, Edit, Regex, Tabs):<br>**Edit**<br>In addition to the button options, you can access the cut, copy and paste functionality from the Edit menu.<br>**Regex**<br>In addition to the Regex button options, you can access a History dropdown from the Regex menu.<br>The last ten successful matches are stored as history, with the most recent one at the top.<br>**Note:** If the regex is over a certain length, the History dropdown list displays a truncated version of it. |

**Add**
Adds another selection.

**Update**
Updates current selection.

**Edit**
Edits current selection.

**Delete**
Deletes current selection.

**Test**
The definition test button is enabled when editing or creating a definition, but not when opening a definition. Also, it is only available for modeled and native definitions (not scripts).

You use the definition test functionality to execute a definition against all open tabs, and view the results.

You can test definitions using native CLI configuration lines, native commands or device models. You can view results in the evaluation list either in detail, or as a summary.

| Definition Test window elements | Description |
|---|---|
| **Definition Test** window | When you click **Test**, the **Definition Test** window is displayed (it resembles the **Regex Tool** window).<br>When you import definitions from a device, the type of definition you are creating determines what content is imported from the device:<br>**For modeled definitions**<br>Imports the xml configuration from the device.<br>**For native CLI definitions**<br>Imports the CLI configuration for the device.<br>**For native commands definitions**<br>Imports the show commands from the device into the text area in the tab.<br>**Warning:** Importing a text file from a file with an xml extension may result in an error when you execute the test. |

| Definition Test window elements | Description |
|---|---|
| **Tabs** | You can add as many tabs as your memory allows. The definition is applied to each tab and the results are flagged on the tabs.<br>**Green flag**<br>Passed<br>**Red flag**<br>Failed<br>**Yellow flag**<br>Not assessed |
| **Evaluation list** | Results are displayed in the **Evaluation list** under a number of columns.<br>**Evaluation**<br>532: Is the same as XPath<br>533: Is the same as Evaluation Line<br>534: Is the same as Evaluation Line<br>This is the search criteria for the Definition or the XPath to search for in the case of Device Models<br>**Match Criteria**<br>The criteria used to match the device configuration: Match All, Match Any, None, One, Exactly, Specific Number<br>**Match Criteria Argument**<br>532: Is the same as Number<br>533: Is the same as Number<br>534: Is the same as Number<br>Only available on group parameters and extractions. Same as Match Specific Number.<br>**Default Result**<br>The default result is the value defined in the **Evaluation Result if Context not found** option, that is, one of Fail, Pass, Not Assessed, and Not Applicable.<br>**Note:** If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.<br>User can opt to choose the result they wish to receive if the context is not found. The options are: Fail, Pass, Not Assessed, Not Applicable.<br>If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.<br>**Result**<br>Green text = Pass, Red text = Fail, Yellow text = Not Assessed/Not Applicable, Blue text =Error<br>**Restriction:** Script parameters and extractions are not supported. If any are found in the evaluation they will not be assessed during the test, and the overall definition result will be not assessed. |

| Definition Test window elements | Description |
|---|---|
| **Details mode** | You can toggle between Details and Summary mode to select the level of detail displayed in the test results. When in Summary mode, you can click on each evaluation to display detailed results. |
| **Clear all** | Clears the results from the Evaluation List and tabs. |
| **Test** | Click to run the test |
| **Close** | Closes the **Definition Test** window.<br>**Note:** The test tabs are only available when the window is open. |
| Menu bar | All options described are also available from the menu bar (File, Edit, Mode, Tabs). |

5. When an argument in the Evaluation List is selected, the evaluation details in the lower section of the window are populated. If changes are required to the evaluation details, they can be made at this point. Select the Update button to save amendments to the Evaluation.

   The **Choose a Save Location** window displays.
6. Navigate through the tree structure, and choose the location to which you want to save the Compliance Definition. Otherwise, it is possible to create a new folder from here if required.
7. Click **Finish** to complete the creation of the compliance definition.

You can create another compliance definition using Native Commands by following the instructions in this procedure.

**Related tasks**

Searching for device configurations
Searches can also be conducted on device configurations: Search using native CLI configuration lines, Search using native commands and Search using device models.

## Creating compliance definitions using device models

Modeled definitions are based on modeled device configurations. Modeled definitions are all based on XPaths. An XPath is a search mechanism used in XML, and models an XML document as a tree of nodes. Use this procedure to create Compliance Definitions using device models.

A compliance definition created based on one device schema may be used against devices that are modeled using a different device schema, as long as those schemas share the nodes included in the compliance definition With other words the scope of a compliance definition using a device model is not limited to the devices defined by the VTMOS that was used to retrieve the schema based on which the definition was built.

Read the following information about parameters before beginning this procedure:

- Parameters defined in Modelled Definitions will automatically be passed to remedial actions, if configured to do so.
- Parameters passed to remedial actions can be viewed in the Remedial queue under the “parameters” column.
- Parameters defined in remedial commandsets need to have the same name as parameters defined in remedial command sets in ITNCM - Base.

  **Note:** Placing a parameter inside another parameter is not supported.

It is simple for a user to copy an existing definition, and modify some of its components to create a new definition.

Use the **Create a Definition** window of the User Interface to create a new compliance definition using device models.

Follow these steps to create a Compliance Definition using device models.

1. Select **Create->Compliance Definition**.

   The **Create a Definition** window displays.
2. Use the following descriptions as a guide to entering the appropriate information in the **Create a Definition** window.

   **Name**
   Name chosen to identify the compliance definition. The maximum number of characters for the name is 255. This is a mandatory field.

   **Description**
   Brief narrative attached to the compliance definition to be created that explains its function and use. The maximum number of characters is 4000.

   **Revision**
   This number is automatically assigned and initially given a value of 1. Each time the compliance definition is edited, the revision number increments by 1. This is for versioning control. The revision changes only if the entity is active.

   **Select Definition Type**
   Radio buttons that allow you to create the following types of compliance definitions:

| Radio button | Description |
|---|---|
| **Create compliance definition using CLI configuration lines** | Select this definition type if you want to define a Compliance Definition with a native definition that uses a stored configuration. Selecting this option causes the **Enter Native Definition Details** (CLI configuration lines) window to display. |
| **Create compliance definition using Native Commands** | Select this definition type if you want to define a Compliance Definition with Native Commands. Selecting this option causes the **Enter Native Definition Details** (Native Commands) window to display. |
| **Create compliance definition using a Device Model** | Select this definition type if you want to define a Compliance Definition with a modeled definition. Selecting this option causes the **Enter Modeled Definition Details** window to display. |
| **Create compliance definition using a Script** | Select this definition type if you want to define a Compliance Definition with a script. Selecting this option causes the **Enter Script-Based Definition Details** window to display. |
| **Create compliance definition using a Golden Configuration** | Select this definition type if you want to define a Compliance Definition using a device's golden configuration as a template for automatically generating evaluations. Selecting this option causes the **Select a Golden Device** window to display. |

   **Prev**
   Go to the previous selection.

   **Next**
   Go to the next selection.

   **Finish**
   Complete process.

   **Cancel**
   Cancel activities.
3. Select the **Create compliance definition using a Device Model** radio button, and then click Next.

   The **Enter Modeled Definition Details** window displays.

4. Use the following descriptions as a guide to entering the appropriate information in the **Enter Modeled Definition Details** window.

**VTMOS**
Choose a device schema by selecting VTMOS combination.

**Retrieve Model**
Selecting the **Retrieve Model** button, will present an XML model (or device schema) of all configurable parameters available for the VTMOS selected.

**Modeled Definition**
Direct XPath is more commonly used in a simple definition, where only one logical entity is being searched for. If the entity is not unique, or there are more than one nodes, only the first occurrence of the entity being searched for will be tested. The schema should be chosen using the node navigation tree.

Contextual XPath should be used to test all nodes of a certain type, for example, test all FastEthernet Interfaces where the context becomes FastEthernet. The context should be chosen using the node navigation tree in the left hand window pane. Once the context of the validation has been set the nodes must be selected in the right hand pane that will be validated within this context.

**XPath**
XPath will be populated with the schema path chosen.

**Add Evaluation**
This button invokes the wizard for adding a modeled definition evaluation.

**Evaluation List**
Lists all XPaths alongside test conditions and match criteria.

**Evaluation List Criteria**
Use the following evaluation list criteria.

- **Match All** — Match All evaluations added to the Compliance Definition.
- **Match Any** — Match Any of the evaluations added to the Compliance Definition.
- **Match None** — Match None of the evaluations added must be found in the Device Configuration.
- **Match One** — Match only One of the evaluations added to the Definition. If more than one of the evaluations are matched, the match fails.
- **Match Exactly** — Identically match all evaluations added to the definition; including the number of evaluations selected.

  **Note:** When using Match Exactly logic with an extraction or group parameter, the XPath option 'matches' must be selected. This is only applicable to modeled definitions.
- **Match Specific Number** — Matches a specific number of evaluations as defined by the user. For example, Match 2 out of the 6 evaluations listed. This choice activates an integer field called Specific Number.

**Number**
This is activated when the Match Specific Number is chosen. An integer must be entered here.

**Manual Override**
This allows the XPath to be overridden through a process of manually altering the Context/ Defined XPath.

**Update**
Updates screen.

**Edit**
Edits current selection.

**Delete**
Deletes current selection.

**Test**

The definition test button is enabled when editing or creating a definition, but not when opening a definition. Also, it is only available for modeled and native definitions (not scripts).

You use the definition test functionality to execute a definition against all open tabs, and view the results.

You can test definitions using native CLI configuration lines, native commands or device models. You can view results in the evaluation list either in detail, or as a summary.

| Definition Test window elements | Description |
|---|---|
| **Definition Test** window | When you click **Test**, the **Definition Test** window is displayed (it resembles the **Regex Tool** window).<br>When you import definitions from a device, the type of definition you are creating determines what content is imported from the device:<br>**For modeled and golden configuration definitions**<br>Imports the xml configuration from the device.<br>**For native CLI definitions**<br>Imports the CLI configuration for the device.<br>**For native commands definitions**<br>Imports the show commands from the device into the text area in the tab.<br>**Warning:** Importing a text file from a file with an xml extension may result in an error when you execute the test. |
| **Tabs** | You can add as many tabs as your memory allows. The definition is applied to each tab and the results are flagged on the tabs.<br>**Green flag**<br>Passed<br>**Red flag**<br>Failed<br>**Yellow flag**<br>Not assessed |
| **Evaluation list** | Results are displayed in the **Evaluation list** under a number of columns.<br>**Evaluation**<br>532: Is the same as XPath<br>533: Is the same as Evaluation Line<br>534: Is the same as Evaluation Line<br>This is the search criteria for the Definition or the XPath to search for in the case of Device Models<br>**Match Criteria**<br>The criteria used to match the device configuration: Match All, Match Any, None, One, Exactly, Specific Number<br>**Match Criteria Argument**<br>532: Is the same as Number<br>533: Is the same as Number<br>534: Is the same as Number |

| Definition Test window elements | Description |
|---|---|
| | Only available on group parameters and extractions. Same as Match Specific Number.<br>**Default Result**<br>The default result is the value defined in the **Evaluation Result if Context not found** option, that is, one of Fail, Pass, Not Assessed, and Not Applicable.<br>**Note:** If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.<br>User can opt to choose the result they wish to receive if the context is not found. The options are: Fail, Pass, Not Assessed, Not Applicable.<br>If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.<br>**Result**<br>Green text = Pass, Red text = Fail, Yellow text = Not Assessed/Not Applicable, Blue text =Error<br>**Restriction:** Script parameters and extractions are not supported in test evaluation lists. If any are found in the evaluation they will not be assessed during the test, and the overall definition result will be not assessed. |
| **Details mode** | You can toggle between Details and Summary mode to select the level of detail displayed in the test results. When in Summary mode, you can click on each evaluation to display detailed results. |
| **Clear all** | Clears the results from the Evaluation List and tabs. |
| **Test** | Click to run the test |
| **Close** | Closes the **Definition Test** window.<br>**Note:** The test tabs are only available when the window is open. |
| Menu bar | All options described are also available from the menu bar (File, Edit, Mode, Tabs). |

5. If you clicked the Add Evaluation button, the **Add Modelled Definition Evaluation** window displays. The fields on this window allow the user to define the parameters to the command. Use the following descriptions as a guide to filling in the fields displayed in the **Add Modelled Definition Evaluation** window.

   **Node**
   The node chosen for the modeled definition.

   **Node description**
   The description of the logical entity and name of the node selected are automatically populated here. This information is retrieved from the device schema based on the XPATH defined in the previous step and cannot be changed by the user.

   **XPath Function**
   The following table describes the syntax associated with an XPath Function:

| XPath syntax | Description |
|---|---|
| = | Equal to |
| != | Not equal to |
| > | Greater than |
| >= | Greater than or equal to |
| < | Less than |
| <= | Less than or equal to |
| Matches | Allows Regex to be entered. |
| Contains | Indicates that the specified argument is contained in the string. |
| Starts-with | The string starts with the specified argument. |
| Ends-with | The string ends with the specified argument. |

**Argument**
The value you want to search on specifically. This can be left empty to find all.

**Show CLI Text Boxes**
When selected this will show unmodeled commands. Normally the node will be ARG.999.

**Parameters**
This is an optional field. This field provides a drop down list for the type of parameter you want. There is also an **Insert Parameter** button used to insert the parameter.

**Note:** Placing a parameter inside another parameter is not supported.

When an argument in the Argument List is selected, the Argument Details in the lower section of the screen is populated. If changes are required to the Argument Details, they can be made at this point. Select Update to save amendments to the argument.

6. Click Next to continue.

The **Enter test condition** window displays. The test conditions are used to decide whether you want to test for the presence or absence of the CLI, or in the case of some CISCO commands, to check for the presence of the no form of the command (for example, `no ip http server`).

7. Use the following descriptions as a guide to filling in the fields displayed in the **Enter test condition** window.

**Test Condition**
Specifies one of the following test conditions that you can select from the dropdown list:

| Test condition | Description |
|---|---|
| **Present in Config** | Searches to locate the test condition in the configuration. |
| **Not Present in Config** | Search to ensure that the test condition does not appear in the configuration. |
| **Present and Disabled in Config** | Search to locate the test condition in the configuration. However, contrary to the **Present in Config** condition, this search looks for conditions in the configuration that are present but are disabled. For |

| Test condition | Description |
|---|---|
| | instance, in most CISCO devices entities are prefixed by "no" if they are disabled but present, for example, 'no ip proxy-arp' or 'no ip bootp' server. |

**Match Criteria**
The following table describes the **Match Criteria** syntax:

- **Match All** - Match all hits in the target device configuration. For example, if a contextual XPath gets 3 hits in a target device configuration, each hit must satisfy the defined XPath, or the match will fail.
- **Match Any** - Match any of the hits in the target device configuration.
- **Match None** - Match none of the hits in the target device configuration.
- **Match One** - Match any of the hits in the target device configuration. If more than one are matched, the match fails.
- **Match Exactly** - Identically match all hits in the target device configuration.
- **Match Specific Number** - Matches a specific number of hits in the target device configuration as defined by the user. For example, Match 2 out of the 6 hits listed. This choice activates an integer field called Specific Number.

**Specific Number**
This is activated when the Match Specific Number is chosen. An integer must be entered here.

**Evaluation result if context not found**
Specifies the result to receive if the context is not found. The options are: Fail, Pass, Not Assessed, and Not Applicable.

If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.

8. Click Finish to complete the Modeled Definition Evaluation.

   The **Enter Modeled Definition Details** window displays again.
9. Click Next to continue.

   The **Choose a Save Location** window displays.
10. Navigate through the tree structure, and choose the location to which you want to save the Compliance Definition. Otherwise, it is possible to create a new folder from here if required.
11. Click Finish to complete the creation of the Compliance Definition.

You can create another Compliance Definition using a device model by following the instructions in this procedure.

**Related tasks**
Searching for device configurations
Searches can also be conducted on device configurations: Search using native CLI configuration lines, Search using native commands and Search using device models.

## Creating compliance definitions using scripts

Script-based definitions allow you to compose your own validation logic, thereby enhancing your control over what you are trying to validate. Use this procedure to create compliance definitions using JavaScript.

For more information on using scripts, see “Compliance definitions scripting” on page 245.

You use the **Create a Definition** window of the Compliance user interface to create a new compliance definition.

**Tip:** You can copy an existing definition and modify it to create a new definition.

1. Select **Create->Definition** from the menu.

   The **Create a Definition** window displays.
2. Use the following descriptions as a guide to entering the appropriate information in the **Create a Definition** window.

   **Name**
   Name chosen to identify the compliance definition. The maximum number of characters for the name is 255. This is a mandatory field.

   **Description**
   Brief narrative attached to the compliance definition to be created that explains its function and use. The maximum number of characters is 4000.

   **Revision**
   This number is automatically assigned and initially given a value of 1. Each time the compliance definition is edited, the revision number increments by 1. This is for versioning control. The revision changes only if the entity is active.

   **Select Definition Type**
   Radio buttons that allow you to create the following types of compliance definitions:

| Radio button | Description |
|---|---|
| **Create compliance definition using CLI configuration lines** | Select this definition type if you want to define a Compliance Definition with a native definition that uses a stored configuration. Selecting this option causes the **Enter Native Definition Details** (CLI configuration lines) window to display. |
| **Create compliance definition using Native Commands** | Select this definition type if you want to define a Compliance Definition with Native Commands. Selecting this option causes the **Enter Native Definition Details** (Native Commands) window to display. |
| **Create compliance definition using a Device Model** | Select this definition type if you want to define a Compliance Definition with a modeled definition. Selecting this option causes the **Enter Modeled Definition Details** window to display. |
| **Create compliance definition using a Script** | Select this definition type if you want to define a Compliance Definition with a script. Selecting this option causes the **Enter Script-Based Definition Details** window to display. |
| **Create compliance definition using a Golden Configuration** | Select this definition type if you want to define a Compliance Definition using a device's golden configuration as a template for automatically generating evaluations. Selecting this option causes the **Select a Golden Device** window to display. |

   **Prev**
   Go to the previous selection.

   **Next**
   Go to the next selection.

   **Finish**
   Complete process.

   **Cancel**
   Cancel activities.
3. Select the **Create compliance definition using a script** radio button, and then click **Next**.

   The **Enter Script-Based Definition Details** window displays.
4. Edit the definition:

   **Script Type drop-down**
   Currently only JavaScript can be used to create a script-based definition.

**Script syntax and examples**

**Remember:** A script definition must return a boolean value **`true`** or **`false`**

You can use a number of methods that form part of a helper class specifically designed to help you write scripts. For more information on using scripts, see “Compliance definitions scripting” on page 245.

**Validate Syntax**
Checks to see if the JavaScript syntax entered is valid.

**Script Parameters**
These are external parameters that can be used by the JavaScript. They could be Global, Group or Extraction values.

For more information on script parameters, see “Creating script parameters” on page 272.

5. Click **Next**.

   The **Choose a Save Location** window displays.
6. Navigate through the tree structure, and choose the location to which you want to save the compliance definition. Otherwise, it is possible to create a new realm from here if required.
7. Click **Finish** to complete the creation of the compliance definition.

**Related reference**

Compliance definitions scripting
Standard native, native command and modelled definitions support basic ‘matching' and ‘not matching' capability. Use cases have arisen whereby other forms of matching logic are required and have led to the creation of a script-based definition. Script-based definitions allow the user to compose their own validation logic and hence are in full control of what they are trying to validate. Scripting also allows users to extract and retrieve information from an external source to be used as part of the compliance check.

## Compliance definitions scripting

Standard native, native command and modelled definitions support basic ‘matching' and ‘not matching' capability. Use cases have arisen whereby other forms of matching logic are required and have led to the creation of a script-based definition. Script-based definitions allow the user to compose their own validation logic and hence are in full control of what they are trying to validate. Scripting also allows users to extract and retrieve information from an external source to be used as part of the compliance check.

### Syntax

The script **must** include a function named `calculate` that accepts one parameter and returns `true` or `false` to indicate that the compliance evaluation has succeeded or failed.

**Note:** The parameter names are not fixed.

Here is an example of the script syntax:

```
function calculate(helper) {
    //enter javascript logic here
    return true;
}
```

This could also be written as:

```
function execute(helperMethods) {
    //enter javascript logic here
    return true;
}
```

At script runtime, the workflow engine passes the helper class to the function. Whatever name is chosen for the parameter, the name must be used within the body of the function.

## Methods

In order to describe the methods that are available for each class, the parameter names in the first example from the Syntax section will be used.

The helper class that is passed into the script function provides a set of utility methods for accessing network resource data, running regular expressions and xpaths and also the ability to run external commands to retrieve information from an external source.

*Table 56. Helper methods that support the helper class*

| Method | Description | Example |
|---|---|---|
| String getDeviceName() | Retrieves the device name for the device being validated | var name = helper.getDeviceName(); |
| String getDeviceVendor() | Retrieves the device vendor for the device being validated | var name = helper.getDeviceVendor(); |
| String getDeviceType() | Retrieves the device type for the device being validated | var dType = helper.getDeviceType(); |
| String getDeviceModel() | Retrieves the device normalised model for the device being validated | var model = helper.getDeviceModel(); |
| String getDeviceActualModel() | Retrieves the device actual model for the device being validated | var actualModel = helper.getDeviceActualModel(); |
| String getDeviceOS() | Retrieves the device OS for the device being validated | var os = helper.getDeviceOS(); |
| String getGlobalParameter(String parameterName) | Retrieves a global parameter value that was added to the parameter list within the script definition. | var ntpServerIP = helper.getGlobalParameter (“NTPServerIP”); |
| List<String> getGroupParameter(String parameterName) | Retrieves values for a group parameter that was added to the parameter list within the script definition. | var loghostList = helper.getGroupParameter (“LoggingServers”); |
| List<String> getExtractionParameter (String parameterName) | Retrieves values for a extraction parameter that was added to the parameter list within the script definition. | var FEsList = helper.getExtractionParameter (“ExtractFEs”); |
| void addInfo(String info) | Adds user defined messages to the evaluation log. These messages will be shown in the results data. | helper.addInfo(“This is a message that I want displayed in results”); |
| List<String> getInfo() | Retrieves the current list of informational messages | |
| boolean regexSearch(String data, String regex) | This utility method supports running a regular expression on a specified piece of data and returns true or false if it finds a match. | var result = helper.regexSearch (getNativeConfig(), “^hostname\s bfotest$”); |
| boolean xpathSearch(String data, String xpath) | This utility method supports running a xpath on a specified piece of data and returns true or false if it finds a match. | var result = helper.xpathSearch (getModelledConfig(), “configuration/hostname”); |

*Table 56. Helper methods that support the helper class (continued)*

| Method | Description | Example |
|---|---|---|
| String getNativeConfig() | Retrieves the current native configuration for the device being validated | var nativeConfig = helper.getNativeConfig(); |
| String getModelledConfig() | Retrieves the current modelled configuration for the device being validated | var xmlConfig = helper.getModelledConfig(); |
| List<String> getNativeConfigByDevice Name(String deviceName) | Retrieves the current native configuration for a device where name matches the name passed in. | var nativeConfig = helper.getNative ConfigByDeviceName("9.111.21.10"); |
| List<String> getModelledConfigBy DeviceName(String deviceName) | Retrieves the current modelled configuration for a device where name matches the name passed in. | var nativeConfig = helper.getModelled ConfigByDeviceName("9.111.21.10"); |
| String executeSystemCommand (String shellName, String shellArgs, String command, String checksum) | Executes a system command and returns the output of the system command.<br>The system command is a file that contains a shell script. The user must calculate a checksum for the file using icosutil. The checksum must then be entered in a native command set. | var response = helper.executeSystemCommand("/bin/sh", "", "getNetStat.sh", "<generated checksum>");<br>To generate a checksum for the script on the server run the following command: `<install_dir>/bin/icosutil CalculateChecksum getNetStat.sh`<br>**Important:** If an external script is modified after a checksum has been generated, then a new checksum must be generated and the native command set script must be updated. |
| String executeSystemCommand (String shellName, String shellArgs, String command, String responseRegExp, String checksum) | Executes a system command and returns the result of running a regular expression on the output of the system command. Only the first group match is returned.<br>The system command is a file that contains a shell script. The user must calculate a checksum for the file using icosutil. The checksum must then be entered in a native command set. | var response = helper.executeSystemCommand("/bin/sh", "", "getExternalData.sh", "^(w+)\s", <generated checksum>");<br>To generate a checksum for the script on the server run the following command: `<install_dir>/bin/icosutil CalculateChecksum getExternalData.sh`<br>**Important:** If an external script is modified after a checksum has been generated, then a new checksum must be generated and the native command set script must be updated. |

## Disabling scripting

An administration user, that is, a user with View System and Manage System activities, can disable the scripting functionality by setting the following system property to false:

**Scripting – Enable script execution**

The system checks this property at runtime, and if set to 'false', will not allow scripts to be run.

