



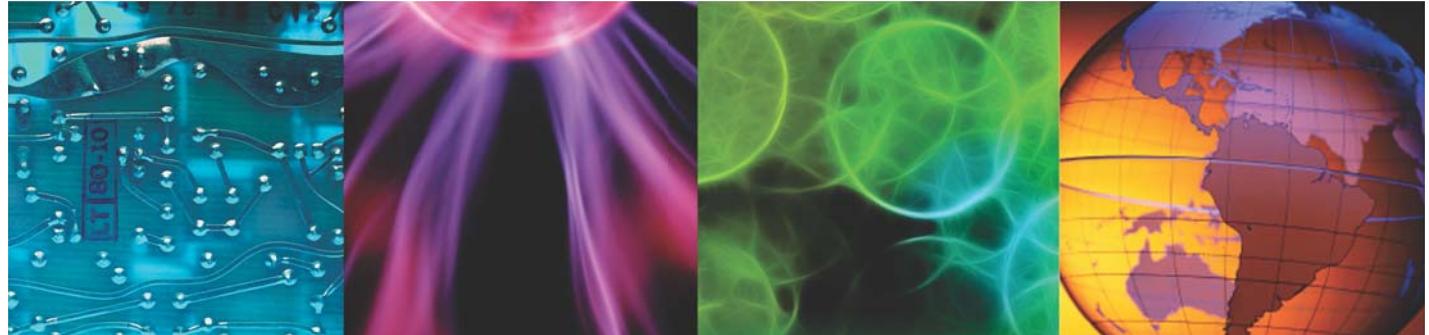
IBM Training

IBM Tivoli Netcool Configuration Manager 6.4.2 Operations and Configuration

Course Exercises

Course code TOD44 ERC 1.0

June 2016



All files and material for this course are IBM copyright property covered by the following copyright notice.

© Copyright IBM Corp. 2016. All Rights Reserved.

US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, and ibm.com are 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.

Trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results.



Contents

About these exercises	vi
Server access	vi
User IDs and passwords	vi
Software	vii
Starting and stopping the software	viii
DB2	viii
Netcool/OMNIbus	viii
IBM Tivoli Network Manager	viii
Dashboard Application Services Hub	viii
Netcool Configuration Manager	ix
Security Directory Server	ix
1 IBM Tivoli Netcool Configuration Manager solution overview exercises	1
Exercise 1. Setting up the lab	1
2 Configuration manager interface exercises.....	6
Exercise 1. Starting the user interface	6
3 Single change configuration management exercises.....	14
Exercise 1 Viewing an authentication resource	14
Exercise 2 Discovering a device from the user interface	17
Exercise 3 Discovering multiple devices with the BulkLoader command	21
Exercise 4 Viewing a device configuration	23
Exercise 5 Making a configuration change with the configuration editor	25
Exercise 6 Connecting to a device with the device terminal	32
Exercise 7 Changing a device configuration by using the device terminal	34
Exercise 8 Verifying that the configuration change was synchronized	36
4 Mass change configuration management exercises	40
Exercise 1 Finding the version, type, model, and operating system for target devices	40
Exercise 2 Viewing a modeled command set	41
Exercise 3 Applying a modeled command set in report only mode	43
Exercise 4 Applying a modeled command set	49
Exercise 5 Creating an interrogative native command set	54
Exercise 6 Applying the interrogative native command set	56
Exercise 7 Creating a native command set	61
Exercise 8 Applying the native command set	63
Exercise 9 Applying command sets from a CSV file	69

5 Administrative tasks exercises	77
Exercise 1 Making changes that require approval	77
Exercise 2 Approving changes	88
Exercise 3 Creating custom searches	91
Exercise 4 Comparing configurations	100
Exercise 5 Running reports	106
6 Netcool integrations exercises	112
Exercise 1 Verifying the component status	112
Exercise 2 Discovering devices with Network Manager	113
Exercise 3 Deleting customer CC devices	117
Exercise 4 Verifying integration with Configuration Manager	120
Exercise 5 Applying a policy to devices from Tivoli Network Manager	124
Exercise 6 Applying a change to a device by using the device terminal	129
Exercise 7 Viewing device history in Activity Viewer	131
7 Authentication and authorization model exercises	135
Exercise 1 Creating a group and a user	135
Exercise 2 Assigning security attributes	140
Exercise 3 Viewing the new user	145
8 Device management exercises	148
Exercise 1 Finding the actual model of a device	148
Exercise 2 Using an authentication resource	151
Exercise 3 Viewing a resource access document	160
Exercise 4 Creating a device script resource	163
Exercise 5 Viewing a file transfer resource	171
Exercise 6 Working with security sets	172
9 Using workflow and scheduling exercises	185
Exercise 1 Scheduling work	185
Exercise 2 Creating a recurring unit of work	193
Exercise 3 Working with time zones	196
10 UOW management exercises	199
Exercise 1 Finding a worker server resource	199
Exercise 2 Splitting a unit of work	201
Exercise 3 Enabling the scheduling alert	207
Exercise 4 Viewing system servers	210
11 IBM device terminal exercises	212
Exercise 1 Using the IBM device terminal	212
Exercise 2 Viewing the synchronization filter	216
Exercise 3 Creating a command filter	221
Exercise 4 Applying and testing the new command filter	226
12 Advanced command sets exercises	234
Exercise 1 Creating a modeled command set to add commands	234
Exercise 2 Creating a modeled command set to modify commands	240

Exercise 3 Testing the command sets	244
Exercise 4 Applying command sets	250
13 Device OS upgrade manager exercises	255
Exercise 1 Modifying an operating system registry	255
Exercise 2 Creating an operating system specification	260
Exercise 3 Testing the network for upgrade compatibility	264
Exercise 4 Viewing the upgrade results	269
14 Out-of-band change (OOBC) daemon exercises	271
Exercise 1 Starting the out-of-band change daemon and making an out-of-band change	271
Exercise 2 Verifying the device synchronization	273
15 Compliance manager interface exercises	276
Exercise 1 Viewing devices, policies, and parameters	276
Exercise 2 Working with processes	286
16 Compliance reports exercises	295
Exercise 1 Running compliance reports	295
Exercise 2 Running remedial actions	308
Exercise 3 Rerunning compliance reports	311
Exercise 4 Running alternative report formats and scheduling a report	314
17 Build and run a policy exercises	321
Exercise 1 Creating a policy realm	321
Exercise 2 Creating definitions	326
Exercise 3 Creating rules	334
Exercise 4 Creating an email action	350
Exercise 5 Creating policies	352
Exercise 6 Working with processes	360
18 Remediation exercises	365
Exercise 1 Creating command sets	365
Exercise 2 Creating remedial actions	372
Exercise 3 Adding remedial actions to rules	377
Exercise 4 Running remedial actions	383
19 Advanced definitions exercises	388
Exercise 1 Creating a policy that uses XPath definitions	388
Exercise 2 Creating a policy that uses an extraction	404
Exercise 3 Testing the new policies	415
Exercise 4 Creating a process	421
20 Preemptive compliance exercises	426
Exercise 1 Enabling preemptive compliance	426
Exercise 2 Testing preemptive compliance	430



About these exercises

Server access

The lab uses two Linux servers that run in VMware. You access these servers through the VMware console.

The primary student image is configured with one Ethernet interface (eth0) as Host-Only and has a static IP address assigned:

- **IP address:** eth0 192.168.100.100
- **Host name:** host1.csite.edu associated with eth0

The second image (GNS3) is configured with one ethernet interface (eth0) as Host-Only and has a static IP address assigned:

- **IP address:** eth0 10.191.101.126
- **Host name:** GNS3 associated with eth0

User IDs and passwords

The user IDs and passwords for this course are listed in the following table.

Table 1 User IDs and passwords

Type	User ID	Password	Usage
Linux	root	object00	Linux super user
Linux	db2inst1	object00	Owns DB2 instance and Reporter database
Linux	ncim	object00	Tivoli Network Manager access to DB2
Linux	tncmdb	object00	Netcool Configuration Manager access to DB2
Linux	netcool	object00	Student user ID
Dashboard Application Services Hub and ObjectServer	itnadmin	object00	Tivoli Network Manager administrative user

Table 1 User IDs and passwords (continued)

Type	User ID	Password	Usage
Dashboard Application Services Hub and ObjectServer	ncoadmin	object00	Web GUI administrative user
ObjectServer	root	object00	Netcool/OMNIbus superuser
Dashboard Application Services Hub	smadmin	object00	Dashboard Application Services Hub administrative user
Netcool Configuration Manager	engineer	object00	Netcool Configuration Manager user
Netcool Configuration Manager	operator	object00	Netcool Configuration Manager user
Netcool Configuration Manager	administrator	object00	Netcool Configuration Manager user
Netcool Configuration Manager	Intelliden	object00	Super user that is required to stop components

Unless directed in the instructions, all command-line activities are performed as the Linux **netcool** user.

Table 2 Image GNS3 user IDs and passwords

Type	User ID	Password	Usage
Linux	root	object00	Linux super user
router/switch	intelliden	p4ssw0rd	Router or switch console user
router/switch		3n4bl3	Router or switch enable password

Software

The student image is configured with the following software:

- Netcool®/OMNIbus V8.1.0.5 and Web GUI V8.1.0.4
- IBM® Tivoli Network Manager V4.2
- IBM Tivoli® Netcool Configuration Manager V6.4.2
- Jazz™ for Service Management V1.1.2.1
- Tivoli Common Reporting V3.1.2.1
- IBM DB2® V10.5.0.3 Enterprise Server Edition
- IBM Security Directory Server v6.3

All files that are required for student exercises are in various subdirectories in the **/workshop** directory.

Starting and stopping the software

Methods for starting and stopping the software are described in this section.

DB2

DB2 is installed as the **root** user and is configured to start automatically when the system starts:

```
/etc/init.d/db2_tcr [start, stop]
```

Netcool/OMNIbus

IBM Tivoli Netcool/OMNIbus is installed as the **netcool** user and is configured to be managed by Netcool Process Activity. Process Activity is configured to run all Netcool/OMNIbus components as the **netcool** user. Process Activity runs as the **netcool** user and starts when the system starts:

```
/etc/init.d/nco [start, stop]
```

IBM Tivoli Network Manager

IBM Tivoli Network Manager is installed as the **netcool** user. IBM Tivoli Network Manager is configured to use DB2 as the topology store. IBM Tivoli Network Manager Control is configured to run all IBM Tivoli Network Manager components as the **netcool** user. IBM Tivoli Network Manager Control runs as the **netcool** user and starts at system start:

```
/etc/init.d/ncp [start, stop]  
/etc/init.d/storm [start, stop]
```

 **Note:** The following IBM Tivoli Network Manager commands can be used to manually start, stop, and check the status of IBM Tivoli Network Manager.

```
itnm_start [ncp, storm]  
itnm_stop [ncp, storm]  
itnm_status [ncp, storm]
```

Dashboard Application Services Hub

Dashboard Application Services Hub is installed as the **netcool** user. Dashboard Application Services Hub is configured to use LDAP as the default user repository. Dashboard Application Services Hub is configured to run as the **netcool** user and starts at system start:

```
/etc/init.d/jazz [start, stop]
```

Netcool Configuration Manager

Netcool Configuration Manager is installed as the **netcool** user. The components start automatically at system start:

```
/etc/init.d/itncm [start, stop]
```

The following commands can be used to start, stop, and check the status of Netcool Configuration Manager:

```
itncm.sh start  
itncm.sh stop  
itncm.sh status
```

The super user that is required to stop Configuration Manager components is **Intelliden** with password **object00**.

Security Directory Server

Security Directory Server is installed as the **root** user. Security Directory Server uses a separate installation of DB2. Security Directory Server and the associated DB2 instance are configured to start at system start:

```
/etc/init.d/db2_sds [start, stop]  
/etc/init.d/ibmslapd [start, stop]
```

About these exercises

x

IBM Tivoli Netcool Configuration Manager 6.4.2 Operations and Configuration

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

© Copyright IBM Corp. 2016



1 IBM Tivoli Netcool Configuration Manager solution overview exercises

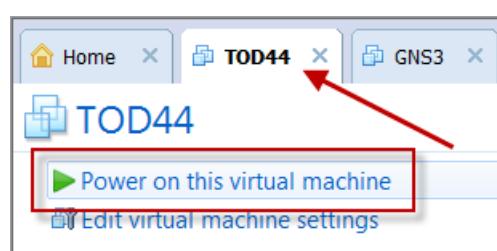
In this unit, you start the lab images.

Exercise 1. Setting up the lab

In these exercises, you use the following two virtual machine images:

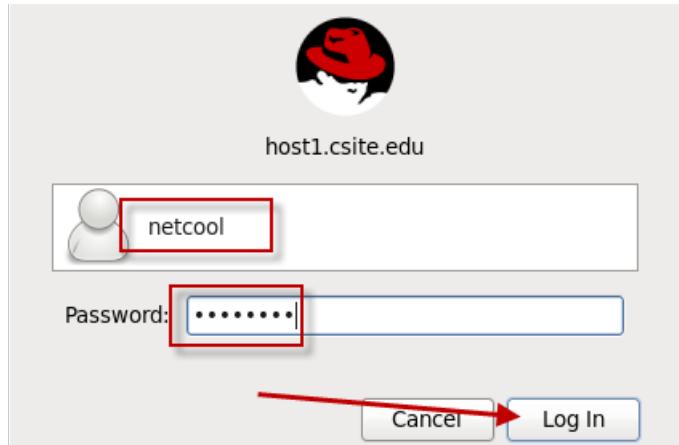
- **TOD44:** This image has the IBM® Tivoli® Netcool Network Manager suite of software installed. This software includes the Tivoli Netcool/OMNIbus, Tivoli Network Manager, Netcool Configuration Manager, and Dashboard Application Services Hub. This VM is also running the DB2 database software to support these servers.
- **GNS3:** This image has simulation software for creating virtual routers that are like physical routers on a network. You can use Netcool Configuration Manager to log in and manage these virtual devices as though they are actual devices on the network.

1. Locate the tab that is labeled **TOD44** in the VMware console.
2. Click the tab to select it.
If the image is running, skip the following step.
3. Click the green power-on icon to start the image, if necessary.

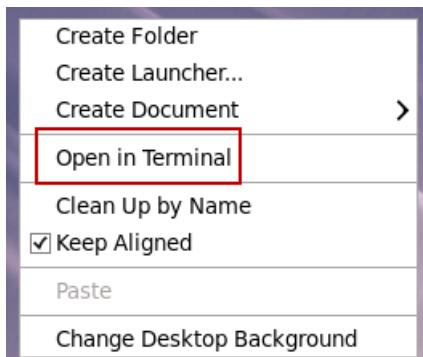


Wait for the image to start. The image is started when the login window opens.

4. Log in as user **netcool** with password **object00**.



5. Right-click the desktop and click **Open In Terminal**.



6. Verify the status of the Netcool Configuration Manager server with the following command:

```
itncm.sh status
```

```
netcool@host1:~/Desktop
File Edit View Search Terminal Help
[netcool@host1 Desktop]$ itncm.sh status
-----
IBM Tivoli Netcool Configuration Manager Status
-----
Deployment Type = GUI + Worker Server
Base Worker Server = Enabled
Compliance Core = Enabled
Components
-----
Worker Server = RUNNING
Compliance Core = RUNNING
GUI Server = RUNNING
```



Note: The components take several minutes to start after you start the VMware image. If the components are not active, wait a short time and repeat the command.

- Verify the status of the Network Manager components with the following command:

```
itnm_status
```

Component	Status	Domain
ncp_ctrl	RUNNING	NOI_AGG_P
ncp_store	RUNNING	NOI_AGG_P
ncp_class	RUNNING	NOI_AGG_P
ncp_model	RUNNING	NOI_AGG_P
ncp_disco	RUNNING	NOI_AGG_P
ncp_d_helpserv	RUNNING	NOI_AGG_P
ncp_config	RUNNING	NOI_AGG_P
ncp_poller_default	RUNNING	NOI_AGG_P
ncp_poller_admin	RUNNING	NOI_AGG_P
nco_p_ncpmonitor	RUNNING	NOI_AGG_P
ncp_g_event	RUNNING	NOI_AGG_P
ncp_webtool	RUNNING	NOI_AGG_P
ncp_virtualdomain	RUNNING	NOI_AGG_P
Apache Storm:		
supervisord	RUNNING	PID=4316
storm_nimbus	RUNNING	PID=4325
storm_supervisor	RUNNING	PID=4326
zookeeper	RUNNING	PID=4324
Storm topologies:		
NMStormTopology	ACTIVE	



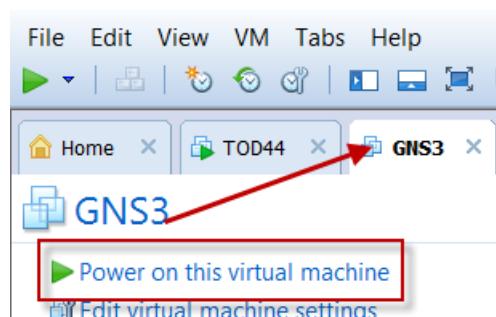
Note: The components take several minutes to start after you start the VMware image. If the components are not active, wait a short time and repeat the command.

- Locate the tab that is labeled **GNS3** in the VMware console.

- Click the tab to select it.

If the image is running, skip the following step.

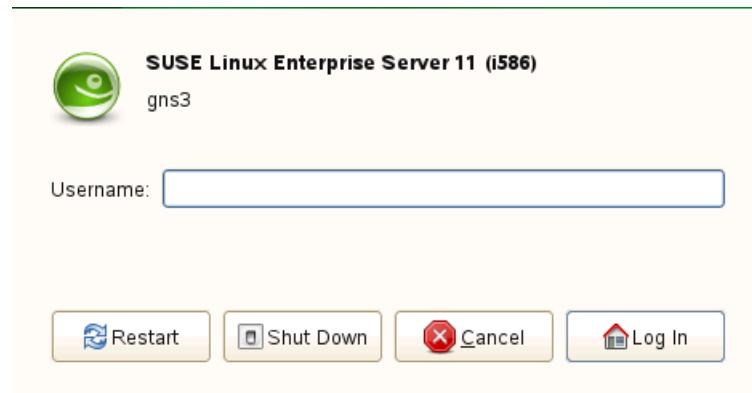
- Click the green power-on icon to start the image, if necessary.



Exercise 1. Setting up the lab

Wait for the image to start. The image is started when the login window opens.

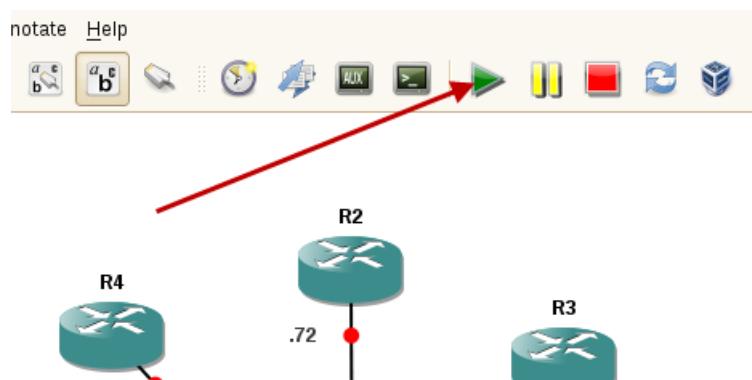
11. Log in as user **root** with password **object00**.



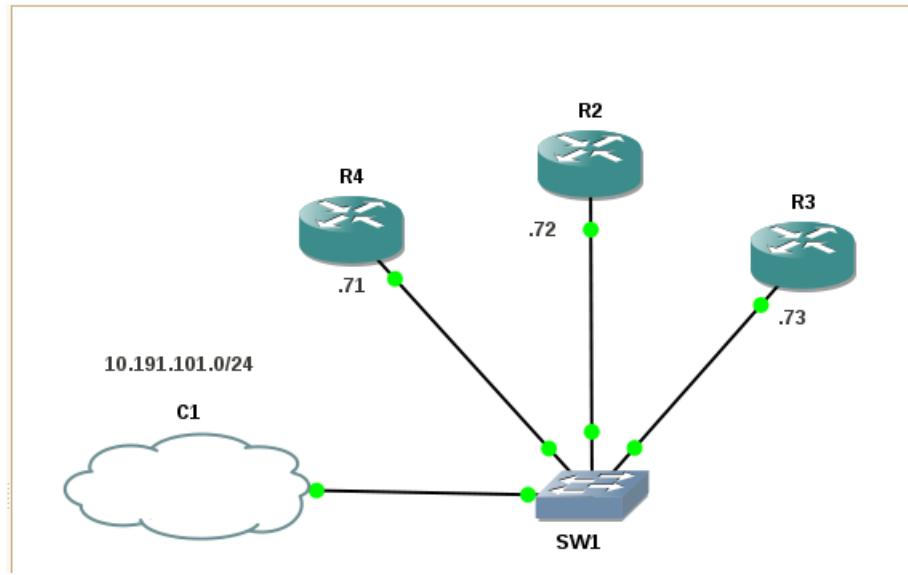
12. On the desktop, double-click the **TNCMTraining-lab1** icon to start the simulator.



13. Click the green start icon in the GNS3 toolbar to start the simulation.



The dots under each router turn from red to green.



14. After the simulator starts, click the **TOD44** tab.

15. Verify access from the TOD44 image to the simulated devices.

```
ping 10.191.101.71
```

```
netcool@host1:~$ ping 10.191.101.71
PING 10.191.101.71 (10.191.101.71) 56(84) bytes of data.
64 bytes from 10.191.101.71: icmp_seq=1 ttl=255 time=19.2 ms
64 bytes from 10.191.101.71: icmp_seq=2 ttl=255 time=8.18 ms
64 bytes from 10.191.101.71: icmp_seq=3 ttl=255 time=8.63 ms
^C
--- 10.191.101.71 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2735ms
rtt min/avg/max/mdev = 8.187/12.031/19.270/5.122 ms
[netcool@host1:~]$
```

The images are started, and ready for use.



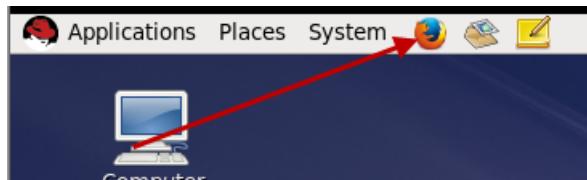
2 Configuration manager interface exercises

In this unit, you start the Netcool Configuration Manager user interface and view some of the available features.

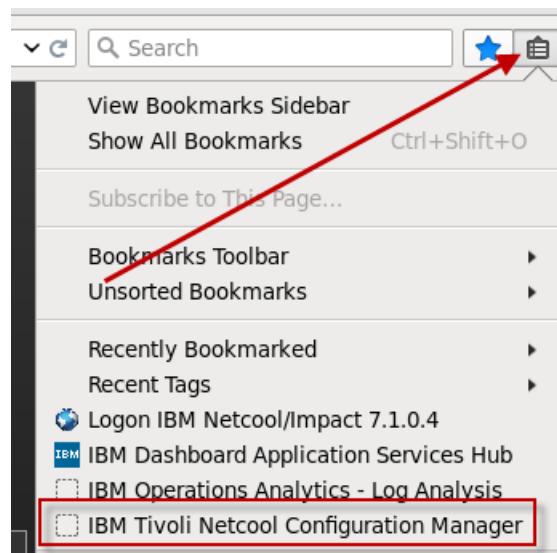
Exercise 1. Starting the user interface

Start the Netcool Configuration Manager user interface.

1. Open a Firefox browser.



2. Open the list of bookmarks, and select **IBM Tivoli Netcool Configuration Manager**.



3. Enter the user name **engineer** and the password **object00**. Click **Login**.

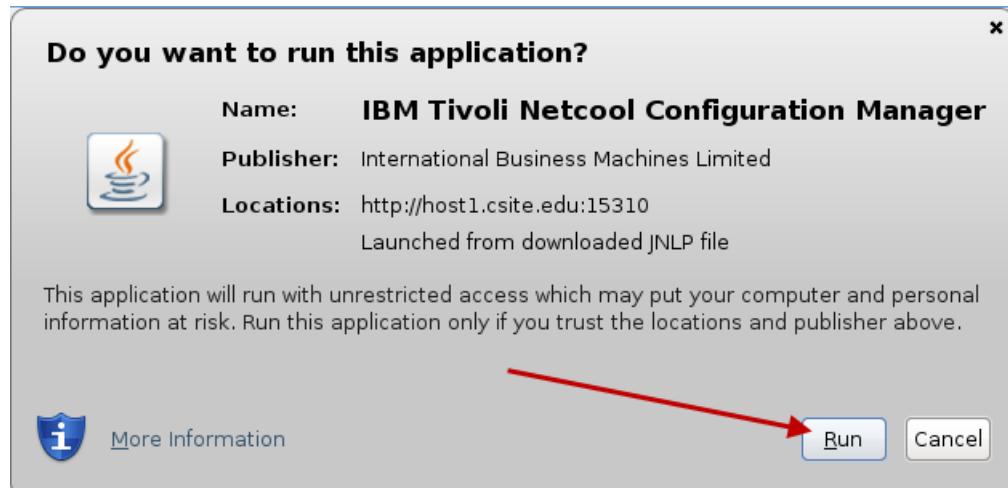


4. Click **ITNCM Webstart GUI**.



The Java Webstart client starts.

5. Click **Run**.

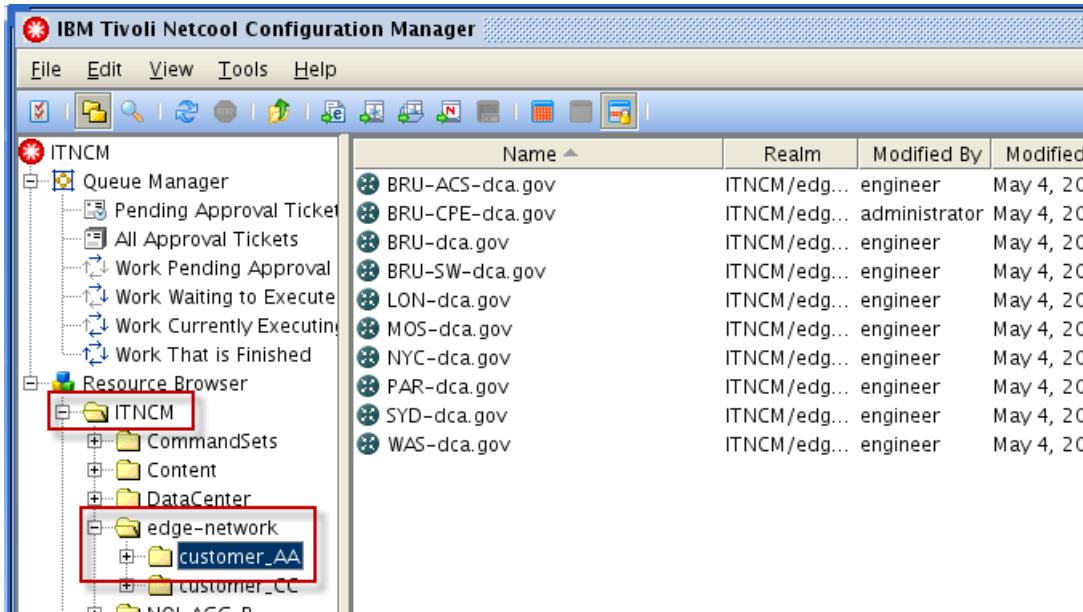


Look at some managed devices in the *resource browser*.

2 Configuration manager interface exercises

Exercise 1. Starting the user interface

6. Click **ITNCM > edge-network > customer_AA** in the resource browser.

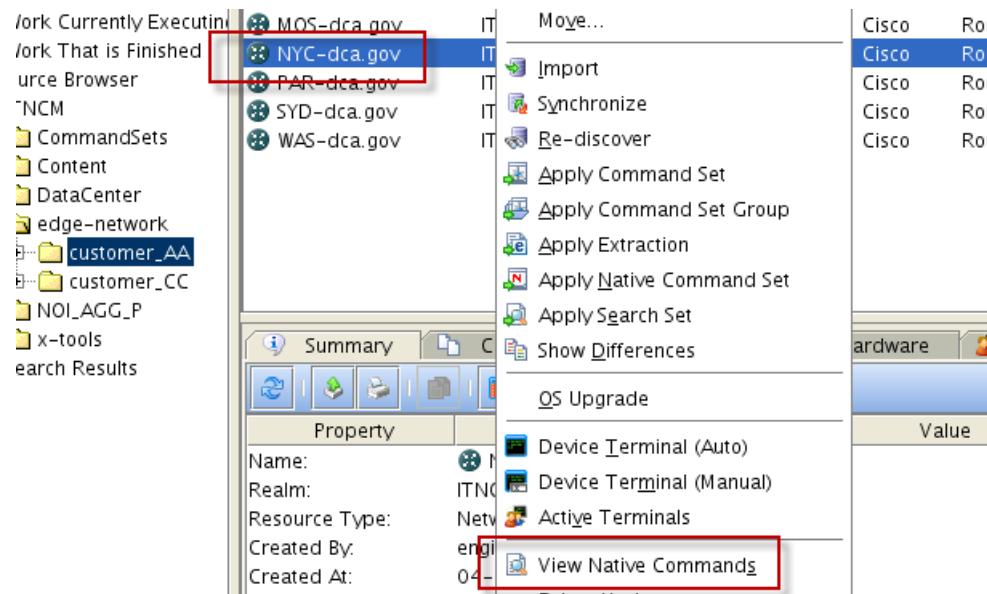


7. Examine the vendor, type, model, and operating system (VTMOS) of these devices.

Name	Realm	Modified By	Modified At	Vendor	Type	Model	OS
BRU-ACS-dca.gov	ITNCM/e...	engineer	May 4, 2016 ...	Cisco	Router	3640	C3640-I03-M-12.2(32)
BRU-CPE-dca.gov	ITNCM/e...	administrator	May 4, 2016 ...	Cisco	Router	3640	C3640-I03-M-12.2(32)
BRU-dca.gov	ITNCM/e...	engineer	May 4, 2016 ...	Cisco	Router	7206VXR	C7200-JK9035-M-12.3(18)
BRU-SW-dca.gov	ITNCM/e...	engineer	May 4, 2016 ...	Cisco	Router	3660	C3660-JK9035-M-12.4(12)
LON-dca.gov	ITNCM/e...	engineer	May 4, 2016 ...	Cisco	Router	7206VXR	C7200-JK9035-M-12.3(18)
MOS-dca.gov	ITNCM/e...	engineer	May 4, 2016 ...	Cisco	Router	7206VXR	C7200-JK9035-M-12.3(18)
NYC-dca.gov	ITNCM/e...	engineer	May 4, 2016 ...	Cisco	Router	7206VXR	C7200-JK9035-M-12.3(18)
PAR-dca.gov	ITNCM/e...	engineer	May 4, 2016 ...	Cisco	Router	7206VXR	C7200-JK9035-M-12.3(18)
SYD-dca.gov	ITNCM/e...	engineer	May 4, 2016 ...	Cisco	Router	7206VXR	C7200-JK9035-M-12.3(18)
WAS-dca.gov	ITNCM/e...	engineer	May 4, 2016 ...	Cisco	Router	7206VXR	C7200-JK9035-M-12.3(18)

Look at the native configuration of the device named NYC-dca.gov.

8. Right-click the **NYC-dca.gov** device and click **View Native Commands**.



The configuration opens in a new window.

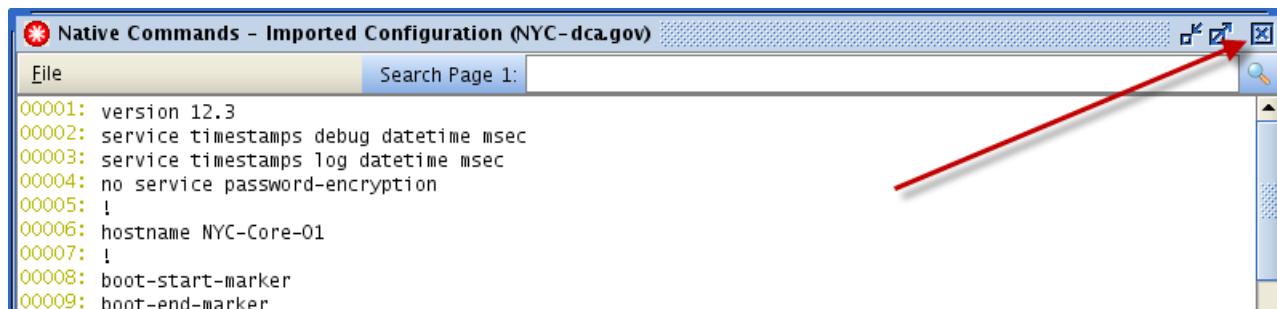
The window title is "Native Commands - Imported Configuration (NYC-dca.gov)". The content area displays the following configuration code:

```

00001: version 12.3
00002: service timestamps debug datetime msec
00003: service timestamps log datetime msec
00004: no service password-encryption
00005: !
00006: hostname NYC-Core-01
00007: !
00008: boot-start-marker
00009: boot-end-marker
00010: !
00011: enable password object00
00012: !
00013: aaa new-model
00014: !
00015: !
00016: aaa session-id common
00017: ip subnet-zero
00018: !
00019: !
00020: !
00021: ip cef
00022: ip audit po max-events 100
00023: !
00024: !

```

9. Click the X to close the command window.

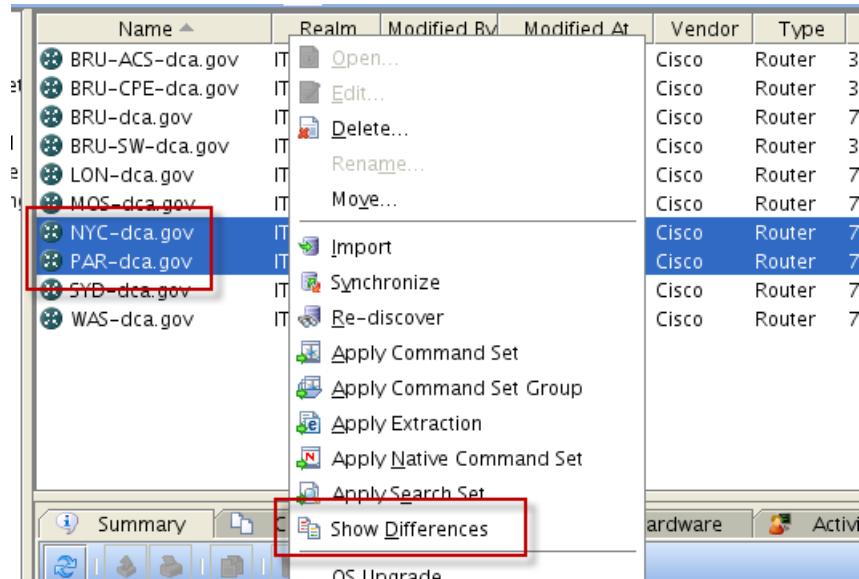


2 Configuration manager interface exercises

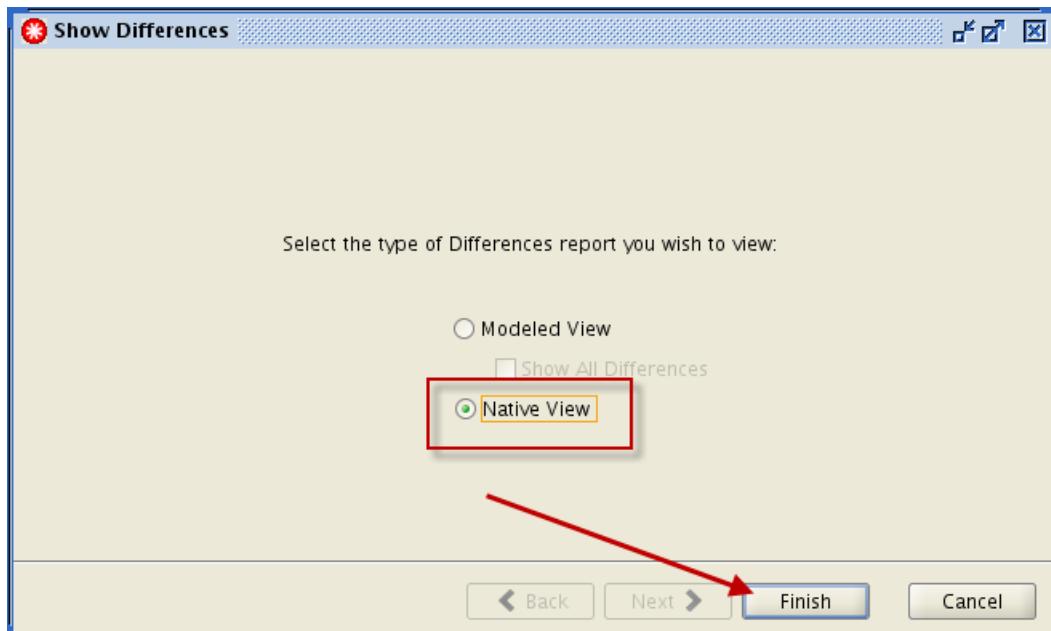
Exercise 1. Starting the user interface

Look at the differences in the configuration between the NYC-dca.gov and the PAR-dca.gov routers.

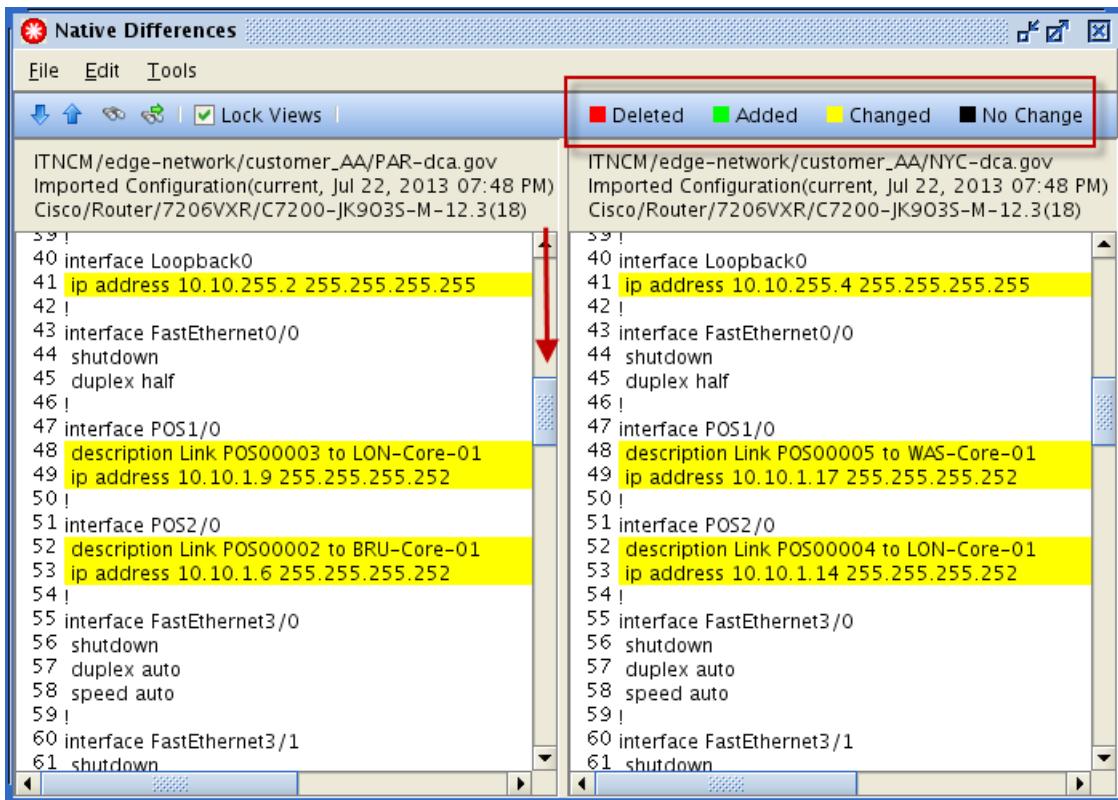
10. Use Ctrl + click to select the **NYC-dca.gov** and the **PAR-dca.gov** routers. Right-click the routers and click **Show Differences**.