The default setting is 'true'

## Disabling external system commands

An administration user, that is, a user with View System and Manage System activities, can disable external system commands by setting the following system property to false:

**Scripting – Enable external system command execution**
The system checks this property at runtime, and if set to 'false', will not allow scripts to be run.

The default setting is 'true'

## Allowing classes and packages in scripting

To allow external Java classes and packages to be used in a script, the following system properties need to be configured:

**Note:** In order to change system properties a user must have View System and Manage System activities assigned to their user group.

**Scripting - Classes allowed in a script**
This system property stores a list of allowed Java classes. It is checked at runtime to determine if classes in a script are permitted.

The default list is empty, which means that no classes are permitted until a system administrator has added them to this list.

The allowed classes list is comma-separated, for example:

```
java.lang.String
```

```
java.lang.String, java.lang.StringBuilder, java.util.ArrayList
```

**Scripting - Packages allowed in a script**
This system property stores a list of allowed Java packages. It is checked at runtime to determine if packages in a script are permitted.

The default list is empty, which means that no packages are permitted until a system administrator has added them to this list.

The allowed classes list is comma-separated, for example:

```
java.util
```

```
java.util, java.util.regex, java.text
```

## Setting scripting timeout

An administration user, that is, a user with View System and Manage System activities, can edit the appropriate system property to define the length of time that scripts within a command set or compliance definition are allowed to run without completing before they are stopped:

**Scripting - Maximum script execution time**
The default script execution limit is 10 minutes, and a system administrator can set a time limit between one and 120 minutes.

If a script within a compliance definition times out, the definition result is marked 'NA'.

**Related tasks**

Creating global parameters
Global parameters are available to all evaluations used in a definition. Use this procedure to create global parameters as part of parameter administration.

Creating group parameters
Parameter groups involve a list of values that are supplied to the definition. Use this procedure to create group parameters.

Editing process parameters
Use this procedure to edit process parameters.

Creating script parameters

The script based parameter allows the user to manipulate extraction values, or if required extract values from an external source. It is very similar to the script based definition where it uses javascript. But in this case the script must return a list of values or single value. The script parameter can use extractions and other parameters types if required. Use this procedure to create script parameters.

Creating compliance definitions using scripts
Script-based definitions allow you to compose your own validation logic, thereby enhancing your control over what you are trying to validate. Use this procedure to create compliance definitions using JavaScript.

## Editing an existing compliance definition

A compliance definition captures the device characteristics that must be validated as part of a specific policy. The scope of a compliance definition may range from a single configuration line that must evaluated to a complex evaluation of multiple configuration snippets with regular expression logic and parameters. Use this procedure to edit an existing compliance definition.

Users have the option of editing an existing compliance definition at any time. When all changes have been saved, the user can activate the policy component as a new version. The previous version becomes inactive.

Follow these steps to edit an existing compliance definition.

1. Select the **Policy Definitions** tab, and select **Definitions**.
2. Right-click on the definition you want to edit, and select **Edit Definition**. Alternatively, select the definition and click the **Edit Definition** icon on the toolbar.

   The **Edit Definition Details** window displays.
3. Make any necessary edits to the compliance definition. Use the following descriptions as a guide to editing the fields displayed in the **Edit Definition Details** window.

   **Evaluation Line**
   The value or expression on which you want to search.

   **Parameters**
   This is an optional field. This field provides a drop down list for the type of parameter you want. There is also an **Insert Parameter** button used to insert the parameter.

   **Note:** Placing a parameter inside another parameter is not supported.

   **Match Criteria**
   Specifies a drop down list for the criteria used to match the device configuration. The following table describes the options in the drop down list:

| Match option | Description |
|---|---|
| **Match All** | Matches all evaluations added to the Compliance Definition. |
| **Match Any** | Matches any of the evaluations added to the Compliance Definition. |
| **Match None** | Matches none of the evaluations added must be found in the Device Configuration. |
| **Match One** | Matches only one of the evaluations added to the Compliance Definition. If more than one of the evaluations are matched, the match fails. |
| **Match Exactly** | Find and match all evaluations, and only these evaluations. If any found outside this criteria, the test result will Fail. |
| **Match Specific Number** | Matches a specific number of evaluations as defined by the user. For example, Match 2 out of the 6 evaluations listed. This choice activates an integer field called Specific Number. |

**Number**
This is activated when the Match Specific Number option is chosen. An integer must be entered here.

**Evaluation Result if Context not found**
You can opt to choose the result you wish to receive if the context is not found. The options are: Fail, Pass, Not Assessed, Not Applicable.

If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.

**Evaluation List Criteria**
Used to match evaluations shown in the list.

See Match Criteria (for Group/Extraction Parameter values) above for explanation of choices available.

**Regex Tool**
You use the regex tool to test native definition regular expressions against a device configuration or a snippet of CLI. The regex tool is available for both definitions using native CLI configuration lines, and using native commands. You can either create your regex in the tool, or edit it using the text in the evaluation field.

| **Regex Tool window elements** | **Description** |
|---|---|
| **Tabs** | You can add as many tabs as your memory allows. The regex in the **Regex Pattern** field is applied to each tab and the matches are highlighted.<br>• To create a new tab, click the green plus (+).<br>• To delete a tab, click the red X.<br>• To rename a tab, double-click the name.<br>**Note:** The test tabs are only available when the wizard is open. |
| **Regex Test Data** evaluation field | Configurations are displayed here, as are any matches when the regex is run.<br>Matches are alternately highlighted in yellow and blue. |
|  | The Import Device icon is displayed under the first tab. Using this, you can import a configuration from a device into the **Regex Test Data** field.<br>When you click this option, the **Device Select** dialog opens. Drill down into the device realms and select a device. Click **OK** to populate the **Regex Test Data** field |
|  | This icon is displayed next to the Device tree icon. Using this, you can import a configuration from a text file into the **Regex Test Data** field.<br>When you click this option, a standard file selection dialog opens. Drill down into your folders and select a file.<br>**Note:** You can only select a text file.<br>Click **Open** to populate the **Regex Test Data** field with the contents of the selected text file. |
|  | These icons are displayed next to the Import File icon. |

| Regex Tool window elements | Description |
|---|---|
|  | Once you have obtained matches, the arrow icons are enabled and you can use them to move from match to match.<br>Matches in the evaluation window are alternately highlighted in yellow and blue.<br>Currently selected matches are highlighted in grey.<br>These are enabled if there are matches on the selected tab. Up arrow highlights the previous match, down arrow highlights the next match. Current highlight matches are highlighted in grey |
| **Regex Pattern** field | Enter the regular expression for testing into the **Regex Pattern** field. |
| **Match** | Execute the test against all open tabs, and highlight the matches in each tab with a count of the number of matches returned on each tab. |
| **Clear Matches** | Clear the matches highlighted, as well as the Match count on each tab. |
| **OK** | Move the regular expression in the Regex Pattern field into the **Regex Test Data** field. |
| **Cancel** | Closes the **Regex Tool** window. |
| Menu bar | All options described are also available from the menu bar (File, Edit, Regex, Tabs):<br>**Edit**<br>In addition to the button options, you can access the cut, copy and paste functionality from the Edit menu.<br>**Regex**<br>In addition to the Regex button options, you can access a History dropdown from the Regex menu.<br>The last ten successful matches are stored as history, with the most recent one at the top.<br>**Note:** If the regex is over a certain length, the History dropdown list displays a truncated version of it. |

**Add**
Adds another selection.

**Update**
Updates screen.

**Edit**
Edits current selection.

**Delete**
Deletes current selection.

**Test**
The definition test button is enabled when editing or creating a definition, but not when opening a definition. Also, it is only available for modeled and native definitions (not scripts).

You use the definition test functionality to execute a definition against all open tabs, and view the results.

You can test definitions using native CLI configuration lines, native commands or device models. You can view results in the evaluation list either in detail, or as a summary.

| Definition Test window elements | Description |
|---|---|
| **Definition Test** window | When you click **Test**, the **Definition Test** window is displayed (it resembles the **Regex Tool** window).<br>When you import definitions from a device, the type of definition you are creating determines what content is imported from the device:<br>**For modeled definitions**<br>Imports the xml configuration from the device.<br>**For native CLI definitions**<br>Imports the CLI configuration for the device.<br>**For native commands definitions**<br>Imports the show commands from the device into the text area in the tab.<br>**Warning:** Importing a text file from a file with an xml extension may result in an error when you execute the test. |
| **Tabs** | You can add as many tabs as your memory allows. The definition is applied to each tab and the results are flagged on the tabs.<br>**Green flag**<br>Passed<br>**Red flag**<br>Failed<br>**Yellow flag**<br>Not assessed |
| **Evaluation list** | Results are displayed in the **Evaluation list** under a number of columns.<br>**Evaluation**<br>532: Is the same as XPath<br>533: Is the same as Evaluation Line<br>534: Is the same as Evaluation Line<br>This is the search criteria for the Definition or the XPath to search for in the case of Device Models<br>**Match Criteria**<br>The criteria used to match the device configuration: Match All, Match Any, None, One, Exactly, Specific Number<br>**Match Criteria Argument**<br>532: Is the same as Number<br>533: Is the same as Number<br>534: Is the same as Number<br>Only available on group parameters and extractions. Same as Match Specific Number.<br>**Default Result**<br>The default result is the value defined in the **Evaluation Result if Context not found** option, that is, one of Fail, Pass, Not Assessed, and Not Applicable. |

| Definition Test window elements | Description |
|---|---|
| | **Note:** If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.<br>User can opt to choose the result they wish to receive if the context is not found. The options are: Fail, Pass, Not Assessed, Not Applicable.<br>If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable; the overall result will be Pass.<br>**Result**<br>Green text = Pass, Red text = Fail, Yellow text = Not Assessed/Not Applicable, Blue text =Error<br>**Restriction:** Script parameters and extractions are not supported. If any are found in the evaluation they will not be assessed during the test, and the overall definition result will be not assessed. |
| **Details mode** | You can toggle between Details and Summary mode to select the level of detail displayed in the test results. When in Summary mode, you can click on each evaluation to display detailed results. |
| **Clear all** | Clears the results from the Evaluation List and tabs. |
| **Test** | Click to run the test |
| **Close** | Closes the **Definition Test** window.<br>**Note:** The test tabs are only available when the window is open. |
| Menu bar | All options described are also available from the menu bar (File, Edit, Mode, Tabs). |

4. Click **Finish** to complete the editing of the specified compliance definition.

The revision number on the modified compliance definition will have been incremented by one, and the compliance definition can now be activated.

It is not necessarily the compliance definition with the highest revision number that is active, as you can return to a previous version and activate it.

**Related tasks**

Editing an existing compliance extraction
Compliance extractions are a compliance component where specific chunks of data can be extracted from the native or modelled configuration or a show command. Use this procedure to edit any of the types of compliance extractions.

Creating global parameters
Global parameters are available to all evaluations used in a definition. Use this procedure to create global parameters as part of parameter administration.

Creating group parameters

Parameter groups involve a list of values that are supplied to the definition. Use this procedure to create group parameters.

## Creating compliance rules

A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Compliance Rules enable the user to combine multiple compliance definitions to build the full validation to which a device must adhere in order to pass a compliance test. Use this procedure to create a compliance rule.

To define new Compliance Rules or edit existing Rules, access to the User Interface wizard is required. Compliance Rules can cover all devices in an entire network, a subset of devices or a specific device. In defining Compliance Rules, a user must specify a VTMOS to which devices the Rule applies. It is simple for a user to copy an existing Rule, and modify some its components in order to create a new Rule.

Follow these steps to create a Compliance Rule.

1. Select **CreateRule**.

   The **Create a Rule** window displays. Mandatory fields are denoted by an * (asterisk).
2. Use the following descriptions as a guide to entering the appropriate information in the **Create a Rule** window.

   **Name**
   Specifies the name of the Compliance Rule. The maximum number of characters for the name is 255. This is a mandatory field.

   **Description**
   Specifies a brief narrative attached to the newly created Compliance Rule that explains its function or use. The maximum number of characters for the description is 4000.

   **Revision**
   This number is automatically assigned and initially given a value of 1. Each time the Compliance Rule is edited, the revision number automatically increments by 1. This is for versioning control.

   **Applicable Device Filter**
   This filter allows the ability to select which device VTMOS applies to this rule. As well as drop down selection for VTMOS, a regular expression is supported for all filters. The selected value entered in the Model Filter will be checked against both 'Model' and 'Actual Model' fields (as in the Device Viewer).

   **Note:** The devices selected in the device filter rule must appropriately reflect the type of devices against which all compliance definitions and remedial actions in the rule can be applied. For example, Juniper routers must not be included if the definitions in a rule are specific to CISCO routers only. If in this example Juniper routers were included in the compliance rule device filter, each of the Juniper routers would fail the compliance evaluation, since the CISCO specific compliance definition would not be found in the Juniper device configuration. On the other hand, if a rule with the device filter is set appropriately is used against a device that is not supported by that rule, the device will be marked NA (not applicable) in the test results.

   **Prev**
   Go to previous selection.

   **Next**
   Go to next selection.

   **Finish**
   Finish current activity.

   **Cancel**
   Cancel current activity without saving.
3. Click next to continue.

The **Build Graphical Rule** window displays. The **Build Graphical Rule** window consists of two panes. The left hand side of the screen consists of the Nodes section, which is used to build the rule graphically. The nodes graphically represent the different components that are used to assemble a rule. The right hand side of the screen is the working area, where the nodes are assembled to construct a rule.

4. Use the following descriptions as a guide to creating the Compliance Rule using the **Build Graphical Rule** window.

   **Start**
   The Start Node represents the starting point for the Rule. Each rule must have a Start Node to proceed.

   **Definition**
   Represents a definition as chosen by the user. The Definition Node is a decision point where an Action may be chosen depending if the outcome of the Definition is true (T) or false (F). Only one definition can be selected per Definition node.

   **Compliant**
   The Compliant node is connected to either the T or F condition of the Definition Node. This Node represents device compliance.

   **Non-Compliant**
   The Non-Compliant node is connected to either the T or F condition of the Definition Node. This Node represents noncompliance of devices. A corrective action can be specified in the event that devices are found to be noncompliant.

   **Note:** Any of the nodes may be removed at any stage in the design of the rule, by right clicking and selecting Delete.

   **Connecting lines**
   The connecting lines link nodes together. The lines are created by dragging the mouse between two nodes, using the small loop on the node graphic to make the connection as shown. In case adjustment of nodes is required, connecting lines may be removed at any time by right clicking, and choosing delete. A label may also be added to the connecting line.

   **Adding Labels**
   If the lines are double clicked - the flow properties can be modified, and a label added to the line.

   **Prev**
   Go to previous selection.

   **Next**
   Go to next selection.

   **Finish**
   Finish current activity.

   **Cancel**
   Cancel current activity without saving.

5. Drag the Nodes from the resource pane over to the working area and drop in place to compose a graphical rule consisting of T and F conditions.

   When the Definition node is dragged across to the working area, the **Select Definition** window displays.

6. You must select one of the previously created Compliance Definitions, or create a new one.

   **Note:** A user can select multiple definitions into a rule by repeating this step. By connecting the next definition to the True (T) outcome of the previous definition, the user can create AND logic between two definitions. For example, a device is compliant if it passes Compliance Definition 1 AND Compliance Definition 2. By connecting the next definition to the False (F) outcome of the previous definition the user can create OR logic between two definitions. For example, a device is compliant if it passes Compliance Definition 1, OR, if Compliance Definition 1 is not passed, it passes Compliance Definition 2.

7. When a user drags the Non Compliant node across to the working area, the **Select Action** window displays. When a definition is non compliant, a corrective action may be applied against the device to bring it back into compliance. Use the following descriptions as a guide to specifying the appropriate corrective action displayed on the **Select Action** window.

   **Remedial Action**
   A remedial action may be applied to the device to bring it back into compliance. These corrective actions can be defined in advance or on-demand when a rule is created. A corrective action is defined based on a command set that must have been defined previously in the ITNCM - Base application If a device violates a rule, the corrective action is run against the device by triggering the appropriate command set in ITNCM - Base.

   **No action**
   No action to be taken.

   **OK**
   Confirms most recent activity and saves.

   **Cancel**
   Cancel current activity without saving.

8. Click Next to continue.

   The**Choose a Save Location** window displays.

9. Navigate through the tree structure, and choose the location where you want to save the newly created Compliance Rule. Otherwise, it is possible to create a new folder from here if required.
10. Click Finish to complete the creation of the Compliance Rule.

The application does not stop the validation process once a Compliant/Non-Compliant verdict has been reached, and will always validate all definitions included in a rule. In other words, even if the first Compliance Definition in the rule already determines the Compliant/Non-Compliant outcome, the application will also present the outcome of another device validation against other Compliance Definitions in the rule.

**Related tasks**

Editing an existing action
Compliance actions can be remedial (invoking a commandset in ITNCM - Base) or informational (e-mail) by nature. Use this procedure to edit any of the types of compliance actions.

Defining advanced VTMOS filters
The Advanced VTMOS filter provides a way to choose multiple options when filtering on devices. Use this procedure to create device filters from multiple options.

## Editing compliance rules

A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Compliance Rules enable the user to combine multiple compliance definitions to build the full validation to which a device must adhere in order to pass a compliance test. Use this procedure to edit an existing Compliance Rule.

To define new Compliance Rules or edit existing Rules, access to the User Interface wizard is required. Compliance Rules can cover all devices in an entire network, a subset of devices or a specific device. Users have the option of editing an existing Compliance Rule at any time. When all changes have been saved, the user can activate Compliance Rule as a new version. The previous version becomes inactive.

Follow these steps to edit an existing Compliance Rule.

1. Access the Policy Definitions tab, and select Rules.
2. Right click on the Rule you want to edit, and select "Edit Rule". Alternatively, select the Rule and Click the Edit Rule icon on the toolbar.

   The **Edit Rule** window displays.

3. Make any necessary edits to the Compliance Rule. Amendments may be made to the graphical rule, and the action required in the event of non compliance. Use the following descriptions as a guide to editing the fields displayed in the **Edit Rule** window.

   **Name**
   Specifies the name of the Compliance Rule. The maximum number of characters for the name is 255. This is a mandatory field.

   **Description**
   Specifies a brief narrative attached to the newly created Compliance Rule that explains its function or use. The maximum number of characters for the description is 4000.

   **Revision**
   This number is automatically assigned and initially given a value of 1. Each time the Compliance Rule is edited, the revision number automatically increments by 1. This is for versioning control.

   **Applicable Device Filter**
   This filter allows the ability to select which device VTMOS applies to this rule. As well as drop down selection for VTMOS, a regular expression is supported for all filters. The selected value entered in the Model Filter will be checked against both 'Model' and 'Actual Model' fields (as in the Device Viewer).

   **Note:** The devices selected in the device filter rule must appropriately reflect the type of devices against which all compliance definitions and remedial actions in the rule can be applied. For example, Juniper routers must not be included if the definitions in a rule are specific to CISCO routers only. If in this example Juniper routers were included in the compliance rule device filter, each of the Juniper routers would fail the compliance evaluation, since the CISCO specific compliance definition would not be found in the Juniper device configuration. On the other hand, if a rule with the device filter is set appropriately is used against a device that is not supported by that rule, the device will be marked NA (not applicable) in the test results.

   **Prev**
   Go to previous selection.

   **Next**
   Go to next selection.

   **Finish**
   Finish current activity.

   **Cancel**
   Cancel current activity without saving.
4. Click Finish to complete the editing of the specified Compliance Rule.

The Revision Number on the modified Rule increments by 1, and the Compliance Rule can now be activated.

It is not necessarily the Compliance Rule with the highest Revision Number that is active, as the user may return to a previous version and activate. A new revision will only be created if the rule being edited is in an "active" or "inactive" state. No new revision will be created when the rule is in "workspace" mode.

**Related tasks**

Editing an existing action
Compliance actions can be remedial (invoking a commandset in ITNCM - Base) or informational (e-mail) by nature. Use this procedure to edit any of the types of compliance actions.

Defining advanced VTMOS filters

The Advanced VTMOS filter provides a way to choose multiple options when filtering on devices. Use this procedure to create device filters from multiple options.

## Creating an e-mail action

Compliance actions can be remedial (invoking a commandset in ITNCM - Base) or informational (e-mail) by nature. Use this procedure to create an e-mail compliance action.

It is simple for a user to copy an existing action, and modify some of its components in order to create a new action.

Use the **Create an Action** window of the User Interface to create a new e-mail compliance action.

Follow these steps to create a new e-mail compliance action.

1. Select **Create->Action**.

   The **Create an Action** window displays. Mandatory fields are denoted by an asterisk (*).
2. Use the following descriptions as a guide to entering the appropriate information in the **Create an Action** window.

   **Name**
   Name chosen to identify the compliance action. The maximum number of characters for the name is 255. This is a mandatory field.

   **Description**
   Brief narrative attached to the compliance action to be created that explains its function and use. The maximum number of characters is 4000.

   **Revision**
   This number is automatically assigned and initially given a value of 1. Each time the compliance action is edited, the revision number increments by 1. This is for versioning control.

   **Select Extraction Type**
   Radio buttons that allow you to create the following types of compliance actions:

| Radio button | Description |
|---|---|
| **E-Mail Template** | Select this option to create a compliance action using an e-mail template. Selecting this option causes the **Create The Action** window to display the e-mail template fields. The e-mail template provides you with the flexibility to construct a comprehensive message detailing the cause of a compliance violation. |
| **Remedial Action** | Select this option to create a compliance action using a remedial action. Selecting this option causes the **Create The Action** window to display the remedial action fields. The remedial action executes a commandset against device configurations, and brings the device back into compliance. |

   **Prev**
   Go to previous selection.

   **Next**
   Go to next selection.

   **Finish**
   Finish current activity.

   **Cancel**
   Cancel current activity without saving.

   **Email**
   Enter the E-mail address(es) of the recipient. Use a semicolon ( ; ) to separate the names.
3. Select the **E-Mail Template** radio button, and then click Next.

The **Create The Action** (e-mail template) window displays.

4. Use the following descriptions as a guide to entering the appropriate information in the **Create The Action** (e-mail template) window.

   **E-mail Header**
   Specifies the section of the e-mail template where you specify e-mail header information.

   **To:**
   Enter the e-mail address or addresses of the recipients for this e-mail compliance action.

   **Cc:**
   Enter the e-mail address or addresses of the recipients who should be copied on this e-mail compliance action.

   **Bcc:**
   Enter the e-mail address or addresses of the recipients who should be silently copied on this e-mail compliance action.

   **Subject**
   Enter a brief description for the subject of this e-mail compliance action.

   **E-mail Body**
   Enter any free text to describe this e-mail compliance action.

   **Prev**
   Go to previous selection.

   **Next**
   Go to next selection.

   **Finish**
   Finish current activity.

   **Cancel**
   Cancel current activity without saving.

5. Click Next to continue.

   The **Choose a Save Location** window displays.

6. Navigate through the tree structure, and choose the location to which you want to save the newly created compliance action. Otherwise, it is possible to create a new folder from this window, if required.
7. Click Finish to complete the creation of the compliance action.

You can create another e-mail compliance action by following the instructions in this procedure.

**Related tasks**

Creating a compliance policy
A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Use this procedure to create a compliance policy.

Editing a compliance policy
Users have the option of editing an existing Compliance Policy at any time. When all changes have been saved and the user has validated that the new version of the policy works correctly, the user can activate the Policy as a new version. Any previous active version becomes inactive.

## Creating a remedial action

Compliance actions can be remedial (invoking a commandset in ITNCM - Base) or informational (e-mail or notification) by nature. Use this procedure to create a remedial compliance action.

It is simple for a user to copy an existing action, and modify some of its components in order to create a new action.

Use the **Create an Action** window of the User Interface to create a new remedial compliance action.

Follow these steps to create a new remedial compliance action.

1. Select **Create->Action**.

   The **Create an Action** window displays. Mandatory fields are denoted by an asterisk (*).
2. Use the following descriptions as a guide to entering the appropriate information in the **Create an Action** window.

   **Name**
   Name chosen to identify the compliance action. The maximum number of characters for the name is 255. This is a mandatory field.

   **Description**
   Brief narrative attached to the compliance action to be created that explains its function and use. The maximum number of characters is 4000.

   **Revision**
   This number is automatically assigned and initially given a value of 1. Each time the compliance action is edited, the revision number increments by 1. This is for versioning control.