11. Click **Native View**. Click **Finish**.



12. Scroll down to view the differences in the configurations.

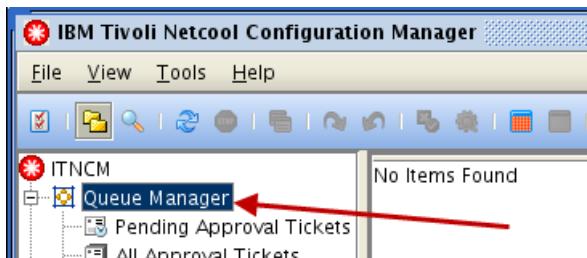


The two configuration files are shown side by side. The files scroll together. Differences between the two files are indicated with colored highlights.

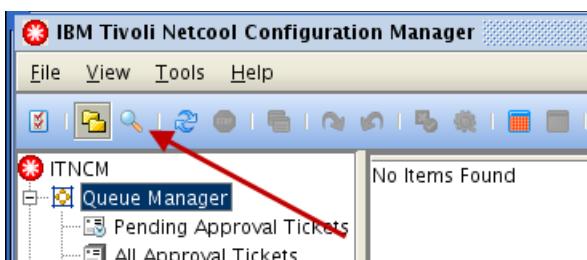
13. Close the differences window when you finish.

Configure the Queue Manager to show all *units of work*.

14. Click **Queue Manager** to select it.



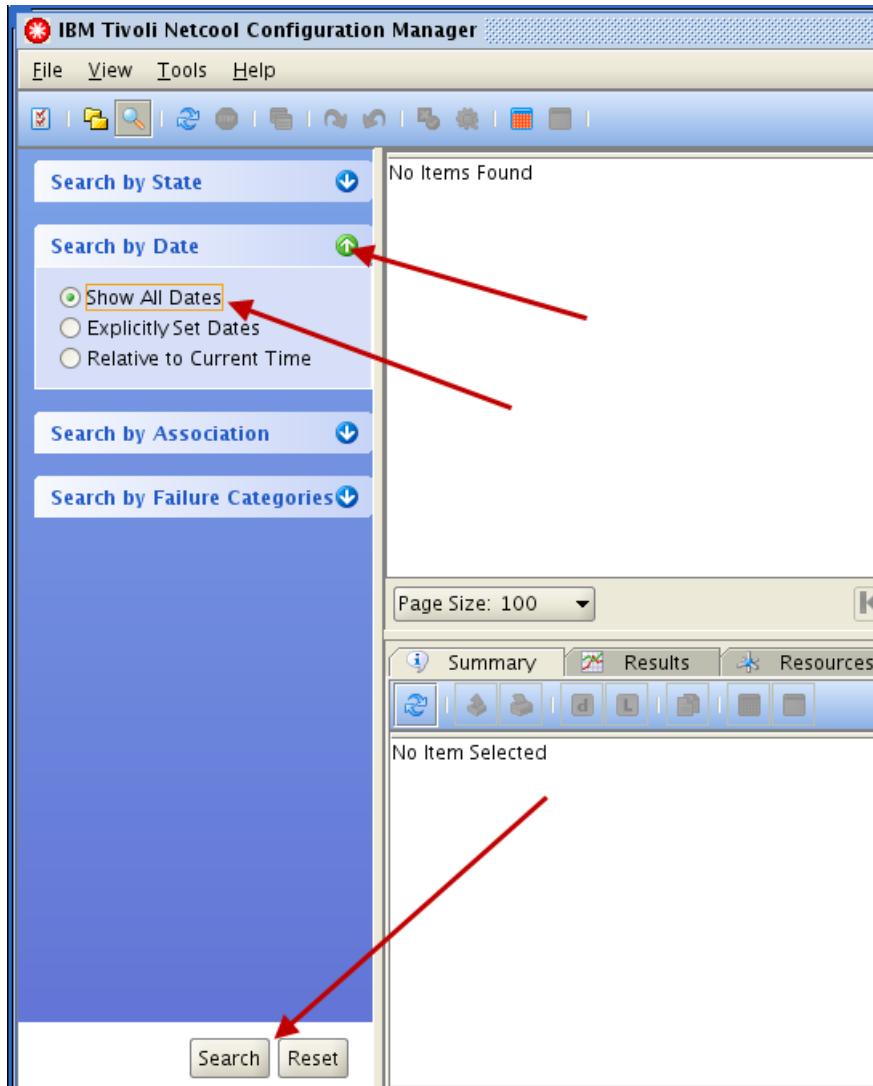
15. Click the **Show/Hide the Search Sidebar** icon at the top of the user interface.



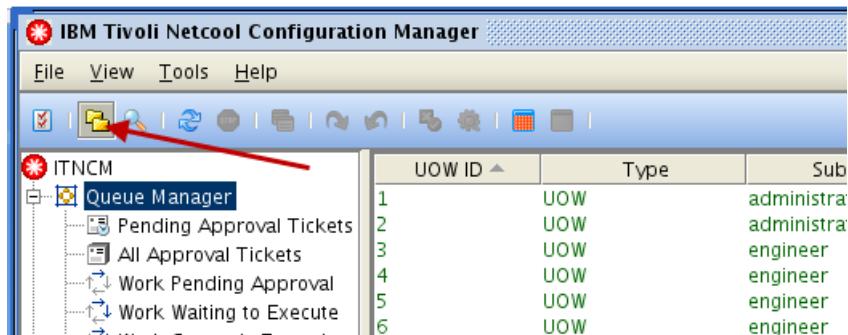
16. Click **Search by Date**. Click **Show All Dates**. Click **Search**.

2 Configuration manager interface exercises

Exercise 1. Starting the user interface



17. Click the Show/Hide the Navigation Tree icon at the top of the user interface.



Look at the *units of work* in the *queue manager*.

UOW ID ▲	Type	Submitter	Request Type	Executive
1	UOW	administrator	Run Autodiscovery	SUCCESS
2	UOW	administrator	Import Configuration	SUCCESS
3	UOW	engineer	Run Autodiscovery	SUCCESS
4	UOW	engineer	Run Autodiscovery	SUCCESS
5	UOW	engineer	Run Autodiscovery	SUCCESS
6	UOW	engineer	Run Autodiscovery	SUCCESS
7	UOW	engineer	Run Autodiscovery	SUCCESS
8	UOW	engineer	Run Autodiscovery	SUCCESS
9	UOW	engineer	Run Autodiscovery	SUCCESS
10	UOW	engineer	Run Autodiscovery	SUCCESS
11	UOW	engineer	Run Autodiscovery	SUCCESS
12	UOW	engineer	Import Configuration	SUCCESS
13	UOW	engineer	Import Configuration	SUCCESS
14	UOW	engineer	Import Configuration	SUCCESS
15	UOW	engineer	Import Configuration	SUCCESS
16	UOW	engineer	Import Configuration	SUCCESS

Look at the work log for one of the units of work.

18. Click a unit of work to select it. Click the **Resources** tab.

UOW ID ▲	Type	Submitter	Request Type
1	UOW	administrator	Run Autodiscovery
2	UOW	administrator	Import Configuration
3	UOW	engineer	Run Autodiscovery
4	UOW	engineer	Run Autodiscovery
5	UOW	engineer	Run Autodiscovery
6	UOW	engineer	Run Autodiscovery
7	UOW	engineer	Run Autodiscovery
8	UOW	engineer	Run Autodiscovery
9	UOW	engineer	Run Autodiscovery
10	UOW	engineer	Run Autodiscovery
11	UOW	engineer	Run Autodiscovery
12	UOW	engineer	Import Configuration
13	UOW	engineer	Import Configuration

Page Size: 100 ▾ ⏪ ⏴ 1 / 1 ⏵ ⏩ ⏺

Summary Results **Resources** Approvals Schedule

19. Click the device in the **Resources** tab. The work log is shown on the right.

Name	Realm	Status	Failure	Server	Set ...
BRU-dca.gov	TNCM/...	Suc...	None	Wor...	

***** Operation Summary *****

Task Start Time: 2016/05/04 13:08:01.358 GMT+00:00

Task: Run Autodiscovery

Device: BRU-dca.gov

Description: Bulk Load

(1) Allocating 20MB of task memory (100% of the de...)

Leave the configuration manager user interface open. You use it again shortly.



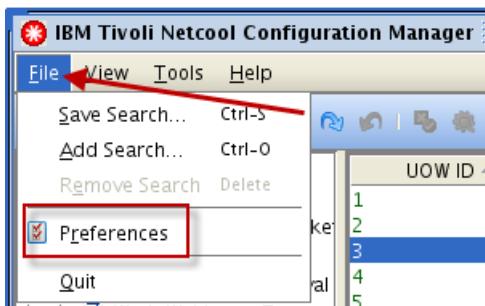
3 Single change configuration management exercises

In this unit, you discover devices and import their configuration files. You learn how to modify the device configurations.

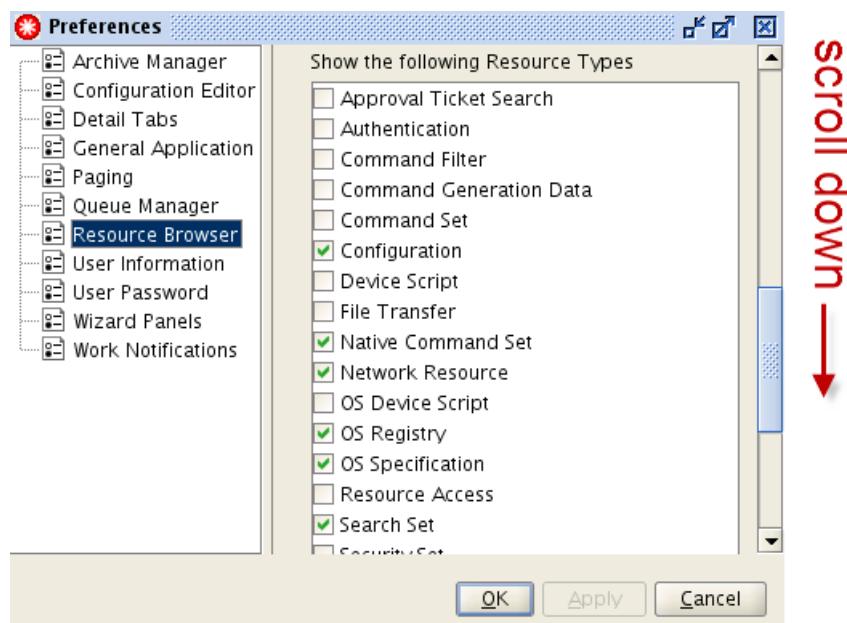
Exercise 1 Viewing an authentication resource

In this exercise, you view an authentication resource, which is a file that contains user names and passwords for the devices you interact with.

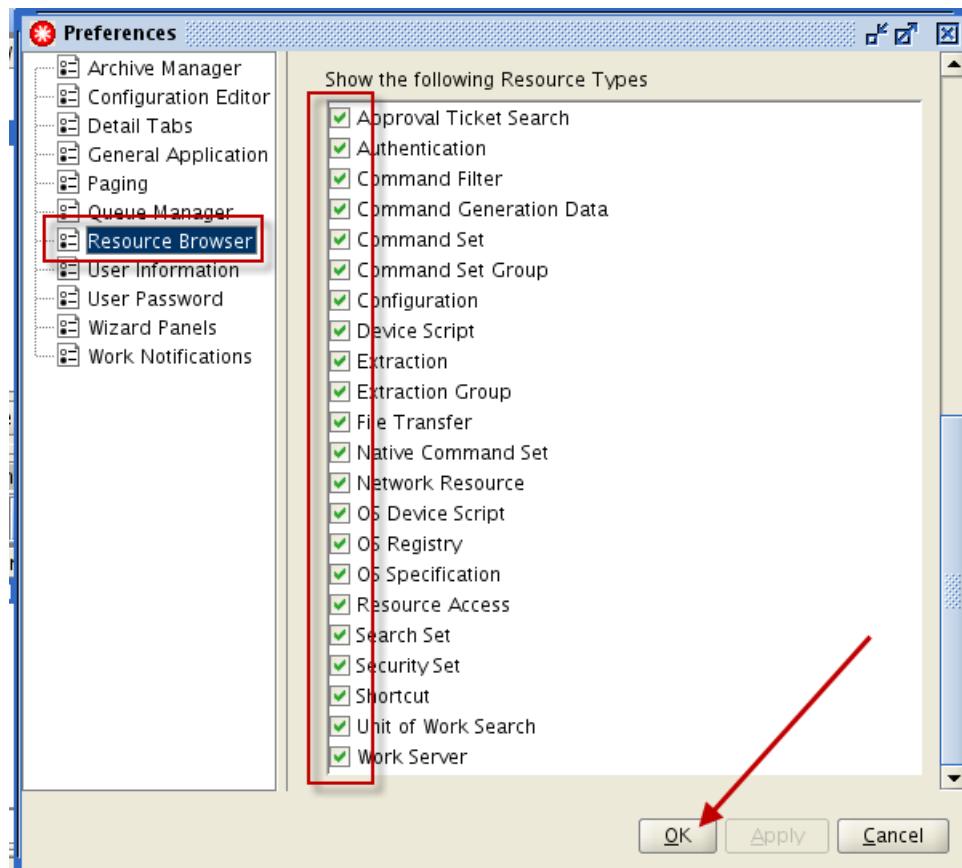
1. In the user interface, click **File > Preferences** to open your user preferences.



2. Find the *resource browser* preferences. Change your preferences to show all resource types.
 - a. Click **Resource Browser** at the left of the preferences window. Scroll down until you see the resources.



- b. Select every option in the **Show the following Resource Types** list. Click **OK**.





Note: These options might already be selected.

3. View the **ITNCM** realm in the *resource browser*. Open the resource named **Passwords**.

- a. Click the **ITNCM** realm in the *resource browser*.

Name	Realm	Modified By
CommandSets	ITNCM	administrator Fel
Content	ITNCM	Installer Fel
DataCenter	ITNCM	engineer Ma
edge-network	ITNCM	engineer Ma
NOI_AGG_P	ITNCM	administrator Fel
x-tools	ITNCM	engineer Ma
Cisco_36x_Device_Script	ITNCM	engineer Ma
DevicePasswords	ITNCM	engineer Ma
File Transfer	ITNCM	engineer Ma
WorkDistribution	ITNCM	administrator Fel

- b. Right-click the **DevicePasswords** object and click **Open**.

- Open**
- Edit...**
- Delete...**
- Rename...**
- Move...**
- Import**
- Synchronize**
- Re-discover**

You see password entries for CLI and SNMP access in the authentication resource.

Position	Username	Password	Enable Password	Retry Co...	Retry ...	Ignore
1	intelliden	p4ssw0rd	3n4bl3	1	0	False
2	ibm	object00	object00	0	0	False
3	user2	bar4	bar4	1	1000	True

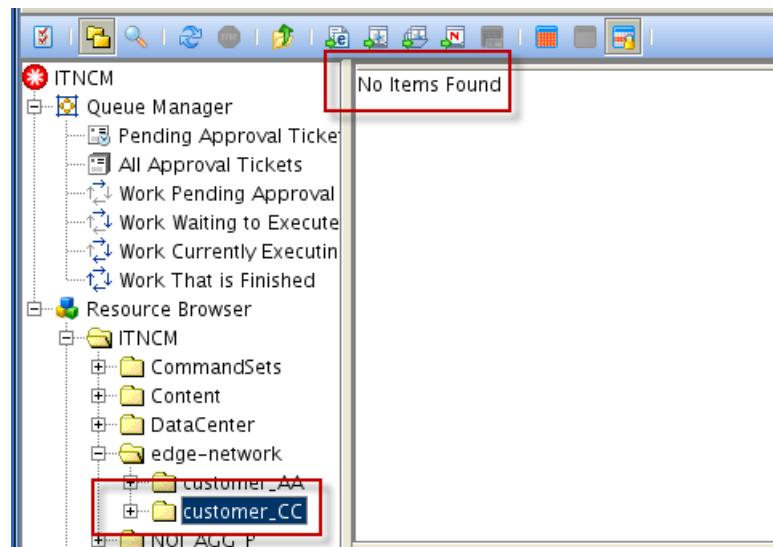
4. Close the password window.

Exercise 2 Discovering a device from the user interface

In this exercise, you discover a single device with the Network Resource Discovery wizard.

Verify the contents of the **customer_CC** realm.

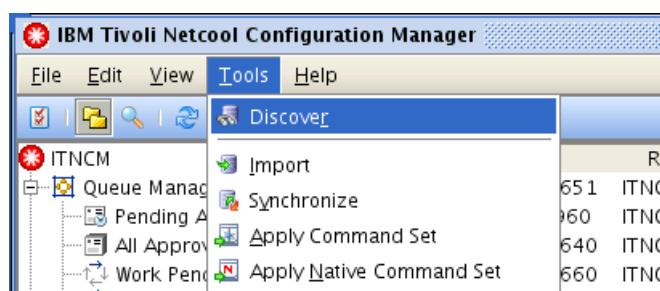
1. Click **ITNCM > edge-network > customer_CC** realm in the *resource browser*.



The realm is empty.

Start the Network Resource Discovery wizard.

2. Click the **customer_CC** realm to select it. Click **Tools > Discover**.

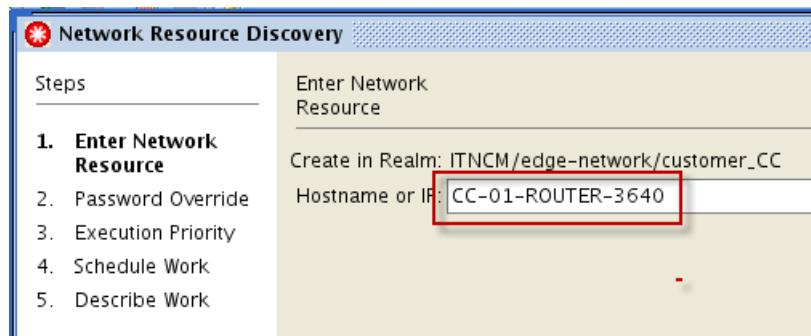


The Network Resource Discovery wizard starts.

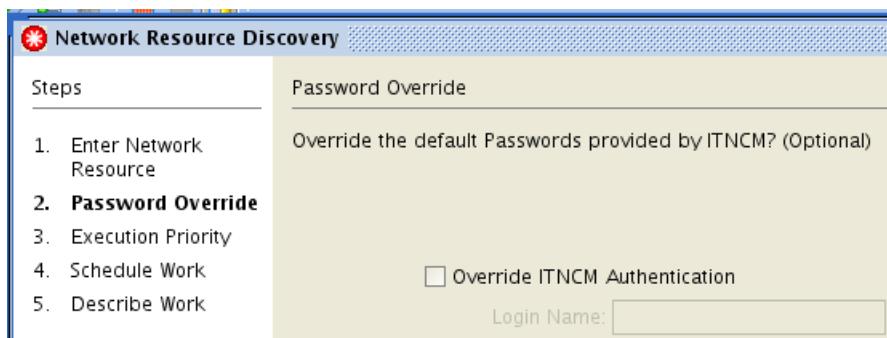
3. Use the values in this table to complete the Network Resource Discovery wizard.

Field	Value
Hostname or IP	CC-01-ROUTER-3640
Password Override	Do not override default passwords. The default passwords are in the authentication resource that is named Passwords that you viewed in the preceding exercise.
Execution Priority	Medium
Schedule Work	Immediate
Describe the Unit of Work	Discovering one device

- a. Enter **CC-01-ROUTER-3640** into the **Hostname or IP** field. Click **Next**.

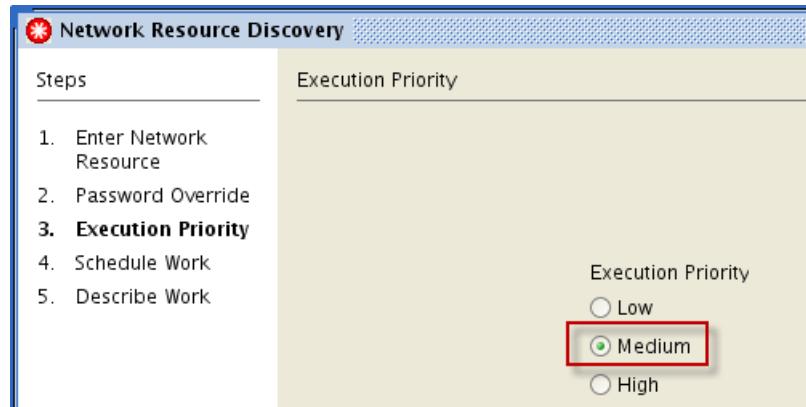


- b. Click **Next** to accept all of the default values on the Password Override window.

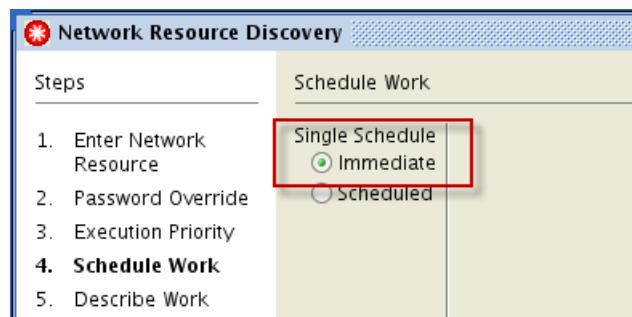


This action does not override default passwords. The default passwords are in the authentication resource that is named **DevicePasswords** that you viewed in the preceding exercise.

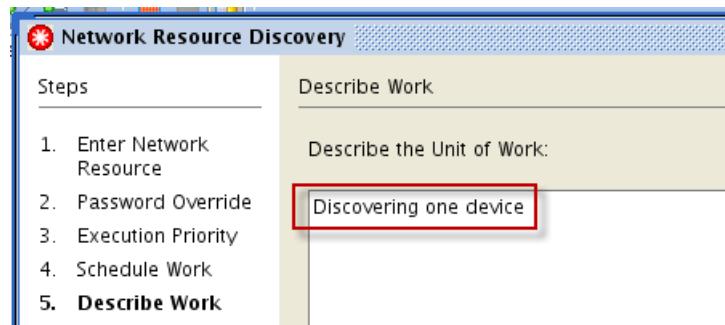
- c. Click **Next** to accept the default priority.



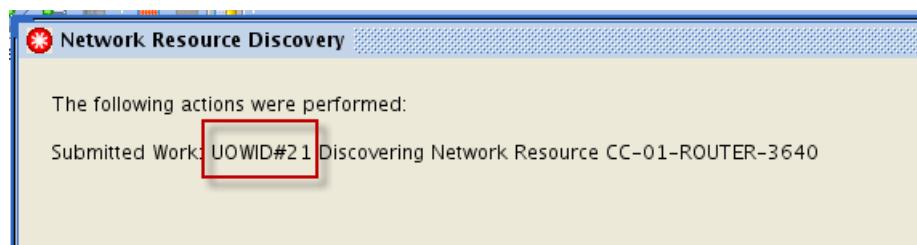
- d. Click **Next** to accept the default schedule.



- e. Enter **Discovering one device**. Click **Finish**.



- f. Note the unit of work number, and click **Close**.



The wizard submits a unit of work to discover the device.

4. Under the Queue Manager, click **Work That is Finished**.

UOW ID	Type	Submitter	Request Type
13	UOW	engineer	Import Configuration
14	UOW	engineer	Import Configuration
15	UOW	engineer	Import Configuration
16	UOW	engineer	Import Configuration
17	UOW	engineer	Import Configuration
18	UOW	engineer	Import Configuration
19	UOW	engineer	Import Configuration
20	UOW	engineer	Import Configuration
21	UOW	engineer	Run Autodiscovery
22	UOW	engineer	Import Configuration

The unit of work for the discovery completes and submits a unit of work to import the configuration.



Important: The *units of works* take a few minutes to complete. If the *units of work* do not appear, click the refresh icon.

Verify the contents of the **customer_CC** realm again.

5. Click **ITNCM > edge-network > customer_CC** realm in the *resource browser*.

Name	Realm	Modified By
CC-01-ROUTER-3640	ITNCM/...	engineer M

The new device, the router CC-01-ROUTER-3640, is in the **customer_CC** realm.

Exercise 3 Discovering multiple devices with the BulkLoader command

In this exercise, you use a command-line utility to discover multiple devices.

1. Enter the following command in the terminal window:

```
cd /home/netcool/bulkload
```

2. Examine the contents of the file named **customer-CC-bulkload-seed-file.csv**:

```
more customer-CC-bulkload-seed-file.csv
```

```
ITNCM/edge-network/customer_CC,CC-01-ROUTER-3640,*,*,*,*  
ITNCM/edge-network/customer_CC,CC-02-ROUTER-3640,*,*,*,*  
ITNCM/edge-network/customer_CC,CC-03-ROUTER-3640,*,*,*,*
```

Use the icosutil BulkLoader command to discover the three devices in the **customer-CC-bulkload-seed-file.csv** file. Use these parameters in the command.

Flag	Value
-l	engineer
-p	object00
-f	customer-CC-bulkload-seed-file.csv
-server	omnihost
-port	7001

3. Enter the following command to discover the three devices:



Note: Enter the text as one continuous line.

```
icosutil BulkLoader -l engineer -p object00 -f  
customer-CC-bulkload-seed-file.csv -server host1.csuite.edu -port 15310
```

```
[netcool@host1 bulkload]$ icosutil BulkLoader -l engineer -p object00 -f customer-CC-bulkload-seed-file.csv -server host1.csuite.edu -port 15310  
=====  
Re-importing: CC-01-ROUTER-3640/*/*/* - On line 1  
Discovering: CC-02-ROUTER-3640/*/*/* - On line 2  
Discovering: CC-03-ROUTER-3640/*/*/* - On line 3  
Imported: CC-01-ROUTER-3640/*/*/* : Result - SUCCESS  
AutoDiscovered: CC-02-ROUTER-3640/*/*/* : Result - SUCCESS  
AutoDiscovered: CC-03-ROUTER-3640/*/*/* : Result - SUCCESS  
[netcool@host1 bulkload]$
```

The command takes several minutes to complete.



Note: The script **icosutil** is in **/opt/IBM/ncm/bin**. This directory is added to the PATH variable for shell.

Verify the contents of the **customer_CC** realm again.

4. Click the *refresh* icon.

The screenshot shows the IBM Tivoli Netcool Configuration Manager (ITNCM) interface. On the left, there are two panes: 'Queue Manager' and 'Resource Browser'. The 'Queue Manager' pane lists several ticket categories. The 'Resource Browser' pane shows a tree structure under 'ITNCM' with nodes like 'CommandSets', 'Content', 'DataCenter', 'edge-network', and 'customer_CC'. The 'customer_CC' node is highlighted with a red box. On the right, a table displays three discovered devices:

Name	Realm	Modified By
CC-01-ROUTER-3640	ITNCM/edg...	engineer
CC-02-ROUTER-3640	ITNCM/edg...	engineer
CC-03-ROUTER-3640	ITNCM/edg...	engineer

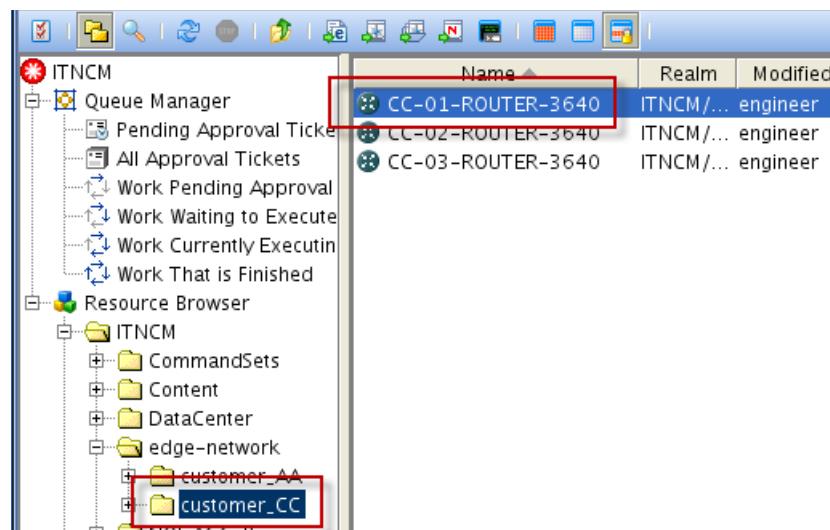
A red arrow points to the refresh icon in the top toolbar. A red box also highlights the 'customer_CC' node in the Resource Browser tree.

The new devices are in the **customer_CC** realm.

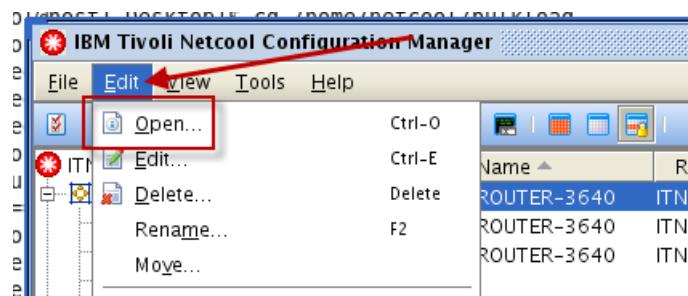
Exercise 4 Viewing a device configuration

In this exercise, you view the modeled and native configuration of a device.

1. Open the modeled configuration of the device named **CC-01-ROUTER-3640** in read-only mode.
 - a. Click the **customer_CC** realm in the *resource browser*. Click the device that is named **CC-01-ROUTER-3640** to select it.



- b. Click **Edit > Open** to open the modeled configuration.

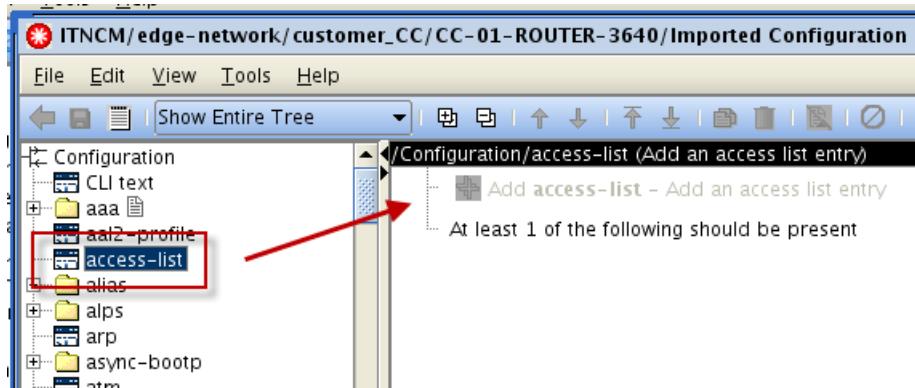


This action opens the modeled configuration in read-only mode. A list of configuration options for the operating system of this device is shown on the left of the window.

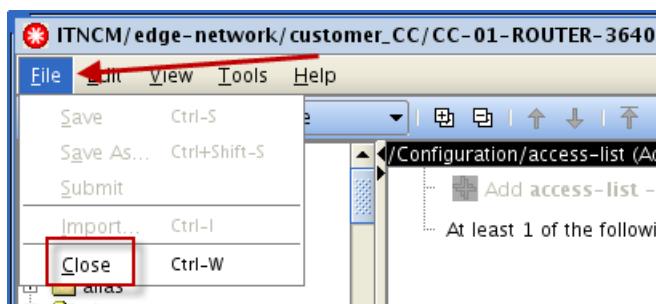
3 Single change configuration management exercises

Exercise 4. Viewing a device configuration

- Click a configuration option to view it on the right of the window.

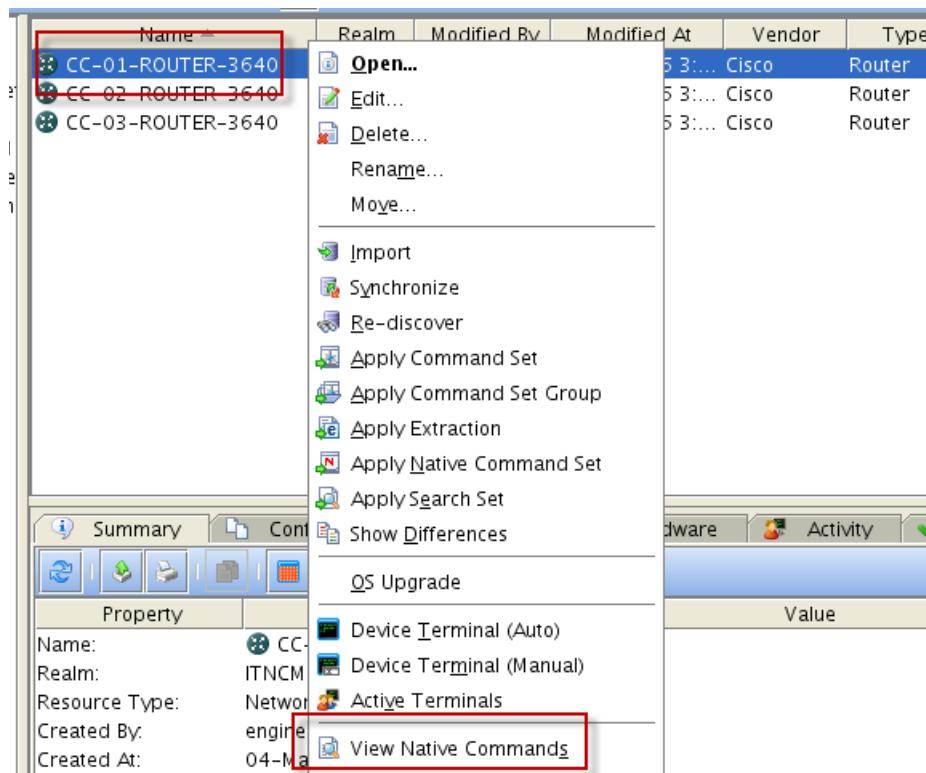


- Click **File** and select **Close** to close the configuration window.

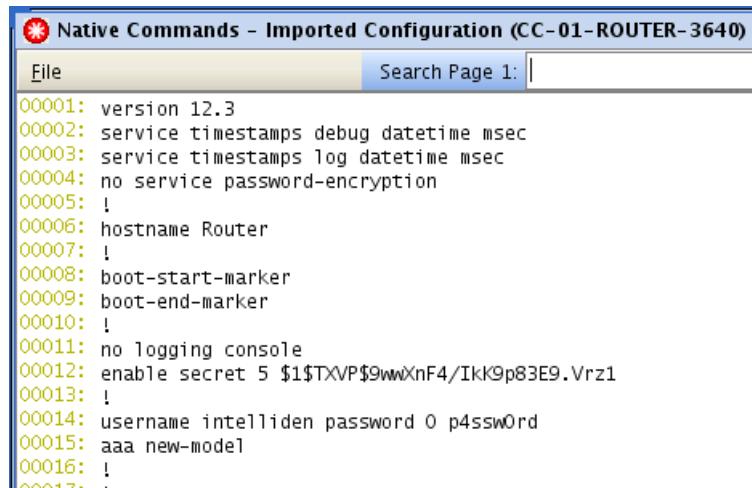


Open the same configuration in the Native Command view.

- Right-click the **CC-01-ROUTER-3640** device in the *resource browser* and click **View Native Commands**.



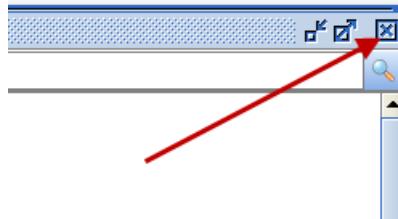
The configuration is shown as it would be in the operating system of the device.



Native Commands - Imported Configuration (CC-01-ROUTER-3640)

```
00001: version 12.3
00002: service timestamps debug datetime msec
00003: service timestamps log datetime msec
00004: no service password-encryption
00005: !
00006: hostname Router
00007: !
00008: boot-start-marker
00009: boot-end-marker
00010: !
00011: no logging console
00012: enable secret 5 $1$TXVP$9wwXnF4/Ikk9p83E9.Vrz1
00013: !
00014: username intelliden password 0 p4ssw0rd
00015: aaa new-model
00016: !
```

3. Click the X to close the window.

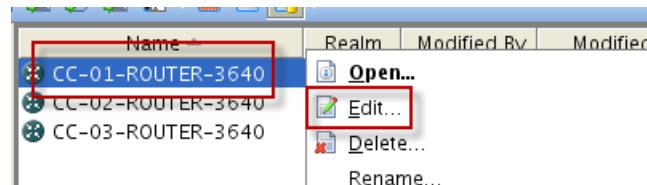


Exercise 5 Making a configuration change with the configuration editor

In this exercise, you use the *configuration editor* to change the configuration of a router. You view the commands that are run before you make the change.

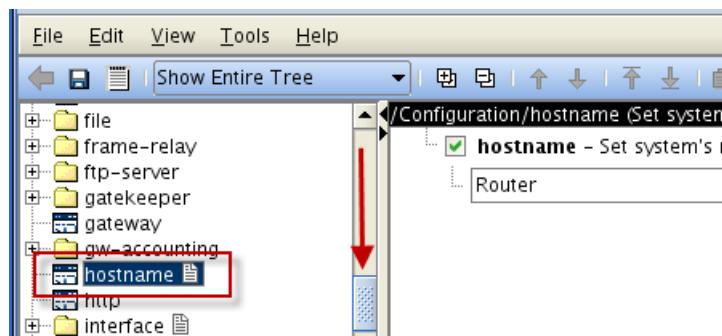
1. You make the following changes to the **CC-01-ROUTER-3640** device configuration to create a draft configuration. Use the *configuration editor*.
 - Change the device host name to reflect the resolvable name. Change the host name to **CC-01-ROUTER-3640**.
 - Add a login banner that shows the message **Unauthorized access is prohibited**.
 - Preview the changes with the Calculate Native Commands Changes tool.
 - Save the draft configuration with the name **hostname and banner**.

- Right-click the CC-01-ROUTER-3640 device and click **Edit**.

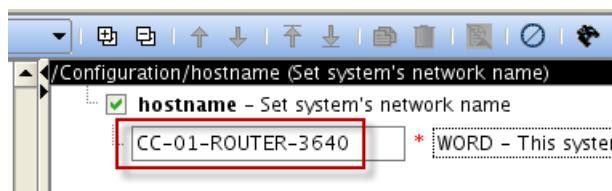


The *configuration editor* starts.

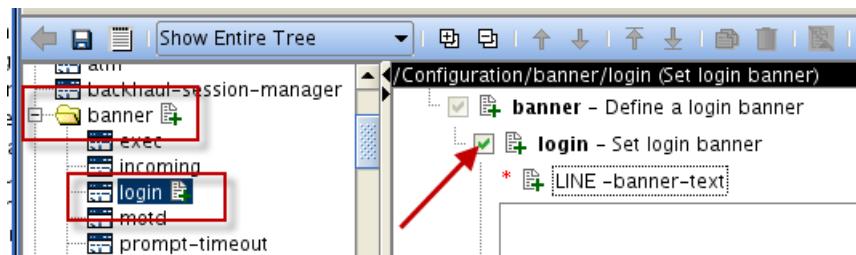
- Scroll down in the list and select **hostname** in the command tree on the left of the window.



- Replace **Router** with **CC-01-ROUTER-3640** in the **WORD** field.

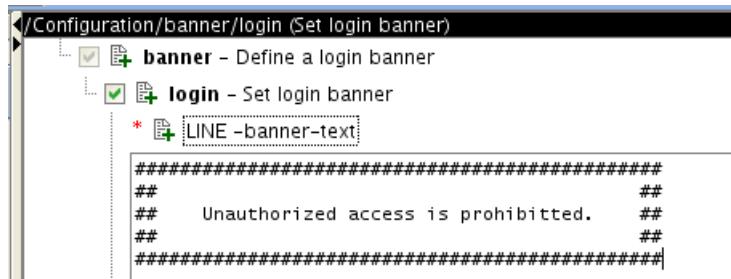


- Expand **banner** in the command tree on the left of the window and click **login**. Select **login** on the right of the window.

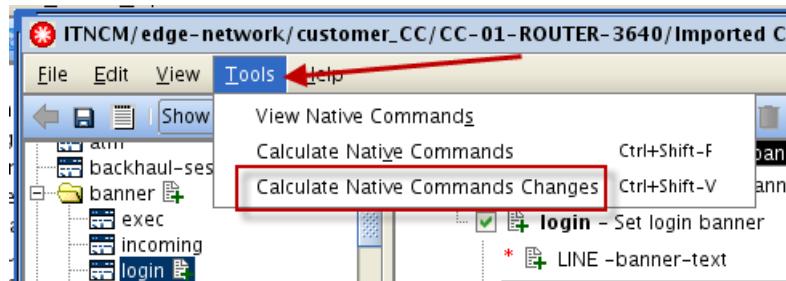


- Enter the following text in the **LINE** field as shown:

```
#####
##                                     ##
##      Unauthorized access is prohibited.  ##
##                                     ##
#####
```

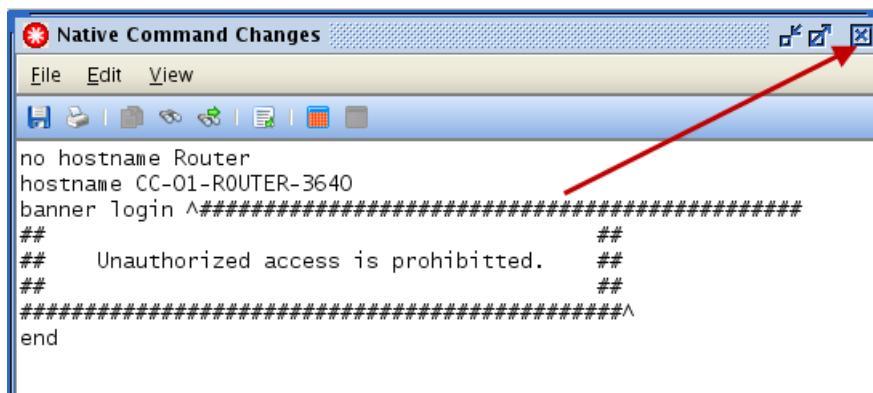


- f. Click Tools > Calculate Native Commands Changes.

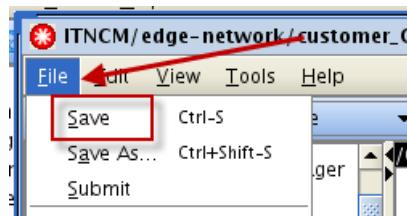


A preview is shown of the commands that are run.

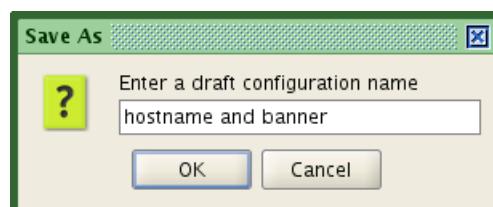
- g. Close the Calculate Native Command Changes window when you finish reviewing the change.



- h. Click File > Save.



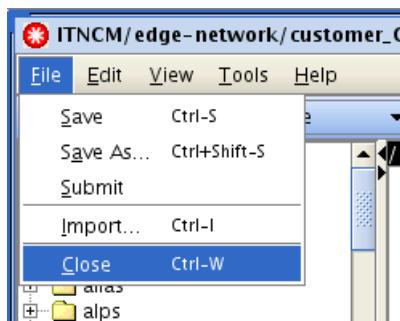
- i. Enter **hostname and banner** and click OK.



3 Single change configuration management exercises

Exercise 5. Making a configuration change with the configuration editor

- j. Close the configuration editor. Click File > Close.



2. Find the draft configuration that you created and submit it. Accept all default values in the wizard. Use **Change hostname** and **the login banner** for the unit of work description.
 - a. Click the device named **CC-01-ROUTER-3640**. Click the **Configurations** tab.

The screenshot shows the 'Configurations' tab selected in the top navigation bar. Below the tabs is a toolbar with various icons. The main area displays two tables. The top table lists devices: CC-01-ROUTER-3640, CC-02-ROUTER-3640, and CC-03-ROUTER-3640. The bottom table lists configurations: 'hostname ...' (Draft), 'Imported ...' (Versioned), and 'Imported ...' (Current). A red arrow points to the 'Configurations' tab, and a red box highlights the 'hostname ...' row in the bottom table.

The draft configuration that you created is shown.

- b. Click the draft configuration to select it. Click the **Submit** icon.

The screenshot shows the 'Configurations' tab selected. A red arrow points to the 'Submit' icon in the toolbar. The 'hostname ...' configuration row is highlighted with a red box. The table below shows three rows: 'hostname ...' (Draft), 'Imported ...' (Versioned), and 'Imported ...' (Current).

- c. Click **Next** at the Password Override window.

Submit Configuration Change

Steps	Password Override
1. Password Override 2. Config Change 3. Execution Priority 4. Rollback Options 5. Schedule Work 6. Describe Work	Override the default Passwords provided by ITNCM? (Optional) <input type="checkbox"/> Override ITNCM Authentication Login Name: <input type="text"/>

- d. Click **Next** at the Config Change window.

Submit Configuration Change

Steps	Config Change (Page 1 of 2)
1. Password Override 2. Config Change 3. Execution Priority 4. Rollback Options 5. Schedule Work 6. Describe Work	Configuration: hostname and banner (draft, May 4, 2016 3:45:04 PM) <input type="checkbox"/> Force Directory Override

- e. Select **Merge** to apply changes to the current configuration. Click **Next**.

Submit Configuration Change

Steps	Config Change (Page 2 of 2)
1. Password Override 2. Config Change 3. Execution Priority 4. Rollback Options 5. Schedule Work 6. Describe Work	<input checked="" type="radio"/> Merge This will add the configuration settings you have made to those currently on the Network Resource. Any settings currently on the Network Resource will remain intact. <input type="radio"/> Replace

- f. Click **Next** at the Execution Priority window.

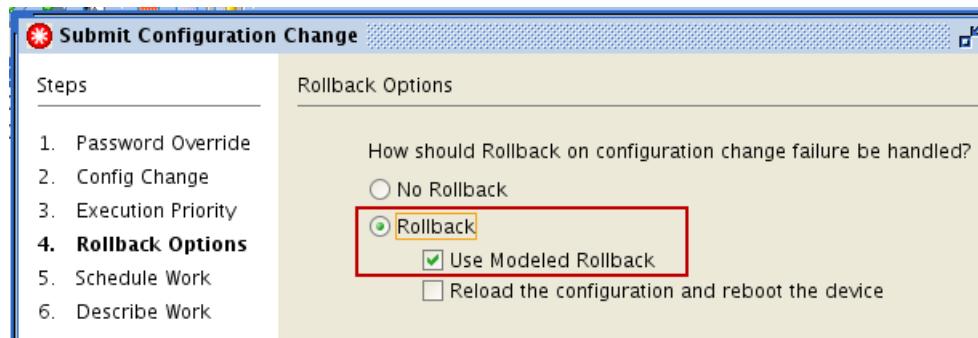
Submit Configuration Change

Steps	Execution Priority
1. Password Override 2. Config Change 3. Execution Priority 4. Rollback Options 5. Schedule Work 6. Describe Work	Execution Priority <input type="radio"/> Low <input checked="" type="radio"/> Medium <input type="radio"/> High

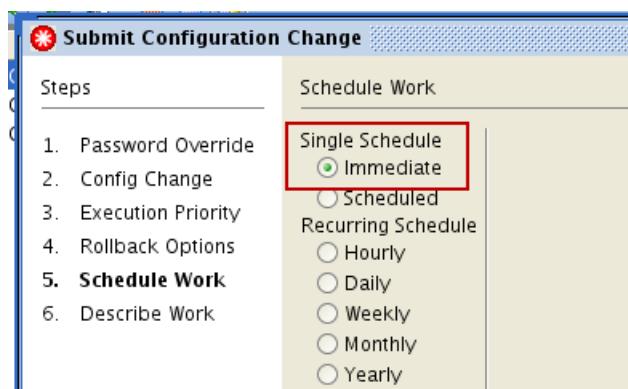
3 Single change configuration management exercises

Exercise 5. Making a configuration change with the configuration editor

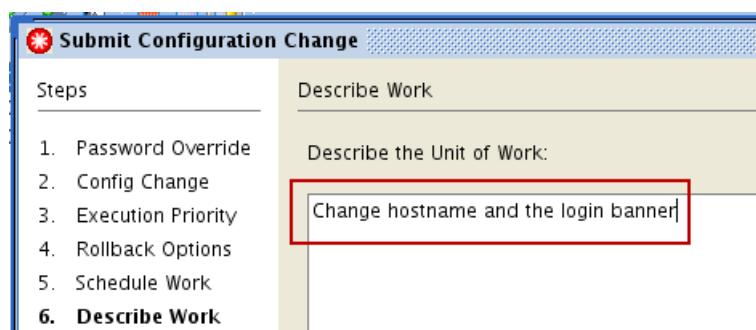
- g. Ensure that it attempts a modeled rollback if a failure occurs. Click **Rollback** and **Use Modeled Rollback**. Click **Next**.



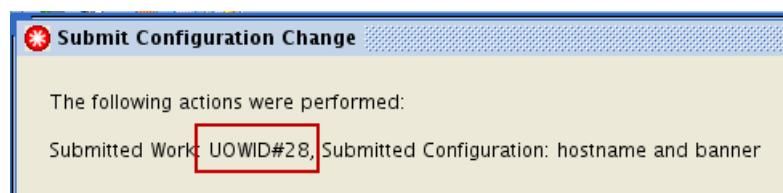
- h. Click **Next** at the Schedule Work window.



- i. Enter **Change hostname and the login banner** in the Describe Work window. Click **Finish**.



- j. Note the unit of work number and click **Close**.

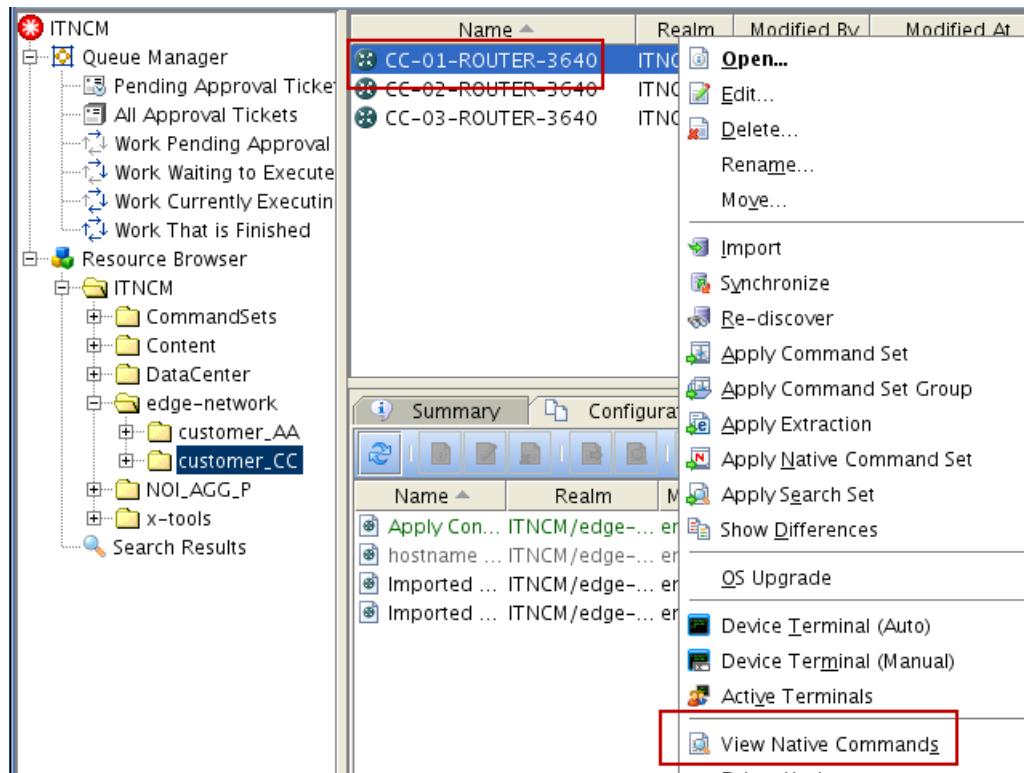


3. After the unit of work completes, open the current configuration to verify the changes.



Note: It takes a short time for the unit of work to complete.

- a. Right-click the CC-01-ROUTER-3640 device and click View Native Commands.



- b. Scroll down in the configuration to view the new host name and login banner.

```

00004: no service password-encryption
00005: !
00006: hostname CC-01-ROUTER-3640
00007: !
00008: boot-start-marker

00048: snmp-server enable traps tty
00049: banner login ^C#####
00050: ##      ##
00051: ##      Unauthorized access is prohibited.      ##
00052: ##      ##
00053: #####^C
00054: !

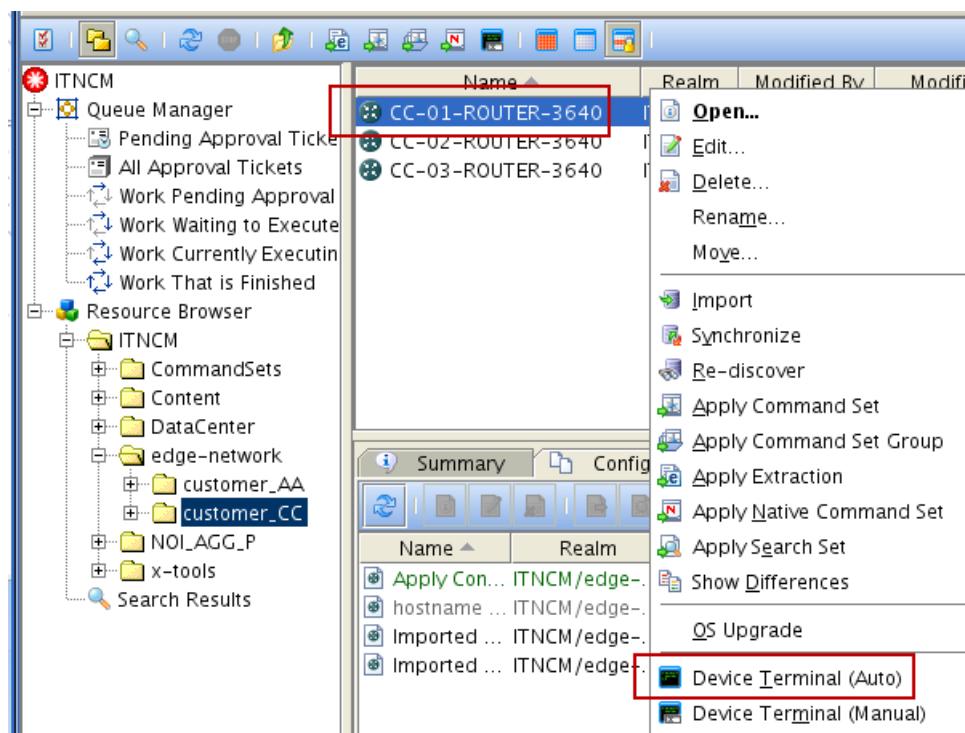
```

- c. Close the native commands window.

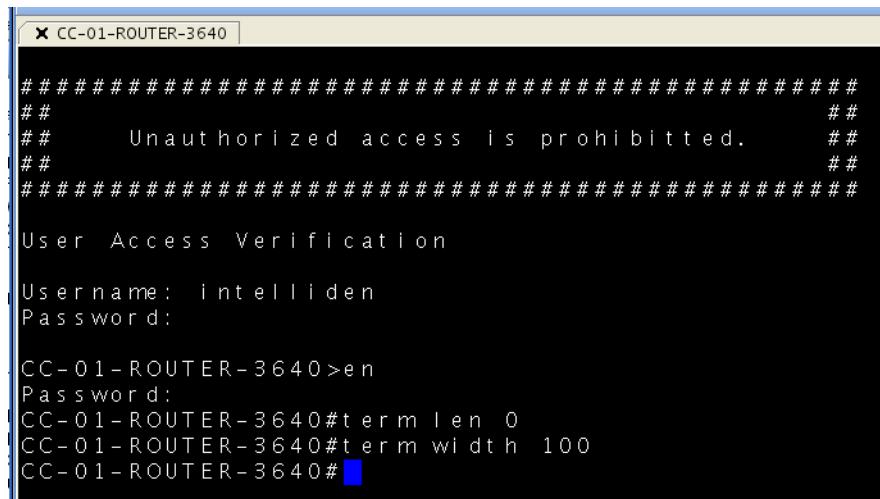
Exercise 6 Connecting to a device with the device terminal

In this exercise, you view the configuration of a device by using the device terminal.

1. Connect to the **CC-01-ROUTER-3640** router with the automatic device terminal. Verify that the login banner is shown and the new host name is present.
 - a. Right-click the device that is named **CC-01-ROUTER-3640** and select **Device Terminal (Auto)**.



A window opens and you are automatically logged in to the device. Notice that the host name is CC-01-ROUTER-3640 and the new banner message.

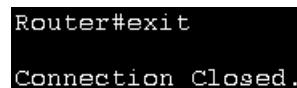


The terminal window title is "CC-01-ROUTER-3640". It displays a banner message:

Unauthorized access is prohibited. #

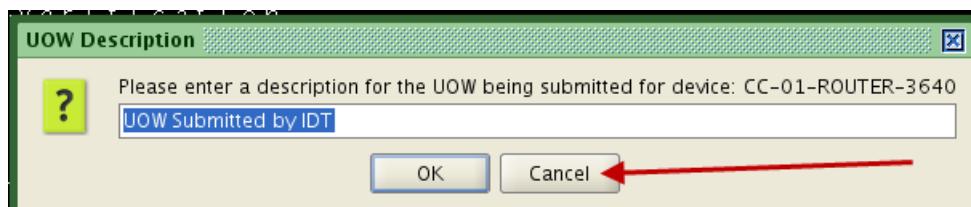
User Access Verification
Username: intelliden
Password:
CC-01-ROUTER-3640>en
Password:
CC-01-ROUTER-3640#term len 0
CC-01-ROUTER-3640#term width 100
CC-01-ROUTER-3640#

b. Enter the command **exit**.

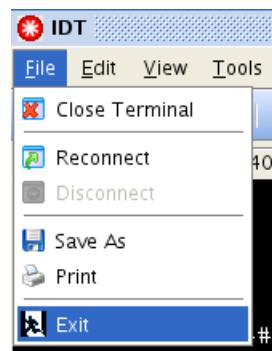


Router#exit
Connection Closed.

c. Click **Cancel**.



d. Click **File > Exit**.



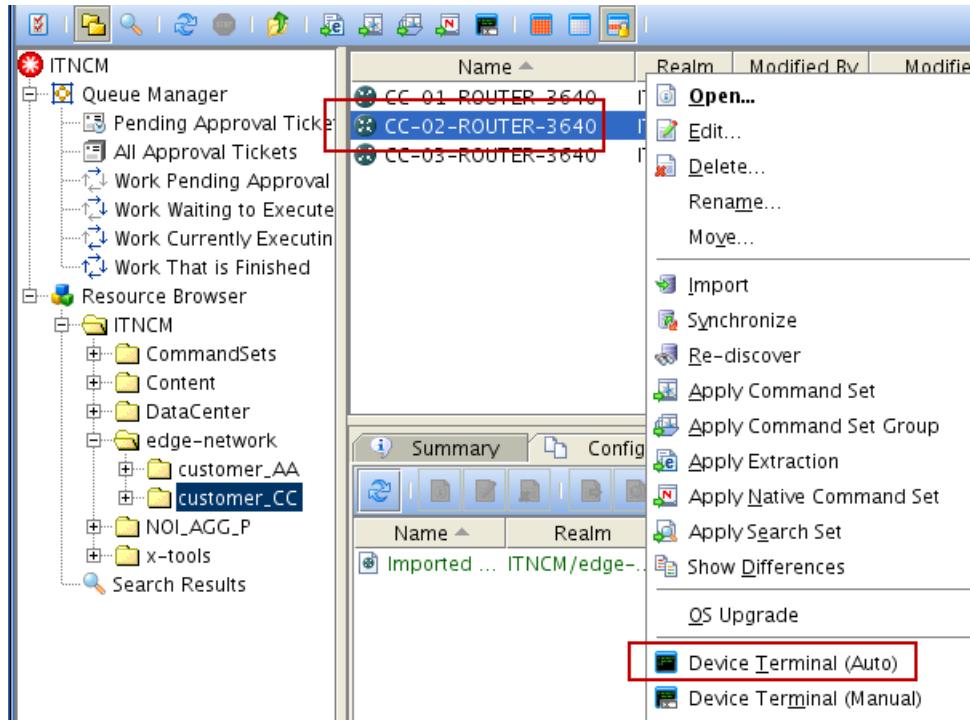
e. Click **OK** to quit.



Exercise 7 Changing a device configuration by using the device terminal

In this exercise, you change the login banner and the host name of a device with the device terminal.

1. Right-click the device that is named **CC-02-ROUTER-3640** and select **Device Terminal (Auto)**.



The device terminal opens and connects to the router.

```

CC-02-ROUTER-3640

User Access Verification

Username: intelidden
Password:

ROUTER-02>en
Password:
ROUTER-02#terminal 0
ROUTER-02#terminal width 100
ROUTER-02#

```

2. Enter the following commands to change the device host name to **CC-02-ROUTER-3640**.

```
config t  
hostname CC-02-ROUTER-3640
```

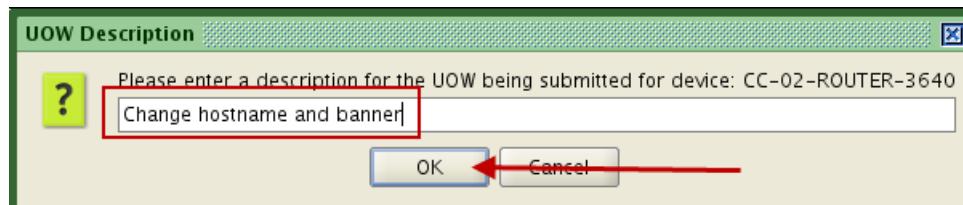
```
ROUTER-02#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
ROUTER-02(config)#hostname CC-02-ROUTER-3640  
CC-02-ROUTER-3640(config)#[
```

3. Enter the following two commands to add a login banner. Make the banner show the message **!!!Unauthorized access is prohibited!!!**.

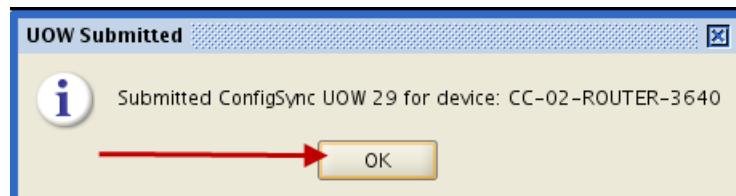
```
banner login ^!!!Unauthorized access is prohibited!!!^  
exit
```

```
CC-02-ROUTER-3640(config)#banner ^!!!Unauthorized access is prohibited!!!^  
CC-02-ROUTER-3640(config)#exit  
CC-02-ROUTER-3640#[
```

4. Type **exit** to leave the terminal session.
5. Enter **Change hostname and banner** and click **OK**.

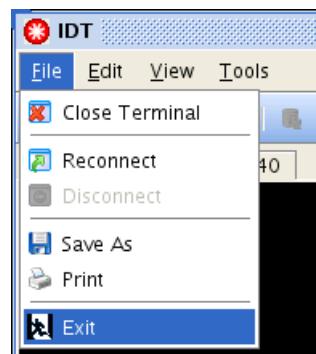


6. Click **OK** to confirm that the unit of work is submitted.



After you type **exit**, it prompts you to enter a description for the changes. The device terminal creates a unit of work to synchronize the device configuration.

7. Click **File > Exit** to close the device terminal.



8. Click **OK** to quit.



Exercise 8 Verifying that the configuration change was synchronized

In this exercise, you verify that the change you made with the device terminal updated the configuration in Netcool Configuration Manager.

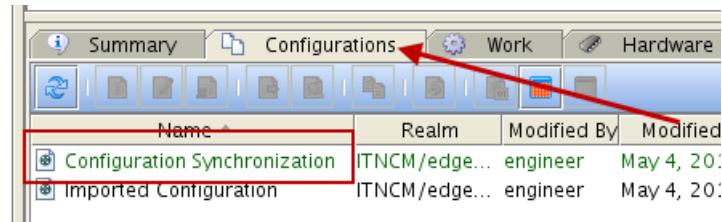
1. Find the **CC-02-ROUTER-3640** device in the *resource browser* and view the list of configurations. Verify that the most recent configuration is now a synchronized configuration.

 - a. Click the device named **CC-02-ROUTER-3640**.

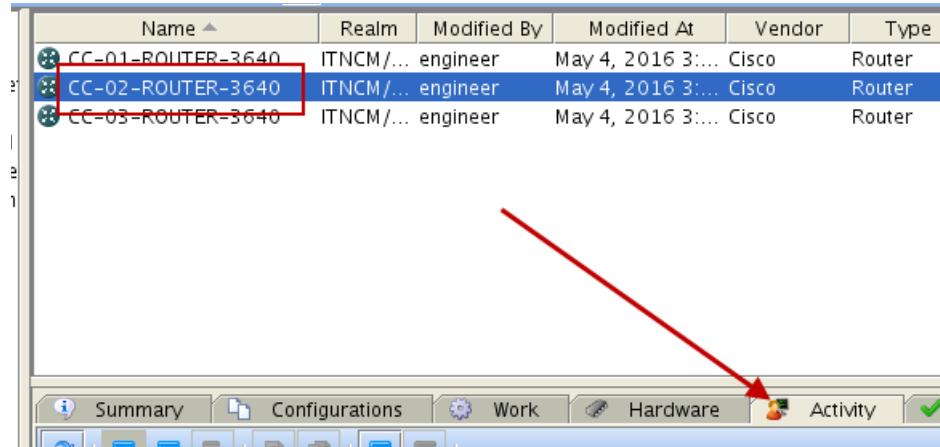
Name	Realm	Modified By	Modified At	Vendor	Type
CC-01-ROUTER-3640	ITNCM/...	engineer	May 4, 2016 3:...	Cisco	Router
CC-02-ROUTER-3640	ITNCM/...	engineer	May 4, 2016 3:...	Cisco	Router
CC-03-ROUTER-3640	ITNCM/...	engineer	May 4, 2016 3:...	Cisco	Router

Name	Realm	Modified By	Modified At	Vendor	Type	Model	OS
Configurat...	ITNCM/edge...	engineer	May 4, 2016 ...	Cisco	Router	3640	C3640-I-M-
Imported ...	ITNCM/edge...	engineer	May 4, 2016 ...	Cisco	Router	3640	C3640-I-M-

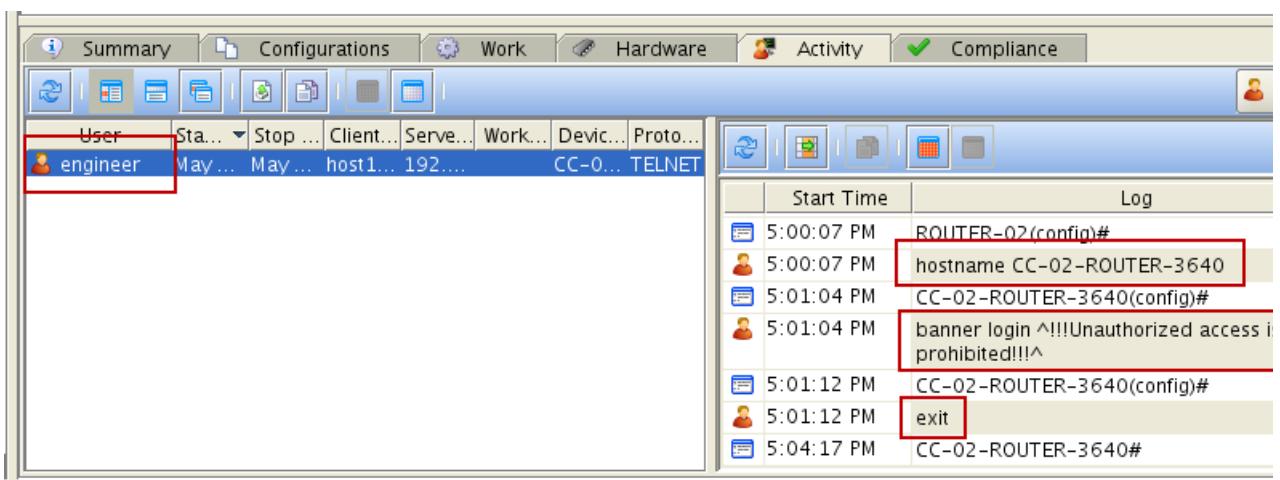
- b. Click the **Configurations** tab and verify that the most recent configuration is now a synchronized configuration.



2. Look at the recent activity on the **CC-02-ROUTER-3640** device. Find the commands that you sent to the device in the activity log.
- a. Click the **CC-02-ROUTER-3640** device and click the **Activity** tab.



- b. Click the device terminal session that you started in the preceding exercise. The commands that you entered are listed in the log column.



3 Single change configuration management exercises

Exercise 8. Verifying that the configuration change was synchronized

3. Look in the *queue manager* for the unit of work that is submitted for the change made to **CC-02-ROUTER-3640** through the device terminal. Find the commands that you sent to the device in the work log.
 - a. Click **Queue Manager**. Find the recent unit of work that synchronized the configuration from the **CC-02-ROUTER-3640** device to Netcool Configuration Manager.

The screenshot shows the Queue Manager interface. On the left, there's a tree view with nodes like 'ITNCM', 'Queue Manager' (which is expanded), 'Pending Approval Tickets', 'All Approval Tickets', 'Work Pending Approval', 'Work Waiting to Execute', 'Work Currently Executing' (which is highlighted with a red box), and 'Work That is Finished' (which is also highlighted with a red box). On the right, there's a table titled 'UOW ID' with columns: UOW ID, Type, Submitter, and Request Type. The table lists several entries, with the last one (UOW ID 29) highlighted with a red box. The 'Request Type' column for entry 29 shows 'Configuration Synchronization (Device to ITNCM)'.

UOW ID	Type	Submitter	Request Type
17	UOW	engineer	Import Configuration
18	UOW	engineer	Import Configuration
19	UOW	engineer	Import Configuration
20	UOW	engineer	Import Configuration
21	UOW	engineer	Run Autodiscovery
22	UOW	engineer	Import Configuration
23	UOW	engineer	Import Configuration
24	UOW	engineer	Run Autodiscovery
25	UOW	engineer	Run Autodiscovery
26	UOW	engineer	Import Configuration
27	UOW	engineer	Import Configuration
28	UOW	engineer	Configuration Change
29	UOW	engineer	Configuration Synchronization (Device to ITNCM)

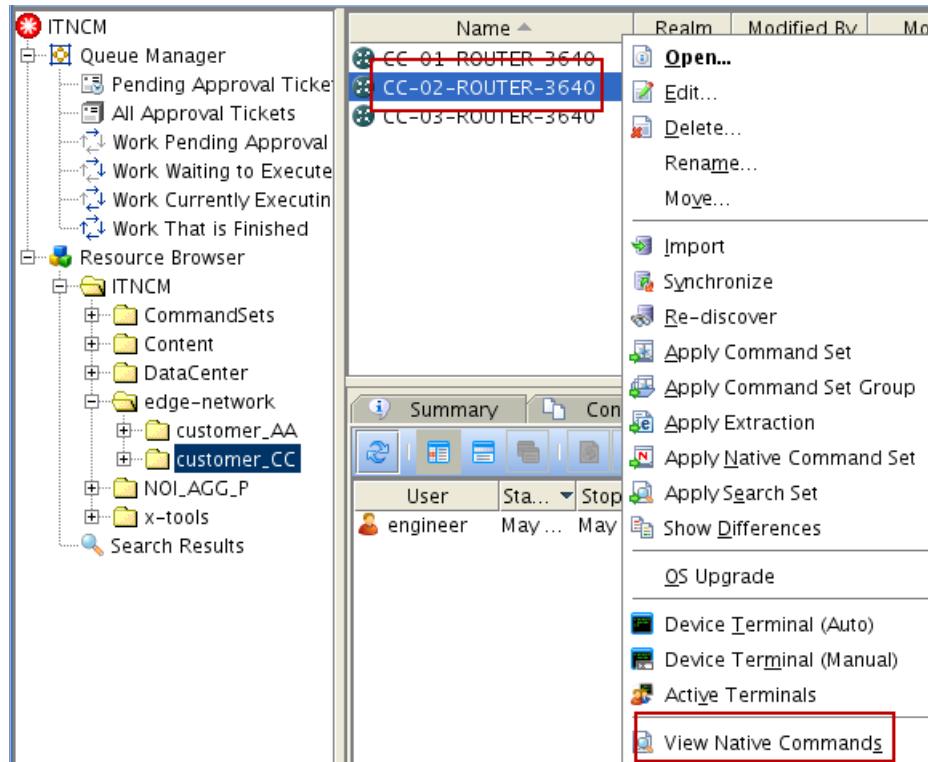
- b. Click the **Resources** tab in the unit of work. Click the **CC-02-ROUTER-3640** device. Scroll down in the work log to find the configuration changes.

The screenshot shows the Resources tab for the CC-02-ROUTER-3640 device. The 'Name' column is highlighted with a red box. The work log on the right side shows several log entries. Log entry (53) shows new values for the device. Log entry (54) shows the path to configuration. Log entry (55) shows old values. Log entry (56) shows new values including a banner/login message. Log entry (57) indicates the operation finished. Log entry (58) shows the operation started on the worker server. Log entry (59) marks the imported configuration as current.

Name	Realm	Status	Failure	Se...	Se...
CC-02-ROUTER-3640	ITNCM...	P	Su...	None	W...

```
(53) New values: CC-02-ROUTER-3640
(54) Path: configuration
(55) Old values:
(56) New values: banner/login/!!!Unauthorized access prohibited!!!
(57) <<< Operation Finished in 0 seconds (diffConfig)
2016/05/04 17:06:58.546 GMT+00:00
(58) >>> Operation Started on Worker Server 'Worker'
(storeConfig): 2016/05/04 17:06:58.547 GMT+00:00
(59) Imported configuration marked as current for d...
```

4. View the native commands for the current configuration of the **CC-02-ROUTER-3640** device.
Verify that the changes are in the configuration.
 - a. Click **customer_CC**. Right-click the device that is named **CC-02-ROUTER-3640** and click **View Native Commands**.



- b. Scroll down in the configuration to view the new host name and login banner.

```
00001: version 12.4
00002: service timestamps debug datetime msec
00003: service timestamps log datetime msec
00004: service password-encryption
00005:
00006: hostname CC-02-ROUTER-3640
00007:
00093:
00094: banner login ^C!!!Unauthorized access is prohibited!!!^C
00095:
00096: line con 0
```

5. Close the native commands window.
6. Leave the configuration manager user interface open. You use it again shortly.



4 Mass change configuration management exercises

In the exercises for this unit, you view and apply command sets to lab devices.

Exercise 1 Finding the version, type, model, and operating system for target devices

In this exercise, you find the vendor, type, model, and operating system (VTMOS) of the lab devices.

1. Click the **customer_CC** realm.

The screenshot shows the IBM Tivoli Netcool Configuration Manager interface. On the left, there is a navigation tree with nodes like 'ITNCM', 'Queue Manager' (expanded to show 'Pending Approval Tickets', 'All Approval Tickets', 'Work Pending Approval', 'Work Waiting to Execute', 'Work Currently Executing', and 'Work That is Finished'), 'Resource Browser' (expanded to show 'ITNCM' which contains 'CommandSets', 'Content', 'DataCenter', 'edge-network', and 'customer_AA' which contains 'customer_CC'), and 'NOI_UGG_P'. On the right, there is a table titled 'Name' with three rows: 'CC-01-ROUTER-3640', 'CC-02-ROUTER-3640', and 'CC-03-ROUTER-3640'. Below the table are tabs for 'Summary' and 'Configurations', and buttons for 'User', 'Start', 'Stop', and 'Client'. A red box highlights the 'customer_CC' folder under 'customer_AA' in the Resource Browser.

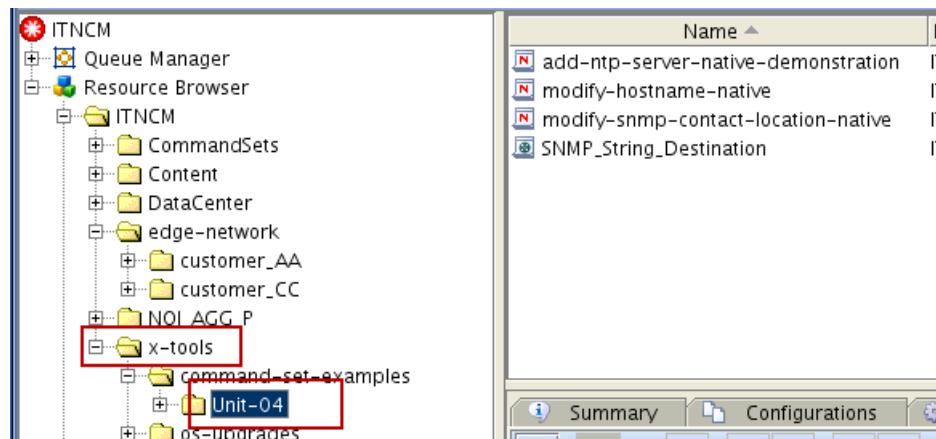
2. Resize the width of the columns in the resource table to show the **Vendor**, **Type**, **Model**, and **OS** columns. Note the values for each device.

Name	Realm	Modifi...	Modified At	Vendor	Type	Model	OS
CC-01-ROUTER-3640	ITNC...	engi...	May 4, 20...	Cisco	Router	3640	C3640-I-M-12.3(5b)
CC-02-ROUTER-3640	ITNC...	engi...	May 4, 20...	Cisco	Router	3640	C3640-I-M-12.4(25c)
CC-03-ROUTER-3640	ITNC...	engi...	May 4, 20...	Cisco	Router	3640	C3640-IK9S-M-12.4(25c)

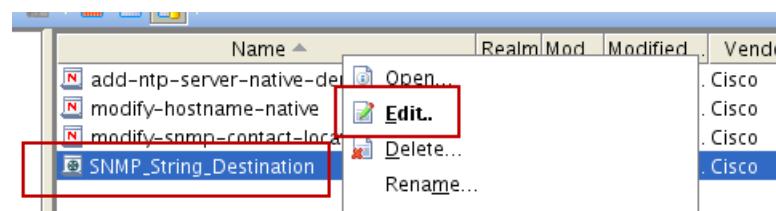
Exercise 2 Viewing a modeled command set

In this exercise, you view a simple modeled command set with a parameter.