   **Select Extraction Type**
   Radio buttons that allow you to create the following types of compliance actions:

| Radio button | Description |
|---|---|
| **E-Mail Template** | Select this option to create a compliance action using an e-mail template. Selecting this option causes the **Create The Action** window to display the e-mail template fields. The e-mail template provides you with the flexibility to construct a comprehensive message detailing the cause of a compliance violation. |
| **Remedial Action** | Select this option to create a compliance action using a remedial action. Selecting this option causes the **Create The Action** window to display the remedial action fields. The remedial action executes a commandset against device configurations, and brings the device back into compliance. |

   **Prev**
   Go to previous selection.

   **Next**
   Go to next selection.

   **Finish**
   Finish current activity.

   **Cancel**
   Cancel current activity without saving.

   **Email**
   Enter the E-mail address(es) of the recipient. Use a semicolon ( ; ) to separate the names.
3. Select the **Remedial Action** radio button, and then click Next.

   The **Create The Action** (remedial action) window displays.
4. Use the following descriptions as a guide to entering the appropriate information in the **Create The Action** (remedial action) window.

   **Select the Remedial Action you wish to apply**
   Enter the required commandset. Navigate through the directories to locate the commandset you want to apply as a remedial action.

   **Restrict remedial action to one per rule.**
   Check this box to indicate that the rule will only generate one remedial action, regardless of whether there are multiple failure lines. This single remedial action performs a blanket fix and parameters are not assigned to it. By default, this check box is not checked. In this case, the rule will generate a remedial action against each failure.

**Prev**
Go to previous selection.

**Next**
Go to next selection.

**Finish**
Finish current activity.

**Cancel**
Cancel current activity without saving.

5. Click **Next** to continue.

   The **Choose a Save Location** window displays.
6. Navigate through the tree structure, and choose the location to which you want to save the newly created compliance action. Otherwise, it is possible to create a new folder from this window, if required.
7. Click **Finish** to complete the creation of the compliance action.

You can create another remedial compliance action by following the instructions in this procedure.

## Editing an existing action

Compliance actions can be remedial (invoking a commandset in ITNCM - Base) or informational (e-mail) by nature. Use this procedure to edit any of the types of compliance actions.

Use the **Edit Action** window of the User Interface to edit an existing compliance action. You use this window to edit the following types of compliance actions at any time:

- E-mail compliance action
- Remedial compliance action

When all changes have been saved, the user can activate the Policy Component as a new version. The previous version becomes inactive.

Follow these steps to edit an existing compliance action.

1. Access the Policy Actions tab, and select Actions.
2. Right click on the Action you want to edit, and select "Edit Action". Alternatively, select the Action and click the Edit Action icon on the toolbar.

   The **Edit Action** window displays.
3. Make any necessary edits to the compliance action.
4. Click Finish to complete the modifications.

The Revision Number on the modified compliance action increments by 1. The modified compliance action can now be activated.

It is not necessarily the compliance action with the highest Revision Number that is active, as the user can choose to activate a previous version .

**Related tasks**

Creating compliance rules
A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Compliance Rules enable the user to combine multiple compliance definitions to build the full validation to which a device must adhere in order to pass a compliance test. Use this procedure to create a compliance rule.

Editing compliance rules
A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Compliance Rules enable the user to combine multiple compliance definitions to build the full validation

to which a device must adhere in order to pass a compliance test. Use this procedure to edit an existing Compliance Rule.

## Creating compliance extractions

Compliance extractions are a compliance component where specific chunks of data can be extracted from the native or modelled configuration or a show command. You can create extractions that uses native CLI configuration lines, native commands, or device models.

**Tip:** Instead of creating a new extraction, you can copy an existing extraction and then modify its details.

1. In the Compliance UI, select **Extractions** in the left pane.
2. Select **Create** > **Extraction** from the menu. The **Create an Extraction** window is displayed.
3. Use the following descriptions as a guide to entering the appropriate information in the **Create an Extraction** window.

   Mandatory fields are denoted by an asterisk (*).

   **Name**
   Name chosen to identify the compliance extraction. The maximum number of characters for the name is 255. This is a mandatory field.

   **Description**
   Brief narrative attached to the compliance extraction to be created that explains its function and use. The maximum number of characters is 4000.

   **Revision**
   This number is automatically assigned and initially given a value of 1. Each time the compliance extraction is edited, the revision number increments by 1. This is for versioning control.

   **Select Extraction Type**
   Radio buttons that allow you to create the following types of compliance extractions:

| Radio button | Description |
|---|---|
| **Create extraction using CLI configuration lines** | Select this option to create a compliance extraction that uses native CLI configuration lines. A compliance extraction is very similar to a native definition. However, in the case of an extraction using native CLI configuration lines, a specific piece of data can be extracted from the matching CLI line or lines as specified in the extraction criteria. |
| **Create extraction using Native Commands** | Select this option to create a compliance extraction that uses Native Commands. In this option, a specific piece of data can be extracted from the matching native (show) commands as specified in the extraction criteria. The native commands are used for the search data and not the native configuration. |
| **Create extraction using a Device Model** | Select this option to create a compliance extraction that uses a device model. Modeled extractions are based on modeled device configurations. Modeled extractions use XPaths. An extraction XPath can be constructed to extract a certain piece of data from the modelled configuration. |

   **Prev**
   Go to previous selection.

   **Next**
   Go to next selection.

   **Finish**
   Finish current activity.

   **Cancel**
   Cancel current activity without saving.

4. Select the type of extraction you wish to create, and then click **Next**.
5. Define the extraction using the following information:

**Create extraction using CLI configuration lines**

You define the extraction using the **Enter Native Extraction Details** window.

Use the following descriptions as a guide to entering the appropriate information:

**Extraction Detail Line**
Enter the extraction line you want to match. Regex logic may also be used here.

**Parameters (Optional)**
Add local or global parameters to the extractions.

**Note:** When exported, the parameters will be exported and recreated on an import as for definitions.

**Insert Parameter**
Select either Local Parameter or Global Parameter, then click **Insert Parameter**.

**Extract What**
Choose the position of words you want to extract in the extraction line, for example, the second, fifth, or sixth word.

**Prev**
Go to previous selection.

**Next**
Go to next selection.

**Finish**
Finish current activity.

**Cancel**
Cancel current activity without saving.

**Create extraction using Native Commands**

**Native Commands**
Native Commands must be entered to indicate the Evaluation Source. Any type of show command may be entered in the Native command(s) criteria, for example, `show version`, `show config`, and so forth.

**Use cached show command response**
This option uses cached show commands from the last device import, and may be used to speed up response time.

**Extraction Detail Line**
Enter the extraction line you want to match.

**Parameters (Optional)**
Add local or global parameters to the extractions.

**Note:** When exported, the parameters will be exported and recreated on an import as for definitions.

**Insert Parameter**
Select either Local Parameter or Global Parameter, then click **Insert Parameter**.

**Extract What**
Choose the position of words you want to extract in the extraction line, for example, the second, fifth, or sixth word.

**Prev**
Go to previous selection.

**Next**
Go to next selection.

**Finish**
Finish current activity.

**Cancel**
Cancel current activity without saving.

**Create extraction using a Device Model**

**Model based on VTMOS**
Choose a device schema by selecting a VTMOS combination. Please note that a compliance Extraction created based on one device schema may be used against devices that are modeled using a different device schema, as long as those schemas share the nodes included in the compliance Extraction. With other words the scope of a compliance Extraction using a device model is not limited to the devices defined by the VTMOS that was used to retrieve the schema based on which the Extraction was built.

**Retrieve Model**
Selecting the "Retrieve Schema" button, will present an XML model (or device schema) of all configurable parameters available for the VTMOS selected.

**Model**
This is used in a simple definition. The schema should be chosen using the node navigation tree.

**Selected XPath**
XPath will be populated with the schema path chosen.

**Add Extraction**
This button invokes the **Add Modelled Extraction** window, which can be used to edit argument details.

**Extraction Content**
Displays the context for the chosen Modelled Definition.

**Node to Extract**
Displays the node chosen for extraction within the context.

**Edit**
Edit current selection.

**Prev**
Go to previous selection.

**Next**
Go to next selection.

**Finish**
Finish current activity.

**Cancel**
Cancel current activity without saving.

Once the selected XPath has been populated with the desired nodes and path, click **Add Extraction** to populate the **Add Modelled Extraction** window.

Use the following descriptions as a guide to entering the appropriate information in the **Add Modelled Extraction** window:

**Node**
The node chosen for the modelled extraction.

**Node description**
The description of the logical entity and name of the node selected are automatically populated here. This information is retrieved from the device schema based on the XPATH defined in the previous step and cannot be changed by the user.

**XPath Function**
Specifies the following XPath functions:

| XPath function | Description |
|---|---|
| = | Equal to |

| XPath function | Description |
|---|---|
| != | Not equal to |
| > | Greater than |
| >= | Greater than or equal to |
| < | Less than |
| <= | Less than or equal to |
| Matches | Allows Regex to be entered. |
| Contains | Indicates that the argument specified is contained in the string. |
| Starts-with | The string starts with the specified argument. |
| Ends-with | The string ends with the specified argument. |

**Argument**
The value you want to search on specifically. This can be left empty to find all.

**Show CLI Text Boxes**
When selected this will show unmodelled commands. Typically, the node will be ARG.999.

**Node to Extract**
Displays the node chosen for extraction within the context.

**Update**
Update screen following recent activity.

**Prev**
Go to previous selection.

**Next**
Go to next selection.

**Finish**
Finish current activity.

**Cancel**
Cancel current activity without saving.

To make changes to an argument, select it in the **Argument List** field.

To save changes, click **Update**.

6. Click **Next** to continue.
   The **Choose a Save Location** window is displayed.
7. Navigate through the tree structure, and choose the location to which you want to save the newly created compliance extraction. You can create a new folder from this window.
8. Click **Finish** to complete the creation of the compliance extraction.

You can create another compliance extraction, or edit the existing extraction.

**Related tasks**

Editing an existing compliance extraction
Compliance extractions are a compliance component where specific chunks of data can be extracted from the native or modelled configuration or a show command. Use this procedure to edit any of the types of compliance extractions.

Creating global parameters

Global parameters are available to all evaluations used in a definition. Use this procedure to create global parameters as part of parameter administration.

Creating group parameters
Parameter groups involve a list of values that are supplied to the definition. Use this procedure to create group parameters.

## Editing an existing compliance extraction

Compliance extractions are a compliance component where specific chunks of data can be extracted from the native or modelled configuration or a show command. Use this procedure to edit any of the types of compliance extractions.

Use the **Edit Extraction** window of the Compliane UI to edit an existing compliance extraction. You use this window to edit the following types of compliance extractions:

- Compliance extraction using native CLI configuration lines
- Compliance extraction using native commands
- Compliance extraction using a device model

When all changes have been saved, you can activate the Policy Component as a new version. The previous version becomes inactive.

1. Access the **Policy Extractions** tab, and select **Extractions**.
2. Right-click the extraction you want to edit, and select **Edit Extraction** from the context menu. Alternatively, select the **Extraction** and click the **Edit Extraction** icon on the toolbar.

   The **Edit Extraction** window displays.
3. Make any necessary edits to the compliance extraction.
4. Click **Finish** to complete the modifications.

The revision number on the modified compliance extraction increments by one. The modified compliance extraction can now be activated.

**Tip:** It is not necessarily the compliance extraction with the highest revision number that is active, as you can choose to activate a previous version .

**Related tasks**

Creating compliance extractions
Compliance extractions are a compliance component where specific chunks of data can be extracted from the native or modelled configuration or a show command. You can create extractions that uses native CLI configuration lines, native commands, or device models.

Editing an existing compliance definition
A compliance definition captures the device characteristics that must be validated as part of a specific policy. The scope of a compliance definition may range from a single configuration line that must evaluated to a complex evaluation of multiple configuration snippets with regular expression logic and parameters. Use this procedure to edit an existing compliance definition.

## Creating global parameters

Global parameters are available to all evaluations used in a definition. Use this procedure to create global parameters as part of parameter administration.

A Corrective Action may take parameters from the policy components to define a command set. For example, a parameter may be defined in the corrective action for IP Address and be provided to the corrective action through the compliance policy component. Use the **Parameter Administration** window to create global parameters.

**Note:** Avoid using the '-' (dash) character in global parameters if global parameters are to be used in a JavaScript definition or parameter.

Global parameters can be created within a cvompliance definition, or as part of parameter administration. Follow these steps to create global parameters as part of parameter administration.

1. Select **Admin** > **Parameter Administration**.

   The **Parameter Administration** window displays. Use the following descriptions as a guide to understanding the fields and icons on the **Parameter Administration** window.

   **Global Parameters**
   Specifies the tab that, when clicked, displays all global parameters. When a global parameter is specified within the **Parameter Administration** window, it is assigned a value which comes into effect when the Process is executed.

   When a global parameter is required within a Compliance Definition, the list of global parameters shown on the **Parameter Administration** window will be available for selection.

   **Parameter Groups**
   Specifies the tab that, when clicked, displays all parameter groups.

   **Process Parameters**
   Specifies the tab that, when clicked, displays all process parameters.

   **Parameter**
   Depending on which tab is clicked, displays all global parameters, parameter groups, or process parameters.

   **Description**
   Depending on which tab is clicked, displays descriptions for all global parameters, parameter groups, or process parameters.

   **Value**
   Depending on which tab is clicked, displays values for all global parameters, parameter groups, or process parameters.

   **Realm**
   Depending on which tab is clicked, displays the realms in which the global parameters, parameter groups, or process parameters reside.

   **New**
   Creates new record.

   **Delete**
   Deletes current selection.

   **Edit**
   Edit current selection.

   **OK**
   Confirm current activity.
2. Click the **Global Parameters** tab.

   All available global parameters are displayed on the **Parameter Administration** window.
3. To create a new global parameter, click the **New** button.

   The **Parameter Global Administration** window displays
4. Use the following descriptions as a guide to entering the appropriate information in the **Parameter Global Administration** window.

   **Enter Parameter Definition**
   Specifies that this is the window used to create a new global parameter.

   **Parameter**
   Enter the name for the global parameter you want to create.

   **Description**
   Enter a description for the global parameter specified in **Parameter**.

   **Value**
   Enter a value for the global parameter specified in **Parameter**.

**Realm**
Use the dropdown menu to select the realm in which the global parameter specified in **Parameter** will reside.

**Cancel**
Cancels current activity without saving.

**Apply**
Applies current activity,

5. Click the **Apply** button to confirm the creation of the global parameter. Alternatively, click the **Cancel** button to cancel the creation of the global parameter.

You can create another global parameter by following the instructions in this procedure.

**Related tasks**

Creating compliance extractions
Compliance extractions are a compliance component where specific chunks of data can be extracted from the native or modelled configuration or a show command. You can create extractions that uses native CLI configuration lines, native commands, or device models.

Editing an existing compliance definition
A compliance definition captures the device characteristics that must be validated as part of a specific policy. The scope of a compliance definition may range from a single configuration line that must evaluated to a complex evaluation of multiple configuration snippets with regular expression logic and parameters. Use this procedure to edit an existing compliance definition.

**Related reference**

Compliance definitions scripting
Standard native, native command and modelled definitions support basic ‘matching' and ‘not matching' capability. Use cases have arisen whereby other forms of matching logic are required and have led to the creation of a script-based definition. Script-based definitions allow the user to compose their own validation logic and hence are in full control of what they are trying to validate. Scripting also allows users to extract and retrieve information from an external source to be used as part of the compliance check.

## Creating group parameters

Parameter groups involve a list of values that are supplied to the definition. Use this procedure to create group parameters.

The string of values associated with parameter groups can be created manually or by importing them from a file in CSV format. Use the **Parameter Administration** window to create group parameters as part of parameter administration.

**Note:** Avoid using '-' (dash) character in group parameter names as it may cause problems when using it in JavaScript definitions or parameters

Group parameters can be created within a Compliance Definition, or as part of parameter administration. When a parameter group is specified within the **Parameter Administration** window, it is assigned a value which comes into effect when the process is executed. The parameter group is also associated with a realm.

Follow these steps to create group parameters as part of parameter administration.

1. Select **Admin->Parameter Administration**.

   The **Parameter Administration** window displays. Use the following descriptions as a guide to understanding the fields and icons on the **Parameter Administration** window.

   **Global Parameters**
   Specifies the tab that, when clicked, displays all global parameters. When a global parameter is specified within the **Parameter Administration** window, it is assigned a value which comes into effect when the Process is executed.

   When a global parameter is required within a Compliance Definition, the list of global parameters shown on the **Parameter Administration** window will be available for selection.

**Parameter Groups**
Specifies the tab that, when clicked, displays all parameter groups.

**Process Parameters**
Specifies the tab that, when clicked, displays all process parameters.

**Parameter**
Depending on which tab is clicked, displays all global parameters, parameter groups, or process parameters.

**Description**
Depending on which tab is clicked, displays descriptions for all global parameters, parameter groups, or process parameters.

**Value**
Depending on which tab is clicked, displays values for all global parameters, parameter groups, or process parameters.

**Realm**
Depending on which tab is clicked, displays the realms in which the global parameters, parameter groups, or process parameters reside.

**New**
Creates new record.

**Delete**
Deletes current selection.

**Edit**
Edit current selection.

**OK**
Confirm current activity.

2. Click the **Parameter Groups** tab.

   All available parameter groups are displayed on the **Parameter Administration** window.
3. To create a new parameter group, click the **New** button.

   The **Parameter Group Administration** window displays.
4. Use the following descriptions as a guide to entering the appropriate information in the **Parameter Group Administration** window.

**Parameter Group**
Specifies that this is the window used to create a new parameter group.

**Name**
Enter the name for the parameter group that you want to create.

**Description**
Enter a description for the parameter group specified in **Name**.

**Realm**
Use the dropdown menu to select the realm in which the parameter group specified in **Name** will reside.

**Values**
Identifies the values section of the **Parameter Group Administration** window.

**Add Value**
Enter a value for the parameter group specified in **Name**.

**Add**
Adds another selection.

**Update**
Updates view following recent activity.

**Delete**
Deletes current selection.

**Import from file**

**Values**
Displays the values from the CSV file specified after clicking the **Import from file** button.

**Cancel**
Cancels current activity without saving.

**Apply**
Applies current activity,

5. Click the **Apply** button to confirm the creation of the parameter group. Alternatively, click the **Cancel** button to cancel the creation of the parameter group.

You can create another parameter group by following the instructions in this procedure.

**Related tasks**

Creating compliance extractions
Compliance extractions are a compliance component where specific chunks of data can be extracted from the native or modelled configuration or a show command. You can create extractions that uses native CLI configuration lines, native commands, or device models.

Editing an existing compliance definition
A compliance definition captures the device characteristics that must be validated as part of a specific policy. The scope of a compliance definition may range from a single configuration line that must evaluated to a complex evaluation of multiple configuration snippets with regular expression logic and parameters. Use this procedure to edit an existing compliance definition.

**Related reference**

Compliance definitions scripting
Standard native, native command and modelled definitions support basic ‘matching' and ‘not matching' capability. Use cases have arisen whereby other forms of matching logic are required and have led to the creation of a script-based definition. Script-based definitions allow the user to compose their own validation logic and hence are in full control of what they are trying to validate. Scripting also allows users to extract and retrieve information from an external source to be used as part of the compliance check.

## Editing process parameters

Use this procedure to edit process parameters.

Use the **Parameter Administration** window to edit process parameters as part of parameter administration.

Since new process parameters cannot be created in the **Parameter Administration** window, process parameter creation must be carried out as part of process creation or editing. The **Parameter Administration** window can only be used for changing parameter description, value and realm.

When a parameter is specified within a Process, it is assigned a value which comes into effect when the Process is executed. However, if the parameter value specified in the process needs to be temporarily overridden, this can be overridden when building the process.

Follow the steps outlined under 'Procedure' to edit the values and descriptions for group parameters as part of parameter administration.

The only fields that can be modified in the **Parameter Administration** window are the description, value and realm. Changing the values for the parameter here will change the parameter values used in the process.

The **Parameter Administration** window is also useful when the parameter value is left blank when creating the process. The reason for this may be that the parameter value changes each time the process is executed. In this instance, the value entered into the **Parameter Administration** window will be the default parameter value when executed.

1. Select **Admin->Parameter Administration**.

The **Parameter Administration** window displays. Use the following descriptions as a guide to understanding the fields and icons on the **Parameter Administration** window.

**Global Parameters**
Specifies the tab that, when clicked, displays all global parameters. When a global parameter is specified within the **Parameter Administration** window, it is assigned a value which comes into effect when the Process is executed.

When a global parameter is required within a Compliance Definition, the list of global parameters shown on the **Parameter Administration** window will be available for selection.

**Parameter Groups**
Specifies the tab that, when clicked, displays all parameter groups.

**Process Parameters**
Specifies the tab that, when clicked, displays all process parameters.

**Parameter**
Depending on which tab is clicked, displays all global parameters, parameter groups, or process parameters.

**Description**
Depending on which tab is clicked, displays descriptions for all global parameters, parameter groups, or process parameters.

**Value**
Depending on which tab is clicked, displays values for all global parameters, parameter groups, or process parameters.

**Realm**
Depending on which tab is clicked, displays the realms in which the global parameters, parameter groups, or process parameters reside.

**New**
Creates new record.

**Delete**
Deletes current selection.

**Edit**
Edit current selection.

**OK**
Confirm current activity.

2. Click the **Process Parameters** tab.

   All available process parameters are displayed on the **Parameter Administration** window.
3. To edit the description and value for a process parameter, select a process parameter from the list and click the **Edit** button.

   The **Edit Process Parameter Definition** window displays.
4. Use the following descriptions as a guide to understanding the fields on the **Edit Process Parameter Definition** window.

**Enter Parameter Definition**
Specifies that this is the window used to edit the description and value for an existing process parameter.

**Parameter**
Displays the process parameter whose description and value are to be edited. This field cannot be modified.

**Description**
Enter a new description for the process parameter displayed in **Parameter**.

**Value**
Enter a new value for the process parameter specified in **Parameter**.

**Realm**
Use the dropdown menu to display the realm in which the process parameter specified in **Parameter** resides.

**Cancel**
Cancels current activity without saving.

**Apply**
Applies current activity,

5. Modify the Description and Value fields as required.
6. Click the **Apply** button to confirm the edit of the process parameter. Alternatively, click the **Cancel** button to cancel the edit of the process parameter.

You can edit another process parameter by following the instructions in this procedure.

**Related tasks**

Creating a compliance process
Use this procedure to define a new Compliance Process. Defining a new Compliance Process requires access to the User Interface wizard.

Editing a compliance process
Use this procedure to modify an existing Compliance Process. Modifying a new Compliance Process requires access to the User Interface wizard.

**Related reference**

Compliance definitions scripting
Standard native, native command and modelled definitions support basic ‘matching' and ‘not matching' capability. Use cases have arisen whereby other forms of matching logic are required and have led to the creation of a script-based definition. Script-based definitions allow the user to compose their own validation logic and hence are in full control of what they are trying to validate. Scripting also allows users to extract and retrieve information from an external source to be used as part of the compliance check.

## Creating script parameters

The script based parameter allows the user to manipulate extraction values, or if required extract values from an external source. It is very similar to the script based definition where it uses javascript. But in this case the script must return a list of values or single value. The script parameter can use extractions and other parameters types if required. Use this procedure to create script parameters.

Use the **Parameter Administration** window to edit process parameters as part of parameter administration.

Script parameters are very similar to script definitions, but the return type must be a string or a list of strings. Typically you would use script parameters to manipulate extraction data before returning the list of values to an existing native, native command or modelled definition. The script must include a function named `calculate` that accepts one parameter and returns `String` or `List<String>`.

**Note:** The parameter names are not fixed.

The following example extracts a list of NTP Server IP addresses from the device, parses the last octet of each IP and returns the list.

```
function calculate(helper) {

importClass(java.util.ArrayList);
var newList = new ArrayList();
var x =0;

var extractList = helper.getExtractionParameter("extractNTPServer").toArray();
//parse out the last octet of IP
for(x in extractList){
  var ip = extractList[x];
  var splitArray = ip.split("\\.");
  newList.add(splitArray[3]);
```

```
}

return newList;
}
```

**Restriction:** Any calls to `helper.addInfo("message")` within the script parameter will not be shown in results information, as this is only supported in the script definition.

This task describes how to create script parameters.

1. Select **Parameter->Parameter Administration**.

   The **Parameter Administration** window displays. Use the following descriptions as a guide to understanding the fields and icons on the **Parameter Administration** window.
2. Click the **Script Parameters** tab.

   All available script parameters are displayed on the **Parameter Administration** window.
3. To add a new script parameter, select the **New** button. The **Add Script Parameter Definition** window displays.
4. Use the following descriptions as a guide to understanding the fields on the **Add Script Parameter Definition** window.

   **Name**
   Identifier for the script parameter.

   **Description**
   Narrative to accompany the script parameter.

   **Realm**
   Realm where the script parameter will be placed

   **Script Type**
   The only option is JavaScript. JavaScript must be entered here.

   For more information on scripts, see "Compliance definitions scripting" on page 245.

   **Validate Syntax**
   This is used to validate the syntax of the JavaScript entered. See below for an example of a script parameter.

   **Script Parameters**
   Add parameters.
5. Click the **OK** button to confirm the addition of the script parameter. Alternatively, click the **Cancel** button to cancel.

The following example shows how a script definition can be used to check a device configuration has only one ntp server defined:

```
function calculate(helper) {

var ntpServerExtractionList = helper.getExtractionParameter("extractNTPServer");
helper.addInfo("Testing device "+helper.getDeviceName());

if(ntpServerExtractionList.size() == 1){
  helper.addInfo("Success = Only one NTP Server defined");
  return true;
}
helper.addInfo("Failed - There are "+ntpServerExtractionList.size()+" NTP servers present");
return false;
}
```

**Related reference**

Compliance definitions scripting

Standard native, native command and modelled definitions support basic 'matching' and 'not matching' capability. Use cases have arisen whereby other forms of matching logic are required and have led to the creation of a script-based definition. Script-based definitions allow the user to compose their own validation logic and hence are in full control of what they are trying to validate. Scripting also allows users to extract and retrieve information from an external source to be used as part of the compliance check.

## Defining advanced VTMOS filters

The Advanced VTMOS filter provides a way to choose multiple options when filtering on devices. Use this procedure to create device filters from multiple options.

The limitation of the VTMOS filter is that you can only choose one option or all options (*). The main advantage of the Advanced VTMOS filter is that you can choose multiple options. Alternatively, you can select all and eliminate some options. The Advanced VTMOS option is available only for Policies and Rules, and may be chosen on the dropdown menus that relate to Model and Operating System.

Follow these steps to define an advanced VTMOS filter.

1. Access the **Applicable Device Filter** window.

   Use the following descriptions as a guide to entering the appropriate information in the **Applicable Device Filter** window.

   **Vendor**
   The Vendor type should be selected from the dropdown menu. The contents of this listing are based on the vendor type of devices on the network, for example, CISCO and Juniper.

   **Type**
   By selecting a Vendor, the Type dropdown will be populated with only the device types pertaining to the previous Vendor selection, for example, router.

   **Model**
   The Model dropdown menu is populated with only the device model related to the previous Type selection.

   **OS**
   The OS dropdown menu is populated with only the device operating system corresponding to the previous Model selection.

   **Note:** Please note that Regex logic may be entered in the OS filter for the creation and editing of Policies and Rules only.
2. Click the **Advanced** button on the Model dropdown menu.

   The **Model Advanced** window displays.
3. Use the following descriptions as a guide to including or excluding specific device models that are displayed in the **Model Advanced** window.

   **List of device models**
   The Model list on the **Model Advanced** window replicates the previous listing on the dropdown menu. This enables the user to include or exclude specific Models, using the selection pane in the center of the window.
4. Click the **Advanced** button on the OS dropdown menu.

   The **OS Advanced** window displays.
5. Use the following descriptions as a guide to specifying values for the fields in the **OS Advanced** window.

   **>=**
   Used to filter all device operating systems that are greater than or equal to a particular version. For example: `>= 7.4`.

   **<=**
   Used to filter all device operating systems that are less than or equal to a particular version. For example: `<= 12.2`.

   **Range From**
   To filter device operating systems between certain version ranges use the **Range From** and **To** dropdown menus. For example, `From 7.4 To 12.2` returns devices with operating systems that range between version 7.4 and version 12.2 inclusive. These keywords also allow you to enter the same value. For example, `From 12.2 To 12.2` returns only those devices whose operating system is version 12.2.

The data displayed in the **Range From** dropdown menu is the operating system versions for the VTM level chosen. The OS Filter is useful where more than one Model type has been chosen.

**Note:** The asterisk (*) acts as a wildcard, and if left in any of the fields will return the results for all options in that particular selection.

**Related tasks**

Creating a compliance policy
A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Use this procedure to create a compliance policy.

Editing a compliance policy
Users have the option of editing an existing Compliance Policy at any time. When all changes have been saved and the user has validated that the new version of the policy works correctly, the user can activate the Policy as a new version. Any previous active version becomes inactive.

Creating compliance rules
A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Compliance Rules enable the user to combine multiple compliance definitions to build the full validation to which a device must adhere in order to pass a compliance test. Use this procedure to create a compliance rule.

Editing compliance rules
A Compliance Policy stipulates conditions that the devices must adhere to. A Compliance Policy contains Compliance Rules and can be configured to send an e-mail action in the event that a policy fails. Compliance Rules enable the user to combine multiple compliance definitions to build the full validation to which a device must adhere in order to pass a compliance test. Use this procedure to edit an existing Compliance Rule.

## Creating compliance definitions using a golden configuration

Fix Pack 1 Use this procedure to create compliance definitions using a golden configuration.

Golden configuration definitions are based on modeled device configurations, which is similar to SmartModel definitions. However, for golden configuration definitions you select a golden device, and the definition's evaluations are then automatically generated based on the modeled configuration of the golden device. Modeled definitions are all based on XPaths. An XPath is a search mechanism used in XML, and models an XML document as a tree of nodes.

A Golden compliance definition created based on one device's configuration may be used against devices that are modeled using a different device schema, as long as those schemas share the nodes included in the compliance definition. This also means that the scope of a compliance definition using a Device Golden configuration is not limited to the devices with the same VTMOS as the device in the compliance definition.

Only evaluations originating from specially marked regex fields in the golden configuration will be presented in the compliance definition GUI.

Automatically generated evaluations presented in the GUI can be edited and deleted like any manually created evaluation.

You can add evaluations (just as with SmartModel definitions), which will not override automatically generated evaluations, but rather be executed in addition to the automatic evaluations.

Automatically generated evaluations have the following test criteria by default:

**Test Condition**
Present in config

**Match Criteria**
Match All

**Evaluation result if context not found**
Fail

Automatically generated evaluations have the same default variable details as seen in the GUI when creating an evaluation, except in the case where a Regex has been specified in the golden configuration. In such a case the XPath function value will be ‘matches’.

When an '@@@(valid value)P@' Regex has been specified for an argument in the golden configuration, the evaluation will be marked as overridden, and will therefore be handled as an overridden evaluation in the GUI.

**Note:** The Regex will appear as '@@@P@' in the SmartModel XML configuration.

Automatically generated evaluations will not have parameters by default. If you add or update an evaluation to contain parameters, note the following information:

- Parameters defined in modeled definitions will automatically be passed to remedial actions, if configured to do so.
- Parameters passed to remedial actions can be viewed in the Remedial queue under the 'parameters' column.
- Parameters defined in remedial command sets need to have the same name as parameters defined in remedial command sets in Netcool Configuration Manager - Base.
- Placing a parameter inside another parameter is not supported.

**Tip:** You can copy an existing definition and modify some of its components to create a new definition.

1. Click **Create** > **Compliance Definition**.
   The **Create a Definition** window is displayed.
2. Enter a **Name** to identify the compliance definition. The maximum number of characters for the name is 255.
   This is a mandatory field.
3. Enter a brief **Description** that will be attached to the compliance definition to explain its function and use.
   The maximum number of characters is 4000.

   **Note:** For version control, a **Revision** number is automatically assigned and initially given a value of one. Each time the compliance definition is edited, the revision number increments. The revision changes only if the entity is active.
4. Use the following **Select definition type** information as a guide to create the required types of compliance definitions:

| Option | Description |
|---|---|
| **Create compliance definition using CLI configuration lines** | Select this definition type if you want to define a compliance definition with a native definition that uses a stored configuration. Selecting this option causes the **Enter Native Definition Details (CLI configuration lines)** window to display. |
| **Create compliance definition using Native Commands** | Select this definition type if you want to define a compliance definition with native commands. Selecting this option causes the **Enter Native Definition Details (Native Commands)** window to display. |
| **Create compliance definition using a Device Model** | Select this definition type if you want to define a compliance definition with a modeled definition. Selecting this option causes the **Enter Modeled Definition Details** window to display. |
| **Create compliance definition using a Script** | Select this definition type if you want to define a compliance definition with a script. Selecting this option causes the **Enter Script-Based Definition Details** window to display. |

| Option | Description |
|---|---|
| **Create compliance definition using a Golden Configuration** | Select this definition type if you want to define a compliance definition using a device's golden configuration as a template for automatically generating evaluations. Selecting this option causes the **Select a golden device** window to display. |

**Note:** You can navigate using the **Prev**, **Next**, **Finish**, and **Cancel** buttons.

5. Select **Create compliance definition using a Golden Configuration**, and then click **Next**.

   The **Select a Golden Device** window displays.

6. Choose a golden device either by selecting a realm, or by selecting a VTMOS combination, and then click **Next**.

   The **Modify Golden Config Evaluations** window is displayed.

7. If the evaluations automatically generated from the golden configuration are sufficient, click **Next**. Otherwise, use the following information to modify them:

| Option | Description |
|---|---|
| **Modeled Definition** | **Direct XPath:** Most commonly used in a simple definition, where only one logical entity is being searched for. If the entity is not unique, or there are more than one nodes, only the first occurrence of the entity being searched for will be tested. The schema should be chosen using the node navigation tree.<br><br>**Contextual XPath:** Can be used to test all nodes of a certain type, for example to test all FastEthernet Interfaces where the context becomes FastEthernet. The context should be chosen using the node navigation tree in the left hand window pane. Once the context of the validation has been set, the nodes must be selected in the right hand pane that will be validated within this context. |
| **XPath** | Will be populated with the schema path chosen. |
| **Add Evaluation** | This button invokes the wizard for adding a modeled definition evaluation. |
| **Evaluation List** | Lists all XPaths alongside test conditions and match criteria. Contains the same Evaluation list columns as described in the Test window below. |
| **Evaluation List Criteria** | Use the following:<br>**Match All**<br>Match All evaluations added to the Compliance Definition.<br>**Match Any**<br>Match Any of the evaluations added to the Compliance Definition.<br>**Match None**<br>Match None of the evaluations added must be found in the Device Configuration.<br>**Match One**<br>Match only one of the evaluations added to the Definition. If more than one of the evaluations are matched, the match fails.<br>**Match Exactly**<br>Identically match all evaluations added to the definition; including the number of evaluations selected.<br>**Match Specific Number**<br>Matches a specific number of evaluations as defined by the user. For example, Match 2 out of the 6 evaluations listed. This choice activates an integer field called Specific Number. |
| **Number** | Activated when the Match Specific Number is chosen. An integer must be entered here. |

| Option | Description |
|---|---|
| **Manual Override** | Allows the XPath to be overridden through a process of manually altering the Context/Defined XPath. |
| **Manual Override window elements** | Click **Manual Override** to display the Manual Override window with the following fields:<br>**Context XPath**<br>This field is populated when a Context XPath has been specified. It is the initial part of the overall XPath and is used as a search criteria. It can result in multiple hits in the target configuration.<br>**Context Nodes**<br>XML child Nodes of the context XPath whose values will be output in the evaluation results when the context XPath gets a hit.<br>**Defined XPath**<br>This field is always populated. It can be a complete XPath, or just the last part of an XPath(if a Context XPath has been specified).<br>If Context XPath has been specified, the defined XPath will be the last part of the XPath and will be applied to the child node(s) XML tree for each hit of the contextual XPath.<br>If Context XPath has not been specified, the defined XPath will be the complete XPath and will applied to the complete configuration XML tree. |
| **Update, Edit, Delete** | Updates the screen, edits or deletes the current selection. |
| **Test** | The definition test button is enabled when editing or creating a definition, but not when opening a definition. It is only available for modeled, golden and native definitions, but not scripts. You use the definition test functionality to execute a definition against all open tabs, and view the results. You can view results in the evaluation list either in detail, or as a summary. |
| **Definition Test window elements** | When you click **Test**, the **Definition Test** window is displayed. It resembles the Regex Tool window.<br>When you import definitions from a device, the type of definition you are creating determines what content is imported from the device:<br>**For modeled and golden configuration definitions**<br>Imports the xml configuration from the device.<br>**For native CLI definitions**<br>Imports the CLI configuration for the device.<br>**For native commands definitions**<br>Imports the show commands from the device into the text area in the tab.<br>**Warning:** Importing a text file from a file with an xml extension may result in an error when you execute the test. |
| **Tabs** | You can add as many tabs as your memory allows. The definition is applied to each tab and the results are flagged on the tabs.<br>**Green flag**<br>Passed<br>**Red flag**<br>Failed |

| Option | Description |
|---|---|
| | **Yellow flag**<br>Not assessed |
| **Evaluation list** | Results are displayed in the Evaluation list under a number of columns.<br>**ContextXpath**<br>This field is populated when a Context XPath has been specified. It is the initial part of the overall XPath and is used as a search criteria. It can result in multiple hits in the target configuration.<br>**DefinedXpath**<br>This field is always populated. It can be a complete XPath, or just the last part of an XPath (if a Context XPath has been specified).<br>If Context XPath has been specified, the defined XPath will be the last part of the XPath and will be applied to the child node(s) XML tree for each hit of the contextual XPath.<br>If Context XPath has not been specified, the defined XPath will be the complete XPath and will applied to the complete configuration XML tree<br>**Test Condition**<br>The Values as described in the test condition section further on.<br>**Match Criteria**<br>The criteria used to match the device configuration: Match All, Match Any, None, One, Exactly, Specific Number.<br>**Match Criteria Argument**<br>This is the same as Number.<br>Only available on group parameters and extractions. Same as Match Specific Number.<br>**ContextOveride / DefinedOveride / Override Enabled**<br>If Overridden is 'true', then the ContextOveride and DefinedOveride columns contain the override values.<br>**Context Informational Nodes**<br>The context nodes that have been defined.<br>**Default Result**<br>The default result is the value defined in the **Evaluation Result if Context not found** option, that is, one of Fail, Pass, Not Assessed, and Not Applicable.<br>You can choose the result that you wish to receive if the context is not found. The options again are Fail, Pass, Not Assessed, or Not Applicable.<br>**Note:** If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example you may have two Not Applicable result and one Pass, or all Not Applicable, yet the overall result will be Pass.<br>**Result**<br>Green text = Pass<br>Red text = Fail<br>Yellow text = Not Assessed/Not Applicable<br>Blue text =Error<br>**Restriction:** Script parameters and extractions are not supported. If any are found in the evaluation they will not be assessed during the test, and the overall definition result will be not assessed. |

| Option | Description |
|---|---|
| | **Note:** You can toggle between Details and Summary mode to select the level of detail displayed in the test results. When in Summary mode, you can click on each evaluation to display detailed results. |
| **Clear all, Test, Close** | Clears the results from the Evaluation List and tabs.<br>Click **Test** to run the test.<br>**Close** closes the Definition Test window.<br>**Note:** The test tabs are only available when the window is open. The File, Edit, Mode, and Tabs options are also available from the menu bar. |

**Note:** You can navigate using the **Rev**, **Next**, **Finish**, and **Cancel** buttons.

8. If you chose to click the **Add Evaluation** button, the **Add Modeled Definition Evaluation** window displays. Here you can define the command parameters using the following descriptions as a guide.

| Option | Description |
|---|---|
| **Node** | The node chosen for the modeled definition. |
| **Node description** | The description of the logical entity and name of the node selected are automatically populated here. This information is retrieved from the device schema based on the XPATH defined in the previous step and cannot be changed. |
| **XPath Function** | The following syntax is associated with an XPath Function:<br>**=**<br>Equal to<br>**!=**<br>Not equal to<br>**>**<br>Greater than<br>**>=**<br>Greater than or equal to<br>**<**<br>Less than<br>**<=**<br>Less than or equal to.<br>**Matches**<br>Allows Regex to be entered.<br>**Contains**<br>Indicates that the specified argument is contained in the string.<br>**Starts-with**<br>The string starts with the specified argument.<br>**Ends-with**<br>The string ends with the specified argument. |
| **Argument** | The value you want to search on specifically. This can be left empty to find all. |
| **Show CLI Text Boxes** | When selected this will show un-modeled commands. Normally the node will be ARG.999. |
| **Parameters** | This is an optional field. This field provides a drop down list for the type of parameter you want. There is also an **Insert Parameter** button used to insert the parameter. |

| Option | Description |
|---|---|
| | **Note:** Placing a parameter inside another parameter is not supported.<br>**Note:** When an argument in the Argument List is selected, the Argument Details in the lower section of the screen is populated. If changes are required to the Argument Details, they can be made at this point. Select Update to save amendments to the argument. |

9. Click Next to continue to the **Enter test condition** window. The test conditions are used to decide whether you want to test for the presence or absence of the CLI, or in the case of some CISCO commands, to check for the presence of the no form of the command (for example, no ip http server).
10. Use the following descriptions as a guide to the fields displayed in the **Enter test condition** window.

| Option | Description |
|---|---|
| **Test Condition** | Specifies one of the following test conditions that you can select from the dropdown list: |
| **Present in Config** | Searches to locate the test condition in the configuration. |
| **Not Present in Config** | Search to ensure that the test condition does not appear in the configuration. |
| **Present and Disabled in Config** | Search to locate the test condition in the configuration. However, contrary to the Present in Config condition, this search looks for conditions in the configuration that are present but disabled. For example, in most CISCO devices entities are prefixed by 'no' if they are disabled but present, as in 'no ip proxy-arp' or 'no ip bootp' server. |
| **Match Criteria** | The following table describes the Match Criteria syntax:<br>**Match All**<br>Match All hits in the target device configuration. For example, if a contextual XPath gets 3 hits in a target device configuration, each hit must satisfy the defined XPath, or the match will fail.<br>**Match Any**<br>Match any of the hits in the target device configuration.<br>**Match None**<br>Match none of the hits in the target device configuration.<br>**Match One**<br>Match any of the hits in the target device configuration. If more than one are matched, the match fails.<br>**Match Exactly**<br>Identically match all hits in the target device configuration.<br>**Match Specific Number**<br>Matches a specific number of hits in the target device configuration as defined by the user. For example, Match 2 out of the 6 hits listed. This choice activates an integer field called Specific Number. |
| **Specific Number** | This is activated when the Match Specific Number is chosen. An integer must be entered here. |
| **Evaluation result if context not found** | Specifies the result to receive if the context is not found. The options are: Fail, Pass, Not Assessed, and Not Applicable.<br>If there are a number of different results, the overall result will be Pass as long as there are no Fails in the result. For example, you may have two Not Applicable result and one Pass, or all Not Applicable, and yet the overall result will be Pass. |

11. Click **Finish** to complete the Modeled Definition Evaluation, and display the **Enter Modeled Definition Details** window.
12. Click **Next** to continue to the **Choose a Save Location** window.
13. Navigate through the tree structure, and choose the location to which you want to save the Compliance Definition. Otherwise, it is possible to create a new folder from here if required.
14. Click **Finish** to complete the creation of the Compliance Definition.

You can create another Compliance Definition using a device model, by following the instructions in this procedure.

## Creating compliance definitions using a 'device-specific' golden configuration

Fix Pack 2 Use this procedure to modify compliance definitions using a 'device-specific' golden configuration.

Device-specific golden configuration definitions are used to configure compliance checks on the differences between the device-specific golden and the current configurations for the same device. Two pre-defined device-specific golden configuration definitions are delivered with Netcool Configuration Manager, installed under the ‘Examples/GoldenConfiguration’ realm as a post installation task. One for each mode, they are:

**Non-strict mode**
NonStrictDeviceSpecificGolden

**Strict mode**
StrictDeviceSpecificGolden

Per default, the strict definition provided as an example is set to non-Strict.

**Important:** If strict mode is required, you must change this by editing the definition in the Netcool Configuration Manager - Compliance GUI, as described in What to do next.

These two definitions can cover all device-specific golden configuration definition handling, and they can be re-used in multiple Definition/Rule/Policy/Process combinations. If required, these definitions can be copied and edited in the GUI, but not created.

As part of the same post-installation task a default Rule/Policy combination that uses these definitions is created. The ‘Non Strict’ definition will produce an evaluation failure if a command in the device-specific configuration is changed or removed in the current configuration. The ‘Strict’ definition will produce the same failures as ‘Non Strict’, and in addition it will produce an evaluation failure if a command is changed or added in the current configuration. In other words, ‘Strict’ mode performs a cross-check from 'current' against 'device-specific golden', and vice versa. ‘Non Strict’ only checks 'device-specific golden' against current.

For example, if between the device-specific golden and current versions command A is added, command B is changed, and command C is removed, the following evaluation failures will be produced:

**NonStrictDeviceSpecificGolden failures**
A failure for the version of command B in the device-specific golden configuration

A second failure for command C in the device-specific golden configuration

**StrictDeviceSpecificGolden failures**
Both device-specific golden configuration failures as above.

A third failure for the version of command B in the current configuration

A fourth failure for command A in the current configuration

The additional evaluations produced as a result of the strict mode will have the following line in the evaluation result:

```
This evaluation XPath was generated as a result of 'Strict mode' being set and
compares elements in the current configuration against those in the 'device-
specific' configuration.
```

Instead of specifying evaluations in the definition, device-specific golden definition evaluations are generated 'on the fly' when compliance is running, based on the current and device golden smart-modeled configurations of the target device. This allows for simplified handling, as definitions do not have to be created for each device with a device-specific golden configuration specified. The evaluations automatically generated are based on XPaths,which require smart-modeled configurations.

**Note:** An XPath is a search mechanism used in XML, and models an XML document as a tree of nodes.

An example could be a hundred devices with device-specific golden configurations specified in a particular realm. In order to run device-specific golden compliance on all of these, the realm could just be included in the scope of a compliance process that contains one of the pre-defined policies delivered with Netcool Configuration Manager, such as the `Examples/GoldenConfiguration/NonStrictDeviceSpecificGolden` policy. When the process is run, compliance will automatically create and execute evaluations for each of the hundred devices.

**Non comparable values**

- Certain values in a configuration can be expected to be different between configuration versions, for example a timestamp or password value. These types of values are identified in the Driver schema for the device, and assigned a 'NonComparable' attribute. If a field is marked as 'Non Comparable', differences in the field values will not produce an evaluation failure. The evaluation will contain the wildcard (*) to accept all values. If a field value has been wild-carded due to a 'NonComparable' attribute, this will be indicated in the evaluation result with the following line:

  ```
  Elements in the Evaluation XPath have been wildcarded due to the presence
  of a NON_COMPARABLE attribute on that element in the Driver schema.
  ```

  **Note:** A new XML file is now delivered with the Drivers in order to support the 'NonComparable' checking. If the file is not present, an updated driver must be installed.

**Evaluation Criteria**

Device-specific evaluations are not defined via, or visible in, the Compliance Definition GUI. When generated at compliance execution, they have the following test criteria:

**Test Condition**
Present in config

**Match Criteria**
Match All

**Evaluation result if context not found**
Fail

The evaluation list criteria will be 'Match All'. (Match All evaluations added to the Compliance Definition).

The generated evaluations will be 'Defined' XPath evaluations, and will have same default variable details as seen in the GUI when creating an evaluation in, for example, a smart model definition. The generated evaluations will not have parameters.

**Tip:** You can copy an existing definition and modify its components to create a new definition.

1. To import the provided Strict or Non-Strict device specific definition, run the following command.

   **Note:** You perform this step after any installation and database upgrade steps are completed.

   ```
   cd <install_dir>/compliance/db/export/policies
   <install_dir>/compliance/bin/utils/policyImport.sh DeviceSpecificGoldenExamples.zip
   ```

2. Right-click an existing device-specific definition, and click **Edit Definition**.

   The **Edit Definition** window is displayed.

3. Enter a brief **Description** that will be attached to the compliance definition to explain its function and use.

   The maximum number of characters is 4000.

**Note:** For version control, a **Revision** number is automatically assigned and initially given a value of one. Each time the compliance definition is edited, the revision number increments. The revision changes only if the entity is active.

4. In the list of compliance definition types, only the **Create Compliance Definition using a device-specific Golden Configuration** radio button is enabled, and preselected.

   **Note:** You can navigate using the **Rev**, **Next**, **Finish**, and **Cancel** buttons.

5. Click **Next**.

   The **Enter device-specific Golden Config** window displays.

6. Select the **Strict** checkbox if strict mode is required.
7. Click **Next** to continue to the **Choose a Save Location** window.
8. Navigate through the tree structure, and choose the location to which you want to save the Compliance Definition. Otherwise, it is possible to create a new folder from here if required.
9. Click **Finish** to complete the creation of the Compliance Definition.

You can create another Compliance Definition using a device model, by following the instructions in this procedure.