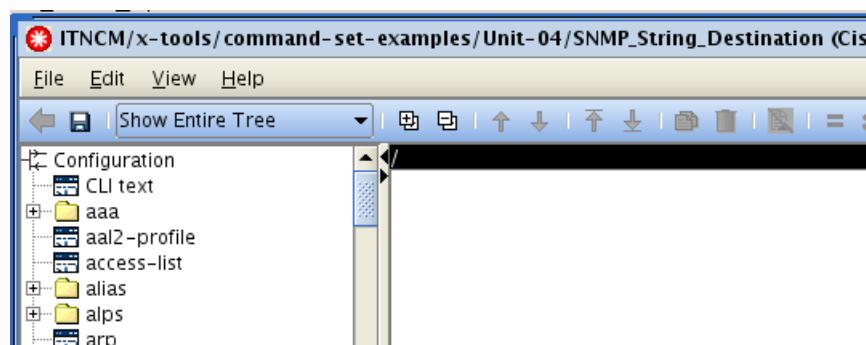
1. In the **ITNCM > x-tools > command-set-examples > Unit-04**, select and edit the **SNMP_String_Destination** command set.
 - a. Browse to the **ITNCM > x-tools > command-set-examples > Unit-04** realm.



- b. Right-click the **SNMP_String_Destination** command set and select **Edit**.



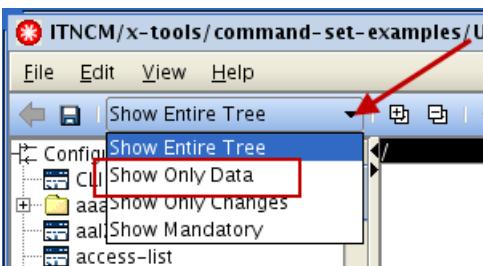
The command set editor window opens.



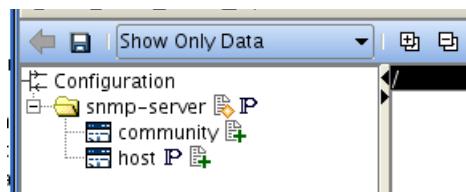
4 Mass change configuration management exercises

Exercise 2 Viewing a modeled command set

2. Filter the view to **Show Only Data** and view the snmp-server folder.
 - a. Click the arrow and select the **Show Only Data** filter.

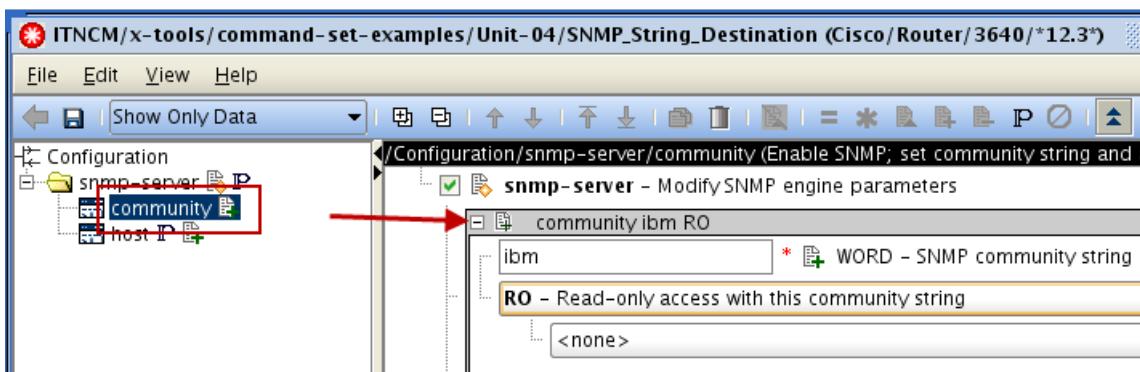


- b. Expand the **snmp-server** folder and notice the two commands.



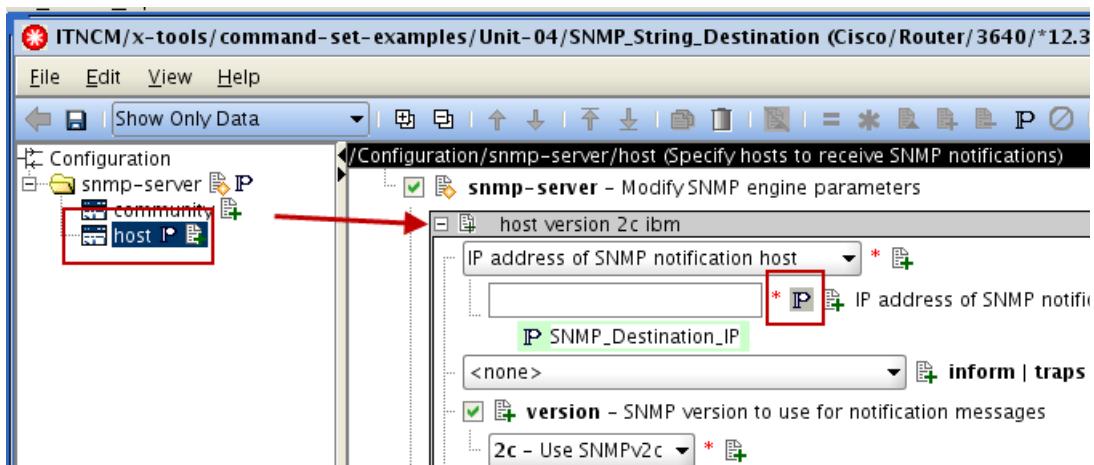
This command set adds a community string and a host.

- c. Select the **community** node and then open the rollout.



Notice that the community string name is **ibm**.

- d. Select the **host** node and click the **P** icon next to the **IP address of the SNMP notification host**.



The parameter name is **SNMP_Destination_IP**.

- e. Close the command set editor window.

Exercise 3 Applying a modeled command set in report only mode

In this exercise, you apply the **SNMP_String_Destination** command set to multiple devices in report only mode. This command tests the changes in the command set without committing any commands to the actual devices.

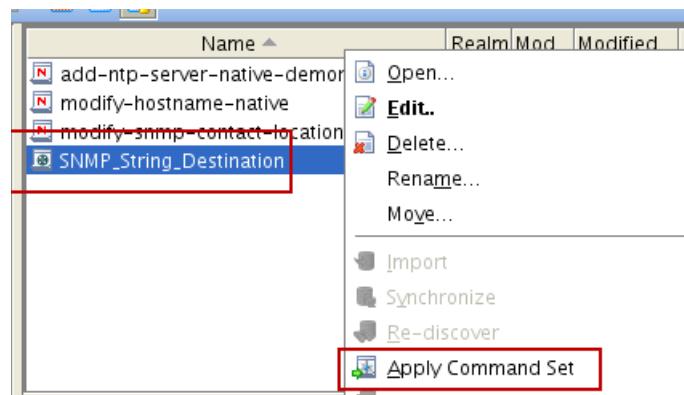
Use the following values to complete the wizard.

Field	Value
Select Command Sets	Leave SNMP_String_Destination as the selected command set
Scope of Application	Network resources in a realm
Select the Realm	customer_CC
Execution Mode	Report only mode
Enter Parameters page 1	local
Enter Parameters page 2	Use 10.191.101.50 as the name of the destination IP address
Password Override	Do not override
Execution Priority	Medium
Schedule Work	Single Schedule > Immediate
Describe Work	Modeled command set applied in report only mode

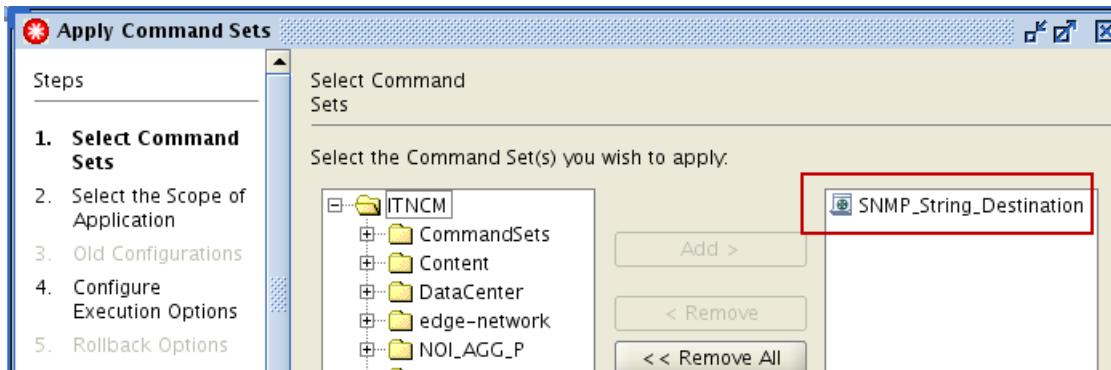
4 Mass change configuration management exercises

Exercise 3 Applying a modeled command set in report only mode

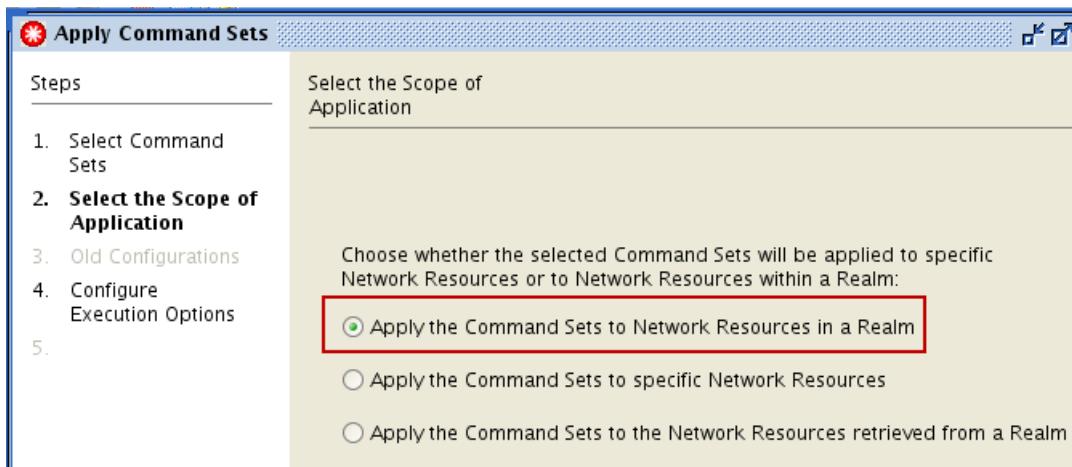
1. Right-click the **SNMP_String_Destination** command set and click **Apply Command Set**. The Apply Command Sets wizard starts.



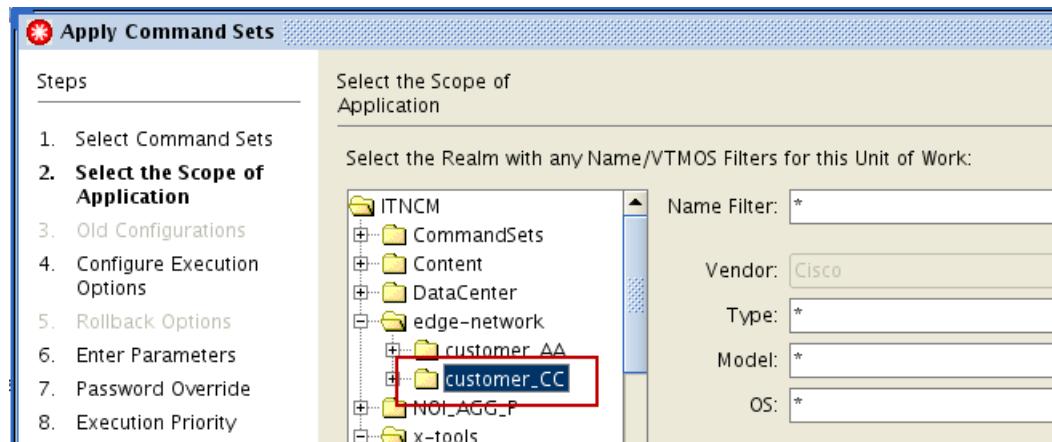
2. Click **Next** in the Select Command Sets window.



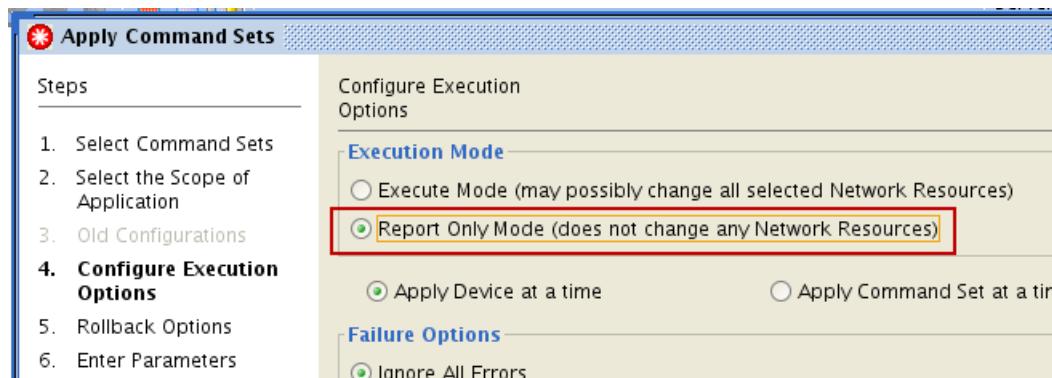
3. Click **Next** in the Select the Scope of Application window.



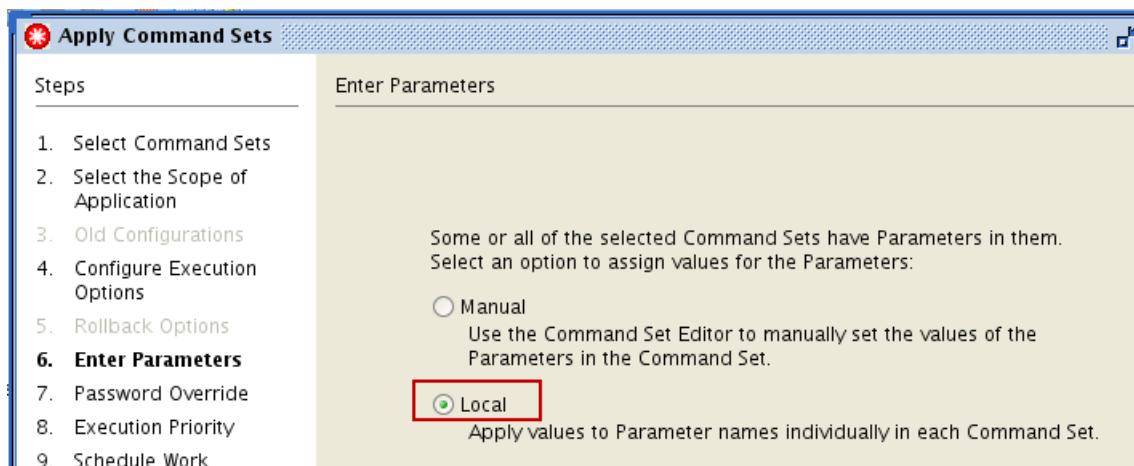
4. Click **edge-network > customer_CC** in the Select the Realm field. Click **Next**.



5. Click **Report Only Mode** in the Configure Execution Options window. Click **Next**.



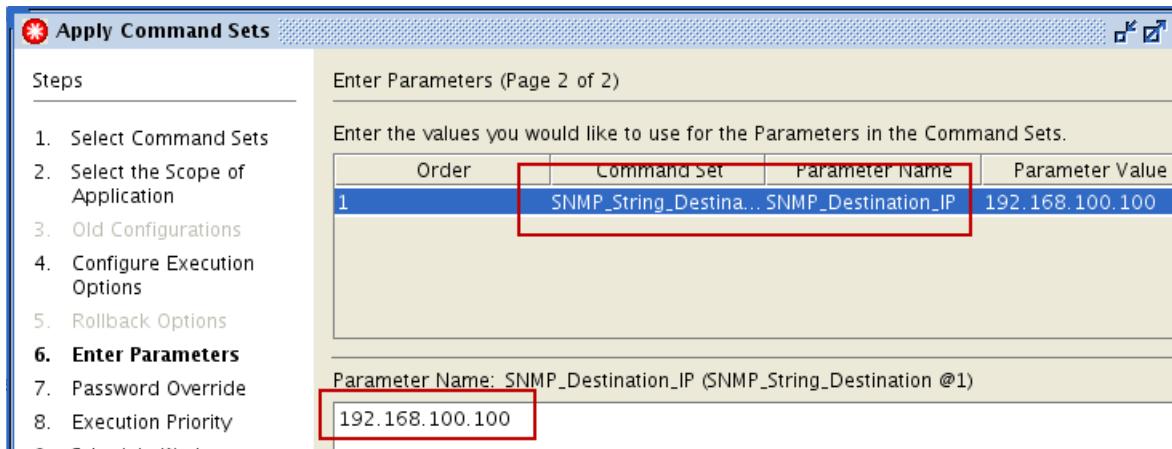
- a. Click **Local** in the Enter Parameters window. Click **Next**.



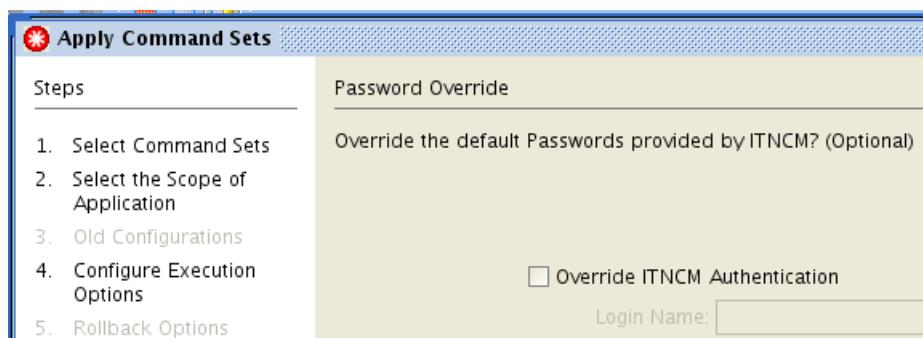
4 Mass change configuration management exercises

Exercise 3 Applying a modeled command set in report only mode

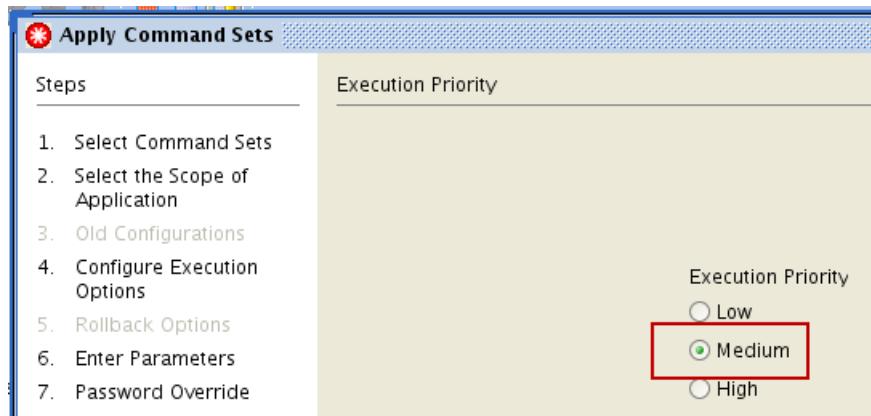
- b. Click the **SNMP_Destination_IP** parameter in the Enter Parameters (Page 2 of 2) window. Enter **192.168.100.100** in the **Parameter Name** field. Click **Next**.



- c. Click **Next** in the Password Override window.



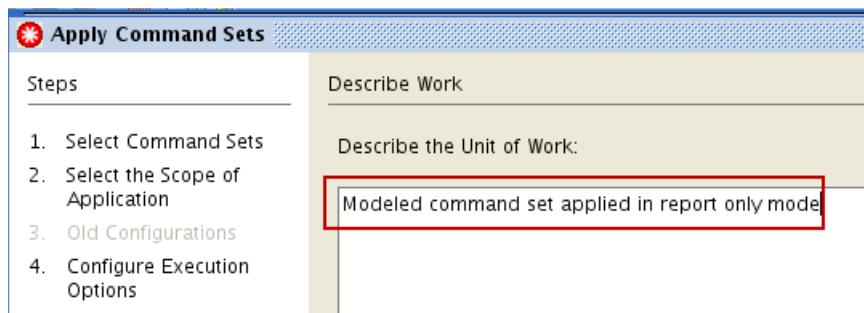
- d. Click **Next** in the Execution Priority window.



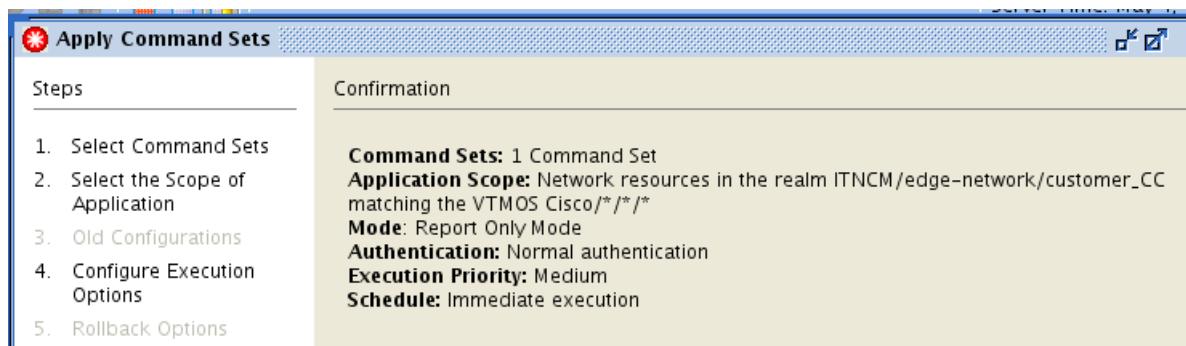
- e. Click **Next** in the Schedule Work window.



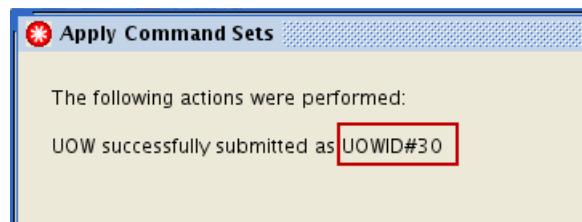
- f. Enter **Modeled command set applied in report only mode** in the Describe Work window. Click **Next**.



- g. Click **Finish** in the Confirmation window.



- h. Note the *unit of work number* and click **Close**.



Use the work log for the unit of work to verify the result of the command set for each device in the **customer_CC** realm. If the command set is applied in execute mode, the work log shows the configurations changes that are made to each device.

4 Mass change configuration management exercises

Exercise 3 Applying a modeled command set in report only mode

6. Find the unit of work in the *queue manager* that applied the command set in report only mode.
Click the unit of work.

The screenshot shows the left navigation pane with 'ITNCM' selected, expanded to show 'Queue Manager' and 'Resource Browser'. Under 'Queue Manager', 'Work That is Finished' is highlighted with a red box. The right pane displays a table of 'UOW ID' (18 to 30), 'Type' (UOW), 'Submitter' (engineer), and 'Request Type'. Row 30 is highlighted with a red box and has a tooltip: 'Configuration Synchronization Device t Command Set (Report Only)'.

UOW ID	Type	Submitter	Request Type
18	UOW	engineer	Import Configuration
19	UOW	engineer	Import Configuration
20	UOW	engineer	Import Configuration
21	UOW	engineer	Run Autodiscovery
22	UOW	engineer	Import Configuration
23	UOW	engineer	Import Configuration
24	UOW	engineer	Run Autodiscovery
25	UOW	engineer	Run Autodiscovery
26	UOW	engineer	Import Configuration
27	UOW	engineer	Import Configuration
28	UOW	engineer	Configuration Change
29	UOW	engineer	Configuration Synchronization
30	UOW	engineer	Command Set (Report Only)

7. Click the **Resources** tab in the unit of work. Click each device and scroll down in the work log to find the result of the command set.

The screenshot shows the 'Resources' tab selected in the top navigation bar. A red arrow points to the 'Resources' tab. The main area lists three devices: 'CC-02-ROUTER-3640', 'CC-01-ROUTER-3640', and 'CC-03-ROUTER-3640'. The log window below shows the command execution process:

```
(20) converting to native  
(21) Command Set applied to config  
(22) Command Set WOULD have resulted in the following changes :  
Non Interactive Commands:  
1 - snmp-server community ibm R0  
2 - snmp-server host 192.168.100.100 version  
2c ibm  
3 - end  
(23) <<< Operation Finished in 0 seconds
```

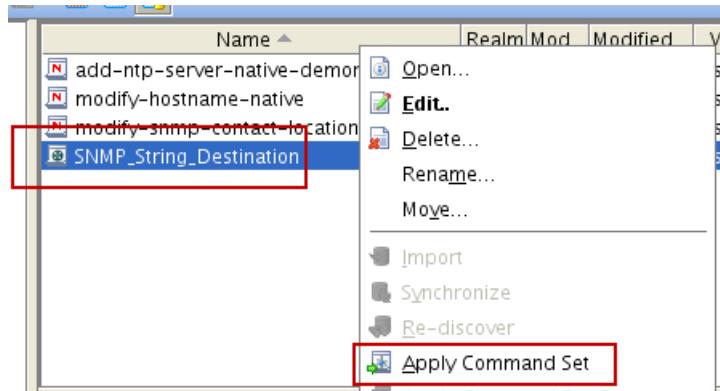
Exercise 4 Applying a modeled command set

In this exercise, you apply a command set to multiple devices.

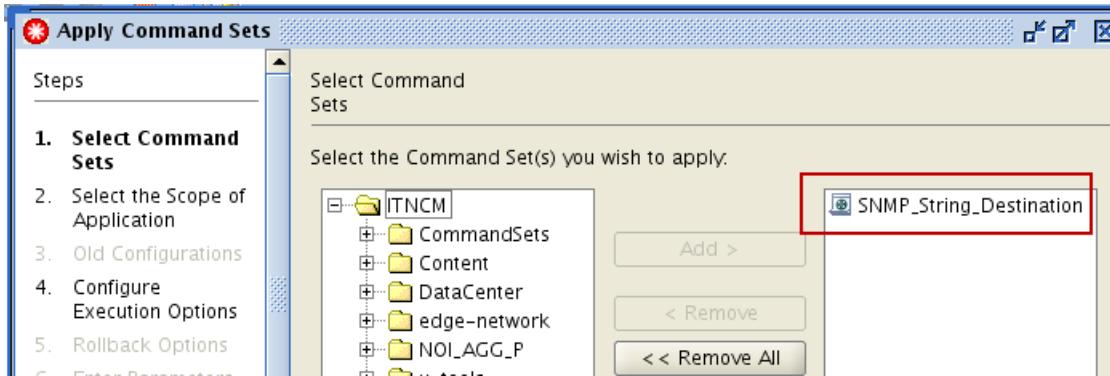
Use the following values to complete the wizard.

Field	Value
Select Command Sets	Leave SNMP_String_Destination as the selected command set
Scope of Application	Network resources in a realm
Select the Realm	customer_CC
Execution Mode	Execute mode
Rollback	Use modeled rollback
Enter Parameters page 1	local
Enter Parameters page 2	Use 10.191.101.50 as the name of the destination host
Password Override	Do not override
Execution Priority	Medium
Schedule Work	Single Schedule > Immediate
Describe Work	Applying SNMP string and trap destination

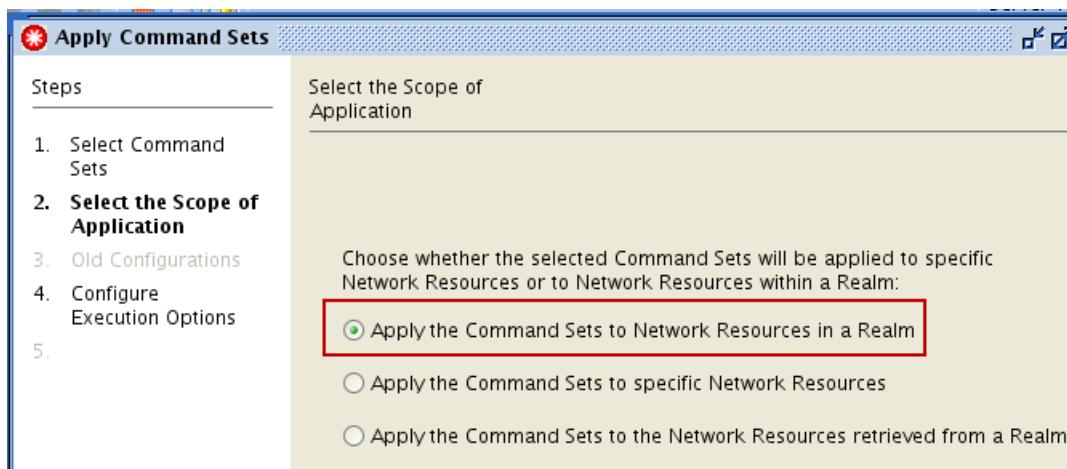
1. Right-click the **SNMP_String_Destination** command set and click **Apply Command Set**. The Apply Command Sets wizard starts.



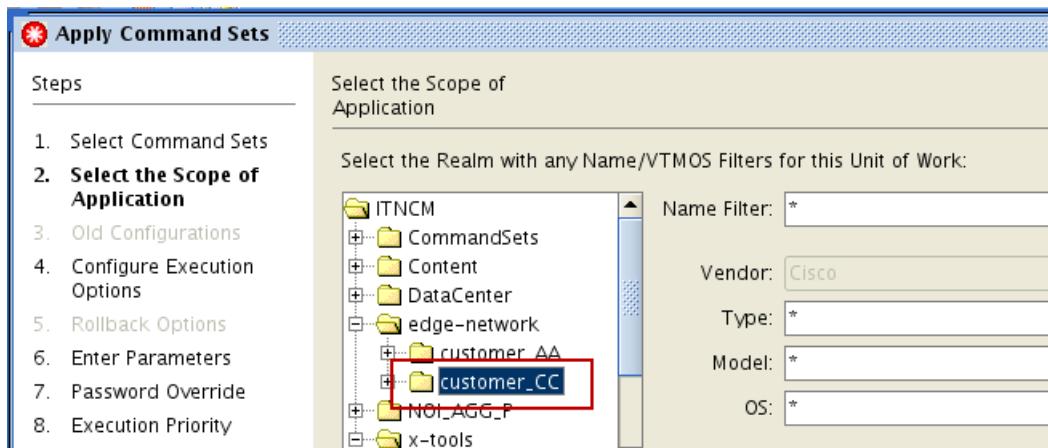
2. Click **Next** in the Select Command Sets window.



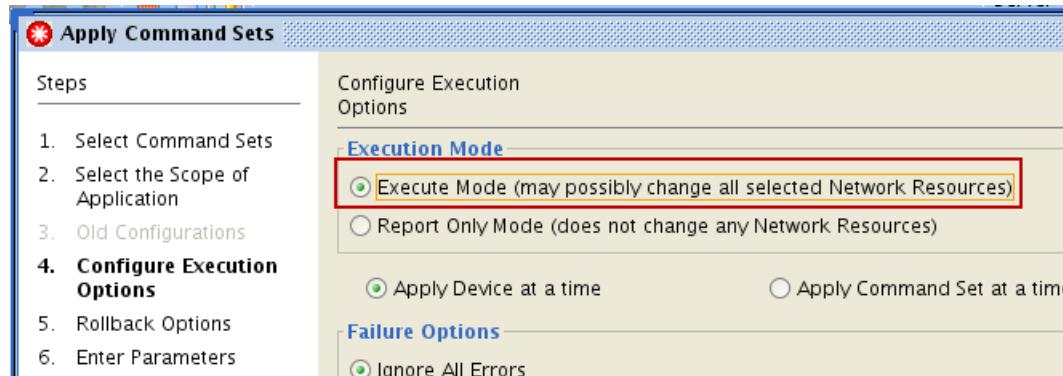
3. Click **Next** in the Select the Scope of Application window.



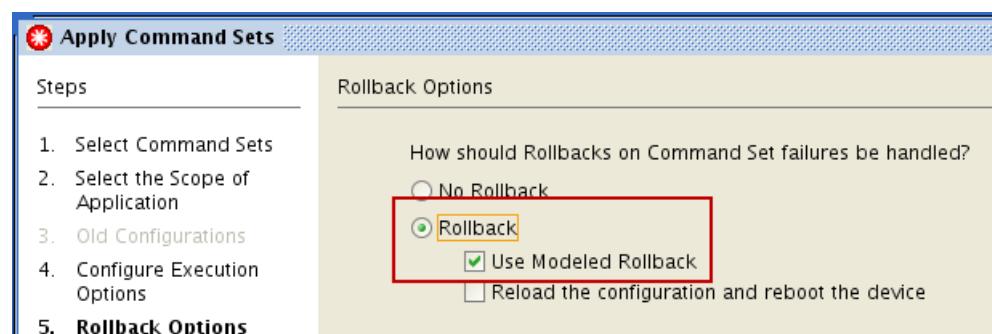
4. Click **edge-network > customer_CC** in the Select the Realm field. Click **Next**.



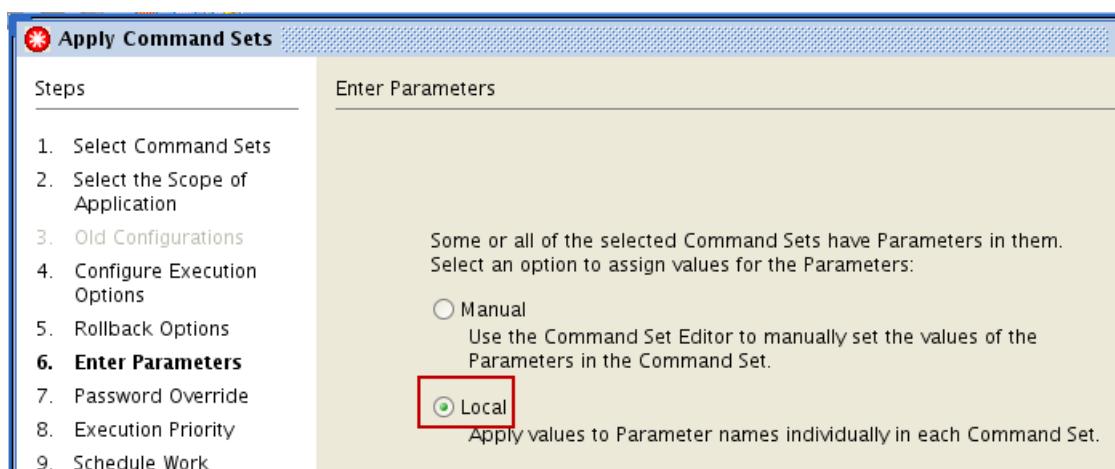
5. Click **Execute Mode** in the Configure Execution Options window. Click **Next**.



6. Click **Rollback** in the Rollback Options. Click **Next**.



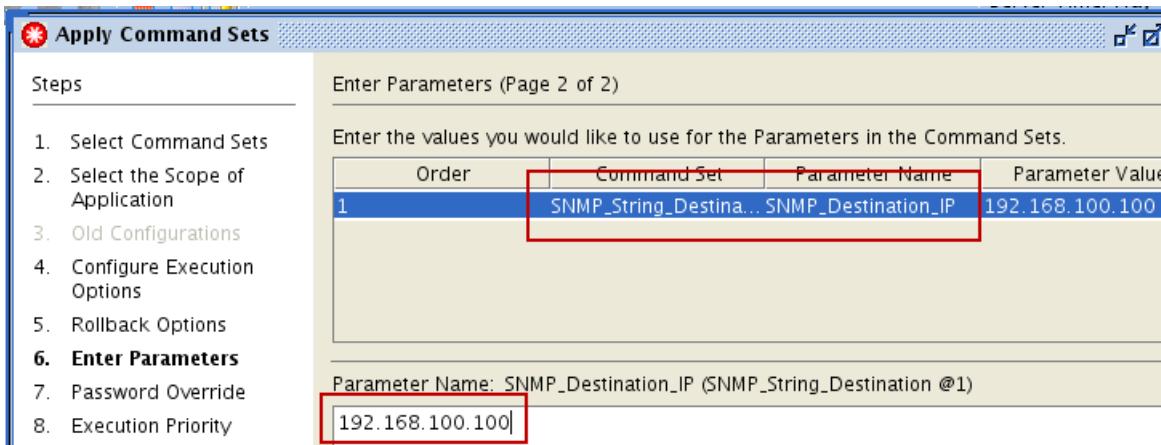
7. Click **Local** in the Enter Parameters window. Click **Next**.



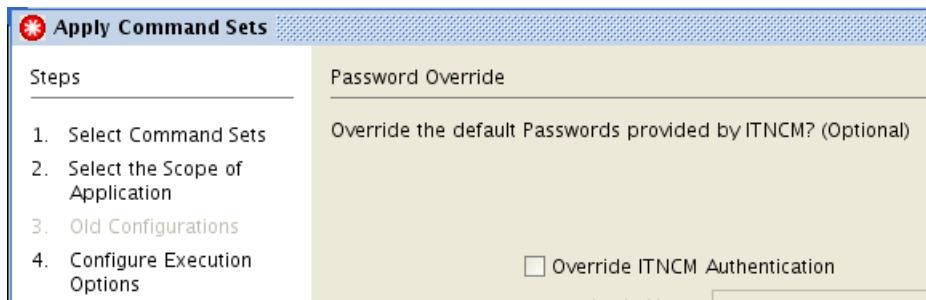
4 Mass change configuration management exercises

Exercise 4 Applying a modeled command set

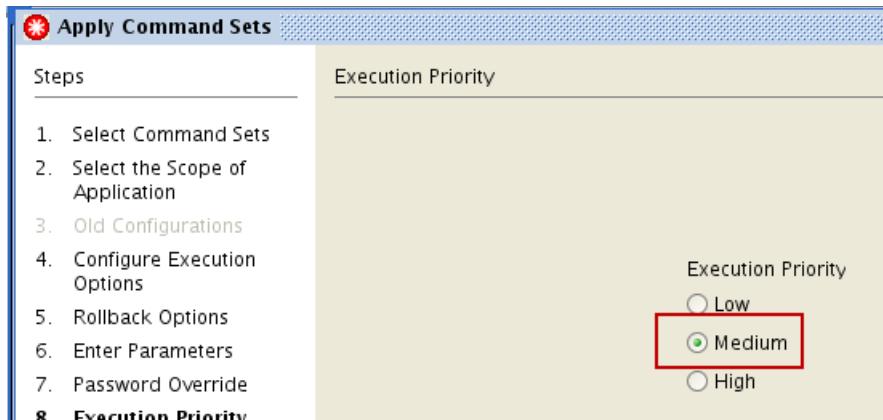
- Click the **SNMP_Destination_IP** parameter in the Enter Parameters (Page 2 of 2) window. Enter **192.168.100.100** in the **Parameter Name** field. Click **Next**.



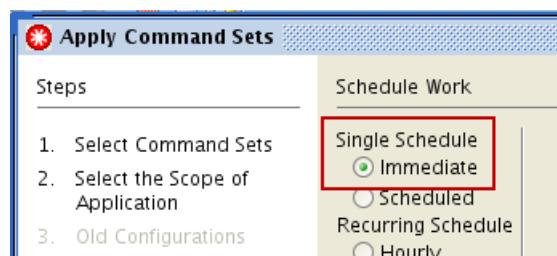
- Click **Next** in the Password Override window.



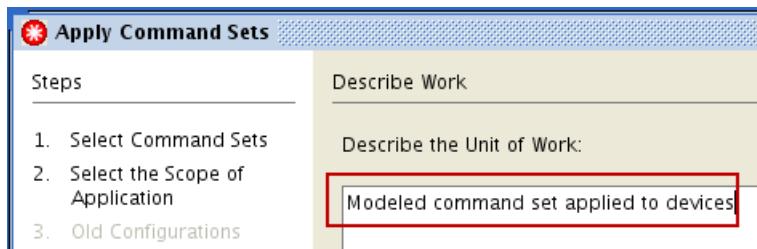
- Click **Next** in the Execution Priority window.