To set the Strict example definition provided in the `/opt/IBM/tivoli/netcool/ncm/compliance/db/export/policiesDeviceSpecificGoldenExamples.zip` file to Strict, complete the following steps:

1. In the Netcool Configuration Manager - Compliance GUI, select the **Definitions** tab.
2. Browse to the **StrictDeviceSpecificGolden** compliance definition, right-click it, then select **Edit Definition**. The **Enter Definition Details** dialog box is displayed.
3. Click **Next** to advance to the **Enter Device Specific Golden Config Details** dialog.
4. Select the **Strict mode** option, and click **Next**.
5. In the **Choose Save Location** dialog, leave the default save location unchanged. and click **Finish**.

## Compliance process

During run time execution, all compliance entities work together to validate network resources against compliance policies. All results across all validations are available for review by the user until they are removed through housekeeping.

During run time execution, all Compliance Entities which have been defined as part of Compliance Administration are required to work together to validate network resources against Compliance Policies. Run time execution covers various aspects such as process and policy execution, search scenarios and scheduling.

The Compliance Management application will run the validation of devices against policies and generate the validation results. All results across all validations will be stored in the Compliance Management database, and are available for review by the user until they are removed through house keeping.

The user may only view those Processes/Devices/Actions for which they have security permissions for. This is controlled through both Netcool Configuration Manager - Base and **Admin** > **User Security Options**.

The Results screens are flexible and easy to use, the user has the abilities to:

- Sort the results based on column headers
- Increase and decrease column width to better view the data
- Hide and unhide rows and columns
- Access Summary and detailed information by allowing the user to drill down on specific devices to view configuration level detail
- Use customizable Paging feature for easy navigation through results
- Export Policies in the Validations screen

# Validating a network against compliance policies

During run time execution, all Compliance Entities which have been defined as part of Compliance Administration are required to work together to validate network resources against Compliance Policies. Run time execution covers various aspects such as process and policy execution, search scenarios and scheduling.

Please ensure that the correct security access is obtained before attempting to execute any processes. The user must be a member of a group who has "Execution" rights. This enables the user to execute compliance entities.

This task describes the run-time processes for validating a network against compliance policies.

- **Process execution** describes the various methods that may be used to invoke and run compliance processes can be validated against the network. It also describes the steps a user must take in order to execute the processes that have been created on the network. Process execution can be triggered by a number of events: on demand initiation, scheduled initiation and automatic initiation.

  **Note:** Please note in the event that realms are moved or renamed, any previously scheduled processes which are set to execute against devices involved in the changed realms shall execute against zero devices. This is only an issue if the realms are changed while the Netcool Configuration Manager - Compliance server is stopped.
- **Automatic initiation**. When a device configuration is updated it is propagated from Netcool Configuration Manager - Compliance to Netcool Configuration Manager - Compliance.

  Any compliance process that is associated with the device, triggers a process in Netcool Configuration Manager - Compliance that will first pull the new device configuration from Netcool Configuration Manager - Base, and then run the appropriate compliance policies against the device. This is known as the automatic Validation Process. This can be configured using the Automatic Validation Parameter in the Admin area of Netcool Configuration Manager - Compliance.
- **Policy execution** describes how compliance policies can be validated against the network. It also describes the steps a user must take in order to execute the policies that have been created on the network.

  **Note:** Please ensure that the correct security access is obtained before attempting to execute any policies. The user must be a member of a group who has "Execution" rights. This enables the user to execute compliance entities.
- **Run time filters** Netcool Configuration Manager - Compliance offers two distinct types of filter during run time to assist the user in choosing the correct policies and devices.

## Initiating on-demand policy validation

Process execution describes the various methods that may be used to invoke and run compliance processes can be validated against the network. On-demand policy validation initiation is invoked by the user. This occurs when a user manually selects a process in the execution tab, and invokes the execution to run immediately.

The following procedure outlines how to execute a process using on-demand initiation.

1. Navigate to the process in the **Execution** tab, either right click and select **execute process** or select the **Execute** icon
2. The **Execute Process Confirmation** screen will be displayed. This screen asks for confirmation that the process should be executed. Choose Yes.
3. When a process executes, the user interface defaults to the **Process Execution Summary** in the Results tab. The progress of the process execution can be tracked with the help of this screen. In the **Process Execution Summary** screen, an on-demand initiation will have an execution type of "unscheduled".

## Initiating scheduled policy validation

Process execution describes the various methods that may be used to invoke and run compliance processes can be validated against the network. Scheduled initiation describes the ability to plan a process execution once (either immediately or at a pre-defined time in the future) or on a regular basis. The execution date and time are required to determine when the next process run shall be.

The scheduling aspect of a process should be setup when the process is being created. However, if process scheduling needs to be added to an existing process, this may be done using the **Edit Process** screen. All dates/times specified in Netcool Configuration Manager - Compliance are server side.

The following procedure outlines how to execute a process using scheduled process initiation.

1. A scheduled process is configured on Step 4: Process Trigger of the **Create a Process** screen.
2. The Date and Time you wish to schedule the process execution is specified on this screen. Using the up and down arrows on the right hand side of the Server Time, configure the date and time as appropriate. The calendar feature can be invoked to assist in choosing the correct date by clicking on the icon to the furthermost right.
3. Click **Next** to proceed to the next screen.
4. When this scheduled process is invoked, the progress of the process execution can be tracked using the Process Execution Summary in the Results tab. On this screen, a scheduled initiation will have an execution type of 'Scheduled'.

An example of how scheduled initiation may be used is to run a security policy on Monday morning at 5 am.

## Initiating scheduled recurring policy validation

Scheduled recurring processes describe those processes which are required to run on a frequent basis at specified intervals (that is, daily, weekly, monthly) as determined by the user. An example of how scheduled initiation may be used is to run all security policies every morning at 5 am.

Process execution describes the various methods that may be used to invoke and run compliance processes that can be validated against the network. It also describes the steps a user must take in order to execute the processes that have been created on the network. Note that in the event that realms are moved or renamed, any previously scheduled processes which are set to execute against devices involved in the changed realms shall execute against zero devices. This is only an issue if the realms are changed while the ITNCM-Compliance server is stopped.

Process execution can be triggered by a number of events: on demand initiation, scheduled initiation and automatic initiation. The following describes each of these in detail.

**Note:** Please ensure that the correct security access is obtained before attempting to execute any processes. The user must be a member of a group who has "Execution" rights. This enables the user to execute compliance entities.

All dates/times specified in ITNCM-Compliance are server side.

Follow these steps to execute a process using scheduled recurring process.

1. A scheduled recurring process is configured on Step 4: Process Schedule of the **Create a Process** window.
2. There are a number of recurrence options available at this stage. Please use the following table to complete this screen as appropriate:

   **Hourly**
   Use this option to specify that the process should run each hour, or every *n* hours after the scheduled start time. For example, Every 3 hours after Scheduled Start.

   **Daily**
   Use this option to specify that the process should run every *n* days. For example, Every 5 days, or else every weekday (Monday - Friday).

**Weekly**
Use this option to specify that the process should run every *n* weeks on a specific day of the week. For example, Every 3 weeks on a Monday.

**Monthly**
Use this option to specify that the process should run on a specific day of every *n* months. For example, Day 30 of every 6 months. Or, you can specify that the process runs on a relative day of every month. For example, The First Monday of every 3 months.

**Yearly**
Use this option to specify that the process runs on a specific day and month of every year. For example, Every January 1st. Or, you can specify that the process should run on a relative day of the week of a specific month. For example, The First Monday of January.

3. Click Next to proceed to the next window.
4. When this scheduled recurring process is invoked, the progress of the process execution can be tracked using the Process Execution Summary in the Results tab. On this window, a scheduled initiation will have an execution type of "Scheduled".

## Initiating automatic policy validation

Process execution describes the various methods that may be used to invoke and run compliance processes can be validated against the network. Scheduled recurring processes describe those processes which are required to run on a frequent basis at specified intervals (i.e daily, weekly, monthly) as determined by the user.

All dates/times specified in Netcool Configuration Manager - Compliance are server side.

When a device configuration is updated it is propagated from Netcool Configuration Manager - Base to Netcool Configuration Manager - Compliance.

Any compliance process that is associated with the device, triggers a process in Netcool Configuration Manager - Compliance that will first pull the new device configuration from Netcool Configuration Manager - Base, and then run the appropriate compliance policies against the device. This is known as the automatic Validation Process. This can be configured using the Automatic Validation Parameter in the Admin area of Netcool Configuration Manager - Compliance.

**Process Results** When this scheduled process is invoked, the progress of the process execution can be tracked using the Process Execution Summary in the Results tab. On this screen, an automatic initiation will have an execution type of "Automated".

## Executing a policy

Policy execution describes the various methods that may be used to invoke and run compliance policies can be validated against the network. It also describes the steps a user must take in order to execute the policies that have been created on the network.

Please note in the event that realms are moved or renamed, any previously scheduled policies which are set to execute against devices involved in the changed realms shall execute against zero devices. This is only an issue if the realms are changed while the Netcool Configuration Manager - Compliance server is stopped.

Policy execution can be triggered by a number of events: on demand initiation, scheduled initiation and automatic initiation.

**Note:** Please ensure that the correct security access is obtained before attempting to execute any policies. The user must be a member of a group who has "Execution" rights. This enables the user to execute compliance entities.

The following outlines the steps required to execute an ad-hoc policy.

1. Navigate to the policy in the Execution tab, either right click and select execute policy or select the 'Execute' icon

2. The **Create & Execute Adhoc Process** screen will be displayed. This screen requests a name and description to be added for the purposes of the policy execution. The Name field will be pre-filled with the server date and time. The name field is mandatory. Click Next to progress.
3. The **Select Devices** screen shall be displayed.
4. The Devices/Realms that are required to execute the Policy against should be selected. Using the navigation tree in the Device pane, select the necessary devices or realms.

   The Check device coverage button will inform if all devices in selection are covered by the policies, which will allow the user to continue to the next step. If there is a problem with the device coverage, the **Policy Coverage Check** screen will be displayed. This will give a reason such as: Policy not applicable or No rule applicable.
5. Click Next on the **Select Device** screen to progress
6. Immediately before the **Parameters** screen is displayed, a pop-up box will appear to confirm the user would like to view parameters. Select 'Yes' to view the parameters (if any) from the selected policies. If parameters have been used in any of the policy definitions that are included in a process, the appropriate override value must be provided in this screen if required.
7. The **Report Options** screen is displayed. The following table describes the options available.

*Table 57. Report options*

| Option | Description |
|---|---|
| Generate Report | When checked this will generate a report each time that the policy is executed. By default this is unchecked. |
| Report Type | Options are Summary, Policy, Device and Validation Detail.<br><br>**Summary** reports provides a bar chart showing the results by result category, and another bar chart showing the breakdown of failed results by severity.<br><br>**Policy** reports list the compliance validation results for each device. The results can be further interrogated to produce the Validation Detail report.<br><br>**Device** Reports list the compliance validation results for each policy. The results can be further interrogated to produce the Validation Detail report.<br><br>The **Validation Detail** reports provides a further level of information on the Device/Policy reports to determine what impact the evaluation criteria had on the result. |
| Show Results | User can choose which Results they wish to report on. By default all validation results are shown, but the user can opt to exclude any of the following results: Pass, Exempt, Fail, Not Assessed |
| Show Severity Levels | User can choose which Severity Levels they wish to report on: Severity 1-5. By default all Severity Levels shall be included in the report, but users have the option to exclude certain severity levels from the report |

**Note:** The Show Results and Show Severity Levels report options are greyed out if the "Summary" report type is chosen. The Summary report is based on all validation results (i.e. Passed, Failed, Exempt, Not Assessed), and also includes all severity levels.

Please enter the information as required, and click Next to continue to the next screen.

8. The **Distribution** screen is displayed. This is an optional screen. Please note that report distribution and report storage options are only available for Scheduled reports.

   As part of report distribution, an e-mail message can be constructed using the template provided. The E-mail body is free-text and can be used to add any comments as required. There are a number of file types supported for the Report email attachment, including: PDF, HTML, Excel, Text, RTF, XML, PostScript and Result File.

   Report Storage provides ability to save the report result on the server for retrieval at a later date. Report storage when checked will store the report in the "Saved Reports" tab for later retrieval.
9. Click Finish to complete the Policy execution.
10. When the policy executes, the user interface defaults to the Process Execution Summary in the Results tab. The progress of the policy execution can be tracked with the help of this screen. In the **Process Execution Summary** screen, a policy executed will have an execution type of "AdHoc".

**Related tasks**

Applying policies (via wizard)
Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

## Applying filters before running policies

Netcool Configuration Manager - Compliance offers two distinct types of filter during run time to assist the user in choosing the correct policies and devices. These are Compliance Validation Policy Filter and Compliance Policy Validation Device Filter.

The following task describes Compliance Validation Policy Filter and Compliance Policy Validation Device Filter.

**Compliance Validation Policy Filter :** Users have the ability to define which compliance policies must be included as part of a specific device validation. An initial policy listing to which the selected devices must apply is presented to the user as shown in . This Policy listing consists of a hierarchy of folders grouping the policies together. The user has the ability to select a single policy, multiple policies or a policy group(s). If a policy is selected for the validation that does not apply to all selected devices, the validation process for that specific policy will skip the devices to which the policy does not apply.

**Compliance Policy Validation Device Filter:** Users have the ability to define the device(s) for which the validation must be executed. The device realm listing is synchronized from Netcool Configuration Manager - Base, and represents the choice of devices available in the Compliance validation process. The user has the ability to select a single device, multiple devices or a group of devices to which a specific policy (group of policies) applies.

# Viewing results

Netcool Configuration Manager - Compliance will run the validation of devices against policies and generate the validation results. All results across all validations will be stored in the Netcool Configuration Manager - Compliance database, and are available for review by the user until they are removed through house keeping.

The user may only view those Processes/Devices/Actions for which they have security permissions for. This is controlled through both Netcool Configuration Manager - Base and **Admin** > **User Security Options**.

The Results screens are flexible and easy to use, the user has the abilities to:

- Sort the results based on column headers

- Increase and decrease column width to better view the data
- Hide and unhide rows and columns
- Access Summary and detailed information by allowing the user to drill down on specific devices to view configuration level detail
- Use customizable Paging feature for easy navigation through results
- Export Policies in the Validations screen

The Results page gives the user access to compliance validation results based on their level of security. There are a number of different views in the Results tab, where validation results can be viewed and analyzed. Whilst the Home page provides a summary of all devices on the network, the Results tab indicates policy status in a greater level of detail.

Users have various methods to review these results. They can review results in context of the ad-hoc, unscheduled, scheduled or automated process that generated the results. Users only interested in policy violations may want to review the notifications that were generated during the various compliance validations. Users also have the ability to perform a detailed search through the results and immediately see the result of their search.

Remedial actions may be generated for devices that violate a policy. These remedial actions will be placed in the remedial actions queue. Network engineers can approve the remedial actions in this queue, which will then trigger a configuration change action to run against the device to bring the device back into compliance.

**Related tasks**

Viewing pre-emptive policies and results
Use the pre-emptive compliance functionality to check proposed configuration changes to a device against predefined compliance policies for that device. Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device. The capability is intended to enable customers to evaluate the impact of configuration changes against predefined compliance policies for a device.

Viewing device configurations
There are a number of options available for viewing device configurations. They can be viewed as Native Commands, Stored 'Show' Commands, or Modelled Configurations (for smart model devices).

Applying policies (via wizard)
Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

## Viewing detailed results

The Results page gives the user access to compliance validation results based on their level of security. There are a number of different views in the Results tab, where validation results can be viewed and analyzed.

This task describes how to view detailed results.

1. The results page allows the user to see the compliance results of individual compliance validation processes. Using the drop down menu on the left hand side of the screen, the result panel to view can be chosen.
2. Selecting the Validations result panel invokes the **Process execution Summary** screen. Compliance validation results for the most recently run processes are displayed in this Summary.
3. When it is first opened it shows the processes that have been started in the past 24 hours and the processes that have been scheduled to run in the next 24 hours. The Process execution summary screen captures the process name, state, number of devices validated, as well as other important information used in analyzing process execution.
4. Use the following table to understand the columns displayed on this screen.

| *Table 58. Process execution summary fields* | |
|---|---|
| **Field Name** | **Description** |
| Name | Name of the Process/Policy Validation |
| State | States may be: Scheduled, Queued, Running, Finished, Error |
| Executed By | The User ID of the user executing the validation is captured. The User ID is "System", if the process is scheduled or automated |
| Devices | The number of devices the validation was run against |
| Process Type | The Process Type is always "Compliance" |
| Execution Type | Types may be : adhoc, one-off scheduled, recurring scheduled, unscheduled, automated |
| Start Time | Date/time the validation started at |
| End Time | Date/time the validation finished at |
| Process RCK | Unique ID used in Netcool Configuration Manager - Compliance database for Process |
| Revision | Process revision number |
| Worker ID | The name of the evaluation engine being used |

5. Users may take advantage of the paging feature at the bottom of the **Process Execution Summary** screen, which provides the user with the ability to show all results at once, or to customize the number of results they see on the screen at a time. The paging buttons allow easy navigation through results.

   The paging feature only pages processes which are in a Finished state.
6. By selecting one of the process icons in the centre of the screen, the user can view finished processes (Finished), currently active processes (Running) and scheduled processes (Scheduled).
7. To view further information from the results provided in the Process execution summary, simply select one of the processes to view the Policy Validation Summary at the bottom of the screen. The Policy Validation Summary provides information on Policy name, Severity, Revision, Date, Count of Results - Pass, Failed, Not Assessed, Exempt.
8. Further information can be obtained on each Policy, by selecting Details.
9. The user can generate an ad-hoc process report from the Results tab, by clicking on the **Run Report** icon. When this is invoked a **Report** dialog is displayed. The parameter options here allow the user to configure a report as required.

   Large Validation reports may take a while to generate. On average every 1000 pages of detailed validations will take around 1 minute to generate.
10. The user has the ability to drill down on the validation to view the results, and then drill down on the results to see the device details. Users have the ability to click on Policies for which there are results, that is, those with Pass, Fail, Exempt or Not Assessed, and access further information on the Policy. This can be achieved by clicking on the **Details** icon on the bottom of the pane, which displays the sub options available for each device.

    **Note:** The 'View modelled config' option is only available for smart model devices.

**Related tasks**

Viewing pre-emptive policies and results

Use the pre-emptive compliance functionality to check proposed configuration changes to a device against predefined compliance policies for that device. Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device.

The capability is intended to enable customers to evaluate the impact of configuration changes against predefined compliance policies for a device.

Viewing device configurations
There are a number of options available for viewing device configurations. They can be viewed as Native Commands, Stored 'Show' Commands, or Modelled Configurations (for smart model devices).

Applying policies (via wizard)
Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

## Filtering results

Information can be filtered by Device and Compliance Status using filtering options.

The Device Filter supports wildcards (*), and may also be used in conjunction with the Compliance Status filter.

1. Results can be filtered by Device and Compliance Status using filtering options at the top of the page.
2. Enter the required filter. Select the **Search** icon.
3. If no results are found, the text "No policy result exists" is displayed.

## Generate validation report

The user can generate an ad-hoc process report from the Results tab.

This task describes how generate a validation report.

1. The user can generate an ad-hoc process report from the Results tab, by clicking on the **Run Report** icon. When this is invoked a **Report** dialog is displayed.
2. The parameter options here allow the user to configure a report as required.
3. Large Validation reports may take a while to generate. On average every 1000 pages of detailed validations will take around 1 minute to generate.

## Exporting policy results

You can export single or multiple policies results and save them as a CSV file.

This task describes the procedure for exporting results for policies.

1. Select the **Export >>** icon at the bottom of the **Process Execution Summary** window.
   The policy validation attributes are displayed.
2. When prompted, specify a location for the file.
   A message will be displayed to indicate if the export was a success.

The policy results will be exported as a CSV file, which contains all policy validation attributes regardless of the attributes chosen for the filter.

**Related tasks**

Exporting devices
The user has the ability to export devices to a user defined location in csv format.

## Approving remedial action

A Remedial Action is a procedure that can be executed in the event that a device violates a Policy. A remedial action approved in Netcool Configuration Manager - Compliance generates a UoW in Netcool Configuration Manager - Base, which will execute the commandset specified in the remedial action against the violating device. This alters the device configuration so that the violation is removed.

- Remedial actions can be defined within a Compliance Action, but are an optional component of a Compliance Rule. Depending on the security option selected, the entry in the Device Remedial Queue

may or may not require approval before it is being sent to the Netcool Configuration Manager - Base application.

- A user wishing to automatically approve and send Commandsets through to Netcool Configuration Manager - Base must be a member of a group with the “Automatic submission of remedial actions to Netcool Configuration Manager - Base security option checked. This setting can be found in Group Options Security.
- A user wishing to process Remedial Commandsets from the Remedial Approval queue, must be a member of a group with the Group Permission “Remedial Work Admin” checked. If this is not checked, the options to Approve/Reject/Delete will be grayed out in the Remedial Approval Results screen.

This task describes how to approve remedial actions.

1. Remedial commandsets may be automatically approved and sent to Netcool Configuration Manager - Base, or they may be placed in the Remedial approval queue awaiting approval. Use the following table to understand the other columns in the Remedial Queue.

*Table 59. Remedial queue fields*

| **Field** | **Description** |
|---|---|
| CommandSetName | Name of commandset violation occurred in |
| CommandSet Realm | Commandset realm affected |
| Policy | Policy associated with commandset |
| Device | Devices which are non-compliant |
| Realm | Realm in which the Policy resides |
| Status | Pending Approval, Ready to Execute, Sent to Netcool Configuration Manager - Base, Finished, Rejected, Error |
| Occurred At | Time at which the Violation occurred |
| Parameter | Parameter where the Violation was identified |
| Result | Pass, Fail, NA, Exempt |
| UOW ID | Corresponds to ITNCM - Base UOW ID |
| Failure Reason | Reason for failure of Policy |
| Execution User | User who executed the Policy |
| Approved By | Login ID of user who processed remedial action |
| Approved At | Time at which the remedial action was processed |
| CommandSetActionCK | Unique ID used in Netcool Configuration Manager - Compliance database for Remedial Actions |

   **Note:** A Remedial Action will not be created for a device that violates a policy if an earlier instance of that remedial action for this device is still in Pending status in the Netcool Configuration Manager - Base approval queue.
2. The approval options are accessed by right clicking on the Commandset in the Remedial Approval queue. If the commandset is approved, it will be pushed down to Netcool Configuration Manager - Base where the configuration shall be updated accordingly.
3. The UOW ID should be noted, when looking for the commandset in Netcool Configuration Manager - Base

   The UoW approval settings defined in the Netcool Configuration Manager - Base platform will also apply to the UoWs submitted through the Netcool Configuration Manager - Base application. This

means that Remedial Actions may require further approvals in Netcool Configuration Manager - Base depending on the authorization of the user who was defined at install time.

Users may take advantage of the paging feature, which provides the user with the ability to show all results at once, or to customize the number of results they see on the screen at a time. The paging buttons allow easy navigation through results. The paging feature only pages processes which are in a Finished state.

## Managing performance of compliance servers

You can configure properties that are designed to influence performance of compliance servers.

To ensure that you have configured the compliance servers correctly, complete the following steps.

1. Split compliance into multiple runs if you have configured more than one compliance server.

   Each compliance run can be processed by only one compliance server; a compliance run cannot be split across multiple servers.
2. Ensure that the server that runs compliance has sufficient memory before adding compliance server instances, or changing the default heap size. Each compliance server instance has a default maximum heap size of 2GB.
3. If needed, change the number of devices evaluated simultaneously in compliance:
   a) Increase or decrease the number of devices that a compliance run can connect to and evaluate simultaneously. The default is 5. Configure the following setting in the `rseries.properties` file on the compliance server:

   ```
   WorkFlowManager/threadsPerProcess=5
   ```

   b) Ensure that the thread pool size for the compliance server is greater than the `threadsPerProcess` value. To change this value, edit the following property in the `WorkFlowManager.process` file:

   ```
   poolSize=10
   ```

# Chapter 5. Using the DASH portlets

The Activity Viewer and wizards, as well as the ability to launch the stand-alone Netcool Configuration Manager UIs, are installed into the DASH. You access them from the context menus in Network Manager IP Edition or Tivoli Netcool/OMNIbus

**Remember:** You can launch the stand-alone Netcool Configuration Manager UIs (sometimes referred to as the thick-client UIs), from the DASH thick-client launch portal.

**Note:** You can also launch the stand-alone Netcool Configuration Manager UIs in context from within Network Manager. Specifically, you can access the Configuration View/Edit, IDT, and Find Device UIs.

## Activity Viewer overview

The Activity Viewer presents information about configuration and compliance events recorded against network devices in a sequential timeline view. This data is extracted from historical and audit logs.

You access the Activity Viewer from Network Manager IP Edition or Tivoli Netcool/OMNIbus.

The **Activity Viewer** displays information for up to two devices selected in Network Manager IP Edition or a single device selected in Tivoli Netcool/OMNIbus, before launching the **Activity Viewer** in context.