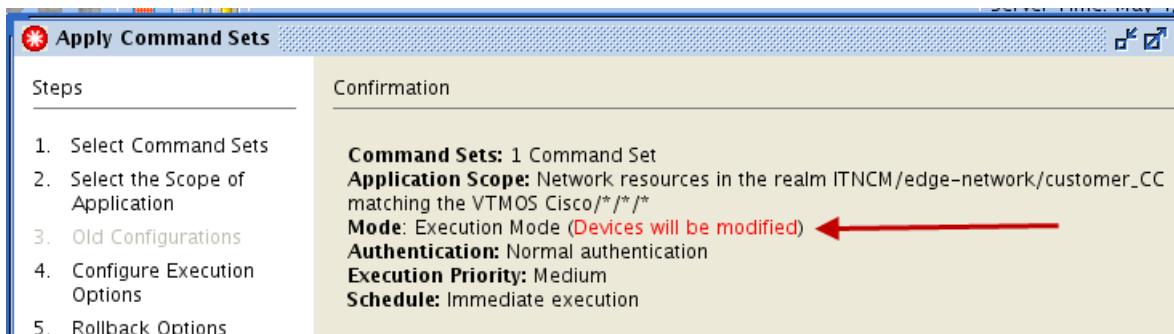
- Click **Next** in the Schedule Work window.



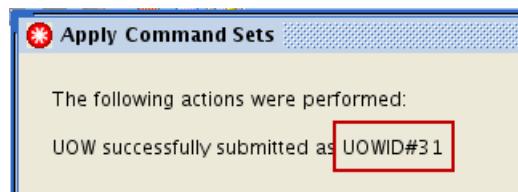
12. Enter **Modeled command set applied to devices** in the Describe Work window. Click **Next**.



13. Click **Finish** in the Confirmation window.



14. Note the unit of work number and click **Close**.



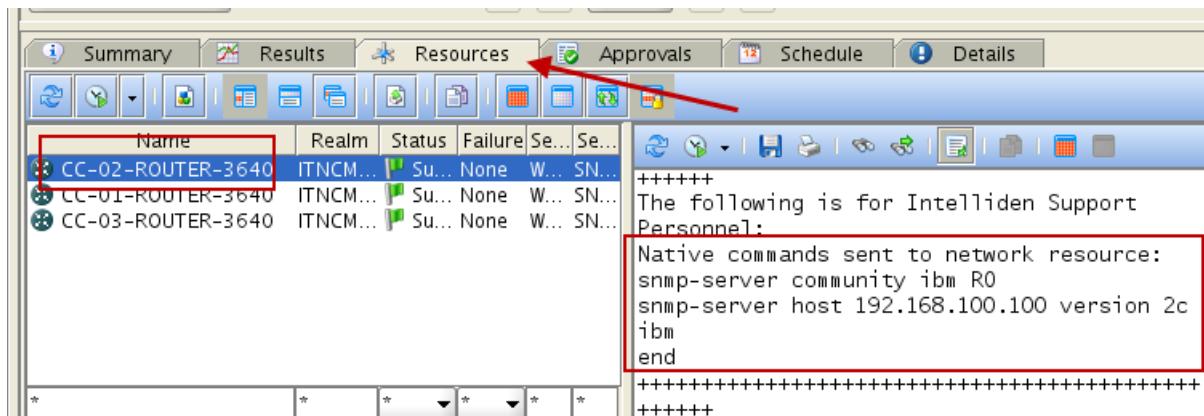
15. Verify that the unit of work ran successfully and that the configuration of each device shows the configuration change.

- Find the unit of work in the *queue manager* that applied the command set. Click the *unit of work*.

	UOW ID	Type	Submitter	Request Type
19	UOW	engineer	Import Configuration	
20	UOW	engineer	Import Configuration	
21	UOW	engineer	Run Autodiscovery	
22	UOW	engineer	Import Configuration	
23	UOW	engineer	Import Configuration	
24	UOW	engineer	Run Autodiscovery	
25	UOW	engineer	Run Autodiscovery	
26	UOW	engineer	Import Configuration	
27	UOW	engineer	Import Configuration	
28	UOW	engineer	Configuration Change	
29	UOW	engineer	Configuration Synchronization (Device)	
30	UOW	engineer	Command Set Report Only	
31	UOW	engineer	Command Set	

Note: The updates run for several minutes.

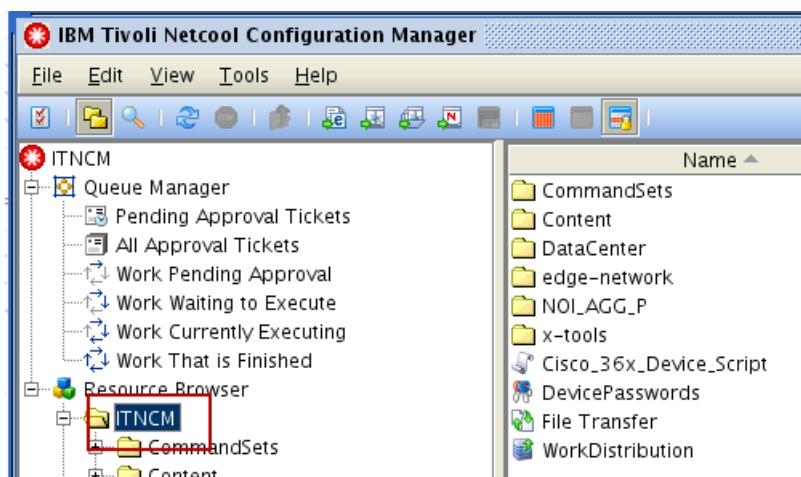
- b. Click the **Resources** tab in the *unit of work*. Click each device and scroll down in the work log to find the result of the command set.



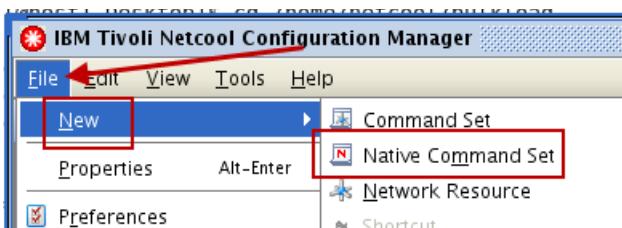
Exercise 5 Creating an interrogative native command set

In this exercise, you create a simple native command set that retrieves information from network devices.

1. Create a new native command set named **show_memory_flash** in the **ITNCM** realm. Use the following VTMOS settings for the command set.
 - Vendor: **Cisco**
 - Type: **Router**
 - Model: *
 - OS: *
- a. Click the **ITNCM** realm in the *resource browser*.



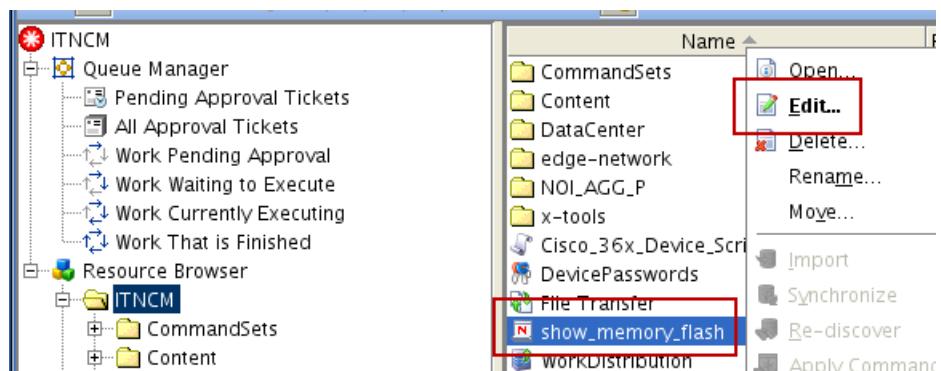
- b. Click **File > New > Native Command Set.**



- c. Enter **show_memory_flash** into the Name field. Choose the VTMOS settings and click **OK**.



2. Configure the new **show_memory_flash** command set to perform the following tasks. Ensure that you create an interrogative command set. Save and close the command set when you finish.
- Set the **Type** of the command set to **Interrogation**.
 - Get memory pool statistics from a router. Use the command **show mem stat**.
 - Get boot flash and flash card information from a router. Use the command **show flash all**.
- a. Right-click the new **show_memory_flash** command set in the **ITNCM** realm and click **Edit**.



4 Mass change configuration management exercises

Exercise 6 Applying the interrogative native command set

- b. Click the arrow and select **Interrogation** in the **Type** field.



- c. Enter the following lines in the command set:

```
show mem stat  
show flash all
```



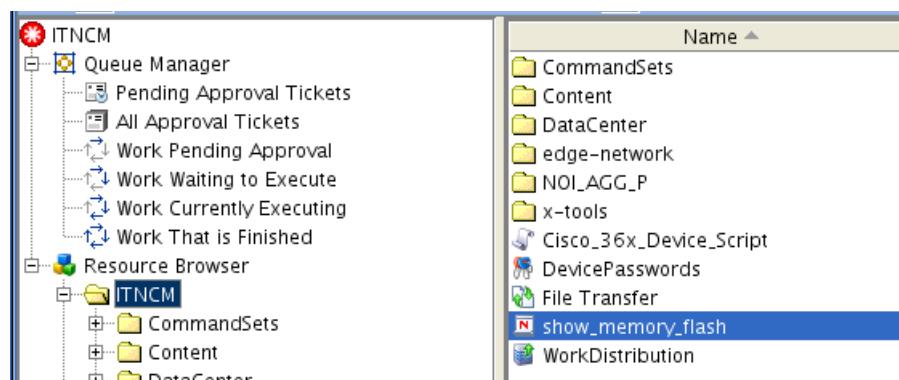
- d. Click **File > Save** and **File > Close**.



Exercise 6 Applying the interrogative native command set

In this exercise, you apply the new native command set to multiple routers.

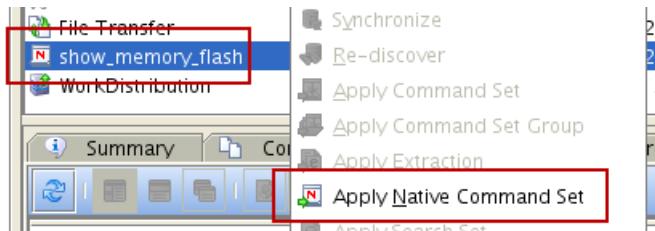
1. Find the **show_memory_flash** native command set. Click the **ITNCM** realm in the *resource browser*.



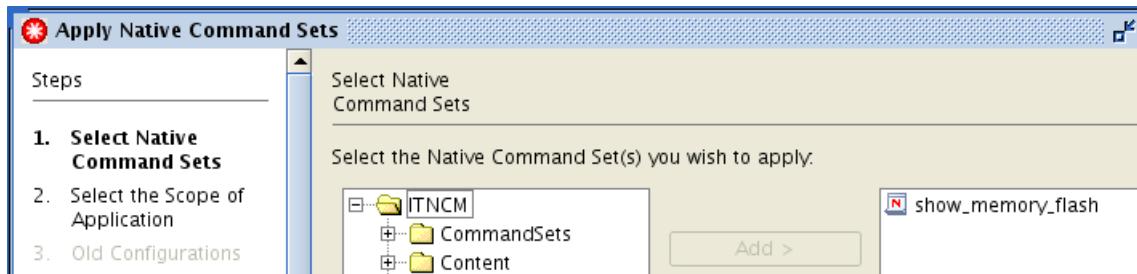
Use the following values to complete the wizard.

Field	Value
Select Command Sets	Leave show_memory_flash as the selected command set
Scope of Application	Network resources in a realm
Select the Realm	customer_CC
Execution Options	Apply Device at a time
Password Override	Do not override
Execution Priority	Medium
Schedule Work	Single Schedule > Immediate
Describe Work	Applying native command set

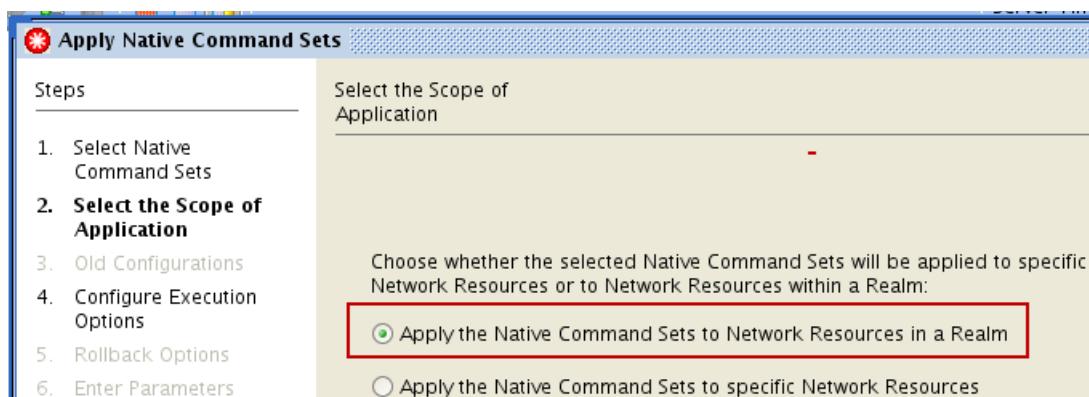
- a. Right-click the **show_memory_flash** command set and click **Apply Native Command Set**.
The Apply Command Sets wizard starts.



- b. Click **Next** in the Select the Native Command Sets window.



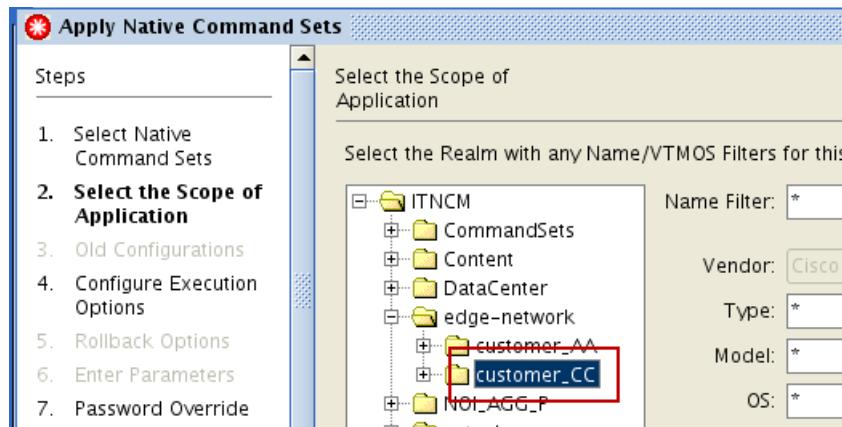
- c. Click **Next** in the Select the Scope of Application window.



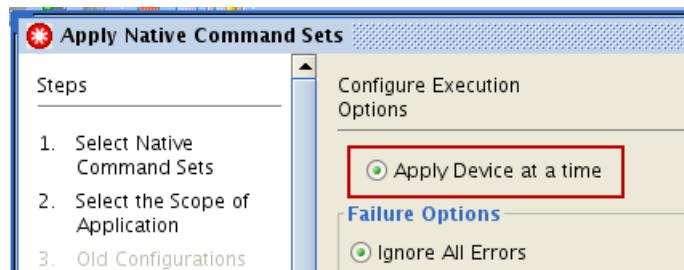
4 Mass change configuration management exercises

Exercise 6 Applying the interrogative native command set

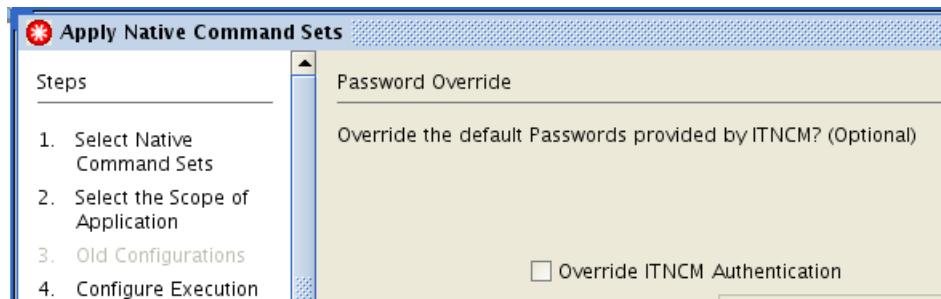
- d. Click **edge-network > customer_CC** in the Select the Realm field. Click **Next**.



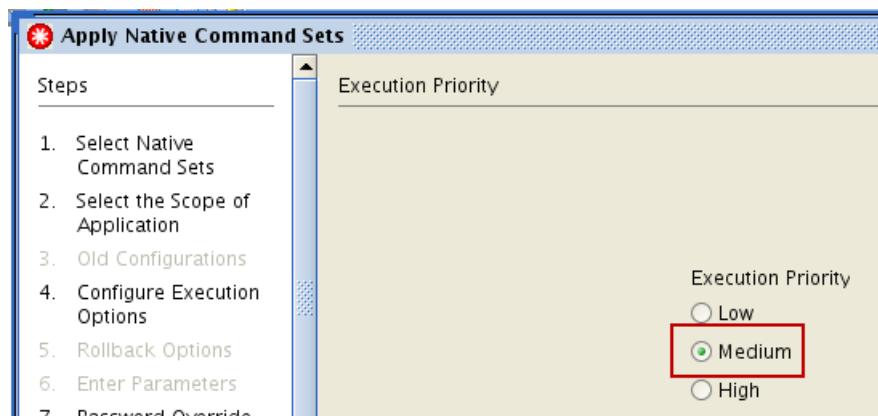
- e. Click **Next** in the Configure Execution Options window.



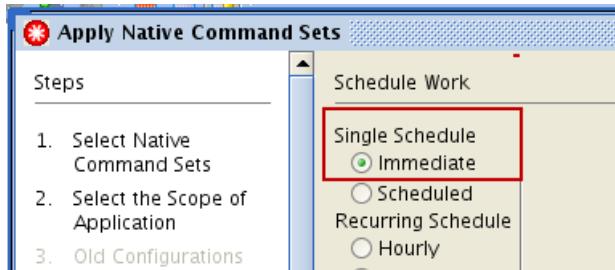
- f. Click **Next** in the Password Override window.



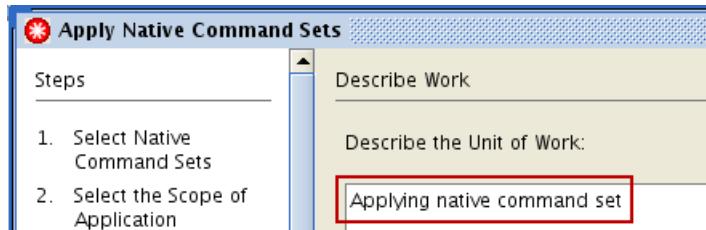
- g. Click **Next** in the Execution Priority window.



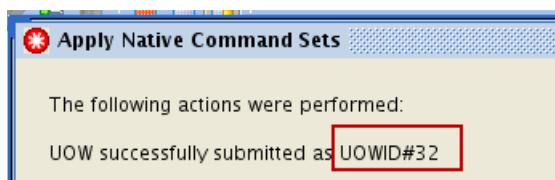
- h. Click **Next** in the Schedule Work window.



- i. Enter **Applying native command set** in the Describe Work window. Click **Finish**.



- j. Note the unit of work number and click **Close**.



2. Verify that the unit of work ran successfully and that the command set shows the result of the show commands.
a. Find the unit of work in the *queue manager* that applied the command set. Click the *unit of work*.

UOW ID	Type	Submitter	Request Type
20	UOW	engineer	Import Configuration
21	UOW	engineer	Run Autodiscovery
22	UOW	engineer	Import Configuration
23	UOW	engineer	Import Configuration
24	UOW	engineer	Run Autodiscovery
25	UOW	engineer	Run Autodiscovery
26	UOW	engineer	Import Configuration
27	UOW	engineer	Import Configuration
28	UOW	engineer	Configuration Change
29	UOW	engineer	Configuration Synchronization
30	UOW	engineer	Command Set (Report Only)
31	UOW	engineer	Command Set
32	UOW	engineer	Native Command Set

- b. Click the **Resources** tab in the *unit of work*. Click each device and scroll down in the work log to find the result of the command set.

The screenshot shows the IBM Tivoli Netcool Configuration Manager interface. The top navigation bar includes tabs for Summary, Results, Resources (which is currently selected), Approvals, Schedule, and Details. Below the tabs is a toolbar with various icons. The main area contains a table with columns for Name, Realm, Status, Failure, and several partially visible columns. The row for 'CC-02-ROUTER-3640' is highlighted with a red box. To the right of the table, a large red box encloses a 'Interrogation Response:' window. This window displays two sets of command outputs:

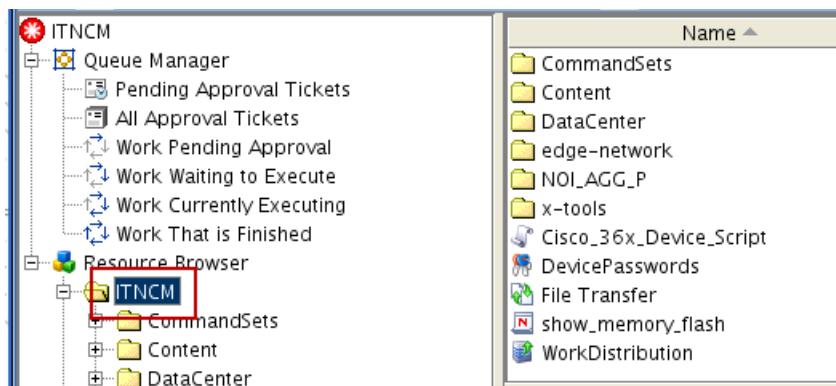
```
show mem stat
      Head   Total(b)    Used(b)
      Free(b) Lowest(b) Largest(b)
Processor 618331A0 24956512 6282844
18673668 18239964 18121100
      I/O    3000000 16777216 2626800
14150416 14122688 14104124
CC-02-ROUTER-3640#show flash all
Partition  Size    Used    Free
Bank-Size State      Copy Mode
1          8191K    OK     8191K
8192K     Read/Write Direct

System flash directory:
No files in System flash
[0 bytes used, 8388604 available, 8388604 total]
```

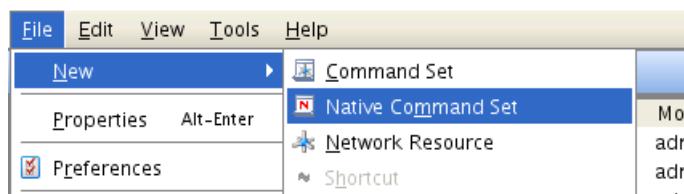
Exercise 7 Creating a native command set

In this exercise, you create a native command set. The command set configures routers to show sequence numbers in logs and to show a message to users when they start an interactive EXEC session.

1. Create a new native command set named **sequence_exec** in the **ITNCM** realm. Use the following VTMOS settings for the command set.
 - Vendor: **Cisco**
 - Type: **Router**
 - Model: **36***
 - OS: ***12.3***
- a. Click the **ITNCM** realm in the *resource browser*.



- b. Click **File > New > Native Command Set**.

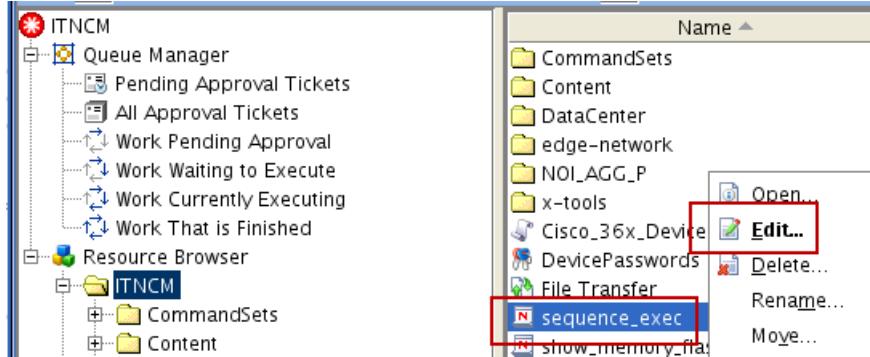


- c. Enter **sequence_exec** into the **Name** field. Choose the VTMOS settings and click **OK**.



2. Configure the new **sequence_exec** command set to perform the following tasks. Save and close the command set when you finish.
- ◆ Show sequence numbers in logs. Use the command **service sequence-numbers**.
 - ◆ Show a banner message to users when they start an interactive EXEC session. Make the banner message a parameter. Use the command **banner exec** followed by a parameter named **exec_banner_message**.

- a. Right-click the new **sequence_exec** command set in the **ITNCM** realm and click **Edit**.

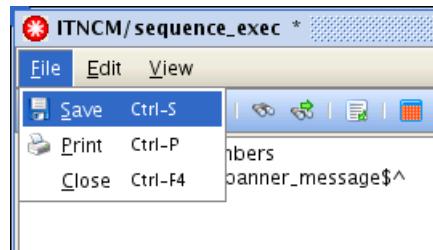


- b. Enter the following two lines in to the command set:

```
service sequence-numbers
banner exec ^$exec_banner_message$^
```



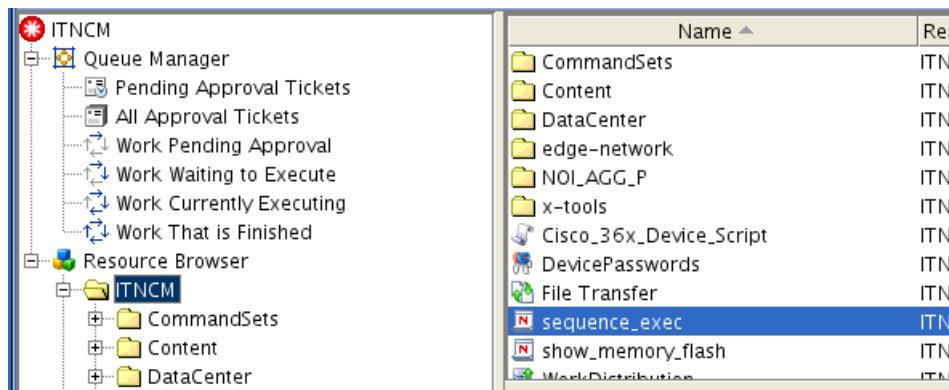
- c. Click **File > Save** and **File > Close**.



Exercise 8 Applying the native command set

In this exercise, you apply the new native command set to multiple routers.

1. Click the **ITNCM** realm in the *resource browser*.

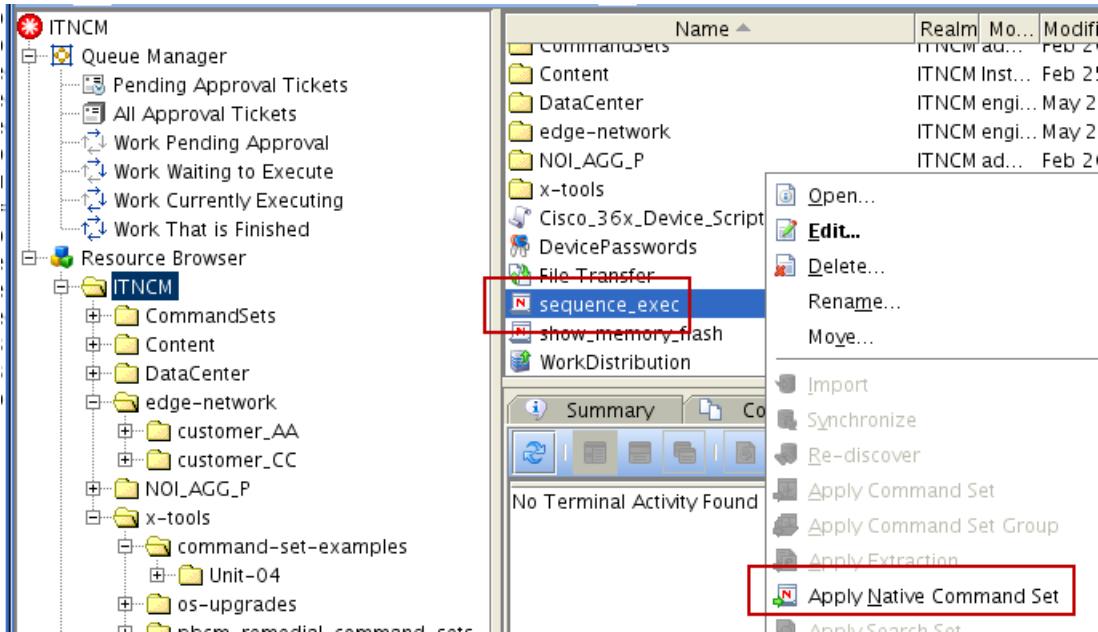


Use the following values to complete the wizard.

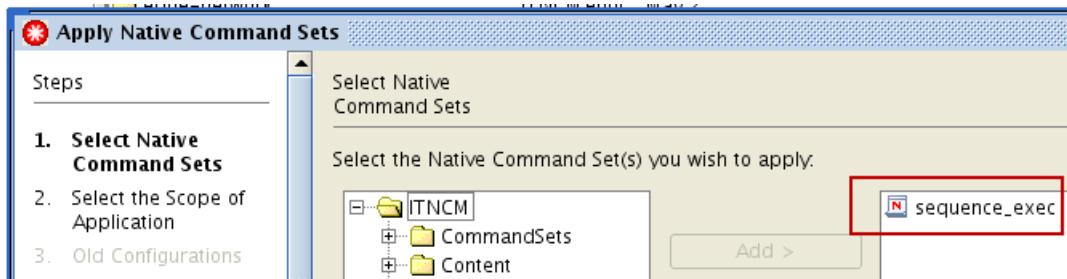
Field	Value
Select Command Sets	Leave sequence_exec as the selected command set
Scope of Application	Network resources in a realm
Select the Realm	customer_CC
Execution Options	Apply Device at a time
Rollback	Use modeled rollback
Enter Parameters	Enter Use Tivoli Netcool Configuration Manager to make changes to this device as the value of the exec_banner_message parameter
Password Override	Do not override
Execution Priority	Medium

Field	Value
Schedule Work	Single Schedule > Immediate
Describe Work	Applying sequence numbers and exec banner

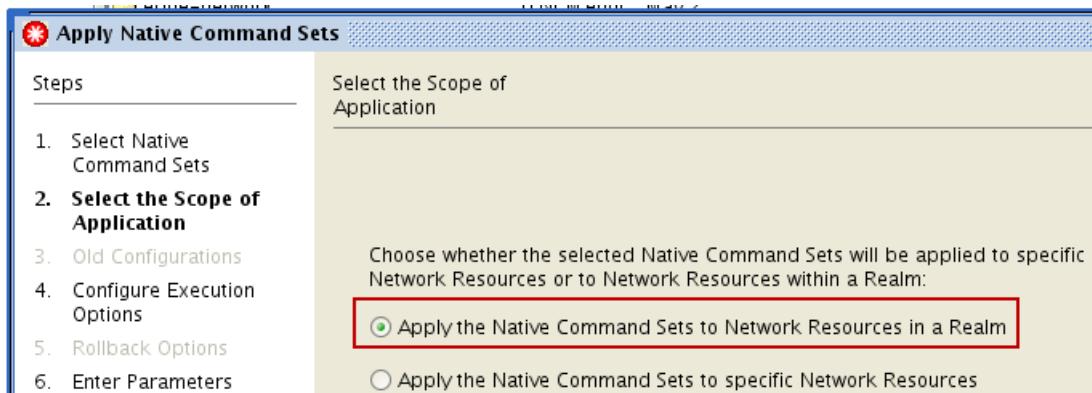
- a. Right-click the **sequence_exec** command set and click **Apply Native Command Set**. The Apply Command Sets wizard starts.



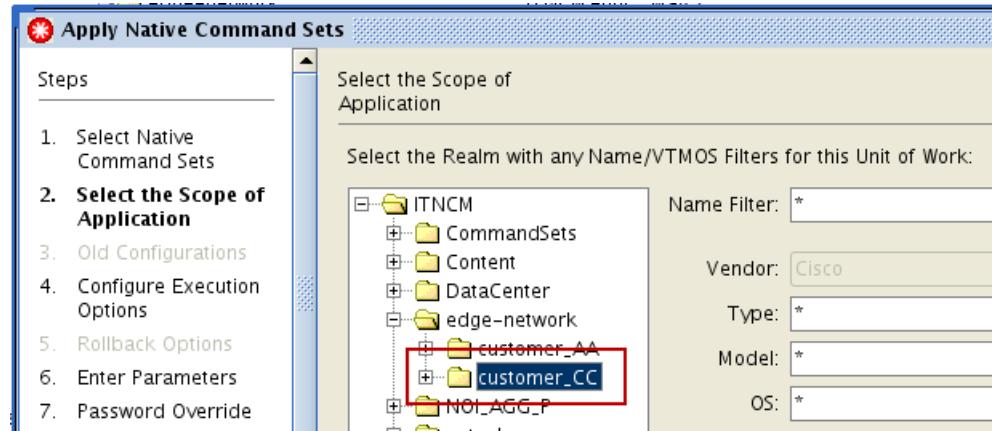
- b. Click **Next** in the Select the Native Command Sets window.



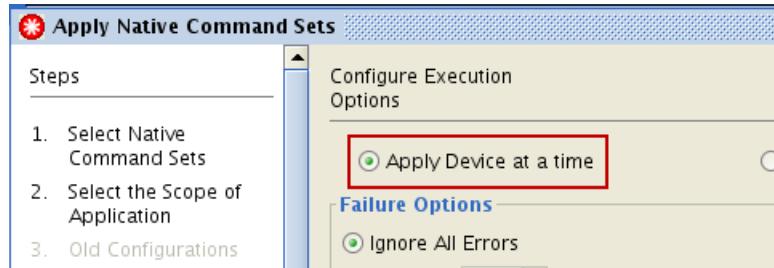
- c. Click **Next** in the Select the Scope of Application window.



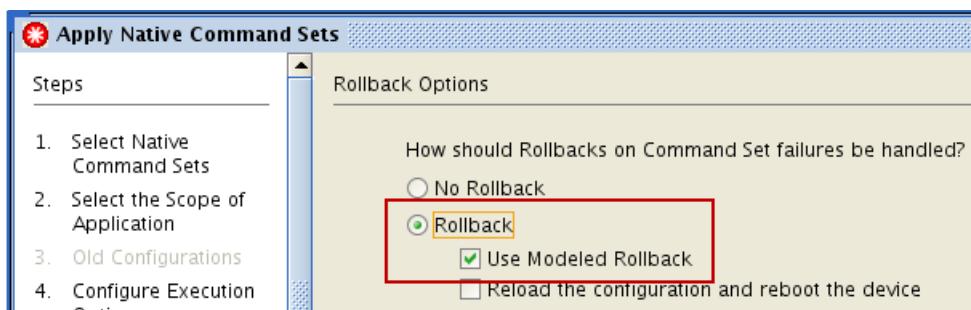
- d. Click **edge-network > customer_CC** in the Select the Realm field. Click **Next**.



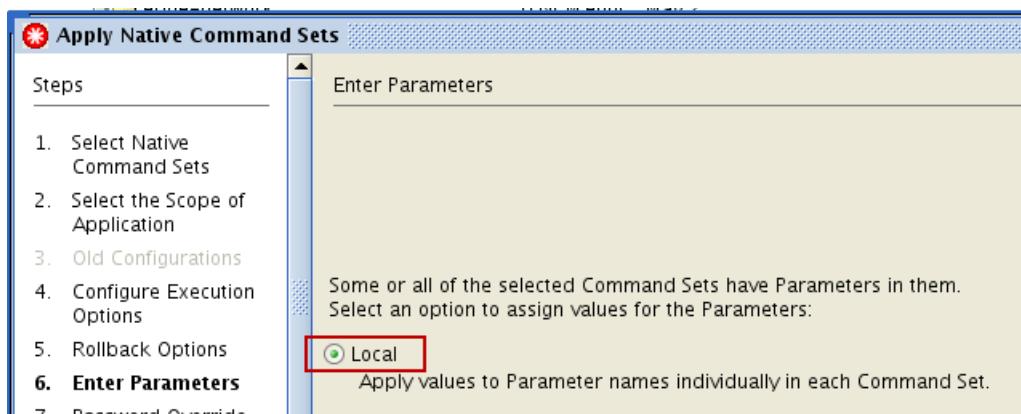
- e. Click **Next** in the Configure Execution Options window.



- f. Select **Rollback** and select **Use Modeled Rollback** in the Rollback Options window. Click **Next**.



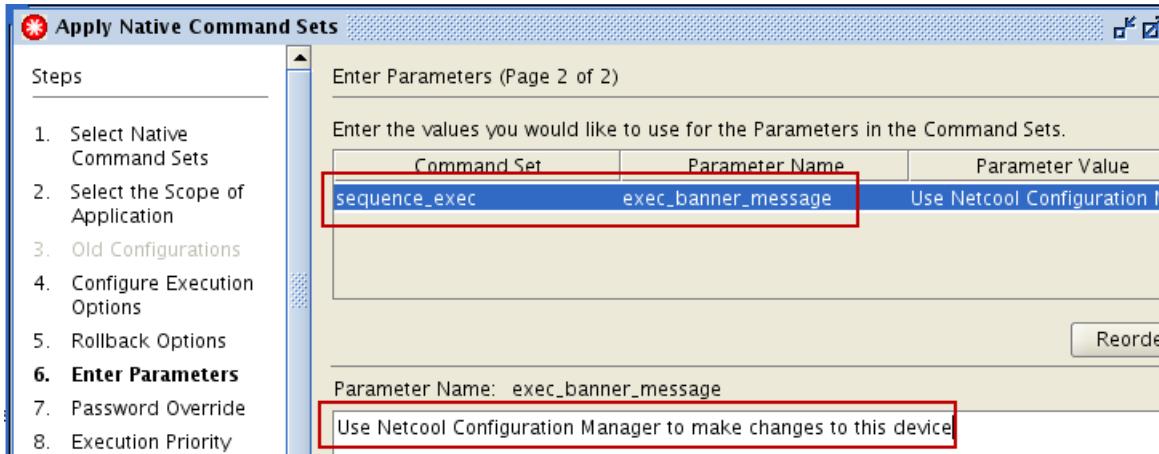
- g. Click **Next** on the Enter Parameters window.



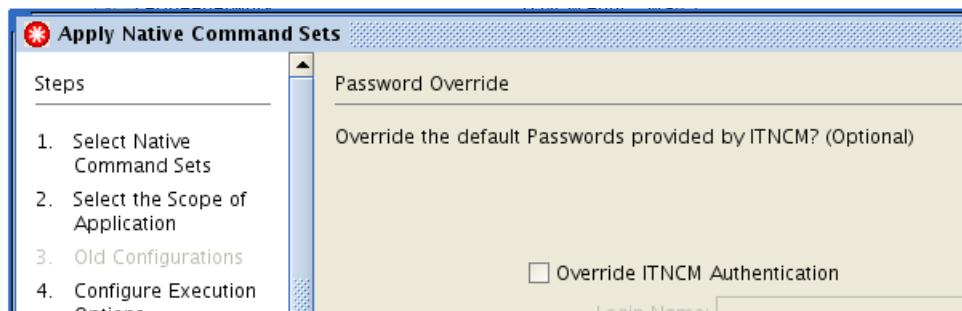
4 Mass change configuration management exercises

Exercise 8 Applying the native command set

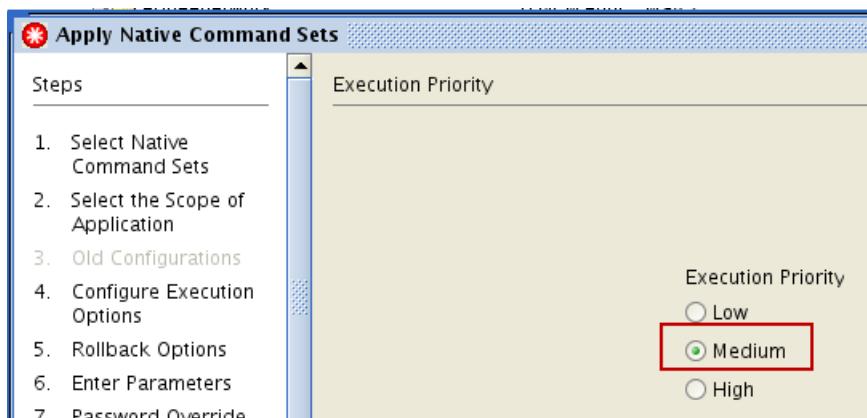
- h. Click the **exec_banner_message** parameter in the Enter Parameters window. Enter **Use Netcool Configuration Manager to make changes to this device** in the Parameter Name field. Click **Next**.



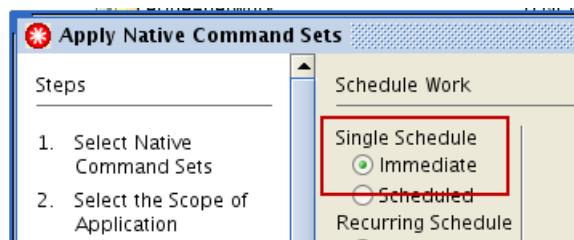
- i. Click **Next** in the Password Override window.



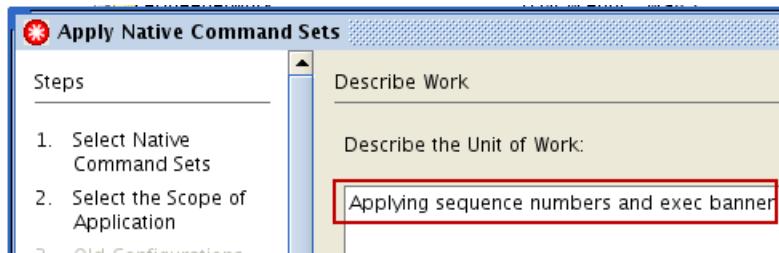
- j. Click **Next** in the Execution Priority window.



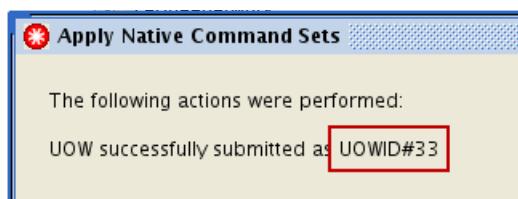
- k. Click **Next** in the Schedule Work window.



- I. Enter **Applying sequence numbers and exec banner** in the Describe Work window. Click **Finish**.

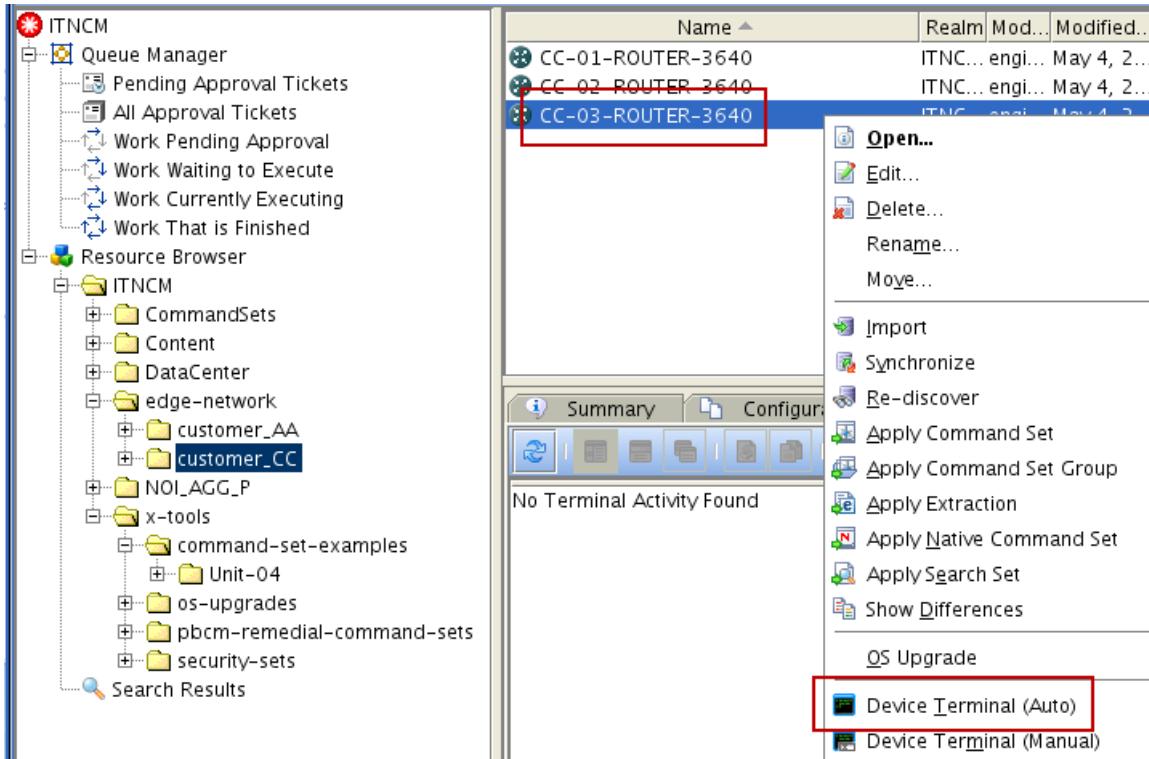


- m. Note the unit of work number and click **Close**.



2. Verify that the unit of work ran successfully by logging in to the CC-03-ROUTER-3640 router and viewing the running configuration. Use the device terminal to access the router. Use the command **show run** to view the running configuration.

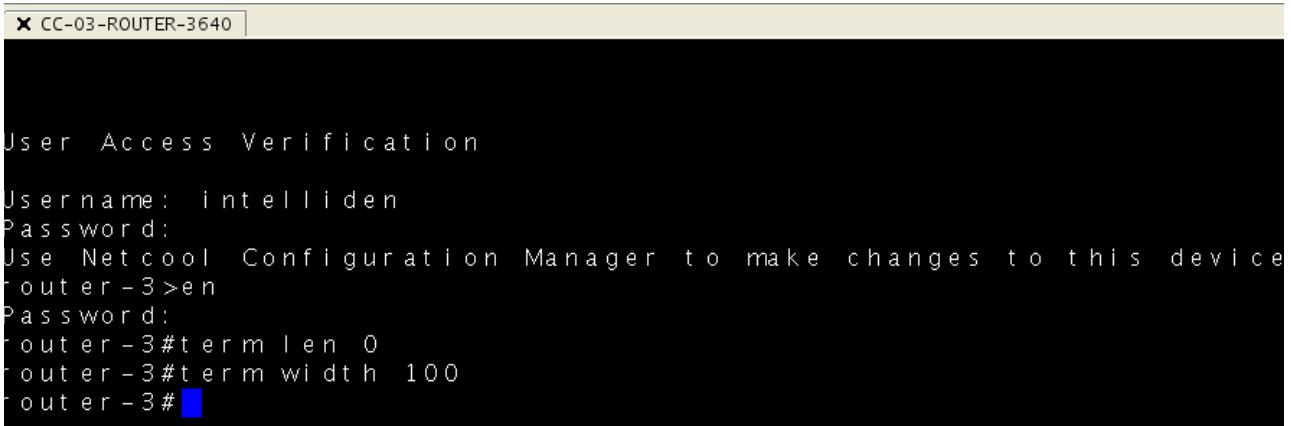
 - a. Click the **customer_CC** realm. Right-click the **CC-03-ROUTER-3640** router and click **Device Terminal (Auto)**.



4 Mass change configuration management exercises

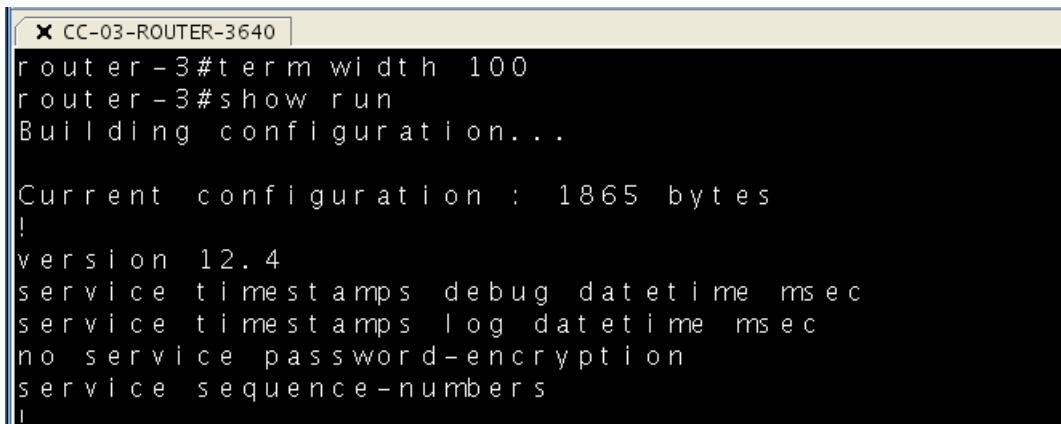
Exercise 8 Applying the native command set

- b. Verify that the exec banner shows when you log in.



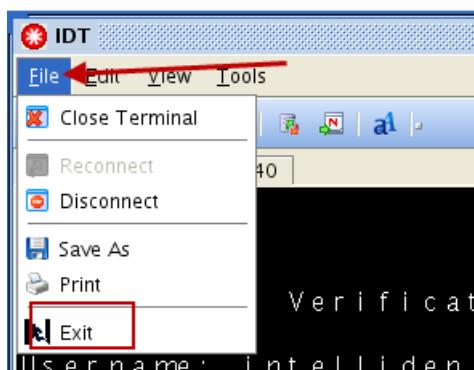
```
x CC-03-ROUTER-3640 |  
  
User Access Verification  
  
Username: intelliiden  
Password:  
Use Netcool Configuration Manager to make changes to this device  
router-3>en  
Password:  
router-3#term len 0  
router-3#term width 100  
router-3#
```

- c. Enter the command **show run**. Verify that the line **service sequence-numbers** is in the configuration.

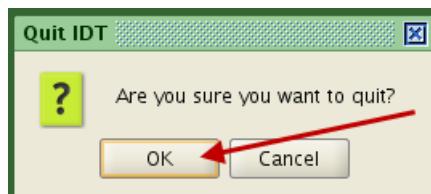


```
x CC-03-ROUTER-3640 |  
router-3#term width 100  
router-3#show run  
Building configuration...  
  
Current configuration : 1865 bytes  
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service sequence-numbers  
!
```

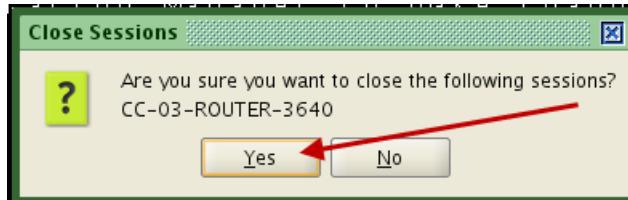
- d. Click **File** and select **Exit** to close the device terminal.



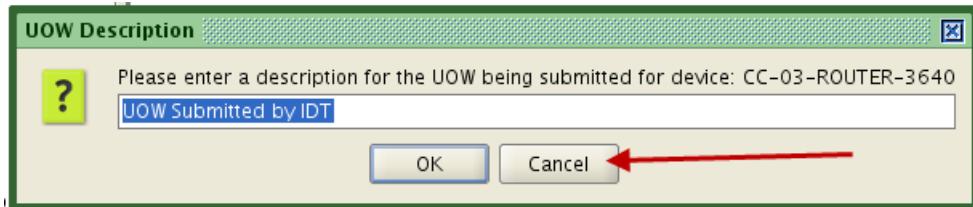
- e. Click **OK**.



- f. Click Yes.



- g. Click Cancel.



Exercise 9 Applying command sets from a CSV file

In this exercise, you apply multiple command sets by using a CSV file.

1. Open the file named **customer-CC-command-sets.csv** on the desktop
 - a. Double-click the **customer-CC-command-sets.csv** file on the image desktop.



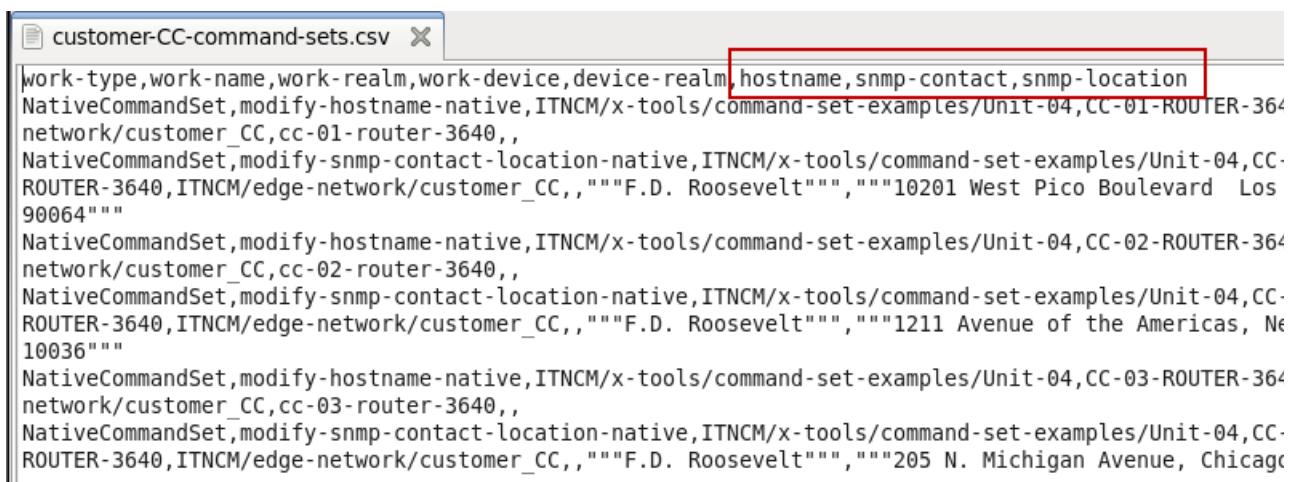
- b. Click **Display**.



The gedit application starts.

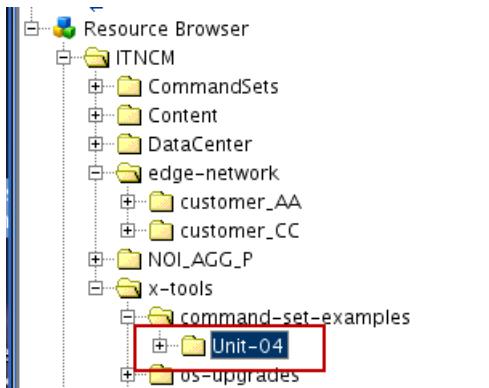
- c. View the lines in this file. This file applies the command sets named **modify-hostname-native** and **modify-snmp-contact-location-native**. This file lists the

CC-01-ROUTER-3640, **CC-02-ROUTER-3640**, and **CC-03-ROUTER-3640** resources. This file lists the **hostname**, **snmp-contact**, and **snmp-location** parameter values.

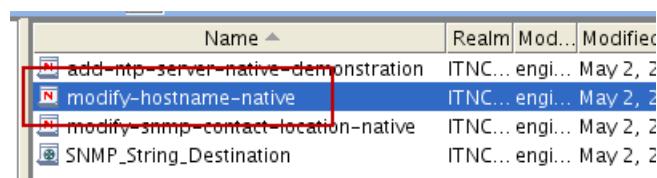


work-type	work-name	work-realm	work-device	device-realm	hostname	snmp-contact	snmp-location
NativeCommandSet	modify-hostname-native	ITNCM/x-tools/	command-set-examples	Unit-04	CC-01-ROUTER-3640		
NativeCommandSet	modify-snmp-contact-location-native	ITNCM/x-tools/	command-set-examples	Unit-04	CC-ROUTER-3640	ITNCM/edge-network/customer_CC	,""F.D. Roosevelt""",""10201 West Pico Boulevard Los 90064""
NativeCommandSet	modify-hostname-native	ITNCM/x-tools/	command-set-examples	Unit-04	CC-02-ROUTER-3640		
NativeCommandSet	modify-snmp-contact-location-native	ITNCM/x-tools/	command-set-examples	Unit-04	CC-ROUTER-3640	ITNCM/edge-network/customer_CC	,""F.D. Roosevelt""",""1211 Avenue of the Americas, Ne 10036""
NativeCommandSet	modify-hostname-native	ITNCM/x-tools/	command-set-examples	Unit-04	CC-03-ROUTER-3640		
NativeCommandSet	modify-snmp-contact-location-native	ITNCM/x-tools/	command-set-examples	Unit-04	CC-ROUTER-3640	ITNCM/edge-network/customer_CC	,""F.D. Roosevelt""",""205 N. Michigan Avenue, Chicago IL 60601""

2. Click **File** and select **Quit** to close the gedit utility.
3. Open the **modify-hostname-native** and **modify-snmp-contact-location-native** command sets. They are in the **ITNCM > x-tools > command-set-examples > Unit-04** realm. Compare the parameters in the command sets to the values in the **customer-CC-command-sets.csv** file.
 - a. Click **ITNCM > x-tools > command-set-examples > Unit-04** in the *resource browser*.



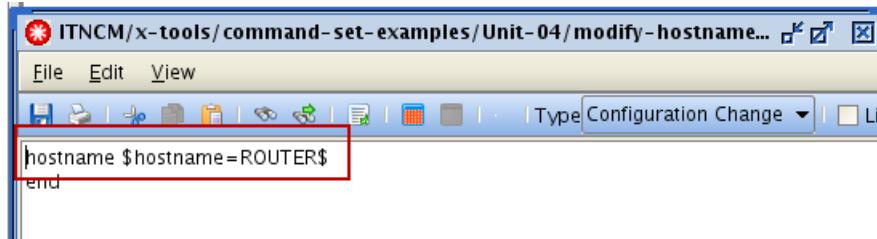
- b. Double-click the **modify-hostname-native** command set.



Name	Realm	Mod...	Modified
add-ntp-server-native-demonstration	ITNC...	engi...	May 2, 2016
modify-hostname-native	ITNC...	engi...	May 2, 2016
modify-snmp-contact-location-native	ITNC...	engi...	May 2, 2016
SNMP_String_Destination	ITNC...	engi...	May 2, 2016

The command set editor window opens.

The value in the **customer-CC-command-sets.csv** file replaces the value for the hostname command.

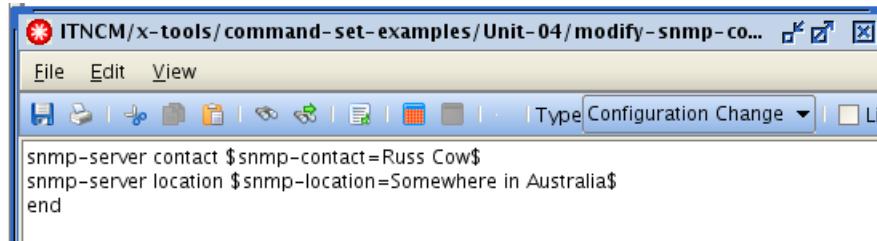


- c. Close the command set editor window.
- d. Double-click the **modify-snmp-contact-location-native** command set.

Name	Realm	Mod...	Modified...	Vendor	Type
add-ntp-server-native-demonstration	ITNC...	engi...	May 2, 2...	Cisco	Router *
modify-hostname-native	ITNC...	engi...	May 2, 2...	Cisco	Router *
modify-snmp-contact-location-native	ITNC...	engi...	May 2, 2...	Cisco	Router *
SNMP String Destination	ITNC...	engi...	May 2, 2...	Cisco	Router 3t

The command set editor window opens.

- e. The values in the **customer-CC-command-sets.csv** file replace the values for the snmp-server contact and snmp-server location commands.

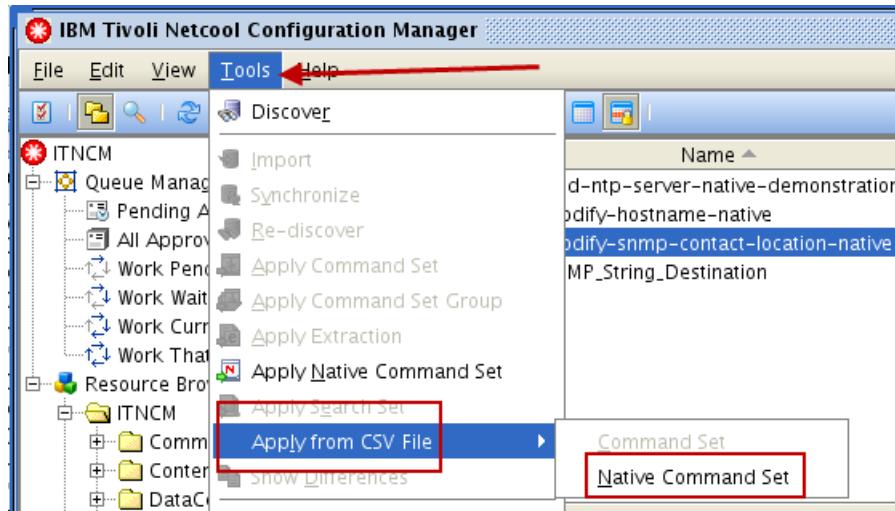


- f. Close the command set editor window.
4. Apply the native command sets from the CSV file. Use the following values to complete the wizard.

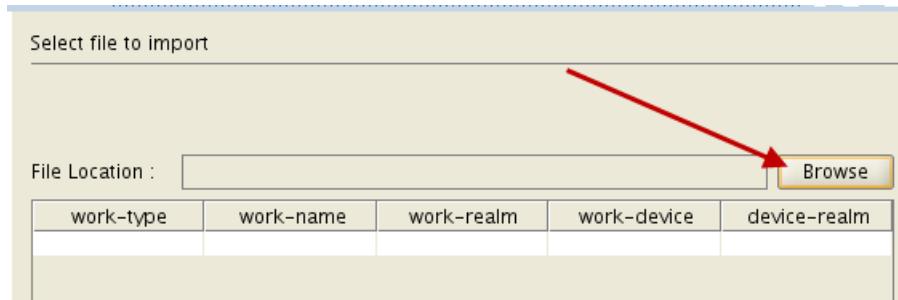
Field	Value
File Location	/netcool/Desktop/customer-CC-command-sets.csv
Configure Execution Options	Apply Device at a time
Failure Options	Ignore All Errors
Rollback Options	Select No Rollback. Rollback only the failed Command Set on the failed Network Resource.
Password Override	Do not override
Execution Priority	Medium

Field	Value
Schedule Work	Single Schedule > Immediate
Describe Work	Applying command sets from a CSV file

- a. Click **Tools > Apply from CSV file > Native Command Set** to apply the native command sets. The Csv - Apply Native Command Sets wizard starts.



- b. Click **Browse** to select the CSV file.



- c. Double-click **Desktop**. Click the **customer-CC-command-sets.csv** file. Click **Open**.



d. Click **Next**.

work-type	work-na...	work-re...	work-de...	device-r...	hostname	snmp-co...
NativeCo...	modify...	ITNCM/x...	CC-01-...	ITNCM/e...	cc-01-r...	"F.D. Roo.
NativeCo...	modify-s...	ITNCM/x...	CC-01-...	ITNCM/e...		
NativeCo...	modify...	ITNCM/x...	CC-02-...	ITNCM/e...	cc-02-r...	"F.D. Roo.
NativeCo...	modify-s...	ITNCM/x...	CC-02-...	ITNCM/e...		
NativeCo...	modify...	ITNCM/x...	CC-03-...	ITNCM/e...	cc-03-r...	"F.D. Roo.
NativeCo...	modify-s...	ITNCM/x...	CC-03-...	ITNCM/e...		

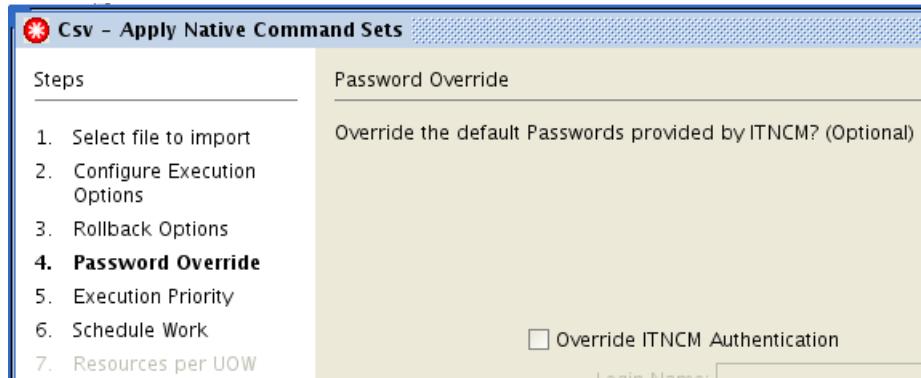
e. Accept the **Apply Device at a time** and **Ignore All Errors** default options. Click **Next**.

f. Select the **Rollback** and **Rollback only the failed Command Set on the failed Network Resource** default options. Click **Next**.

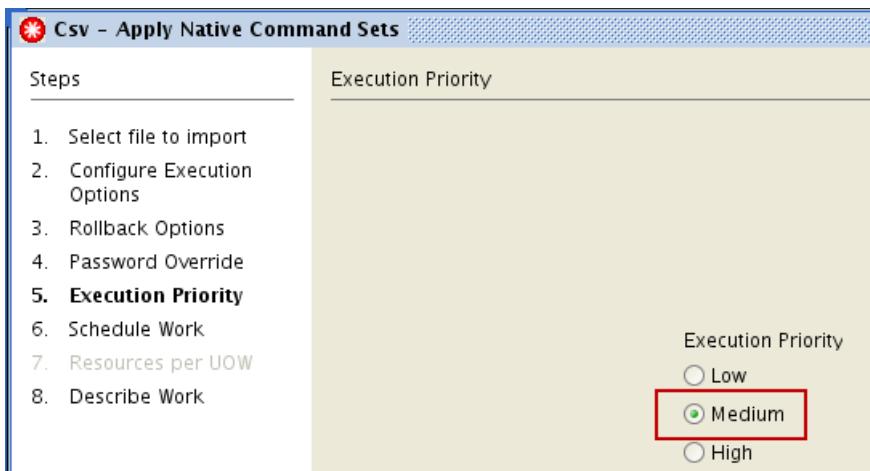
4 Mass change configuration management exercises

Exercise 9 Applying command sets from a CSV file

- g. Accept the default values in the Password Override window. Click **Next**.



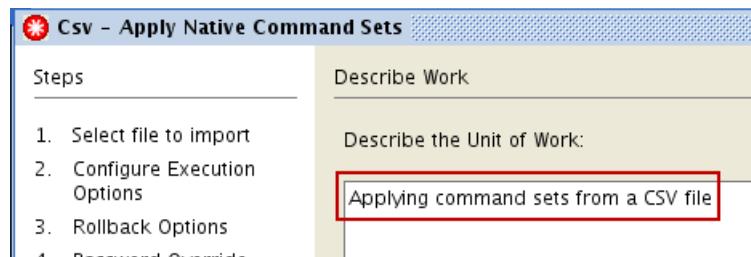
- h. Accept the default value in the Execution Priority window. Click **Next**.



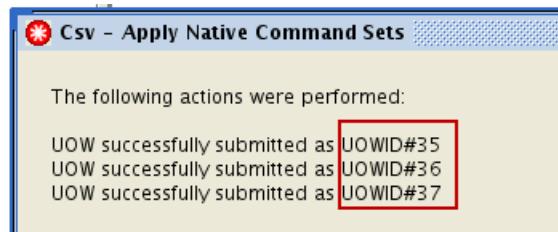
- i. Click **Next**.



- j. Enter **Applying command sets from a CSV file** in the Describe Work window. Click **Finish**.



- k. Note the units of work numbers and click **Close**.



5. Verify that the units of work ran successfully. The units of work have **Native Command Set** as the request type.



Note: The units of work run for a few minutes.

- a. Find the *units of work* that ran the native command sets. Click **Queue Manager > Work That is Finished**.

UOW ID	Type	Submitter	Request Type
29	UOW	engineer	Configuration Synchronization (De
30	UOW	engineer	Command Set (Report Only)
31	UOW	engineer	Command Set
32	UOW	engineer	Native Command Set
33	UOW	engineer	Native Command Set
34	UOW	engineer	Configuration Synchronization (De
35	UOW	engineer	Native Command Set
36	UOW	engineer	Native Command Set
37	UOW	engineer	Native Command Set

- b. Click each unit of work that ran the native command sets from the CSV file. Click the **Resources** tab to verify that both command sets ran successfully.

UOW ID	Type	Submitter	Request Type
35	UOW	engineer	Native Command Set
36	UOW	engineer	Native Command Set
37	UOW	engineer	Native Command Set

Page Size: 100 1 / 1 1 - 37 (37)

Summary Results Resources Approvals Schedule Details

Name Realm Status Failure Se... Se...

CC-02-ROUTER-3640 ITNCM... Su... None W... m...

CC-02-ROUTER-3640 ITNCM... Su... None W... m...

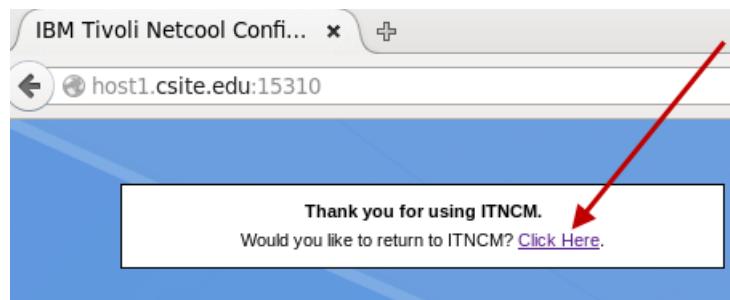
+++++
The following is for Intelliden Support Personnel.
Native commands sent to network resource:
snmp-server contact "F.D. Roosevelt"
snmp-server location "1211 Avenue of the Americas, New York, NY 10036"
end
+++++
Native Command

6. Close the configuration manager user interface.

7. Click **Logoff** to exit the configuration manager browser session.



8. Select **Click Here** to return to the browser log in screen.



Leave the browser session at the log in screen. You use it again shortly.



5 Administrative tasks exercises

In this unit, you submit two changes that require approval. You also stop (dequeue) and start (requeue) a unit of work.

Exercise 1 Making changes that require approval

1. Log in to the Netcool Configuration Manager browser session with the user name **operator**.
The password is **object00**.

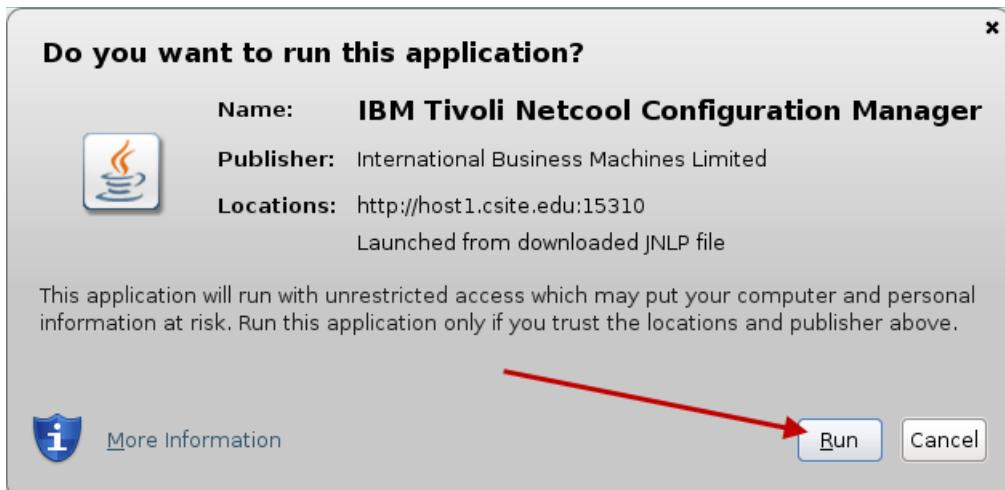


2. Click **ITNCM Webstart GUI**.



The Java Webstart client starts.

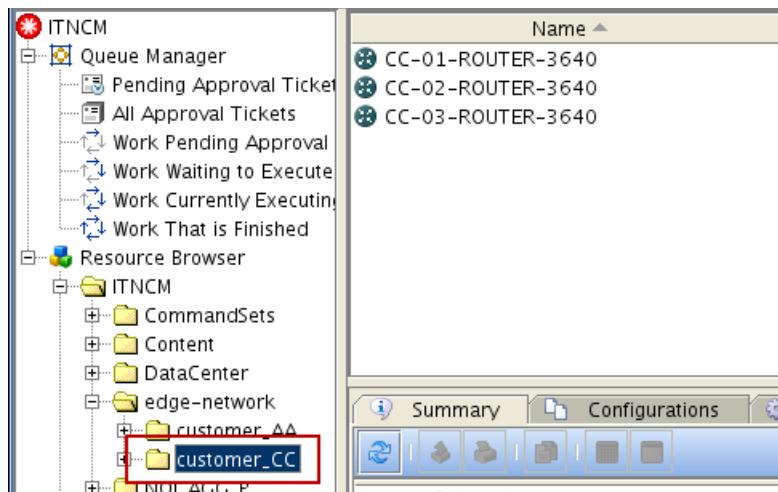
3. Click Run.



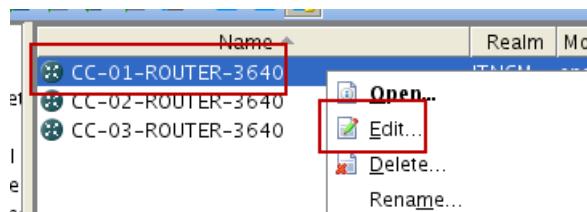
4. Edit the configuration of the CC-01-ROUTER-3640 device. Set the **memory-size iomem** parameter to **25** percent. When you are done editing the configuration, save it and submit the change. Name the configuration **iomem_25**. Use the following values to complete the Submit Configuration Change wizard.

Field	Value
Password Override	Do not override
Config Change	Merge
Execution Priority	Medium
Rollback Options	No rollback
Schedule Work	Single Schedule > Immediate
Describe Work	Changing I/O memory size to 25%

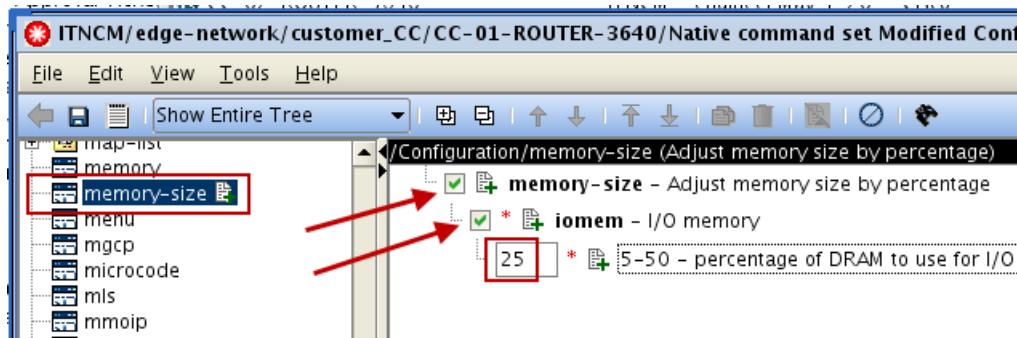
- a. Find the CC-01-ROUTER-3640 device in the *resource browser*. Click **ITNCM > edge-network > customer_CC**.



- b. Right-click **CC-01-ROUTER-3640** and click **Edit**.

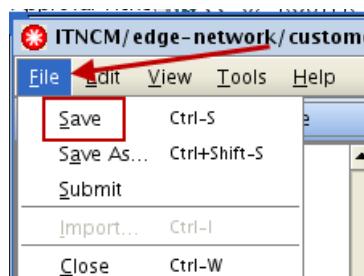


- c. Click the **memory-size** object in the command tree. On the right side of the *configuration editor*, select **memory-size** and **iomem**. Enter **25** in the **percentage of DRAM** field.

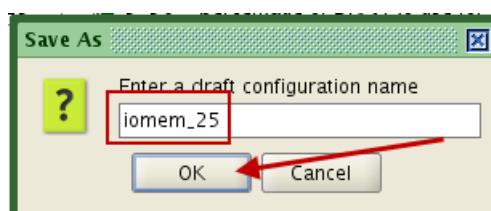


Hint: The box for the memory value is initially red. Click inside the box and the red goes away.

- d. Click **File > Save** to save the configuration.



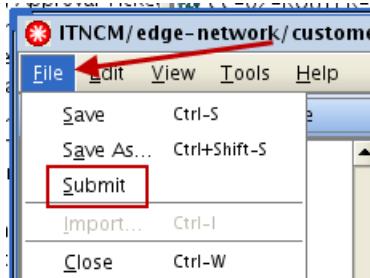
- e. Enter **iomem_25** as the name of the configuration and click **OK**.



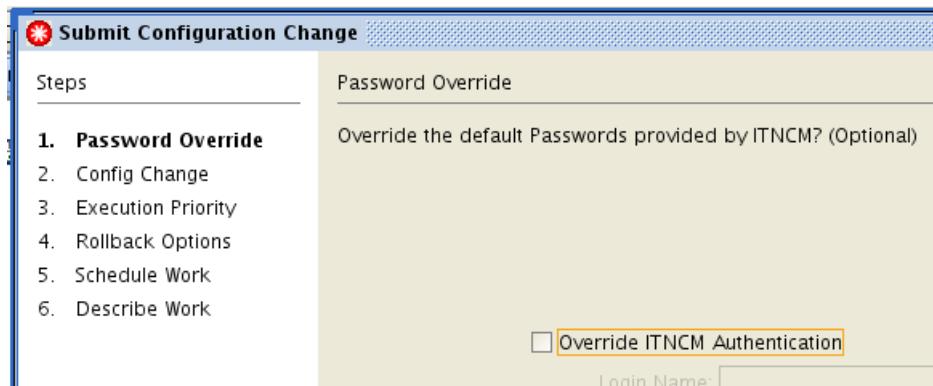
5 Administrative tasks exercises

Exercise 1 Making changes that require approval

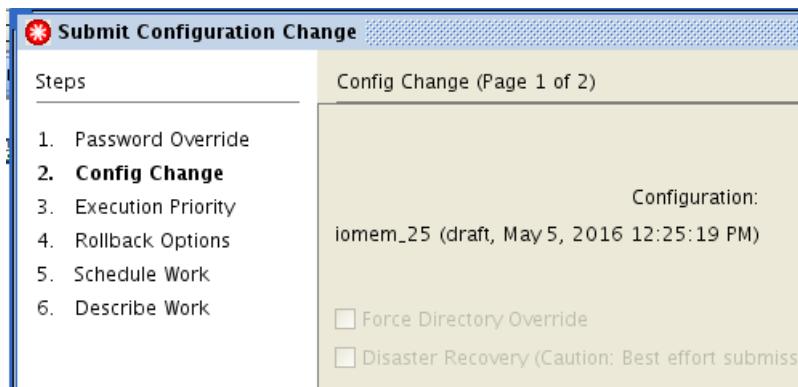
- f. Click **File > Submit** to submit the configuration. The Configuration Change wizard starts.