- You can view the results of network policy compliance checks against a device, and see when a device configuration was last policy-compliant.
- You can see which user initiated an activity, or unit of work (UOW), against a device.
- You can access further details about automated and ad-hoc activities, and view the configurations retrieved from a device. For example, you can view IDT sessions initiated against that device.
- You can refine the data retrieved against a device by applying the following filters:

  **Time**
  Presents you with all activity recorded against a device within a configurable time period.

  You can filter by the Start Date and Time, and End Date and Time.

  **Note:** Times are stored in GMT in the database. Please adjust the time filter based on your current time zone.
- You can launch the following Netcool Configuration Manager user interfaces from the Activity Viewer using the right-click menu:

  **IDT**
  From the IBM Tivoli Netcool Configuration Manager Device Terminal (IDT) you access a device through a telnet, SSH1 or SSH2 session

  **Configuration Editor**
  From the Netcool Configuration Manager Configuration Editor you view and edit configurations and command sets.

  **Netcool Configuration Manager Configuration Diff wizard**
  From the Configuration Diff wizard you view any differences between two configurations.

## Netcool Configuration Manager wizard overview

The wizards deliver streamlined versions of functionality derived from the standard Netcool Configuration Manager user interfaces.

**Tip:** If you hover over a command set or policy resource in the navigation tree, a tooltip is displayed showing the resource's VTMOS.

**Apply Native Command Set wizard**
Use to apply predefined native command sets to a device.

Launch with a device selected either in the **Activity Viewer** or Network Manager IP Edition.

**Apply Modeled Command Set wizard**
Use to apply predefined command sets to a device.

Launch with a device selected either in the **Activity Viewer** or Network Manager IP Edition.

**Policy Validation wizard**
Use this wizard to apply predefined policies to a device.

Launch with a device selected either in the **Activity Viewer** or Network Manager IP Edition.

**Synchronize Configuration wizard**
Use this wizard to ensure that the running and stored (or candidate) configurations on a device are identical.

Launch with a device selected either in the **Activity Viewer** or Network Manager IP Edition.

**Submit Configuration wizard**
Use this wizard to apply a configuration to a device.

Launch with a configuration selected in the **Activity Viewer**.

## Viewing device-specific events in the Activity Viewer

The Activity Viewer displays device-specific activities for up to two devices at a time. You can launch it in context from the Network Manager Network Views and the Tivoli Netcool/OMNIbus Active Event List (AEL).

Before you access the Activity Viewer from Tivoli Netcool/OMNIbus or from Network Manager, you select a device, or an event recorded against a device. You then launch the Activity Viewer from the context menu, and it opens with summary information recorded against a device displayed in a sequential timeline view. You can select up to two devices before launching the Activity Viewer from Network Manager, or one device when launching the Activity Viewer from Tivoli Netcool/OMNIbus.

The Activity Viewer displays the most recent UOW events and configuration changes for a device in the timeline window. This information goes back 30 days, either from the date it is being launched, or from the date of the event (if launched from the AEL).

1. Scroll left to see the device history going back 30 days.

   Depending on the specific device history, some or all of the following general fields and icons are present in the Activity Viewer:

   **Configuration icon** 
   Use this icon and the additional icons superimposed on it to view a graphical representation of the status of the configuration change.

   **Unit of work (UOW) icon** 
   Use this icon and the additional icons superimposed on it to view a graphical representation of the status of the UOW.

   **IDT** 
   This icon indicates that an IDT session was responsible for either a UOW or a configuration change, or both.

   **Report** 
   This icon indicates that a report is available.
2. Use the following information to understand the device history presented on the **Summary** screen.

   **UOW type**

   **Auto-discovery** 
   Indicates a UOW type of Auto-discovery.

**Import**
Indicates a UOW type of Import.

**Synchronize**
Indicates a UOW type of Synchronize.

**Apply command set**
Indicates modeled command set.

**Apply native command set**
Indicates native command set.

**Apply search set**
Indicates search set will be applied.

**Submit configuration**
Indicates that configuration will be submitted.

**Show differences**
Indicates that differences will be retrieved.

**Default**
Default UOW icon

**Execution status**

**Pass**
Indicates execution passed.

**Fail**
Indicates execution failed.

**Unknown**
Indicates execution status was inaccessible.

**Calling process**

**API**
Indicates API calling process.

**GUI**
Indicates GUI calling process.

**Compliance**
Indicates compliance calling process.

**IDT**
Indicates IDT calling process.

**IDT user**
Indicates IDT user calling process.

**Unknown**
Indicates unknown calling process.

**Right-click configuration menu**

**Open configuration**

**Edit configuration**

**Compare versions**

**IDT manual login**

**IDT automatic login**

**Apply native command set**

**Apply command set**

**Perform policy check**

**Synchronize device**

**Submit configuration**

**Right-click UOW and IDT menu**

**View IDT log (IDT only)**

**View UoW log (UOW only)**

**IDT manual login**

**IDT automatic login**

**Apply native command set**

**Apply command set**

**Perform policy check**

**Synchronize**

3. Launch one of the following TIP-based wizards:

**Apply Command Set wizard**
Use the Apply Command Set wizard to apply predefined command sets to devices.

**Policy Validation wizard**
Use the Policy Validation wizard to apply predefined policies to devices.

**Synchronize Configuration wizard**
Use the Synchronize Configuration wizard to ensure that the running and stored (or candidate) configurations on a device that you have selected in the Activity Viewer are identical.

**Submit Configuration wizard**
Use the Submit Configuration wizard to apply a configuration to a device that you have selected in the Activity Viewer.

4. Launch one of the following user interfaces:

**IDT**
From the IBM Tivoli Netcool Configuration Manager Device Terminal you access a device through a telnet, SSH1 or SSH2 session.

Using the IDT, you can:

- View all changes made to devices (via the device log)
- Synchronize device configurations

**Configuration Editor**
From the IBM Tivoli Netcool Configuration Manager Configuration Editor you view and edit configurations and command sets.

All configurations and command sets regardless of VTMOS (vendor, type, model, operating system) are displayed as a graphical folder tree (configuration catalog).

You can have multiple configuration editor/command set editor sessions open at the same time.

**Netcool Configuration Manager Configuration Diff wizard**
From the Configuration Diff wizard you view any differences between two configurations.

The configurations being compared can be any that exist in the database, regardless of whether it has been obtained from an actual network resource or simply entered by a user as a draft configuration.

Regardless of which type of configuration comparison you perform, your access rights (determined by group membership) dictate the commands for which you can view any differences.

Generating a list of configuration differences allows you to view any differences in command values between one configuration (or a part of that configuration) and another.

Network resources may also be compared to each other; the system will simply compare the current configuration of each. If no current configuration exists, the default draft (partial configuration) will be used.

**Related tasks**

Applying native command sets (via wizard)
Native command sets are defined by your administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying native command sets** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager.

Applying modeled command sets (via wizard)
Modeled command sets are defined by an administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying modeled command sets** wizard. You access the wizard from either the Activity Viewer or from the Network View, Hop View and Path View in Network Manager.

Applying policies (via wizard)
Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

Synchronizing configurations (via wizard)
When the running and the stored (or candidate) configurations on a device are out of synch, you identify the correct configuration and use it to replace the incorrect one so that the two are synchronized. To do so you submit a synchronization request as you would any other unit of work (UOW). You access the Synchronization wizard from either the Activity Viewer or from the Network View in Network Manager IP Edition.

Applying configurations (via wizard)
You apply a configuration to a device using the Submit Configuration wizard, which you access from the Activity Viewer.

## Activity Viewer menus

For specific menu items to be displayed, the required roles have to be assigned. Menu items are also filtered based on support levels and managed states of a device or configuration.

*Table 60. Menu items dependencies*

| Menu item | TIP roles | Functionality | Permissions | Support |
|---|---|---|---|---|
| View UOW Log | N/A | N/A | View | N/A |
| View IDT Log | N/A | N/A | View | N/A |
| IDT Automatic | ncmIDTUser | IDT Access<br>IDT Allow Auto Login | View | N/A |

*Table 60. Menu items dependencies (continued)*

| Menu item | TIP roles | Functionality | Permissions | Support |
|---|---|---|---|---|
| IDT Manual | ncmIDTUser | IDT Access<br>IDT Allow Manual Login | View | N/A |
| Apply Command Set | ncmConfig Change | Execute Configuration Change | View<br>Execute | SmartModel Device |
| Apply Native Command Set | ncmConfig Change | Execute Configuration Change<br>Apply Native Command Sets | View<br>Execute | SmartModel/ Standard Device |
| Perform Policy Check | ncmPolicyCheck | Execute Compliance Policy | View | SmartModel/ Standard Device |
| Synchronize Device | ncmConfigSynch | Execute Configuration Synchronization | View<br>Execute | SmartModel/ Standard Device |
| View Configuration | ncmConfig Viewing | N/A | View | SmartModel Configuration |
| Edit Configuration | ncmConfigEdit | N/A | View<br>Modify | SmartModel Configuration |
| View Native Configuration | ncmConfig Viewing | View Native Commands | View | SmartModel/ Standard Configuration |
| Compare Configuration | ncmConfig Viewing | N/A | View | SmartModel/ Standard Configuration |
| Submit Configuration | ncmConfig Change | Execute Configuration Change | View<br>Execute | SmartModel/ Standard Configuration |

## Applying native command sets (via wizard)

Native command sets are defined by your administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying native command sets** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager.

You need the appropriate access permission.

**Remember:** The **Activity Viewer** always displays information for up to two devices or events, which you have selected either in Network Manager or in Tivoli Netcool/OMNIbus (for events).

The wizard is launched against a single specific device only, either from the **Activity Viewer**, or from a view in Network Manager.

**If you launch the wizard from Activity Viewer or Network Manager**

The command sets shown in the command set selection tree are filtered by either the device's vendor only, or by both the device vendor and device type.

**Note:** In order to display device types, the 'Activate Device Type Validation on Command Sets' property for command sets must be set to TRUE. This property can be set via the Netcool Configuration Manager System Properties UI, if you are a member of a group that has 'View System' and 'Manage System' permissions.

**If you launch the wizard from a View**

All command sets are displayed in the command set selection tree.

When applying a command set, Netcool Configuration Manager verifies that the running and stored (or candidate) configurations on each impacted resource are the same. If these are not the same, a mismatch error is returned.

You can also apply command sets using the Netcool Configuration Manager UI.

Command sets are applied, or submitted, as a unit of work (UOW).

**Tip:** Your administrator can change the behavior of the work submitted by editing the system properties. Any changes to system properties are global and therefore apply to all system users. The following system properties are disabled by default, but can be activated if required:

- TIP Wizard - Execution Order
- TIP Wizard - Pre-emptive Compliance
- TIP Wizard - Failure Option Type
- TIP Wizard - Failure Option Total Errors
- TIP Wizard - Failure Option Percentage Errors
- TIP Wizard - Disaster Recovery
- TIP Wizard - Rollback Options
- TIP Wizard - Rollback Verification
- TIP Wizard - Rollback Mode

1. Navigate the Command set tree and select the command set to be applied to a specific device or Network Manager view.

   Expand the tree to find the command sets that have been defined.
2. You can perform the following actions:

   **Add**

   Click **Add** on the menu bar, or double-click the command set. The command set is moved to the main window.

   **Note:** You can add as many command sets as are available in the Command set tree. However, you can only select command sets of the same vendor, or vendor type (if enabled). The first command set added therefore determines which other command sets can be added.

   **Remove**

   Select a command set from the list of command sets on the main window and click **Remove** on the menu bar, or double-click the command set. The command set is removed from the main window.

   **Move up**

   Select a command set and click **Move up** to move it up the list. The order determines the order in which command sets are applied to devices.

   **Move down**

   Select a command set and click **Move down** to move it down the list.

   **Clear all**

   Click **Clear all** to remove all command sets from the list.

**Show VTMOS columns**
Click **Show VTMOS columns** to display the following information for each command set:

**Vendor**
The device vendor, such as Cisco.

**Type**
The device type, such as switch.

**Model**
The device model, such as 2940.

**OS**
The operating system, such as *12.0*.

**Information**
If you launch the wizard via a device, click the Information icon to display the device's VTMOS, managed state, and support level, as well as user assistance.

If you launch the wizard via a view, click the Information icon to display user assistance only.

3. When you have added command sets as required, click **Next**.
   The **Supply Parameters** window is displayed.
4. Enter parameters for each command set.
   Parameters are configurable values you enter for a command set before you apply it. You must assign an actual value to each parameter before a command set can be applied. Parameters are local to each command set, which means that if there is more than one command set with the same parameters, values must be supplied for each command set.
5. Click **Save**, then **Next**.
   The **Enter Description** window is displayed.
6. Type a description for each command set.
   You can use a maximum of 290 characters to describe the work being submitted.
7. Click **Next**.
   The **Custom Labels** window is displayed.
8. Define a label.
   Labels are searchable tags or fields you can populate to capture additional information when you apply a command set. Administrators can define a maximum of three additional device labels, which can be either mandatory or optional. You can use a maximum of 100 characters per label, and cannot use the following characters:
   - "
   - ~
9. Click **Save**, then **Next**.
   The data is validated and the command sets are applied to the device. The **Summary** window is displayed with feedback received. An ID is issued, and a confirmation dialog is displayed.
10. Click **Yes**, then **OK** to close the confirmation dialog.

The command set is applied to the device in the form of a unit of work (UOW) being submitted.

Now, you can analyze the feedback received and take the appropriate action. If a mismatch error is received, you must synchronize the stored and running configurations.

**Tip:** The ID is the UOW ID for the work that has been submitted. You can use it to track and view its results in the Netcool Configuration Manager user interfaces, the Activity Viewer, the Tivoli Netcool/OMNIbus trap, and the Network Manager IP Edition reports.

**Related concepts**
Overview
The Resource Browser is a high level translation of native resource commands. The various drop down lists are dynamically generated based on the type of resource you are working with. Should you want to

view the actual native resource commands for a configuration, you can do so. Your window will show only those system resources for which you have authorization for display or control.

Overview of command sets
Use this information to acquire an understanding of command sets.

**Related tasks**

Viewing device-specific events in the Activity Viewer
The Activity Viewer displays device-specific activities for up to two devices at a time. You can launch it in context from the Network Manager Network Views and the Tivoli Netcool/OMNIbus Active Event List (AEL).

Synchronizing configurations
Use this procedure to either synchronize a single resource, or synchronize all resources of a certain VTMOS at the realm level.

Applying command sets
When applying a command set, the system verifies that the running and stored (candidate) configurations on each impacted resource are the same. If these are not the same, a mismatch error will be presented. This mismatch must be resolved before submitting any changes to the resource. After a successful configuration change, the system writes the running configuration to the stored/candidate configuration on each resource, ensuring that all three configurations (current, running, stored) are in synch.

Applying command sets with parameters
Use the Configuration Editor to apply a command set with parameters.

# Applying modeled command sets (via wizard)

Modeled command sets are defined by an administrator. To apply a network change or fix a policy validation failure, you can apply these predefined command sets to a device using the **Applying modeled command sets** wizard. You access the wizard from either the Activity Viewer or from the Network View, Hop View and Path View in Network Manager.

You need the appropriate access permission.

**Remember:** The **Activity Viewer** always displays information for up to two devices or events, which you have selected either in Network Manager or in Tivoli Netcool/OMNIbus (for events).

The wizard is launched against a single specific device only, either from the **Activity Viewer**, or from a view in Network Manager.

**If you launch the wizard from Activity Viewer or Network Manager**
The command sets shown in the command set selection tree are filtered by either the device's vendor only, or by both the device vendor and device type.

**Note:** In order to display device types, the 'Activate Device Type Validation on Command Sets' property for command sets must be set to TRUE. This property can be set via the Netcool Configuration Manager System Properties UI, if you are a member of a group that has 'View System' and 'Manage System' permissions.

**If you launch the wizard from a View**
All command sets are displayed in the command set selection tree.

When applying a command set, Netcool Configuration Manager verifies that the running and stored (or candidate) configurations on each impacted resource are the same. If these are not the same, a mismatch error is returned.

You can also apply command sets using the Netcool Configuration Manager UI.

Command sets are applied, or submitted, as a unit of work (UOW).

**Tip:** Your administrator can change the behavior of the work submitted by editing the system properties. Any changes to system properties are global and therefore apply to all system users. The following system properties are disabled by default, but can be activated if required:

- TIP Wizard - Execution Order

- TIP Wizard - Pre-emptive Compliance
- TIP Wizard - Failure Option Type
- TIP Wizard - Failure Option Total Errors
- TIP Wizard - Failure Option Percentage Errors
- TIP Wizard - Disaster Recovery
- TIP Wizard - Rollback Options
- TIP Wizard - Rollback Verification
- TIP Wizard - Rollback Mode

1. Navigate the Command set tree and select the command set to be applied to a specific device or Network Manager view.

   Expand the tree to find the command sets that have been defined.
2. You can perform the following actions:

   **Add**
   Click **Add** on the menu bar, or double-click the command set. The command set is moved to the main window.

   **Note:** You can add as many command sets as are available in the Command set tree. However, you can only select command sets of the same vendor, or vendor type (if enabled). The first command set added therefore determines which other command sets can be added.

   **Remove**
   Select a command set from the list of command sets on the main window and click **Remove** on the menu bar, or double-click the command set. The command set is removed from the main window.

   **Move up**
   Select a command set and click **Move up** to move it up the list. The order determines the order in which command sets are applied to devices.

   **Move down**
   Select a command set and click **Move down** to move it down the list.

   **Clear all**
   Click **Clear all** to remove all command sets from the list.

   **Show VTMOS columns**
   Click **Show VTMOS columns** to display the following information for each command set:

   **Vendor**
   The device vendor, such as Cisco.

   **Type**
   The device type, such as switch.

   **Model**
   The device model, such as 2940.

   **OS**
   The operating system, such as *12.0*.

   **Information**
   If you launch the wizard via a device, click the Information icon to display the device's VTMOS, managed state, and support level, as well as user assistance.

   If you launch the wizard via a view, click the Information icon to display user assistance only.
3. When you have added command sets as required, click **Next**.

   The **Supply Parameters** window is displayed.
4. Enter parameters for each command set.

   Parameters are configurable values you enter for a command set before you apply it. You must assign an actual value to each parameter before a command set can be applied. Parameters are

local to each command set, which means that if there is more than one command set with the same parameters, values must be supplied for each command set.

5. Click **Save**, then **Next**.

   The **Enter Description** window is displayed.

6. Type a description for each command set.

   You can use a maximum of 290 characters to describe the work being submitted.

7. Click **Next**.

   The **Custom Labels** window is displayed.

8. Define a label.

   Labels are searchable tags or fields you can populate to capture additional information when you apply a command set. Administrators can define a maximum of three additional device labels, which can be either mandatory or optional. You can use a maximum of 100 characters per label, and cannot use the following characters:

   - "
   - ~

9. Click **Save**, then **Next**.

   The data is validated and the command sets are applied to the device. The **Summary** window is displayed with feedback received. An ID is issued, and a confirmation dialog is displayed.

10. Click **Yes**, then **OK** to close the confirmation dialog.

The command set is applied to the device in the form of a unit of work (UOW) being submitted.

Now, you can analyze the feedback received and take the appropriate action. If a mismatch error is received, you must synchronize the stored and running configurations.

**Tip:** The ID is the UOW ID for the work that has been submitted. You can use it to track and view its results in the Netcool Configuration Manager user interfaces, the Activity Viewer, the Tivoli Netcool/OMNIbus trap, and the Network Manager IP Edition reports.

**Related concepts**

Overview

The Resource Browser is a high level translation of native resource commands. The various drop down lists are dynamically generated based on the type of resource you are working with. Should you want to view the actual native resource commands for a configuration, you can do so. Your window will show only those system resources for which you have authorization for display or control.

Overview of command sets

Use this information to acquire an understanding of command sets.

**Related tasks**

Viewing device-specific events in the Activity Viewer

The Activity Viewer displays device-specific activities for up to two devices at a time. You can launch it in context from the Network Manager Network Views and the Tivoli Netcool/OMNIbus Active Event List (AEL).

Synchronizing configurations

Use this procedure to either synchronize a single resource, or synchronize all resources of a certain VTMOS at the realm level.

Applying command sets

When applying a command set, the system verifies that the running and stored (candidate) configurations on each impacted resource are the same. If these are not the same, a mismatch error will be presented. This mismatch must be resolved before submitting any changes to the resource. After a successful configuration change, the system writes the running configuration to the stored/candidate configuration on each resource, ensuring that all three configurations (current, running, stored) are in synch.

Applying command sets with parameters

Use the Configuration Editor to apply a command set with parameters.

## Applying policies (via wizard)

Compliance policies are defined by an administrator. To validate a device or group of devices against one or more defined policies, you can apply a policy by using the **Applying policies** wizard. You access the wizard from either the Activity Viewer or from the Network Views portlet in Network Manager IP Edition.

You need the appropriate access permission.

You can also apply policies using the Netcool Configuration Manager UI.

1. Navigate the Policy Selection tree and select the policy to be applied to a specific device.

   Policies in the Policy Selection tree are arranged by realm, matching the realm structure that is defined in the Compliance UI. Policies are not filtered by vendor or type and all policies defined for the selected device are displayed. You can add any policy to the list of policies to applied regardless of vendor or type. Expand the tree to find the policies that have been defined.
2. You can perform the following actions:

   **Add**
   Click **Add** on the menu bar, or double-click the policy. The policy is moved to the main window.

   **Note:** You can add as many policies as are available in the Policy Selection tree.

   **Remove**
   Select a policy from the list of policies on the main window and click **Remove** on the menu bar, or double-click the policy. The policy is removed from the main window.

   **Move up**
   Select a policy and click **Move up** to move it up the list.

   **Note:** The order in which policies are applied is not important.

   **Move down**
   Select a policy and click **Move down** to move it down the list.

   **Clear all**
   Click **Clear all** to remove all policies from the list.

   **Show VTMOS columns**
   Click **Show VTMOS columns** to display the following information for each policy:

   **Vendor**
   The device vendor, such as Cisco.

   **Type**
   The device type, such as switch.

   **Model**
   The device model, such as 2940.

   **OS**
   The operating system, such as *12.0*.

   **Information**
   If you launch the wizard via a device, click the Information icon to display the device's VTMOS, managed state, and support level, as well as user assistance.

   If you launch the wizard via a view, click the Information icon to display user assistance only.
3. When you have added policies as required, click **Next**.

   The **Supply Parameters** window is displayed.
4. Enter parameters for each policy.

   Parameters are configurable values you enter for a policy before you apply it. You must assign an actual value to each parameter before a policy can be applied. Parameters are global to all policies, which means that if one or more policies have the same parameter, then only one value can be

supplied for that parameter, and it is applied to all policies that have that parameter. These parameters have 'Multiple' listed in the Resource column.

5. Click **Save**, then **Next**.

   The **Enter Description** window is displayed.

6. Type a description for each policy.

   You can use a maximum of 290 characters to describe each policy.

7. Click **Save**, then **Next**.

   The data is validated and the policy is applied to the device as a process. The **Summary** window is displayed with feedback received, as is a confirmation dialog, and a process ID is issued.

8. Click **Yes**, then **OK** to close the confirmation dialog.

The results of the applied policies are stored in the Netcool Configuration Manager user interfaces, until they are removed through housekeeping. They are also available in the Activity Viewer, and the Network Manager IP Edition reports.

Now, you can analyze the results and take the appropriate action.

**Tip:** The process ID is the ID for the compliance process that has been submitted. You can use it to track the process and view its results.

**Related tasks**

Viewing device-specific events in the Activity Viewer
The Activity Viewer displays device-specific activities for up to two devices at a time. You can launch it in context from the Network Manager Network Views and the Tivoli Netcool/OMNIbus Active Event List (AEL).

Executing a policy
Policy execution describes the various methods that may be used to invoke and run compliance policies can be validated against the network. It also describes the steps a user must take in order to execute the policies that have been created on the network.

Viewing results
Netcool Configuration Manager - Compliance will run the validation of devices against policies and generate the validation results. All results across all validations will be stored in the Netcool Configuration Manager - Compliance database, and are available for review by the user until they are removed through house keeping.

Viewing detailed results
The Results page gives the user access to compliance validation results based on their level of security. There are a number of different views in the Results tab, where validation results can be viewed and analyzed.

Viewing pre-emptive policies and results
Use the pre-emptive compliance functionality to check proposed configuration changes to a device against predefined compliance policies for that device. Pre-emptive compliance is a mechanism whereby proposed configuration changes can be checked for compliance before being provisioned on the device. The capability is intended to enable customers to evaluate the impact of configuration changes against predefined compliance policies for a device.