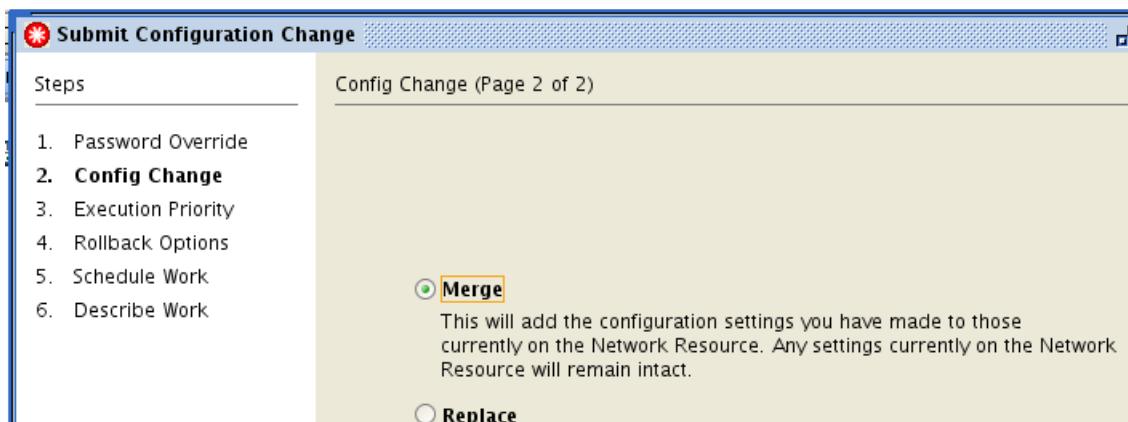
- g. Click **Next** in the Password Override window.



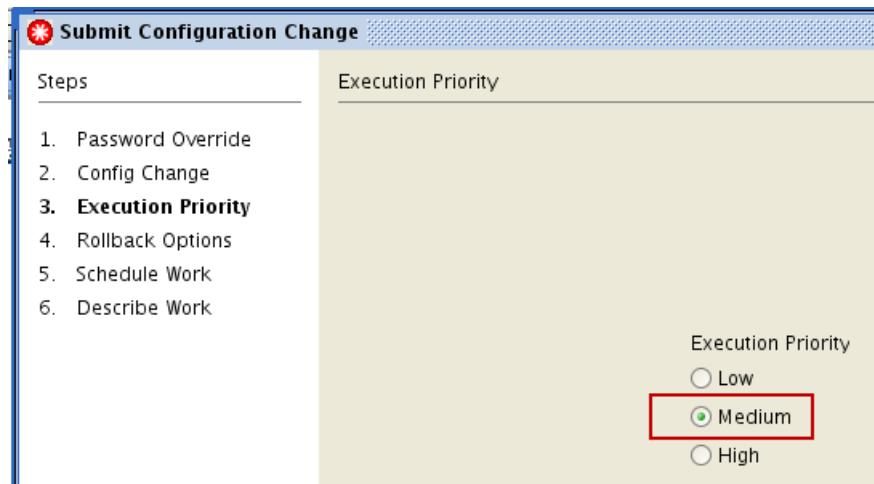
- h. Click **Next** in the Config Change window.



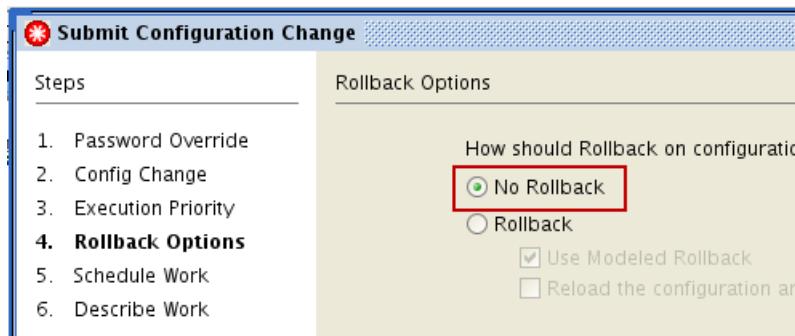
- i. Select **Merge** and click **Next** on the Config Change window.



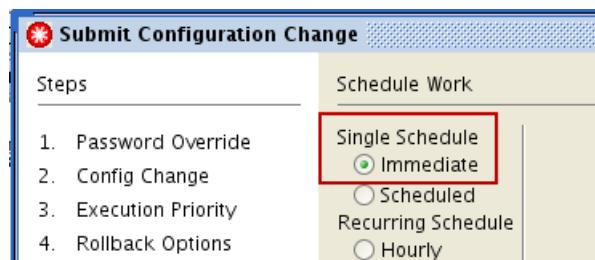
- j. Click **Next** in the Execution Priority window.



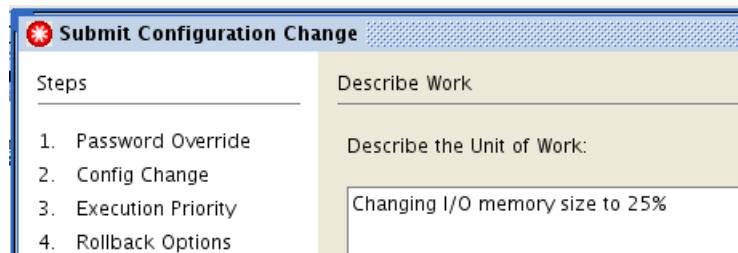
- k. Click **Next** in the Rollback Options window.



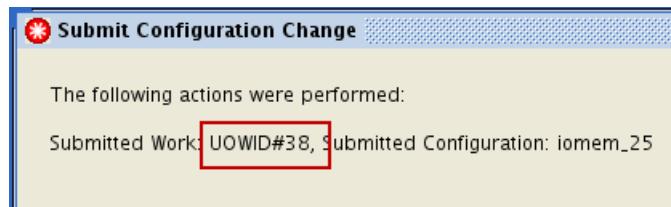
- l. Click **Next** in the Schedule Work window.



- m. Enter **Changing I/O memory size to 25%** in the Describe Work window. Click **Finish**.



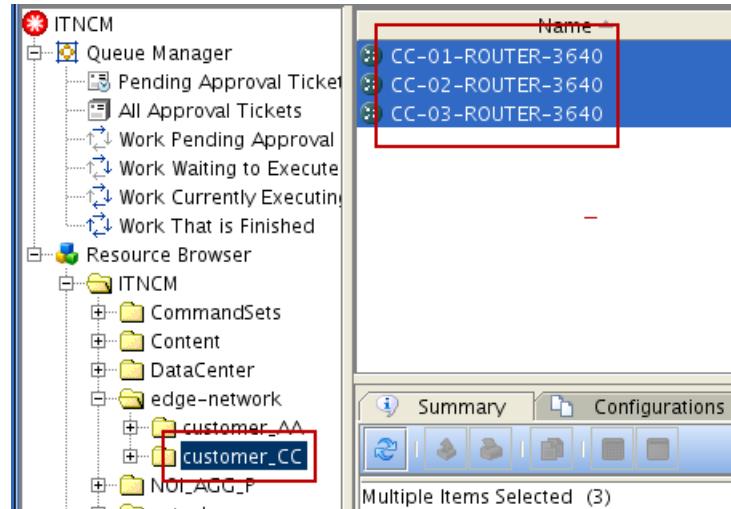
- n. Note the unit of work number and click **Close**.



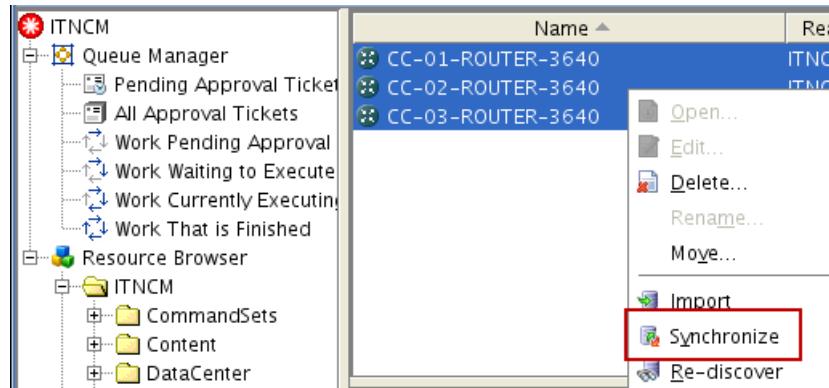
5. Select all three devices in the customer_CC realm. Synchronize them. Use the following values to complete the Configuration Synchronization wizard.

Field	Value
Select Network Resources	CC-01-ROUTER-3640, CC-02-ROUTER-3640, and CC-03-ROUTER-3640
Configure Failure Options	Ignore All Errors
Password Override	Do not override
Execution Priority	Low
Synchronization Option	Synchronize from Network Resource to IBM Tivoli Netcool Configuration Manager
Schedule Work	Schedule the change for 1 hour from the current time
Describe Work	Synchronization of customer_CC routers

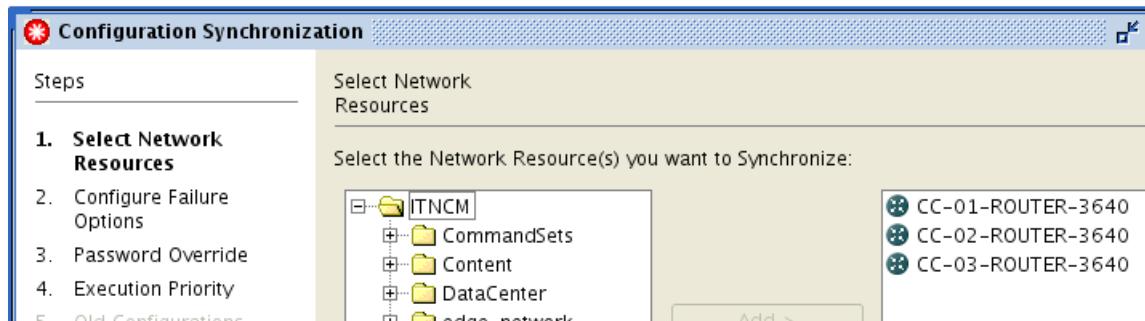
- a. Click **ITNCM > edge-network > customer_CC**. Select all three devices in the **customer_CC** realm.



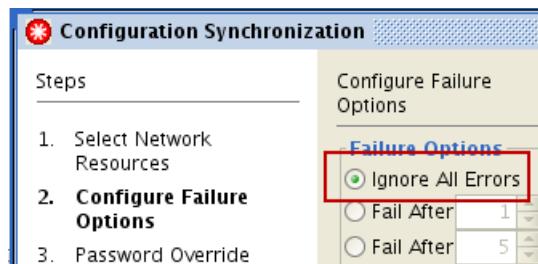
- b. Right-click the devices and click **Synchronize**. The Configuration Synchronization wizard starts.



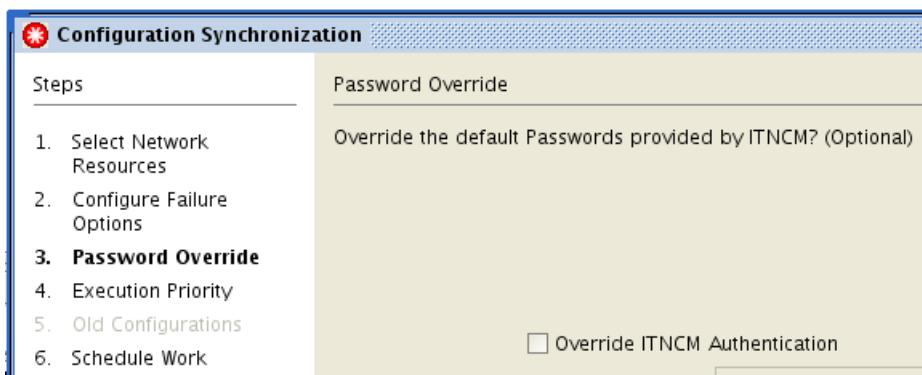
- c. Click **Next** in the Select Network Resources window.



- d. Click **Next** at the Configure Failure Options window.



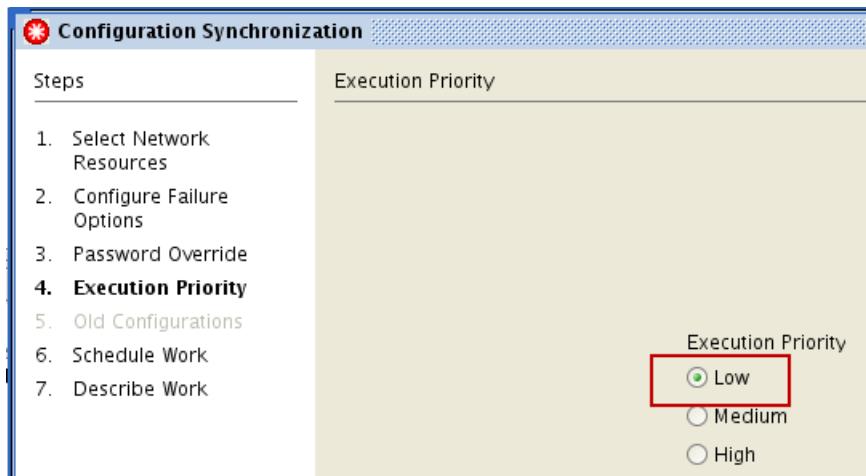
- e. Click **Next** in the Password Override window.



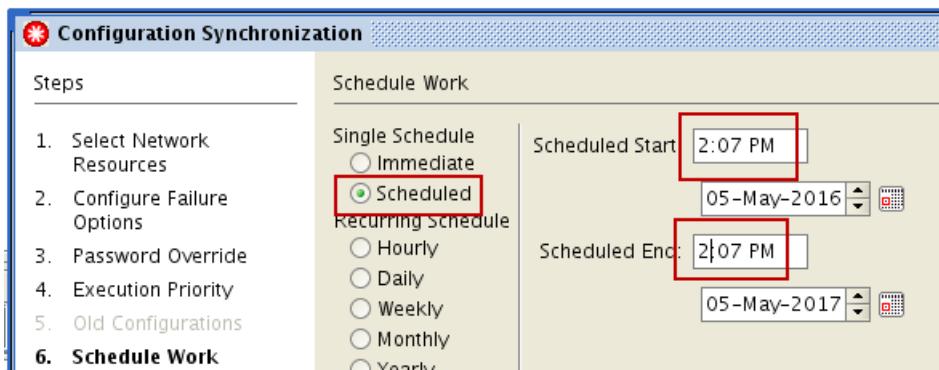
5 Administrative tasks exercises

Exercise 1 Making changes that require approval

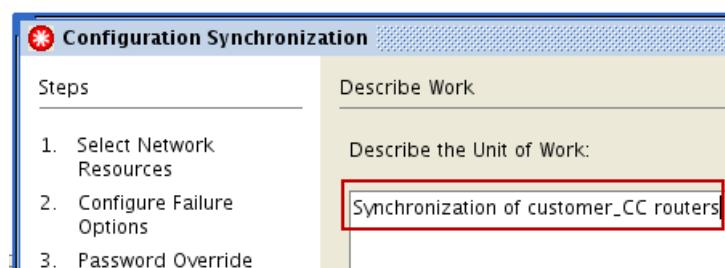
- f. Click **Next** in the Execution Priority window.



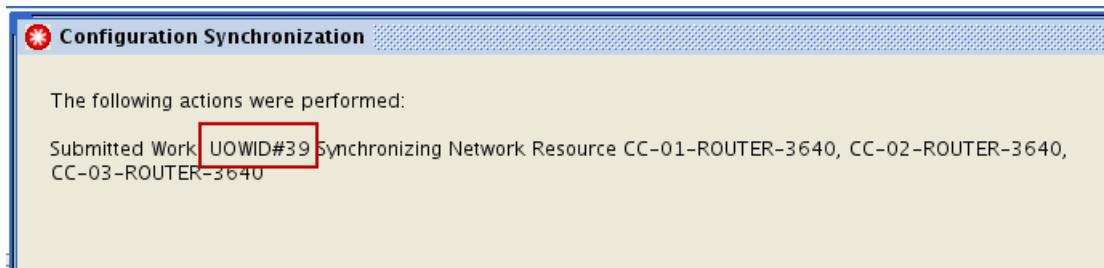
- g. Click **Scheduled** in the Schedule Work window. Change the scheduled start and end times to 1 hour from the current time.



- h. Enter **Synchronization of customer_CC routers** in the Describe Work window. Click **Finish**.

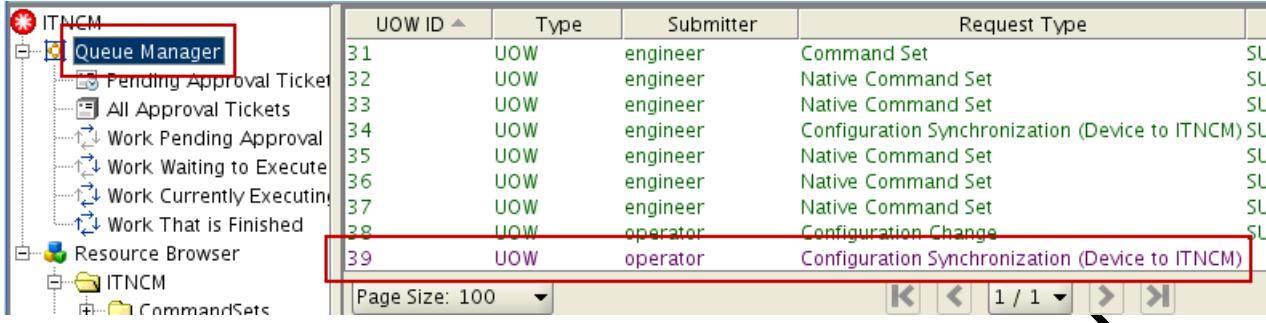


- i. Note the unit of work number and click **Close**.

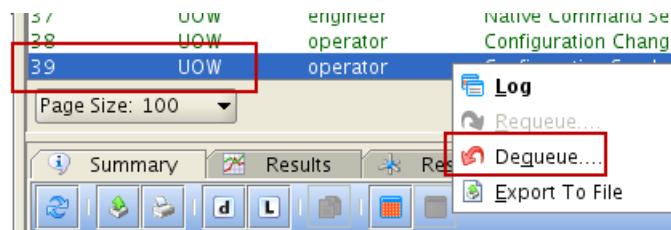


6. Stop (Dequeue) the unit of work that synchronizes the configuration of the customer_CC routers. Enter **change of schedule** as the reason for unit of work dequeue.

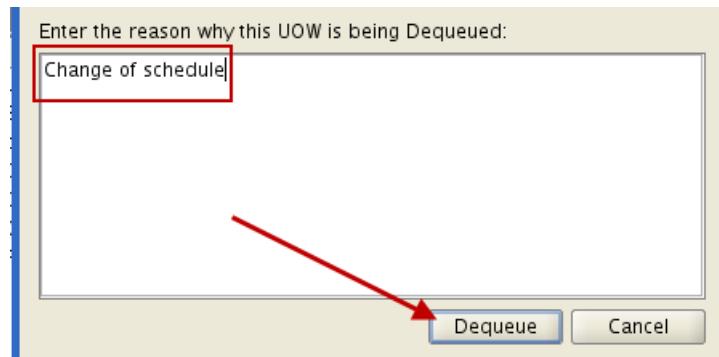
 - a. Find the unit of work that synchronizes the configuration of the customer_CC routers. Click the *queue manager*. The most recent unit of work is the synchronization.



- b. Right-click the unit of work and click **Dequeue**.



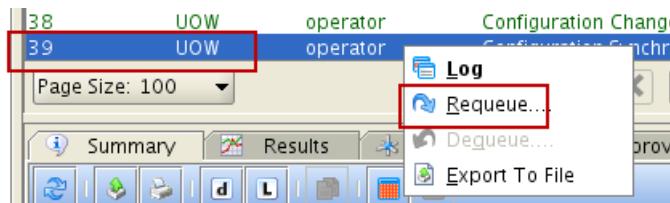
- c. Enter **Change of schedule** and click **Dequeue**.



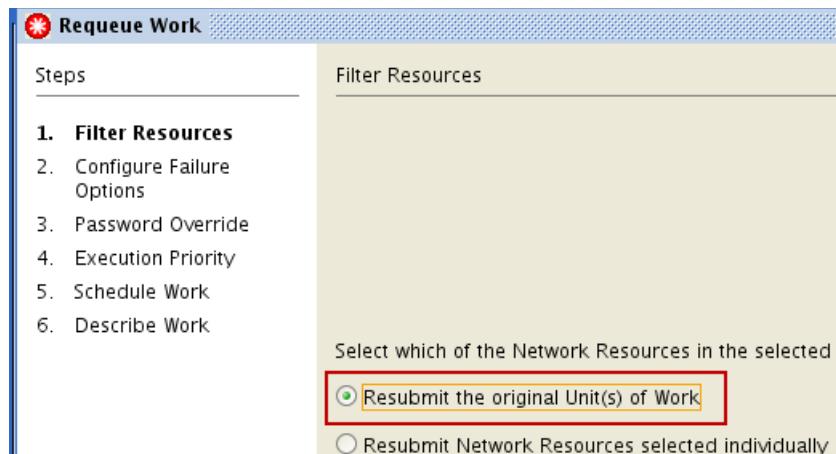
7. Requeue the unit of work. Use the following values to complete the wizard. Notice that the unit of work is requeued with a new ID.

Field	Value
Filter Resources	Resubmit the original Units of Work
Configure Failure Options	Ignore all errors
Password Override	Do not override
Execution Priority	Low
Schedule Work	Single Schedule > Immediate
Describe Work	Change of schedule

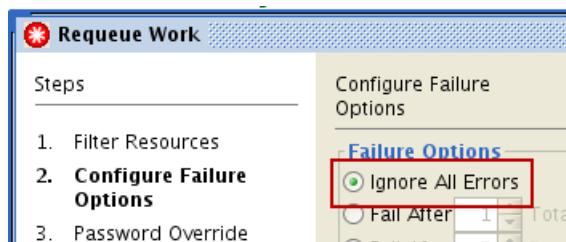
- a. Right-click the unit of work and click **Requeue**. The Requeue Work wizard starts.



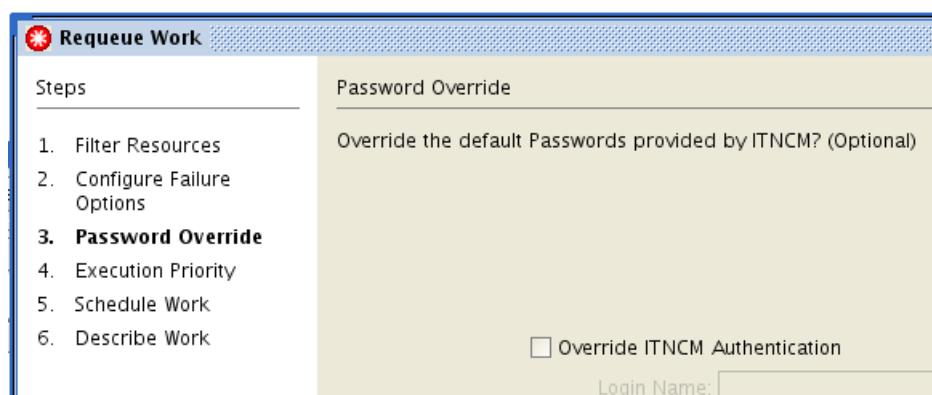
- b. Click **Resubmit the original Units of Work** in the Filter Resources window. Click **Next**.



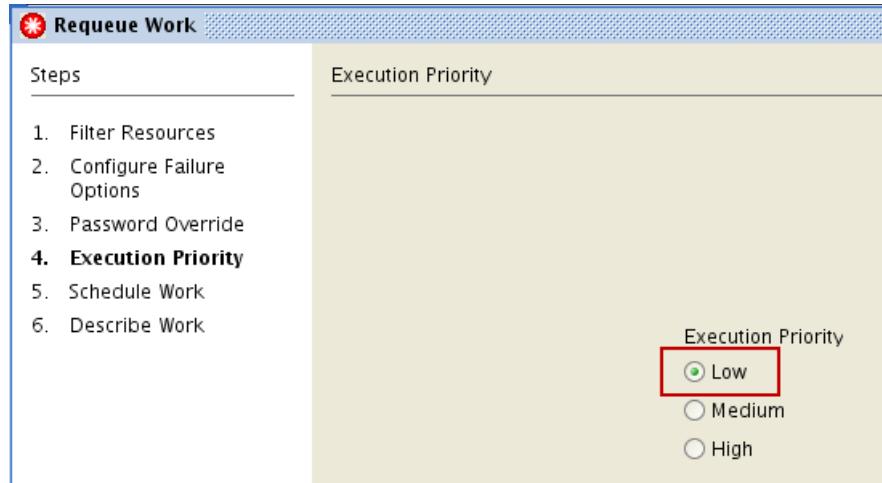
- c. Click **Next** in the Configure Failure Options window.



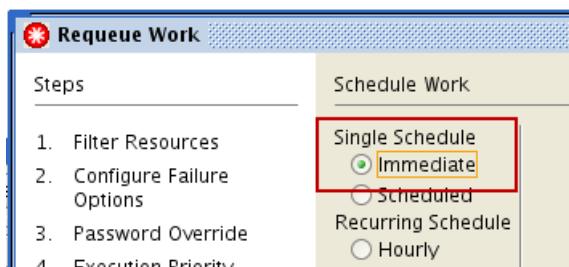
- d. Click **Next** in the Password Override window.



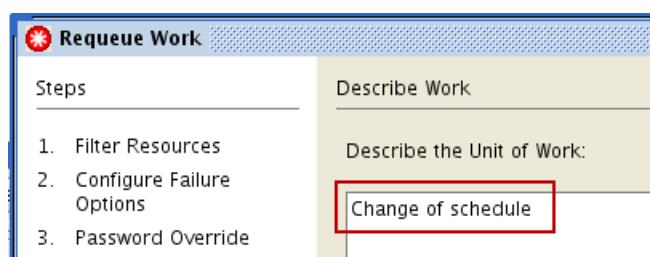
- e. Click **Next** in the Execution Priority window.



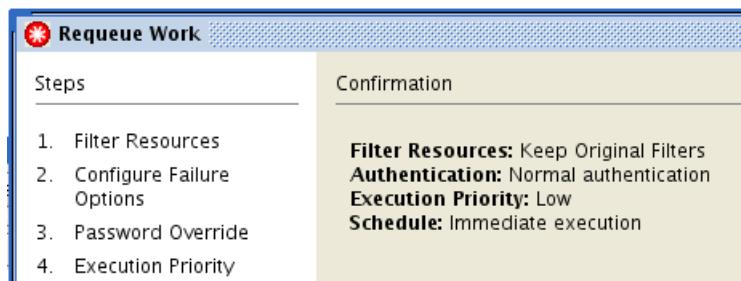
- f. Click **Single Schedule > Immediate** in the Schedule Work window. Click **Next**.



- g. Enter **Change of schedule** in the Describe Work window. Click **Next**.

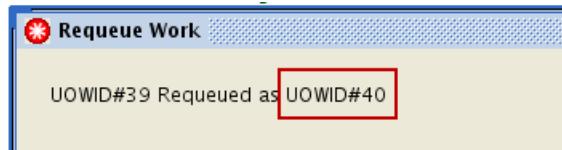


- h. Click **Finish** in the Confirmation window.



Notice that the unit of work is requeued by using a new ID.

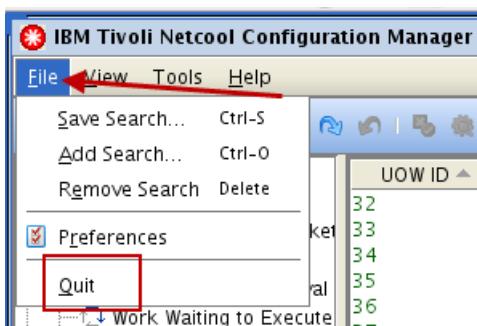
- Note the new unit of work number and click **Close**.



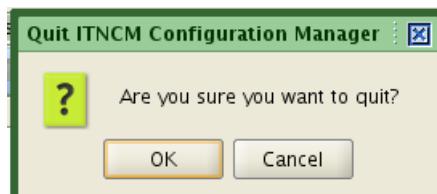
Exercise 2 Approving changes

In this exercise, you approve the changes that you made in the preceding exercise.

- Log out of the user interface and log in again with the user name **engineer**. The password is **object00**.
 - Click **File > Quit** to log out.



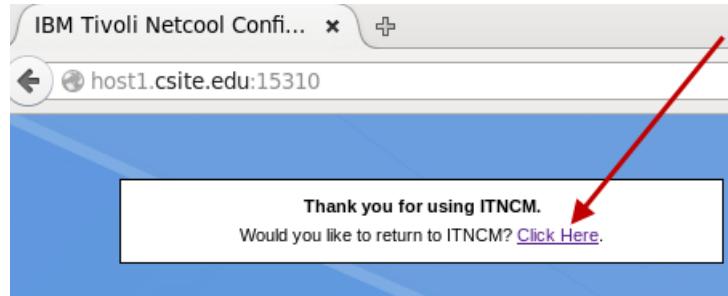
- Click **File > Quit** to log out. Click **OK** to quit.



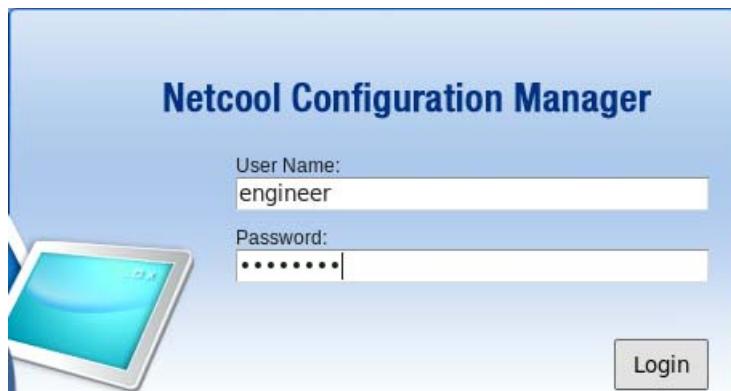
- Click **Logoff** to exit the configuration manager browser session.



3. Select **Click Here** to return to the browser login screen.



- a. Enter **engineer** and **object00** as the user name and password. Click **Login**.

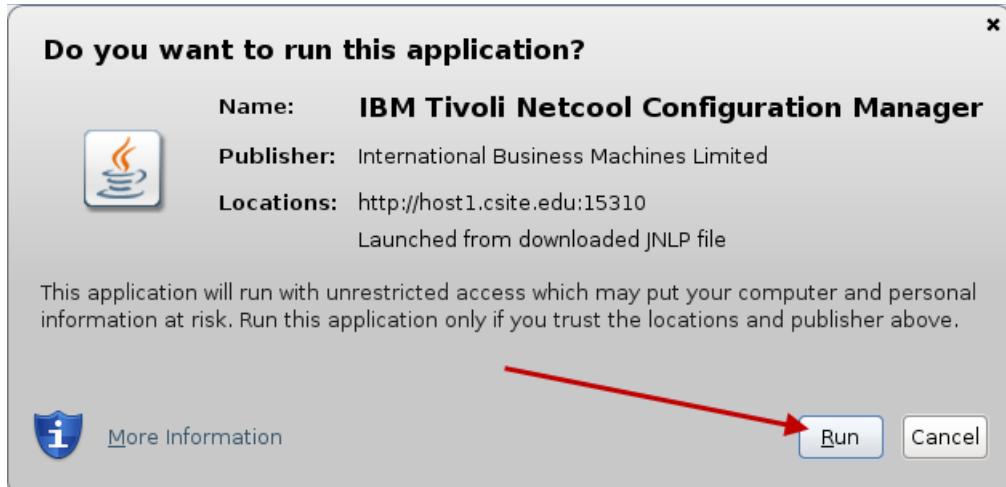


- b. Click **ITNCM Webstart GUI**.



The Java Webstart client starts.

- c. Click Run.

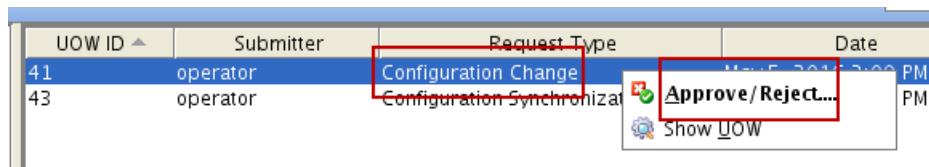


4. Approve the two units of work that you created as the **operator** user. Enter **Change approved** as the reason for approval.

- a. Click **Pending Approval Tickets** in the *queue manager*. The two approval tickets are shown in the queue table.

UOW ID	Submitter	Request Type
41	operator	Configuration Change
43	operator	Configuration Synchronization (Dev.)

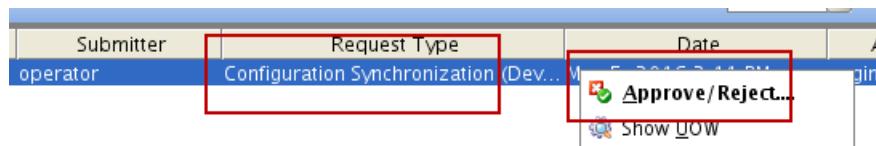
- b. Right-click the configuration change approval ticket. Click **Approve/Reject**.



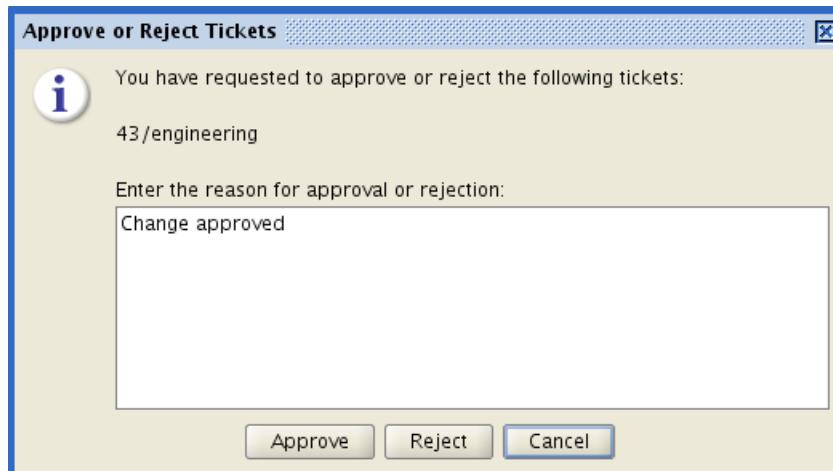
- c. Enter **Change approved** as the reason for approval. Click **Approve**.



- d. Right-click the synchronization approval ticket. Click **Approve/Reject**.



- e. Enter **Change approved** as the reason for approval. Click **Approve**.



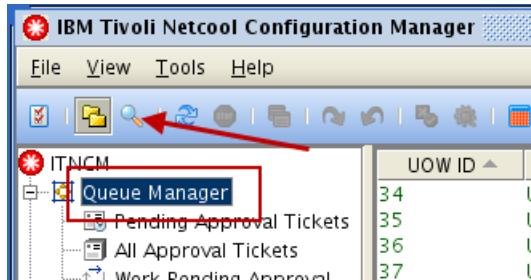
Exercise 3 Creating custom searches

In this exercise, you create two custom searches and add them to the *queue manager*.

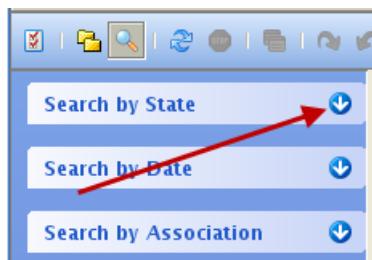
1. Use the values in the following table to create a custom search. The search shows *units of work* that were created 12 hours before and after the current time. Save the search when you finish.

Field	Value
State	All states
Date	12 hours before and after current time
Association	Group
Failure Categories	none
Name of the search	12 Hour Work
Realm to save the search in	ITNCM

- a. Click Queue Manager, and click the Show/Hide the Search Sidebar icon.



- b. Expand Search by State.



- c. Select Units of Work and verify that all states are selected.



- d. Expand Search by Date.



e. Select **Relative to Current Time** and enter **12 Hours** in the **Before** and **After** fields.



f. Expand **Search by Association**.



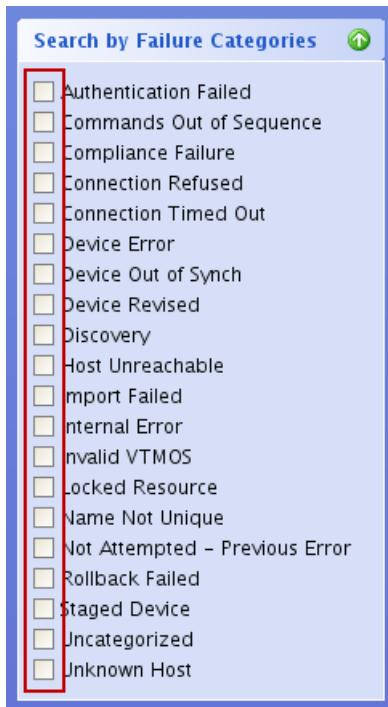
g. Select **Group**.



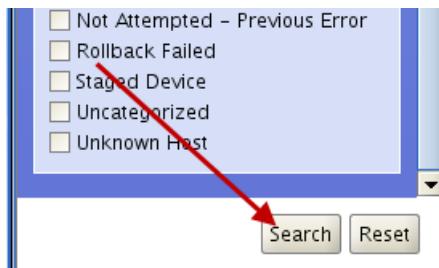
h. Expand **Search by Failure Categories**.



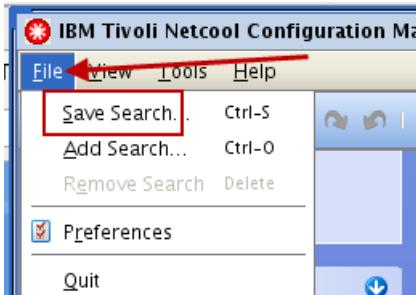
- i. Verify that all of the options are cleared.



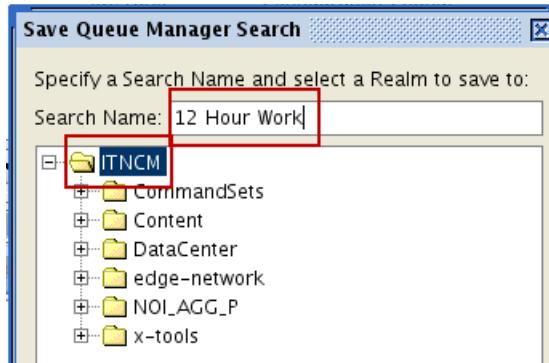
- j. Click **Search**.



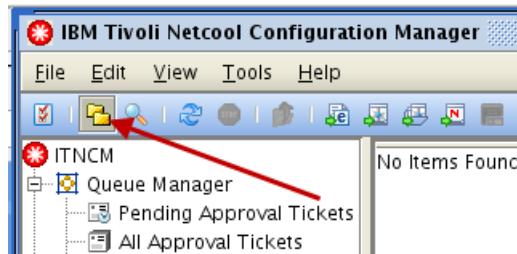
- k. Click **File > Save Search**.



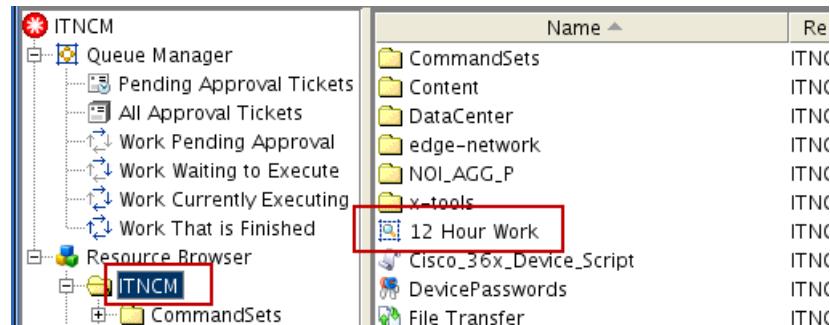
- I. Select the ITNCM realm and enter **12 Hour Work** in the **Search Name** field. Click **OK**.