**Related information**

Compliance overview
Netcool Configuration Manager compliance management functionality focuses on the early detection and remediation of network vulnerabilities associated with compliance violations.

Compliance entities
Compliance Administration refers to the management of compliance entities which require configuration in order for the Netcool Configuration Manager compliance functionality to execute correctly. In addition Compliance Administration describes the relationship between each of these entities. Compliance entities encompass the compliance process, compliance policy, compliance definition, compliance rule, and the corrective action.

# Synchronizing configurations (via wizard)

When the running and the stored (or candidate) configurations on a device are out of synch, you identify the correct configuration and use it to replace the incorrect one so that the two are synchronized. To do so you submit a synchronization request as you would any other unit of work (UOW). You access the Synchronization wizard from either the Activity Viewer or from the Network View in Network Manager IP Edition.

You need the appropriate access permission.

**Remember:** The **Activity Viewer** always displays information for up to two devices or events, which you have selected either in Network Manager or in Tivoli Netcool/OMNIbus (for events).

The Synchronization wizard is launched against a specific device, either from the **Activity Viewer**, or from a view in Network Manager IP Edition. You use the stored (or candidate) configuration of that device to update the running configuration.

**Note:** You can also synchronize configurations using the Netcool Configuration Manager UI, which has additional functionality allowing you to synchronize all the devices of a selected VTMOS at the realm level, either by replacing the stored device configuration with the running device configuration, or the running configuration with the stored configuration.

1. The Synchronization wizard is launched with a device already selected, and the **Enter Description** window is displayed. Type a description.

   You can use a maximum of 290 characters to describe the device configuration synchronization you are about to perform.
2. Click **Save**, then **Next**.

   The **Custom Labels** window is displayed.
3. Define a label.

   Labels are searchable tags or fields you can populate to capture additional information when you synchronize configurations for a device. Administrators can define a maximum of three additional device labels, which can be either mandatory or optional. You can use a maximum of 100 characters per label, and cannot use the following characters:

   - "
   - ~
4. Click **Save**, then **Next**.

   The data is validated and the configurations are synchronized. The **Summary** window is displayed with feedback received, and an ID is issued. A confirmation window is displayed.
5. Click **Yes**, then **OK** to close the confirmation window.

The stored (or candidate) configuration of the selected device is copied to the Netcool Configuration Manager database, thereby replacing the running configuration.

Now, you can analyze the feedback received and take the appropriate action.

**Tip:** The ID is the UOW ID for the work that has been submitted. You can use it to track and view its results in the Netcool Configuration Manager user interfaces, the Activity Viewer, the Tivoli Netcool/OMNIbus trap, and the Network Manager IP Edition reports.

**Related concepts**

Overview

The Resource Browser is a high level translation of native resource commands. The various drop down lists are dynamically generated based on the type of resource you are working with. Should you want to view the actual native resource commands for a configuration, you can do so. Your window will show only those system resources for which you have authorization for display or control.

Overview of the Configuration Editor

The Configuration Editor is an applet used for viewing and editing configurations and command sets.

**Related tasks**

Viewing device-specific events in the Activity Viewer
The Activity Viewer displays device-specific activities for up to two devices at a time. You can launch it in context from the Network Manager Network Views and the Tivoli Netcool/OMNIbus Active Event List (AEL).

Synchronizing configurations
Use this procedure to either synchronize a single resource, or synchronize all resources of a certain VTMOS at the realm level.

# Applying configurations (via wizard)

You apply a configuration to a device using the Submit Configuration wizard, which you access from the Activity Viewer.

You need the appropriate access permission.

**Remember:** The **Activity Viewer** always displays information for up to two devices or events, which you have selected either in Network Manager or in Tivoli Netcool/OMNIbus (for events).

To apply configurations, you first select a (versioned) previous or current configuration for a device in the **Activity Viewer**, and then access the Submit Configuration wizard to apply the configuration to the device. Both the running and stored (or candidate) configurations are replaced.

You can also apply configurations using the Netcool Configuration Manager UI, which has additional functionality.

**Tip:** Your administrator can change the behavior of the work submitted by editing the system properties. Any changes to system properties are global and therefore apply to all system users. The following system properties are disabled by default, but can be activated if required:

- TIP Wizard - Execution Order
- TIP Wizard - Pre-emptive Compliance
- TIP Wizard - Failure Option Type
- TIP Wizard - Failure Option Total Errors
- TIP Wizard - Failure Option Percentage Errors
- TIP Wizard - Disaster Recovery
- TIP Wizard - Rollback Options
- TIP Wizard - Rollback Verification
- TIP Wizard - Rollback Mode

1. The Submit Configuration wizard is launched from the **Activity Viewer** with a configuration already selected for a device, and the **Enter Description** window is displayed. Type a description.

   You can use a maximum of 290 characters to describe the configuration change you are about to perform.
2. Click **Save**, then **Next**.

   The **Custom Labels** window is displayed.
3. Type a label.

   Labels are searchable tags or fields you can populate to capture additional information when you apply a configuration to a device. Administrators can define a maximum of three additional device labels, which can be either mandatory or optional. You can use a maximum of 100 characters per label.
4. Click **Save**, then **Next**.

   The data is validated and the configuration is submitted. The **Summary** window is displayed with feedback received, and an ID is issued. A confirmation window is displayed.
5. Click **Yes**, then **OK** to close the confirmation window.

Both the running and the stored (or candidate) configurations are replaced.

Now, you can analyze the feedback received and take the appropriate action.

**Tip:** The ID is the UOW ID for the work that has been submitted. You can use it to track and view its results in the Netcool Configuration Manager user interfaces, the Activity Viewer, the Tivoli Netcool/OMNIbus trap, and the Network Manager IP Edition reports.

**Related concepts**

Overview
The Resource Browser is a high level translation of native resource commands. The various drop down lists are dynamically generated based on the type of resource you are working with. Should you want to view the actual native resource commands for a configuration, you can do so. Your window will show only those system resources for which you have authorization for display or control.

Overview of the Configuration Editor
The Configuration Editor is an applet used for viewing and editing configurations and command sets.

**Related tasks**

Viewing device-specific events in the Activity Viewer
The Activity Viewer displays device-specific activities for up to two devices at a time. You can launch it in context from the Network Manager Network Views and the Tivoli Netcool/OMNIbus Active Event List (AEL).

Applying versioned configurations
Use this procedure to apply an earlier configuration version to a network resource.

# Chapter 6. Viewing reports

You access ITNCM-Reports via DASH installed by Network Manager (if Netcool Configuration Manager is integrated with Network Manager) or the instance of DASH installed as part of a stand-alone installation of ITNCM-Reports.

Reports allow users to evaluate results including configurations, devices, user accounts, UOW and workflow. The reporting capabilities also provide a means to achieve a summary level to gain an insight into the overall status of the network.

You can access Netcool Configuration Manager reports from the TCR/COGNOS portlet or Netcool Configuration Manager Network View.

When you log into DASH, you can navigate to the Tivoli Common Reporting reporting area by selecting **Reporting** > **Common Reporting** in the left menu pane. The contents of the Public Folder may also contain reporting folders from other products such as Network Manager. When Netcool Configuration Manager reports has been selected, all available reports are listed. These are discussed in the following sections.

**CAUTION:** There is a performance issue when running some Netcool Configuration Manager Reports. The issue may occur after the report completes, and attempts to change the view format to PDF. The report runs for up to 15 minutes, and then outputs a "java.lang.OutOfMemoryError" error. To workaround this: restart the generation of the report, and increase the heap size. It may also be useful to narrow the search criteria to be more specific.

**Note:** You should be aware that any report using a date/time filter will be in local time and you may need to adjust this accordingly to GMT +00 when retrieving data from the server. All information in the database is stored in GMT+00.

For further information on Tivoli Common Reporting features and functionality, including e-mail, scheduling, importing and exporting functionality, see the 'Working with reports' topic in the Tivoli Common Reporting Knowledge Center at the following location: http://www-01.ibm.com/support/knowledgecenter/SSH2DF_2.1.0/ttcr_working.html

## Configuration and OS Change Summary

The configuration and OS change summary report illustrates all completed UOWs; both successful and failed, where change details have been recorded in the log. The report is based on selected work types which have been run against network devices. Realm name, device name, VTMOS, date range and type of work, are the report criteria available to configure this report.

This task describes the criteria required for the configuration and OS change summary report, as well as the results it produces.

1. Enter realm information by selecting the appropriate check-boxes. There are `select all` and `deselect all` options for faster selection. If you want to include the sub-realms of the chosen realms, indicate using the `Include sub-realms` option.
2. Enter the device name and VTMOS filter. The asterix (*) wildcard can be used to choose all device names.
3. Next, enter the type of work using the check-boxes to select the required work types.
4. Enter the date range using the "from" and "to" criteria available.
5. Select **Finish** to run the report.
6. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information grouped by request type:

| *Table 61. Configuration and OS change summary report details.* | |
|---|---|
| **Field** | **Definition** |
| UOW ID | Displays the UOW ID assigned when the UOW was created |
| Device | Device name or IP address |
| VTMOS | Associated VTMOS of device |
| Status | Execution status for example, finished |
| UOW Result | Result of UOW for example, success |
| Task Result | Result of task for example, success. |
| Start Time | Timestamp associated with when the UOW was invoked. |
| End Time | Timestamp associated with when the UOW completed. |
| Submitted By | User name of person who submitted the UOW. |
| Description | Narrative to accompany UOW. |

## Device Inventory List

The device inventory list report illustrates which hardware platforms are running on the network, as well as a listing of VTMOS inventory information. Realm name, device name and VTMOS are the report criteria available to configure this report.

This task describes the criteria required for the device inventory list report, as well as the results it produces.

1. Enter realm information by selecting the appropriate check-boxes. There are `select all` and `deselect all` options for faster selection. If you want to include the sub-realms of the chosen realms, indicate using the `Include sub-realms` option.
2. Enter the device name and VTMOS filter. The asterix (*) wildcard can be used to choose all device names.
3. Select **Finish** to run the report.
4. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information:

| *Table 62. Device inventory list report details.* | |
|---|---|
| **Field** | **Definition** |
| Realm Name | Name of realm where device resides. |
| VTMOS | Device VTMOS. |
| Name | Device name. |
| Status | Device status for example, staged. |
| Last Modified Time | Timestamp associated with when the device was last modified. |
| Last Modified By | User name of person who last modified the device. |

## Device Inventory VTMOS Summary

The device inventory VTMOS summary report illustrates which hardware platforms are running on the network, and is grouped and counted by VTMOS inventory information. Realm name, device name and VTMOS are the report criteria available to configure this report.

This task describes the criteria required for the device inventory VTMOS summary report, as well as the results it produces.

1. Enter realm information by selecting the appropriate check-boxes. There are `select all` and `deselect all` options for faster selection. If you want to include the sub-realms of the chosen realms, indicate using the `Include sub-realms` option.
2. Enter the device name and VTMOS Filter. The asterix (*) wildcard can be used to choose all device names.
3. Select **Finish** to run the report.
4. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information:

*Table 63. Device inventory VTMOS summary report details.*

| Field | Definition |
|---|---|
| VTMOS | Device VTMOS. |
| Device count for OS | Count of all OS which have the same Model. |
| Total Vendors | Count of all the different types of Vendor. |
| Total device inventory | Total number of devices in the inventory. |

## Policy Compliance Detail

The policy compliance detail report illustrates a high level of detail for the validation result. Realm name, policies, device name, VTMOS, policy severity and policy result are the report criteria available to configure this report.

This task describes the criteria required for the policy compliance detail report, as well as the results it produces.

1. Enter realm information by selecting the appropriate check-boxes. There are `select all` and `deselect all` options for faster selection. If you want to include the sub-realms of the chosen realms, indicate using the `Include sub-realms` option.
2. Select the policies using the check-boxes to select the required policy names.
3. Enter the device name and VTMOS Filter. The asterix (*) wildcard can be used to choose all device names.
4. Next, enter the policy severity level required. All policy severity levels (1-5) are already selected by default. There are `select all` and `deselect all` options for faster selection.
5. Enter the policy result you want to report on. All policy results (pass, fail, exempt, not assessed) are selected by default. There are `select all` and `deselect all` options for faster selection.
6. Select **Finish** to run the report.
7. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information:

*Table 64. Policy compliance detail report details.*

| Field | Definition |
|---|---|
| Searched For | Configuration entered as criteria during creation of the compliance definition. |

| *Table 64. Policy compliance detail report details. (continued)* | |
|---|---|
| **Field** | **Definition** |
| Search Result | In the event of a Pass, displays every line of the configuration that's the criteria were found in. |
| Outcome | Validation result of the device against the selected policy. |
| Result Count | Number of results listed in the report. |

## Policy Compliance Detail (By Process)

The policy compliance detail (by process) report illustrates a high level of detail for the validation result, and groups the information by process. A date range is the only report criteria available to configure this report.

This task describes the criteria required for the policy compliance detail (by process) report, as well as the results it produces.

1. Enter the date range using the "from" and "to" criteria available.
2. Select **Next >** to run the report.
3. The resulting report displays the following information:

| *Table 65. Policy compliance detail (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Row Number | Numerical marker to indicate Process. |
| Process Name (appears as hyperlink) | Process name reported on. |
| Device Count | Number of devices process executed against. |
| Executed By | User name of person who executed the process. |
| Start Time | Timestamp associated with when the process was invoked. |
| End Time | Timestamp associated with when the process completed. |
| Policy Count | Number of policies listed in the report. |

4. A further level of detail can be achieved by clicking on the process name, which appears as a hyperlink.
5. This invokes further report criteria in the form of policy result and policy severity. The user can choose the policy result and policy severity levels of those policies associated with the process, that they wish to report on.
6. Next, enter the policy severity level required. All policy severity levels (1-5) are already selected by default. There are `select all` and `deselect all` options for faster selection.
7. Enter the policy result you want to report on. All policy results (pass, fail, exempt, not assessed) are selected by default. There are `select all` and `deselect all` options for faster selection.
8. Select **Finish** to run the report.
9. The resulting report displays the following information:

| *Table 66. Policy compliance detail (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Policy Name | Name of policy associated with process, and matching report criteria. |

| *Table 66. Policy compliance detail (by process) report details. (continued)* | |
|---|---|
| **Field** | **Definition** |
| Searched For | Configuration entered as criteria during creation of the compliance definition. |
| Outcome | In the event of a Pass, displays every line of the configuration that's the criteria were found in. |
| Search Result | Validation result of the device against the selected policy. |
| Result | Policy result. |

## Policy Compliance Grouped by Device

The policy compliance grouped by device report illustrates all policies executed against a device. Realm name, policies, device name, VTMOS, policy severity and policy result are the report criteria available to configure this report.

This task describes the criteria required for the policy compliance grouped by device report, as well as the results it produces.

1. Enter realm information by selecting the appropriate check-boxes. There are `select all` and `deselect all` options for faster selection. If you want to include the sub-realms of the chosen realms, indicate using the `Include sub-realms` option.
2. Select the policies using the check-boxes to select the required policy names.
3. Enter the device name and VTMOS Filter. The asterix (*) wildcard can be used to choose all device names.
4. Next, enter the policy severity level required. All policy severity levels (1-5) are already selected by default. There are `select all` and `deselect all` options for faster selection.
5. Enter the policy result you want to report on. All policy results (pass, fail, exempt, not assessed) are selected by default. There are `select all` and `deselect all` options for faster selection.
6. Select **Finish** to run the report.
7. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information:

| *Table 67. Policy compliance grouped by device report details.* | |
|---|---|
| **Field** | **Definition** |
| Policy Name | Name of policy executed against the device listed at the top of report. |
| Policy Realm | Realm in which policy resides. |
| Severity | Policy severity level. |
| Result (appears as hyperlink) | Policy result. |
| Policy Count | Number of policies listed in the report. |

8. A further level of detail can be achieved by clicking on the result, which appears as a hyperlink.
9. The resulting report displays the following information, grouped by policy:

| *Table 68. Policy compliance grouped by device report details.* | |
|---|---|
| **Field** | **Definition** |
| Searched For | Configuration entered as criteria during creation of the compliance definition. |

| *Table 68. Policy compliance grouped by device report details. (continued)* | |
|---|---|
| **Field** | **Definition** |
| Search Result | In the event of a Pass, displays every line of the configuration that's the criteria were found in. |
| Outcome | Validation result of the device against the selected policy. |

## Policy Compliance Grouped by Device (By Process)

The policy compliance grouped by device (by process) report illustrates all policies executed against a device and groups the information by process. A date range is the only report criteria available to configure this report.

This task describes the criteria required for the policy compliance grouped by device (by process) report, as well as the results it produces.

1. Enter the date range using the "from" and "to" criteria available.
2. Select **Next >** to run the report.
3. The resulting report displays the following information:

| *Table 69. Policy compliance grouped by device (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Row Number | Numerical marker to indicate Process. |
| Process Name (appears as hyperlink) | Process name reported on. |
| Device Count | Number of devices process executed against. |
| Executed By | User name of person who executed the process. |
| Start Time | Timestamp associated with when the process was invoked. |
| End Time | Timestamp associated with when the process completed. |
| Process Count | Number of processes listed in the report. |

4. A further level of detail can be achieved by clicking on the process name, which appears as a hyperlink.
5. This invokes further report criteria in the form of policy result and policy severity. The user can choose the policy result and policy severity levels of those policies associated with the process, that they wish to report on.
6. Next, enter the policy severity level required. All policy severity levels (1-5) are already selected by default. There are `select all` and `deselect all` options for faster selection.
7. Enter the policy result you want to report on. All policy results (pass, fail, exempt, not assessed) are selected by default. There are `select all` and `deselect all` options for faster selection.
8. Select **Finish** to run the report.
9. The resulting report displays the following information:

| *Table 70. Policy compliance detail grouped by device (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Policy Name | Name of policy executed against the device listed at the top of report. |
| Severity | Policy severity level. |

| *Table 70. Policy compliance detail grouped by device (by process) report details. (continued)* | |
|---|---|
| **Field** | **Definition** |
| Revision | Policy revision number. |
| Result (appears as hyperlink) | Policy result. |

10. A further level of detail can be achieved by clicking on the result, which appears as a hyperlink.
11. The resulting report displays the following information, grouped by policy:

| *Table 71. Policy compliance grouped by device (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Searched For | Configuration entered as criteria during creation of the compliance definition. |
| Search Result | In the event of a Pass, displays every line of the configuration that's the criteria were found in. |
| Outcome | Validation result of the device against the selected policy. |

## Policy Compliance Grouped by Policy

The policy compliance grouped by policy report illustrates all devices against which a policy was executed. Realm name, policies, device name, VTMOS, policy severity and policy result are the report criteria available to configure this report.

This task describes the criteria required for the policy compliance grouped by policy report, as well as the results it produces.

1. Enter realm information by selecting the appropriate check-boxes. There are `select all` and `deselect all` options for faster selection. If you want to include the sub-realms of the chosen realms, indicate using the `Include sub-realms` option.
2. Select the policies using the check-boxes to select the required policy names.
3. Enter the device name and VTMOS Filter. The asterix (*) wildcard can be used to choose all device names.
4. Next, enter the policy severity level required. All policy severity levels (1-5) are already selected by default. There are `select all` and `deselect all` options for faster selection.
5. Enter the policy result you want to report on. All policy results (pass, fail, exempt, not assessed) are selected by default. There are `select all` and `deselect all` options for faster selection.
6. Select **Finish** to run the report.
7. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information:

| *Table 72. Policy compliance grouped by policy report details.* | |
|---|---|
| **Field** | **Definition** |
| Device Name | Name of device against which the policy listed at the top of report was executed. |
| Device Realm | Realm in which the device resides. |
| VTMOS | Device VTMOS |
| Result (appears as hyperlink) | Policy result. |

8. A further level of detail can be achieved by clicking on the result, which appears as a hyperlink.
9. The resulting report displays the following information, grouped by policy:

| *Table 73. Policy compliance grouped by policy report details.* | |
|---|---|
| **Field** | **Definition** |
| Searched For | Configuration entered as criteria during creation of the compliance definition. |
| Search Result | In the event of a Pass, displays every line of the configuration that's the criteria were found in. |
| Outcome | Validation result of the device against the selected policy. |

## Policy Compliance Score Trend

The policy compliance score trend report illustrates the compliance score for devices as evaluated by policies. Graphical information is extracted in the form of a compliance score trend for each selected process over the selected time period. The compliance score trend is indicative of the "health" of a network from a compliance perspective. The compliance score is determined using the weight of the compliance policies, and can be calculated at a network or device realm basis. The compliance score also takes into consideration the number of Not Assessed devices, as this may indicate a problem with the coverage of a policy. Processes and date range are the report criteria available to configure this report.

This task describes the criteria required for the policy compliance score trend report, as well as the results it produces.

1. Select the processes using the check-boxes to select the required process names. There are **select all** and **deselect all** options for faster selection.
2. Enter the date range using the "from" and "to" criteria available.
3. Select **Finish >** to run the report.
4. The resulting report displays the following information:

| *Table 74. Policy compliance score trend report details.* | |
|---|---|
| **Field** | **Definition** |
| Score (%) | Compliance score trend is represented as a percentage. |
| Date generated | Date when the compliance score trend was generated. |

## Policy Compliance Grouped by Policy (By Process)

The policy compliance grouped by policy (by process) report illustrates all devices against which a policy was executed and groups the information by process. A date range is the only report criteria available to configure this report.

This task describes the criteria required for the policy compliance grouped by device (by process) report, as well as the results it produces.

1. Enter the date range using the "from" and "to" criteria available.
2. Select **Next >** to run the report.
3. The resulting report displays the following information:

| *Table 75. Policy compliance grouped by policy (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Row Number | Numerical marker to indicate Process. |
| Process Name (appears as hyperlink) | Process name reported on. |

| *Table 75. Policy compliance grouped by policy (by process) report details. (continued)* | |
|---|---|
| **Field** | **Definition** |
| Device Count | Number of devices process executed against. |
| Executed By | User name of person who executed the process. |
| Start Time | Timestamp associated with when the process was invoked. |
| End Time | Timestamp associated with when the process completed. |
| Process Count | Number of processes listed in the report. |

4. A further level of detail can be achieved by clicking on the process name, which appears as a hyperlink.
5. This invokes further report criteria in the form of policy result and policy severity. The user can choose the policy result and policy severity levels of those policies associated with the process, that they wish to report on.
6. Next, enter the policy severity level required. All policy severity levels (1-5) are already selected by default. There are `select all` and `deselect all` options for faster selection.
7. Enter the policy result you want to report on. All policy results (pass, fail, exempt, not assessed) are selected by default. There are `select all` and `deselect all` options for faster selection.
8. Select **Finish** to run the report.
9. The resulting report displays the following information, grouped by policy:

| *Table 76. Policy compliance grouped by policy (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Device Name | Name of device against which the policy listed at the top of report was executed. |
| Device Realm | Realm in which the device resides. |
| VTMOS | Device VTMOS |
| Result (appears as hyperlink) | Policy result. |

10. A further level of detail can be achieved by clicking on the result, which appears as a hyperlink.
11. The resulting report displays the following information, grouped by policy:

| *Table 77. Policy compliance grouped by policy (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Searched For | Configuration entered as criteria during creation of the compliance definition. |
| Search Result | In the event of a Pass, displays every line of the configuration that's the criteria were found in. |
| Outcome | Validation result of the device against the selected policy. |

## Policy Compliance Score & Summary

The policy compliance score and summary report illustrates the compliance score for devices as evaluated by policies. Graphical information may also be extracted in the presence of a compliance score. The compliance score is indicative of the "health" of a network from a compliance perspective. The score is determined using the weight of the compliance policies, and can be calculated at a network or device

realm basis. The Compliance Score also takes into consideration the number of Not Assessed devices, as this may indicate a problem with the coverage of a policy. Realm name, policies, device name and VTMOS are the report criteria available to configure this report.

This task describes the criteria required for the policy compliance score and summary report, as well as the results it produces.

1. Enter realm information by selecting the appropriate check-boxes. There are `select all` and `deselect all` options for faster selection. If you want to include the sub-realms of the chosen realms, indicate using the `Include sub-realms` option.
2. Select the policies using the check-boxes to select the required policy names.
3. Enter the device name and VTMOS Filter. The asterix (*) wildcard can be used to choose all device names.
4. Select **Finish** to run the report.
5. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information:

*Table 78. Policy compliance score and summary report details.*

| **Field** | **Definition** |
|---|---|
| Policy Name (appears as hyperlink) | Name of the policy executed. |
| Severity | Severity level of the policy |
| Passed | Number of devices against which the policy was executed with a pass result. |
| Failed | Number of devices against which the policy was executed with a fail result. |
| Not Assessed | Number of devices against which the policy was executed with a not assessed result. |
| Exempt | Number of devices against which the policy was executed with an exempt result. |
| Policy Weight | The weighted compliance score is based on the most current validation results for the selected devices and the relative importance of each of the policies as defined by the weight of a policy. |
| Policy Count | Number of policies listed in the report. |

6. A further level of detail can be achieved by clicking on the policy name, which appears as a hyperlink.
7. The resulting report displays the following information, grouped by policy:

*Table 79. Policy compliance score and summary report details.*

| **Field** | **Definition** |
|---|---|
| Device Name | Name of device against which the policy listed at the top of report was executed. |
| Device Realm | Realm in which the device resides. |
| Result (appears as hyperlink) | Policy result. |
| Device Count | Number of devices listed in the report. |

8. A further level of detail can be achieved by clicking on the result, which appears as a hyperlink.
9. The resulting report displays the following information, grouped by policy:

| *Table 80. Policy compliance score and summary report details.* | |
|---|---|
| **Field** | **Definition** |
| Searched For | Configuration entered as criteria during creation of the compliance definition. |
| Search Result | In the event of a Pass, displays every line of the configuration that's the criteria were found in. |
| Outcome | Validation result of the device against the selected policy. |

## Policy Compliance Summary (By Process)

The policy compliance summary (by process) report illustrates the process validation summary and failed validation by severity as evaluated by policies, and grouped by process. Graphical information may also be extracted in the form of process validation summary and failed validation by severity. A date range is the only report criteria available to configure this report.

This task describes the criteria required for the policy compliance summary (by process) report, as well as the results it produces.

1. Enter the date range using the "from" and "to" criteria available.
2. Select **Next >** to run the report.
3. The resulting report displays the following information:

| *Table 81. Policy compliance summary (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Row Number | Numerical marker to indicate Process. |
| Process Name (appears as hyperlink) | Process name reported on. |
| Device Count | Number of devices process executed against. |
| Executed By | User name of person who executed the process. |
| Start Time | Timestamp associated with when the process was invoked. |
| End Time | Timestamp associated with when the process completed. |
| Process Count | Number of processes listed in the report. |

4. A further level of detail can be achieved by clicking on the process name, which appears as a hyperlink.
5. The resulting report includes a graphical representation of the process validation summary and failed validation by severity, and also displays the following information, grouped by process:

| *Table 82. Policy compliance summary (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Policy Name (appears as hyperlink) | Name of the policy executed. |
| Severity | Severity level of the policy |
| Passed | Number of devices against which the policy was executed with a pass result. |
| Failed | Number of devices against which the policy was executed with a fail result. |

| *Table 82. Policy compliance summary (by process) report details. (continued)* | |
|---|---|
| **Field** | **Definition** |
| Not Assessed | Number of devices against which the policy was executed with a not assessed result. |
| Exempt | Number of devices against which the policy was executed with an exempt result. |
| Policy Count | Number of policies listed in the report. |

6. A further level of detail can be achieved by clicking on the policy name, which appears as a hyperlink.
7. The resulting report displays the following information, grouped by policy:

| *Table 83. Policy compliance summary (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Device Name | Name of device against which the policy listed at the top of report was executed. |
| Device Realm | Realm in which the device resides. |
| Result (appears as hyperlink) | Policy result. |

8. A further level of detail can be achieved by clicking on the result, which appears as a hyperlink.
9. The resulting report displays the following information, grouped by policy:

| *Table 84. Policy compliance summary (by process) report details.* | |
|---|---|
| **Field** | **Definition** |
| Searched For | Configuration entered as criteria during creation of the compliance definition. |
| Search Result | In the event of a Pass, displays every line of the configuration that's the criteria were found in. |
| Outcome | Validation result of the device against the selected policy. |

## Security Groups

The security groups report shows all users created under a security group. Group name is the only report criteria available to configure this report.

This task describes the criteria required for the security groups report, as well as the results it produces.

1. Enter the group name. The asterix (*) wildcard can be used to choose all group names.
2. Select **Finish** to run the report.
3. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information:

| *Table 85. Security groups report details.* | |
|---|---|
| **Field** | **Definition** |
| Last Name | Last name of user. |
| First Name | First name of user. |
| Login | Login alias of user. |
| E-mail | Email associated with user. |

| *Table 85. Security groups report details. (continued)* | |
|---|---|
| **Field** | **Definition** |
| ID | User ID. |
| Group | Group which the user belongs to. |
| Telephone Number | Telephone number associated with user. |

## Security Users

The security users report lists each user and details their security group membership. The last name of the user is the only report criteria available to configure this report.

This task describes the criteria required for the security users report, as well as the results it produces.

1. Enter the last name. The asterix (*) wildcard can be used to choose all last names.
2. Select **Finish** to run the report.
3. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information:

| *Table 86. Security users report details.* | |
|---|---|
| **Field** | **Definition** |
| User | User name. |
| Group | Name of group which the user belongs to. |
| Group Description | Narrative describing the group. |

## UOW Approval Status

The UOW approval status report illustrates a graphical representation of each UOW status. A date range is the only report criteria available to configure this report.

This task describes the criteria required for the UOW approval status report, as well as the results it produces.

1. Enter the date range using the "from" and "to" criteria available.
2. Select **Finish** to run the report.
3. The resulting report displays the following information:

| *Table 87. UOW approval status report details.* | |
|---|---|
| **Field** | **Definition** |
| Status | UOW approval status for example, No approval required. |
| Record Count | Count of UOW with a particular approval status. |

## UOW Device Configuration Sync Summary

The UOW device configuration sync summary report illustrates all completed UOWs. Realm name, device name, VTMOS, date range and user's login, are the report criteria available to configure this report.

This task describes the criteria required for the UOW device configuration sync summary report, as well as the results it produces.

1. Enter realm information by selecting the appropriate check-boxes. There are `select all` and `deselect all` options for faster selection. If you want to include the sub-realms of the chosen realms, indicate using the `Include sub-realms` option.
2. Enter the device name and VTMOS filter. The asterix (*) wildcard can be used to choose all device names.
3. Next, enter the user's login. The asterix (*) wildcard can be used to choose all user's login.
4. Enter the date range using the "from" and "to" criteria available.
5. Select **Finish** to run the report.
6. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information grouped by request type:

*Table 88. UOW device configuration sync summary report details.*

| Field | Definition |
|---|---|
| UOW ID | Displays the UOW ID assigned when the UOW was created |
| Name | Device name or IP address |
| Status | Execution status for example, finished |
| UOW Result | Result of UOW for example, success |
| Task Result | Result of task for example, success. |
| Start Time | Timestamp associated with when the UOW was invoked. |
| End Time | Timestamp associated with when the UOW completed. |
| Submitted By | User name of person who submitted the UOW. |
| Description | Narrative to accompany UOW. |
| VTMOS | Associated VTMOS of device |

## UOW Status Breakdown

The UOW status breakdown report illustrates a breakdown of UOW status grouped by execution status. Graphical information is extracted in the form of UOW status breakdown and record count. Execution status and date range are the report criteria available to configure this report.

This task describes the criteria required for the UOW status breakdown report, as well as the results it produces.

1. Select the execution status using the check-boxes to select the required status. There are **select all** and **deselect all** options for faster selection.
2. Enter the date range using the "from" and "to" criteria available.
3. Select **Finish >** to run the report.
4. The resulting report displays the following information:

*Table 89. UOW status breakdown report details.*

| Field | Definition |
|---|---|
| Start Date | Start date selected as criteria. |
| End Date | End date selected as criteria. |
| Execution Status | List of all execution status chosen as criteria. |

| *Table 89. UOW status breakdown report details. (continued)* | |
|---|---|
| **Field** | **Definition** |
| Status | Execution status for example, Pending Approval. |
| Record Count | Count of records associated with a particular status. |
| UOW Count | Count of UOW associated with a particular execution status. |

## UOW Summary By Maintenance Window

The UOW summary by maintenance window report illustrates all completed UOWs. Realm name, device name, VTMOS and date range are the report criteria available to configure this report.

This task describes the criteria required for the UOW summary by maintenance window report, as well as the results it produces.

1. Enter realm information by selecting the appropriate check-boxes. There are `select all` and `deselect all` options for faster selection. If you want to include the sub-realms of the chosen realms, indicate using the `Include sub-realms` option.
2. Enter the device name and VTMOS filter. The asterix (*) wildcard can be used to choose all device names.
3. Enter the date range using the "from" and "to" criteria available.
4. Select **Finish** to run the report.
5. The resulting report displays a summary of the report criteria supplied in the previous screen, alongside the following information:

| *Table 90. UOW summary by maintenance window report details.* | |
|---|---|
| **Field** | **Definition** |
| UOW ID | Displays the UOW ID assigned when the UOW was created |
| VTMOS | Associated VTMOS of device |
| Name | Device name or IP address |
| Submitted By | User name of person who submitted the UOW. |
| Request Type | UOW type submitted for example, Run Autodiscovery. |
| Description | Narrative to accompany UOW. |
| Start Time | Timestamp associated with when the UOW was invoked. |
| UOW Result | Result of UOW for example, success |
| Task Result | Result of task for example, success. |

# Chapter 7. Setting user preferences

Use this information to set user preferences for the Netcool Configuration Manager interfaces. Changed preferences take effect the next time you access the interface.

You access the **Preferences** window from the Netcool Configuration Manager GUI. You can set user preferences for the following interfaces:

**Archive Manager**
Select this option to make changes to Archive Manager including queue table, work logs, the display of detail dialogs, and refresh options

**Configuration Editor**
Select this option to select your list view options for roll-up lists.

These settings are stored in the user's home directory. If more than one person uses the same machine, they can have their own settings stored and used as long as each user logs into Netcool Configuration Manager with a unique account. Configuration Editor preferences will follow the user across machines if the user's home directory is shared across machines.

**Detail Tabs**
Select this option to configure the refresh options on the information tabs in the Queue Manager, Archive Manager and Resource Browser.

**General Application**
Select this option to choose general application settings such as the showing of confirmation dialogs.

**Paging**
Select this option to control the page sizes available for selection in the Paging panels.

**Queue Manager**
Select this option to make changes to Queue Manager including queue table, work logs, the display of detail dialogs, and refresh options.

Queue Manager settings are stored in the user's home directory. If more than one person uses the same machine, they can have their own settings stored and used as long as each user logs into Netcool Configuration Manager with a unique account. Queue Manager preferences will follow the user across machines if the user's home directory is shared across machines.

**Resource Browser**
Select this option to change views and refresh options within the resource browser.

**Systems Manager**
Select this option to change refresh and view options for the Systems Manager.

**User Information**
This preference enables you to enter user information including email, telephone, and other identification information.

User Information settings are stored on the server, which means that the client machine can be shared between users.

**User Password**
This preference enables you to change the user password.

**Wizard Panels**
This preference enables the user to remove steps from the UoW submission wizards.

**Work Notifications**
This preference enables you to change Work Notifications and who will be notified, and at what level.

Work Notifications settings are stored on the server, which means that the client machine can be shared between users.

## Setting Archive Manager preferences

The Archive Manager preferences enable you to customize the default view and configure the default behavior of the Archive Manager.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **Archive Manager** on the navigation tree.

   The **Archive Manager Preferences** dialog is displayed.
3. Set the following preferences.

   **Default Refresh**
   Select the desired refresh rate. Regardless of what value you select, you can manually refresh the Queue Manager at any time.

   **Column Resize Mode**
   Select the option for how you want the columns to behave when you resize the queue manager table.

   **No resizing (Scroll Horizontally)**
   When you resize a column, all other columns stay the same size, and a scroll bar is added to the bottom.

   **Resize the Next Column**
   When you resize a column, only the next column changes to compensate.

   **Resize Subsequent Columns**
   When you resize a column, all the columns to the right change to compensate.

   **Resize Last Column**
   When you resize a column, only the last column is changed to compensate.

   **Resize All Columns**
   When you resize a column, all the other columns are changed to compensate.

   **Refresh**

   **Automatically refresh UOW List when actions finish**
   Select this check box to enable automatic refresh of the UOW list when actions complete.
4. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

## Setting Configuration Editor preferences

The Configuration Editor preferences enable you to customize the default view and configure the default behavior of the Archive Manager. You can speed up the Configuration Editor by specifying that it only show a certain number of lines at a time.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **Configuration Editor** on the navigation tree.

   The **Configuration Editor Preferences** dialog is displayed.
3. Set the following preferences.

   **Number of lines to trigger list view**
   Select the minimum number of list commands you want displayed in list mode.

   **Number of lines shown in list view**
   Select the number of lines you want shown, without having to scroll, when list commands are in list mode. This setting will not affect list commands having less commands than the number you entered in the previous field.
4. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

## Setting Detail tabs preferences

The Detail tabs preferences customize the refresh options of the tabs in the Queue Manager, Resource Browser and Archive Manager.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **Detail Tabs** on the navigation tree.

   The **Detail Tabs Preferences** dialog is displayed.
3. Set the following preferences.

   **Refresh Tabs On Selection**
   Select **Always** to ensure that the tab will be refreshed each time it is opened.

   Select **If Resource has Changed** to ensure that the tab will only be refreshed if the resource selected in the main Netcool Configuration Manager table has changed since the last time it was selected.

   **Refresh Tabs After Action**
   Select **Automatically refresh Tab Table when modify actions finish** to ensure that the tab table is refreshed after each action completes.
4. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

## Setting General Application preferences

General Application preferences enable you to control if you want to view verification dialogs when you close the application.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **General Application** on the navigation tree.

   The **General Application Preferences** dialog is displayed.
3. Select **Show confirmation when closing the application** to ensure that a confirmation dialog is displayed when you close the application.
4. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

## Setting Paging preferences

Paging preferences customize the page sizes that are available for selection in the paging panels in the Queue Manager, Archive Manager and Resource Browser.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **Paging** on the navigation tree.

   The **Paging Preferences** dialog is displayed.
3. Set the following preferences.

   **Page sizes**
   Add or remove entries from the page size drop-down list.

   **Restriction:** The system performs error checking when you add a new entry, ensuring that it is a whole number between 1 and 100,000.

   **Refresh Options**
   Select **Disable paging options during refresh** to improve refresh performance.
4. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

## Setting Queue Manager preferences

The Queue Manager preferences enable you to customize the default view and configure the default behavior of the Queue Manager.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **Queue Manager** on the navigation tree.

   The **Queue Manager Preferences** dialog is displayed.
3. Set the following Queue table preferences.

   **Default Refresh**
   Select the desired refresh rate. Regardless of what value you select, you can manually refresh the Queue Manager at any time.

   **Column Resize Mode**

   **No resizing (Scroll Horizontally)**
   When you resize a Queue Manager table column, all other columns stay the same size, and a scroll bar is added to the bottom.

   **Resize the Next Column**
   When you resize a column, only the next column changes to compensate.

   **Resize Subsequent Columns**
   When you resize a column, all the columns to the right change to compensate.

   **Resize Last Column**
   When you resize a column, only the last column is changed to compensate.

   **Resize All Columns**
   When you resize a column, all the other columns are changed to compensate.
4. Select **Automatically refresh Queue Table when modify actions finish** to enable automatic refresh of the queue table when actions complete.
5. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

## Setting Resource Browser preferences

Resource Browser preferences enable you to customize the default view and configure the default behavior of the Resource Browser.

The Resource Browser allows you to view and work with all types of resources used by Netcool Configuration Manager. You can specify settings for the Resource Browser that limit what you can view. For example, if you never work with a certain type of resource, you can remove that type of resources from your view.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **Resource Browser** on the navigation tree.

   The **Resource Browser Preferences** dialog is displayed.
3. Set the following Visibility preferences.

   **Show Hidden Realms**
   Select this option if you want hidden realms to be shown in the browser.

   **Show System Realms**
   Select this option if you want system realms to be shown in the browser. The default is to not show System realms.

   **Restriction:** You won't be able to change this option unless you have Manage System rights.
4. Set the Double Click Action preferences to determine the action to be performed on a resource when it is double-clicked. The default action saved here, is displayed in bold when a right click operation is made on the selected device in the Resource Browser.

Select one of the following options from the Actions drop-down list:

**Note:** When you double click on a device, the default option selected here is overridden based on the support level of the device. If the device does not support the default option chosen here, the action carried out on the device will be the first option in the list below that the device supports. For example, if you double click on a device with a Standard support level and the `View Configuration (Modelled)` action is chosen as the default, the action carried out on the device will be `View Configuration (Native)`.

**View Configuration (Modelled)**
Opens the Configuration Editor with the device's current configuration in read-only mode.

**Edit Configuration (Modelled)**
Opens the Configuration Editor with the device's current configuration in edit mode

**View Configuration (Native)**
Opens the Native Commands dialog with the device's current configuration.

**IDT Manual Launch**
Initiates a manual IDT session with the device.

5. Set the Columns preferences to determine how you want the columns to behave when you resize the Resource Manager table.
Select one of the following Column Resize Mode options:

**No resizing (Scroll Horizontally)**
When you resize a Resource Manager table column, all other columns stay the same size, and a scroll bar is added to the bottom.

**Resize the Next Column**
When you resize a column, only the next column changes to compensate.

**Resize Subsequent Columns**
When you resize a column, all the columns to the right change to compensate.

**Resize Last Column**
When you resize a column, only the last column is changed to compensate.

**Resize All Columns**
When you resize a column, all the other columns are changed to compensate.

6. Select **Show Update Flags** to display the red and orange indicator flags which appear if device drivers need to be updated.
7. Select **Automatically refresh Resource List when modify actions finish** to enable automatic refresh of the resource list when actions complete.
8. Under Show the Following Resource Types, select the resources to be displayed in the Resource Browser.

   **Tip:** Excluded resource types can still be accessed through the search function.
9. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

## Setting Systems Manager preferences

Systems Manager preferences enable you to customize the default view and configure the default behavior of the Systems Manager.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **Systems Manager** on the navigation tree.

   The **Systems Manager Preferences** dialog is displayed.
3. Set the following Visibility preferences.

**Show Active Servers**
Select this option if you want to display all active servers on your network.

**Show Inactive Servers**
Select this option if you want to display all **inactive** servers on your network.

4. Set the Columns preferences to determine how you want the columns to behave when you resize the Systems Manager table.
   Select one of the following Column Resize Mode options:

   **No resizing (Scroll Horizontally)**
   When you resize a Systems Manager table column, all other columns stay the same size, and a scroll bar is added to the bottom.

   **Resize the Next Column**
   When you resize a column, only the next column changes to compensate.

   **Resize Subsequent Columns**
   When you resize a column, all the columns to the right change to compensate.

   **Resize Last Column**
   When you resize a column, only the last column is changed to compensate.

   **Resize All Columns**
   When you resize a column, all the other columns are changed to compensate.
5. Select **Automatically refresh Systems List when modify actions finish** to enable automatic refresh of the systems list when actions complete.
6. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

## Setting user information

Edit your personal information using the User Information dialog.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **User Information** on the navigation tree.
   The **User Information** dialog is displayed.
3. Type the following information:

   **Name Fields**
   Edit your name as necessary. Any changes you make will not affect the login name that is displayed for any work you submit.

   **E-Mail Address**
   If you are going to sign up for work notifications, you must enter a valid email address in this field.

   **Telephone Number**
   Enter a phone number for contact purposes.

   **Note:** This field is not used by Netcool Configuration Manager.

   **Identification**
   Use this field for any other identification that your company requires.

   **Note:** This field is not used by Netcool Configuration Manager.

   **Group Membership**
   This field shows the groups of which you are a member.

   **Time Zone**
   This field shows the time zone where your member status resides.

   **Tip:** For display purposes, it is recommended that you set the system time zone appropriate to your location. When set, all times shown in the application will be converted to your timezone with the exception of the times shown in the UOW log, which will remain in GMT. When the timezone is set, it only applies against the username that was used to set the timezone.
4. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

# Setting user password

You can change the Netcool Configuration Manager password defined by your system administrator.

Ensure you are aware of the minimum password requirements you must adhere to before changing your password.

If single sign-on (SSO) has been enabled between Netcool Configuration Manager and Network Manager, you change the user password from the DASH console of the Netcool Configuration Manager Presentation Server, rather than the native Netcool Configuration Manager GUI.

This procedure only changes the user password that you use to logon to the Netcool Configuration Manager GUI, but not the database or Reporting user passwords. For information on how to change these, see the What to do next section.

Changing the Netcool Configuration Manager user password if single sign-on **has not** been enabled:

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **User Password** on the navigation tree.

   The **Password Change** dialog is displayed.
3. Type the following information:

   **Current Password**
   Type your current password.

   **New Password**
   Type the new password you want to assign to yourself.

   **Confirm Password**
   Type the new password again.
4. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

Changing the Netcool Configuration Manager user password if single sign-on **has** been enabled:

5. Logon to the DASH console of the Netcool Configuration Manager Presentation Server.

   **Note:** The default logon is `http://host:port/ibm/console`
6. Change the password using the DASH interface.

To change the passwords for the reporting user and the database user, follow these steps:

**To change a reporting user password**

1. Logon to the DASH Reporting Server as the user for whom you want to change the password.
2. Select the user icon, then click **Change Password**.
3. Change the password, and save your changes.

**To change the database user password**

Use the `/opt/IBM/tivoli/netcool/ncm/bin/icosadmin` script with ChangeDbPassword as a flag, and the following options defined:

-u (database username)

-p (current database password)

-n (new database password)

For example:

```
icosadmin ChangeDbPassword -u <db_username> -p <old_db_passwd>  -n
    <new_db_passwd>
```

**Note:** If the Netcool Configuration Manager database password is changed, this impacts Reports. Therefore, you must change the Netcool Configuration Manager datasource password in the Reports as described here:

1. From Common Reporting launch Administration.
2. Select **Data Source Connections** > **ITNCM** > **View Signons** > **Set Properties** > **Signon** > **Edit the Signon**, and update the stored database password.

## Setting Wizard Panels preferences

Wizard Panels preferences customize the unit of work (UOW) submission wizard. You can hide specific screens from the display sequence, and use the default value for those screens instead.

Ensure you are aware of the minimum password requirements you must adhere to before changing your password.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **Wizard Panels** on the navigation tree.

   The **Wizard Preferences** dialog is displayed. All possible wizard screens that are displayed during any type of UoW submission are listed. The default value set for each screen in System Properties is indicated in parenthesis after the screen name.
3. For each of the wizard screens listed, you can apply from the following options:

   **Default**
   Select this option to ensure the wizard screen applies the default value as specified in System Properties

   **Hidden**
   Select this option to ensure that this wizard screen is not displayed as part of the UOW Submission wizard screen sequence.

   **Visible**
   Select this option to ensure that this wizard screen is displayed as part of the UOW Submission wizard screen sequence.
4. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

## Setting Work Notifications preferences

Work Notifications allow you keep track of a UOW's progress without having to log in. Instead, you receive emails when the work changes states.

In order to receive work notifications, you must ensure that you have a valid email address entered in the system.

You can be notified when a UOW changes to one or more specific state. UOWs can be those submitted by you, or by a member of your group, or they can be UOWs for which you are an approver.

1. To access the **Preferences** window, click **User Preferences**, or click **File** > **Preferences** from the main dialog.
2. Select **Work Notifications** on the navigation tree.

   The **Work Notifications** dialog is displayed and all work states are listed.
3. columns next to the work states for each association (user, group, approver).
4. For each of the listed UOW states, select one or more of the following options:

   **Note:** To be notified of all state changes, select **All**.

   **User**
   Select the **User** checkbox against a specific state in order to be notified when a UOW you submitted enters that state.

   **Group**
   Select the **Group** checkbox against a specific state in order to be notified when a UOW that was submitted by someone in your user group enters that state.

**Approver**

Select the **Approver** checkbox against a specific state in order to be notified when a UOW for which you are an approver enters that state.

**Restriction:** Selecting the **Approver** checkbox against a specific state will only have an effect if you have 'Manager Work' permissions.

5. Click **Apply** to save the settings, or click **OK** to save the settings and exit the **Preferences** window.

You will start to receive emails as soon as a UOW enters a state for which you signed up.

# Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
958/NH04
IBM Centre, St Leonards
601 Pacific Hwy
St Leonards, NSW, 2069

Australia

IBM Corporation
896471/H128B
76 Upper Ground
London SE1 9PZ
United Kingdom

IBM Corporation
JBF1/SOM1
294 Route 100
Somers, NY, 10589-0100
United States of America

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© your company name (year). Portions of this code are derived from IBM Corp. Sample Programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

## Trademarks

IBM, the IBM logo, ibm.com®, Netcool®, Passport Advantage®, Tivoli®, the Tivoli logo, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, Portable Document Format (PDF), PostScript, and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux® is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

"Powered by Cryptzone MindTerm" is copyright 1997 – 2017 Cryptzone North America, Inc. All rights reserved.

Other company, product, or service names may be trademarks or service marks of others.

# Index

Part Number:

Printed in the Republic of Ireland

(1P) P/N:

2023-4219-01