- m. Click the Show/Hide the Navigation Tree icon.



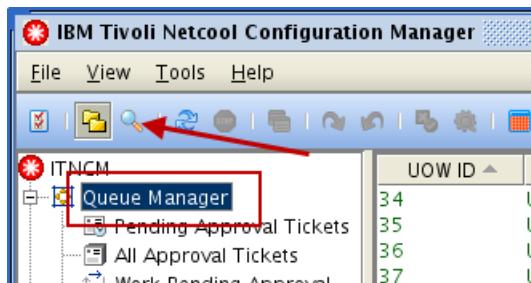
- n. Click **ITNCM** and verify that the **12 Hour Work** search is listed.



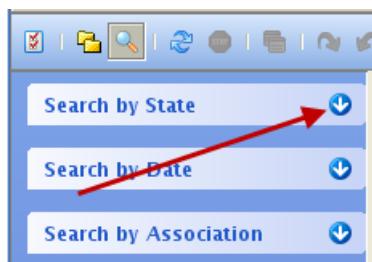
2. Use the values in the following table to create a custom search. The search shows *units of work* that were created 36 hours before and after the current time. Save the search when you finish.

Field	Value
State	All states
Date	36 hours before and after current time
Association	Group
Failure Categories	none
Name of the search	36 Hour Work
Realm to save the search in	ITNCM

- a. Click Queue Manager, and click the Show/Hide the Search Sidebar icon.



- b. Expand Search by State.



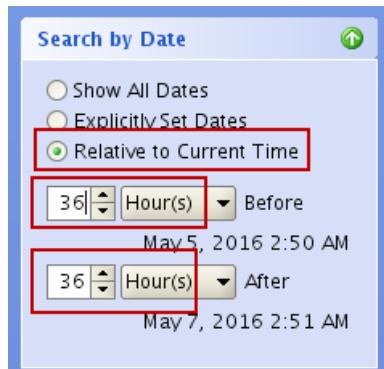
- c. Select Units of Work and verify that all states are selected.



- d. Expand Search by Date.



- e. Select **Relative to Current Time** and enter **36 Hours** in the **Before** and **After** fields.



- f. Expand **Search by Association**.



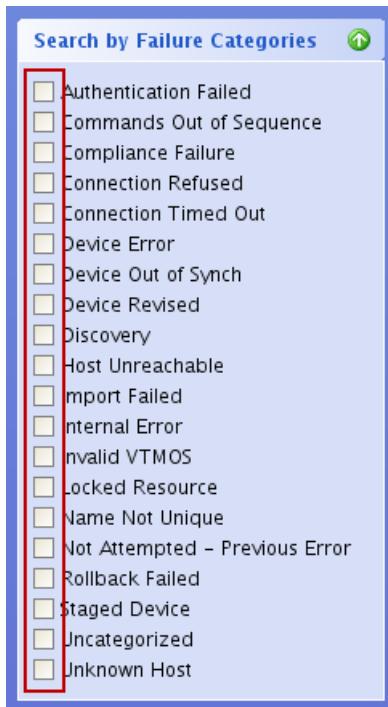
- g. Select **Group**.



- h. Expand **Search by Failure Categories**.



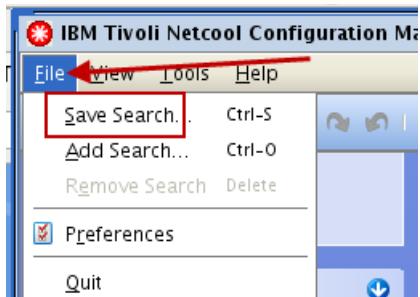
- i. Verify that all of the options are cleared.



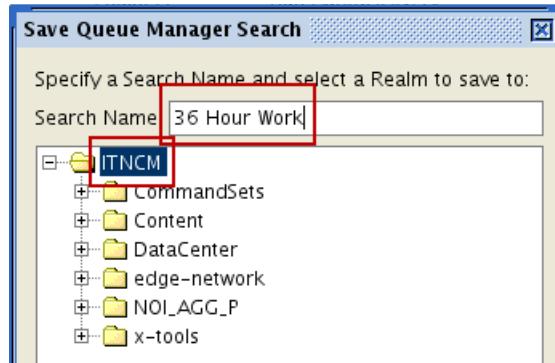
- j. Click **Search**.



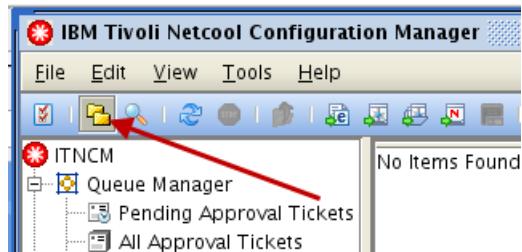
- k. Click **File > Save Search**.



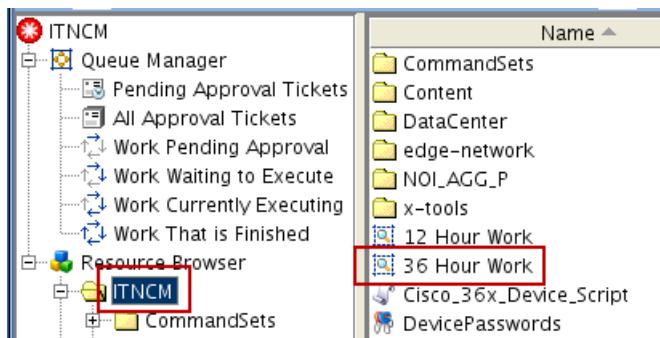
- I. Select the ITNCM realm and enter **36 Hour Work** in the **Search Name** field. Click **OK**.



- m. Click the Show/Hide the Navigation Tree icon.

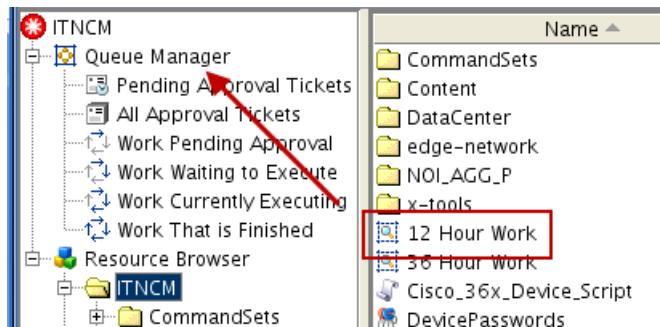


- n. Click **ITNCM** and verify that the **36 Hour Work** search is listed.

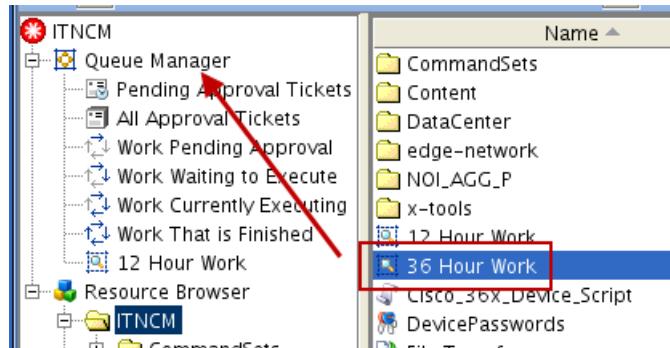


3. Add the two new custom searches to the *queue manager*.

- a. Click the **12 Hour Work** search and drag it to the *queue manager*.



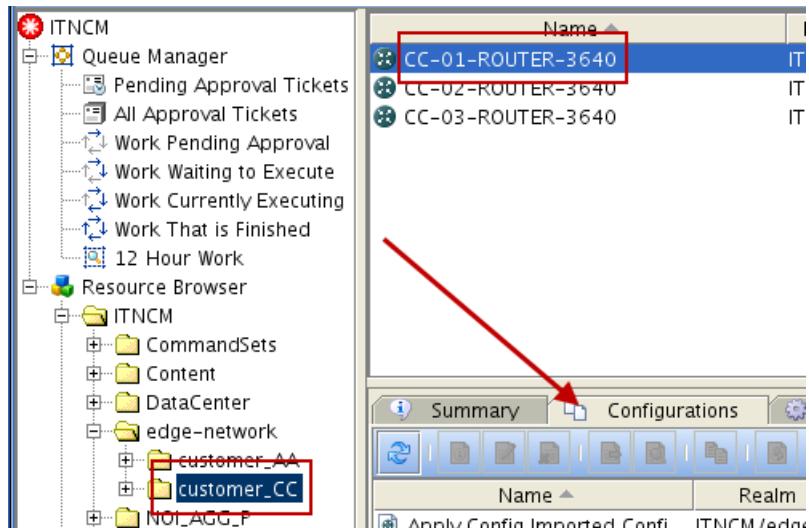
- b. Click the **36 Hour Work** search and drag it to the *queue manager*.



Exercise 4 Comparing configurations

In this exercise, you compare device configurations.

1. Compare the current and the oldest configurations of the CC-01-ROUTER-3640 device.
Compare the configurations in native view.
 - a. Find the CC-01-ROUTER-3640 device in the *resource browser*. Click the **CC-01-ROUTER-3640** device and click the **Configurations** tab.



- a. Click the **Modified At** column heading to sort the list in descending sequence by modification time.

Modified By	Modified At	Vendor	Type	Model	OS
operator	May 5, 2016 2:22 PM	Cisco	Router	3640	C3640-I-M-1... Cur
operator	May 5, 2016 2:09 PM	Cisco	Router	3640	C3640-I-M-1... Loc
operator	May 5, 2016 1:44 PM	Cisco	Router	3640	C3640-I-M-1... Ver
operator	May 5, 2016 12:58 PM	Cisco	Router	3640	C3640-I-M-1... Loc
engineer	May 4, 2016 8:14 PM	Cisco	Router	3640	C3640-I-M-1... Ver
operator	May 4, 2016 8:13 PM	Cisco	Router	3640	C3640-I-M-1... Ver

- c. Select the current configuration and the oldest configuration. Right-click the configurations and click **Show Differences**.

Name	Realm	Modified By	Modified At	Vendor	Type	Model
Apply Config Imported Confi...	ITNCM/edge...	operator	May 05, 2016 2:22 PM	Cisco	Router	3640 C3
iomem_25_2	ITNCM/edge...	op			Router	3640 C3
Apply Config Imported Confi...	ITNCM/edge...	op			Router	3640 C3
iomem_25	ITNCM/edge...	op			Router	3640 C3
Native command set Modifie...	ITNCM/edge...	en			Router	3640 C3
Native command set Modifie...	ITNCM/edge...	en			Router	3640 C3
Native command set Modifie...	ITNCM/edge...	en			Router	3640 C3
Command Set Modified Conf...	ITNCM/edge...	en			Router	3640 C3
Apply Config Imported Confi...	ITNCM/edge...	en			Router	3640 C3
hostname and banner	ITNCM/edge...	en			Router	3640 C3
Imported Configuration	ITNCM/edge...	en			Router	3640 C3
Imported Configuration	ITNCM/edge...	en			Router	3640 C3

- d. Select **Native View** and click **Finish**.

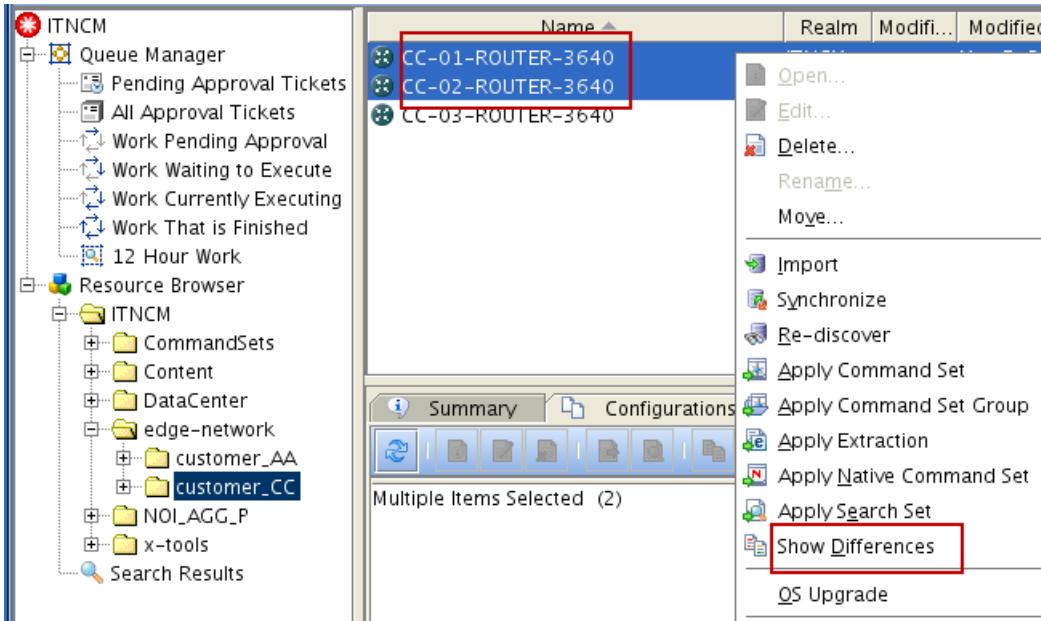


- e. Scroll down to view the differences in the configurations.

Left (Imported Configuration)	Right (Current Configuration)
1 version 12.3	1 version 12.3
2 service timestamps debug datetime msec	2 service timestamps debug datetime msec
3 service timestamps log datetime msec	3 service timestamps log datetime msec
4 no service password-encryption	4 no service password-encryption
5 !	5 !
6 hostname Router	6 hostname cc-01-router-3640
7 !	7 !
8 boot-start-marker	8 boot-start-marker
9 boot-end-marker	9 boot-end-marker
10 !	10 !
11 no logging console	11 no logging console
12 enable secret 5 \$1\$TXVP\$9wwXnF4/IkK9p83E9.Vr	12 enable secret 5 \$1\$TXVP\$9wwXnF4/IkK9p83E9.Vr
13 !	13 !
14 username intelliden password 0 p4ssw0rd	14 username intelliden password 0 p4ssw0rd
15 aaa new-model	15 aaa new-model
16 !	16 !
17 !	17 !
18 aaa session-id common	18 aaa session-id common
19 ip subnet-zero	19 ip subnet-zero
20 !	20 !
	21 ip subnet-zero
	22 !

2. Close the differences window when complete.

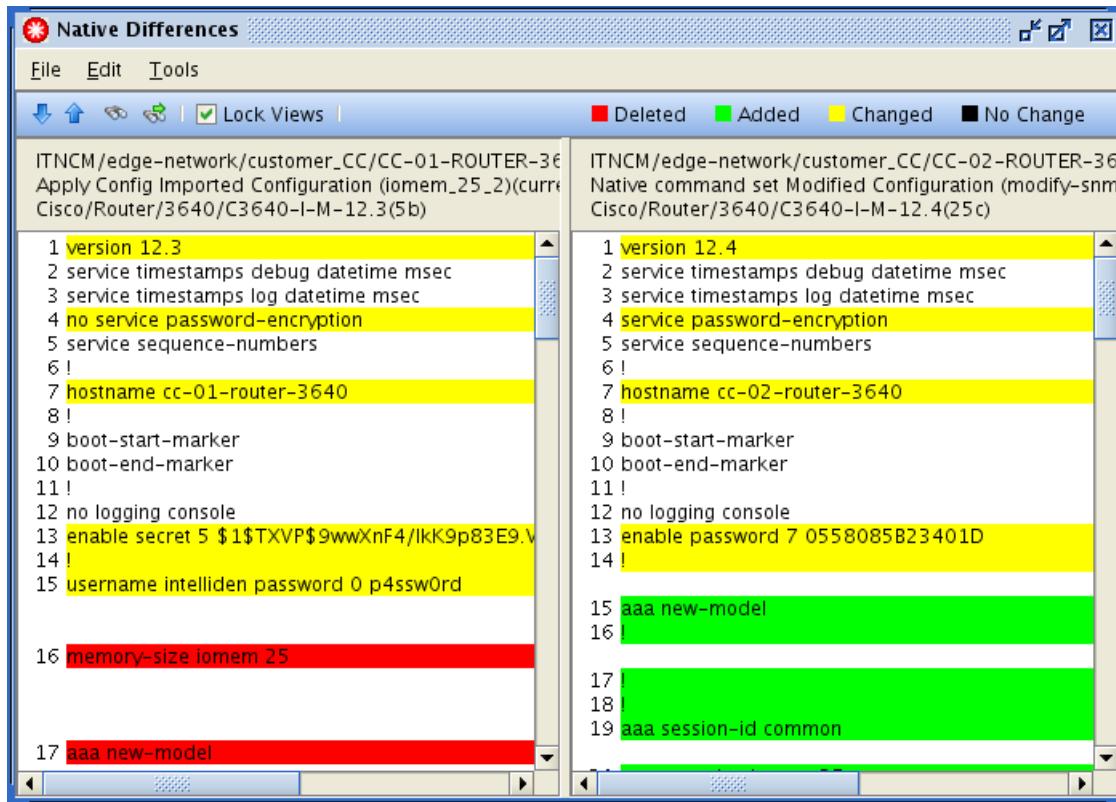
3. Compare the current configurations of the CC-01-ROUTER-3640 and CC-02-ROUTER-3640 devices. Compare the configurations in native view.
- a. Select the **CC-01-ROUTER-3640** and **CC-02-ROUTER-3640** devices in the *resource browser*. Right-click the devices and click **Show Differences**.



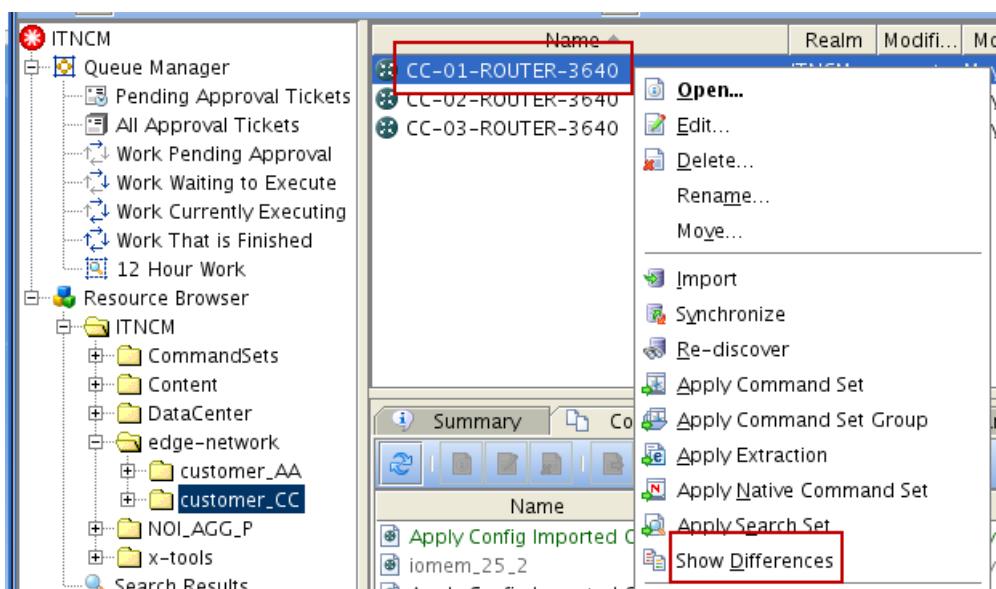
- b. Select **Native View** and click **Finish**.



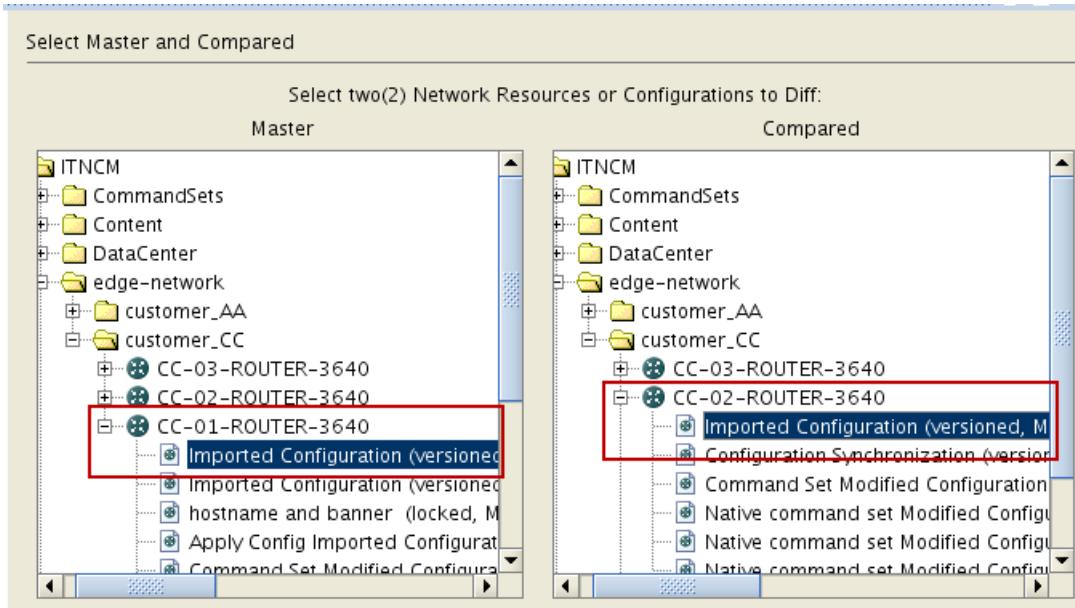
- c. Scroll down to view the differences in the configurations.



- Close the differences window when complete.
- Compare the oldest configurations of the CC-01-ROUTER-3640 and CC-02-ROUTER-3640 devices. Compare the configurations in modeled view.
 - Find the CC-01-ROUTER-3640 device in the *resource browser*. Right-click the **CC-01-ROUTER-3640** device and click **Show Differences**. The Show Differences wizard starts.



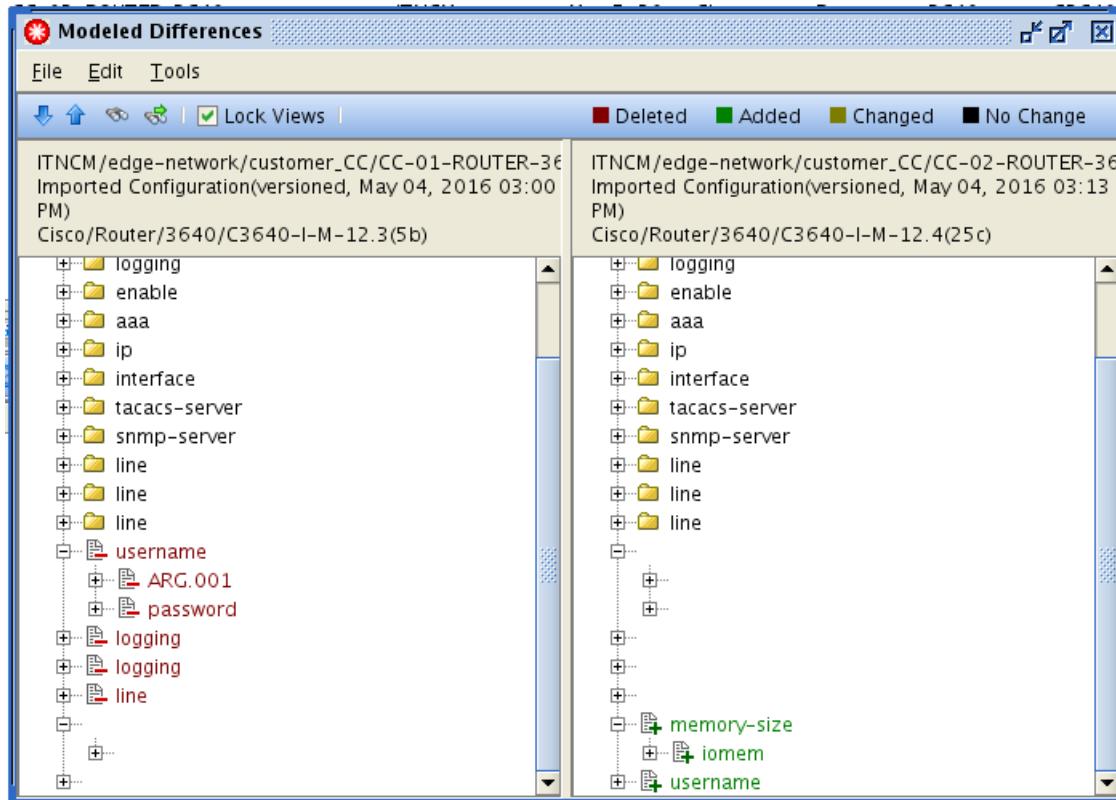
- b. Expand the **CC-01-ROUTER-3640** device and click the oldest configuration in the **Master** area. Expand the **CC-02-ROUTER-3640** device and click the oldest configuration in the **Compared** area. Click **Next**.



- c. Click **Finish** in the View of Report window.



- d. Scroll down to view the differences in the configurations.



6. Close the differences window when complete.
7. Close the configuration manager user interface.
8. Click **Logoff** to exit the configuration manager browser session.

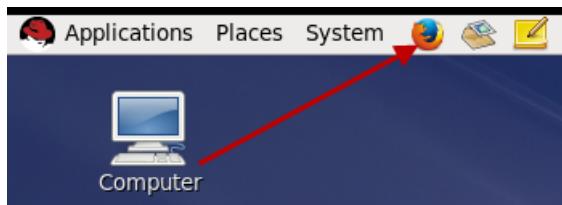


9. Close the Firefox browser.

Exercise 5 Running reports

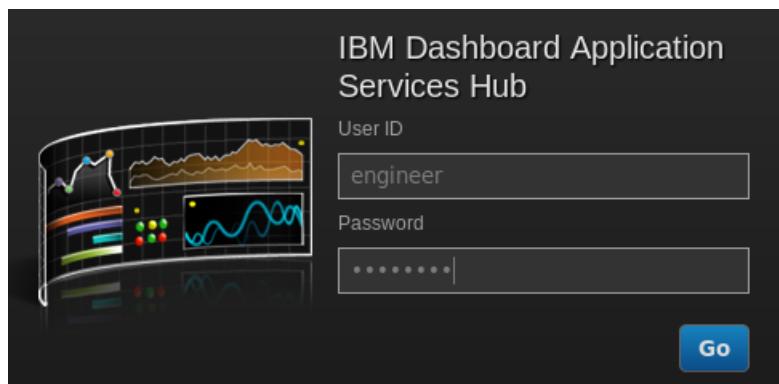
In this exercise, you use the web interface to run reports.

1. Open Firefox browser.



The default home page is Dashboard Application Services Hub.

2. Log in as **engineer** and **object00** as the password.



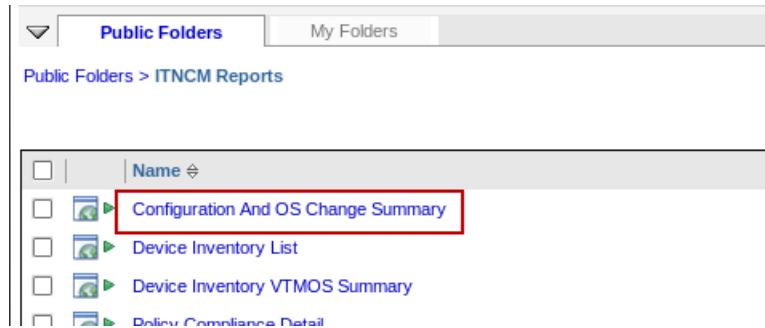
3. Click the icon and select **Common Reporting**.



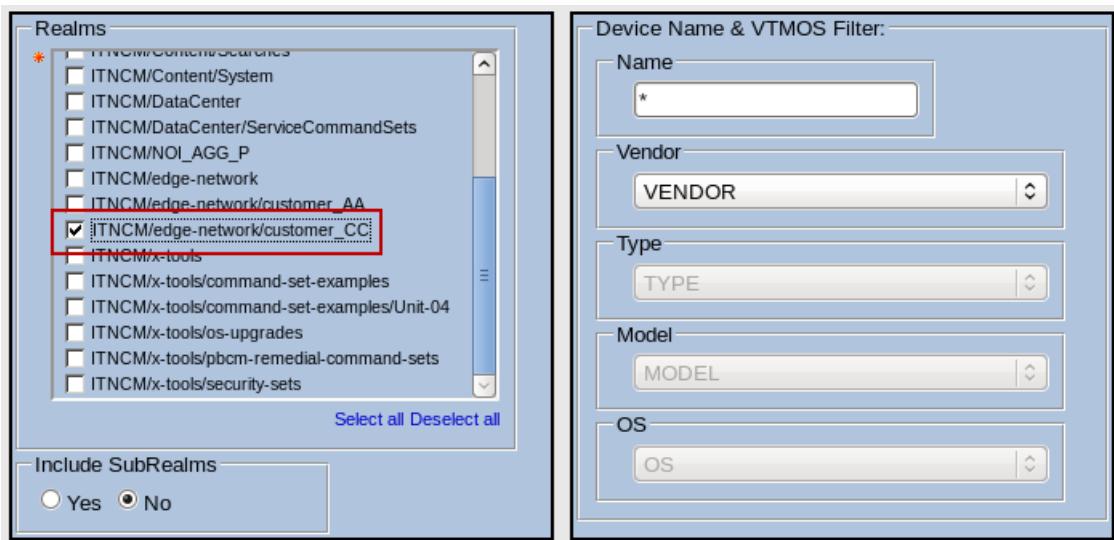
4. Click **ITNCM Reports**.



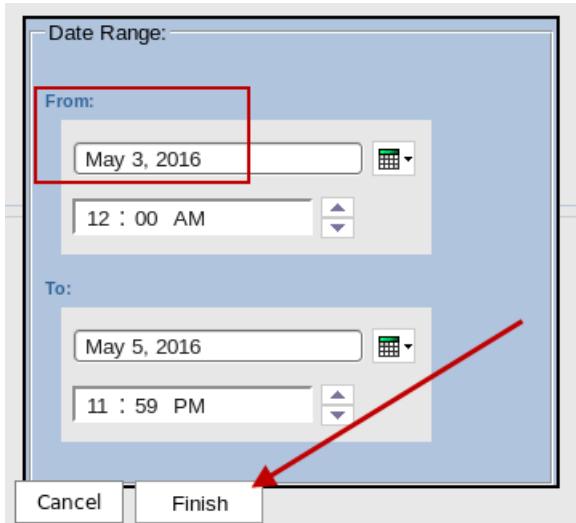
5. Run a Configuration and OS Change Summary report. Run the report for all types of work on all devices in the **ITNCM/edge-network/customer_CC** realm. Select a **From** date that is a few days in the past.
- a. Click the **Configuration And OS Change Summary** report.



- b. Select the **ITNCM/edge-network/customer_CC** realm.



- c. Set the **From** date to two days in the past. Click **Finish**.



- d. View the report.

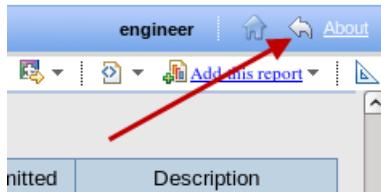
Request Type: Command Set

UOW Id	Device	Vendor	Type	Model	OS	Status	UOW Result	Task Result
31	CC-01-ROUTER-3640	Cisco	Router	3640	C3640-I-M-12.3(5b)	Finished	SUCCESS	SUCCESS
31	CC-02-ROUTER-3640	Cisco	Router	3640	C3640-I-M-12.4(25c)	Finished	SUCCESS	SUCCESS
31	CC-03-ROUTER-3640	Cisco	Router	3640	C3640-IK9S-M-12.4(25c)	Finished	SUCCESS	SUCCESS
Record Count	3							

Request Type: Configuration Change

UOW Id	Device	Vendor	Type	Model	OS	Status	UOW Result	Task Result
28	CC-01-ROUTER-3640	Cisco	Router	3640	C3640-I-M-12.3(5b)	Finished	SUCCESS	SUCCESS
38	CC-01-ROUTER-3640	Cisco	Router	3640	C3640-I-M-12.3(5b)	Finished	SUCCESS	SUCCESS
41	CC-01-ROUTER-3640	Cisco	Router	3640	C3640-I-M-12.3(5b)	Finished	SUCCESS	SUCCESS

- e. Close the report page when you finish by clicking the return icon.



6. Run a Device Inventory VTMOS Summary report. Run the report for all devices in the **ITNCM/edge-network/customer_CC** realm.

- a. Click **Device Inventory VTMOS Summary** report.

Public Folders My Folders

Public Folders > ITNCM Reports

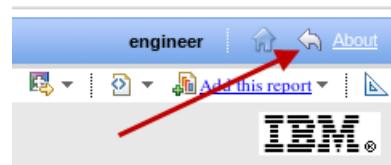
	Name
<input type="checkbox"/>	Configuration And OS Change Summary
<input type="checkbox"/>	Device Inventory List
<input type="checkbox"/>	Device Inventory VTMOS Summary
<input type="checkbox"/>	Policy Compliance Detail

- b. Select the **ITNCM/edge-network/customer_CC** realm. Click **Finish**.

- c. View the report.

Vendor	Device Type	Model	OS
Cisco	Router	3640	C3640-I-M-12.3(5b)
			C3640-I-M-12.4(25c)
			C3640-IK9S-M-12.4(25c)
	Device Count For OS ->		3
Device Count For Model,OS ->		1	3
Device Count For Type,Mode,OS ->		1	3
Total Device Count For Vendor ->			3
Total Vendors		1	
Total Device Inventory		3	

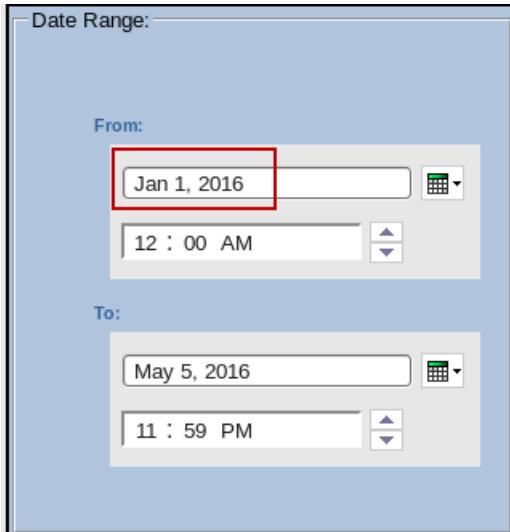
- d. Close the report page when you finish by clicking the return icon.



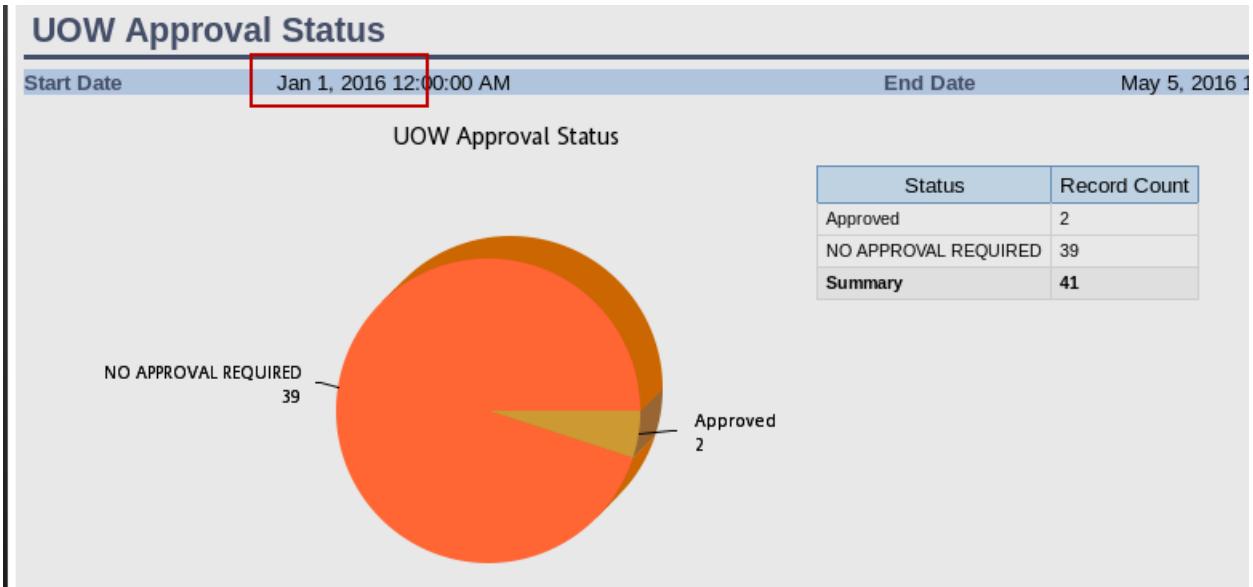
7. Run a UOW Approval Status report with a date range that goes back to January of 2016.

- a. Click **UOW Approval Status** report.

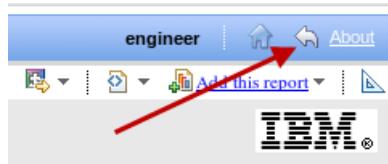
- b. Set the **From** date to Jan 1, 2016 and click **Finish**.



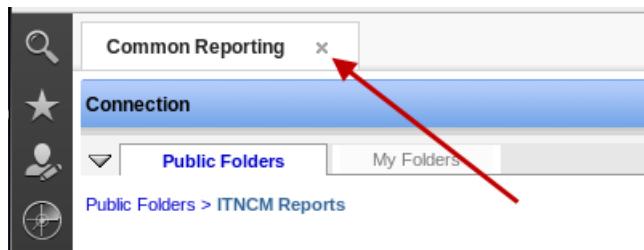
- c. View the report.



- d. Close the report page when you finish by clicking the return icon.



- e. Click the X to close the Common Reporting page.



Leave the browser session as is. You return to it shortly.



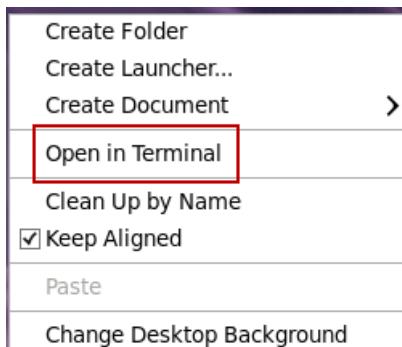
6 Netcool integrations exercises

In this unit, you learn about the integration between Netcool Configuration Manager, Netcool/OMNibus, and Network Manager.

Exercise 1 Verifying the component status

In this exercise, you verify the status of Netcool/OMNibus and Network Manager components.

1. Right-click the desktop and click **Open In Terminal**.



2. Verify the status of Netcool/OMNibus components with the following command:

```
nco_pa_status -server HOST1_PA -password object00
```

```
netcool@host1:~/Desktop
File Edit View Search Terminal Help
[netcool@host1 Desktop]$ nco_pa_status -server HOST1_PA -password object00
-----
Service Name      Process Name      Hostname   User       Status      PID
Core              MasterObjectServer host1.csuite.edunetcool  RUNNING    2469
                  SnmpProbe        host1.csuite.eduroot    RUNNING    2574
InactiveProcesses          ARCHIVEGateway host1.csuite.edunetcool  DEAD        0
                          LogAnalysisGateway host1.csuite.edunetcool  DEAD        0
                          SyslogProbe      host1.csuite.edunetcool  DEAD        0
                          SimnetProbe     host1.csuite.edunetcool  DEAD        0
```

The MasterObjectServer and SnmpProbe processes must be running.

3. Verify the status of the Network Manager components with the following command:

```
itnm_status
```

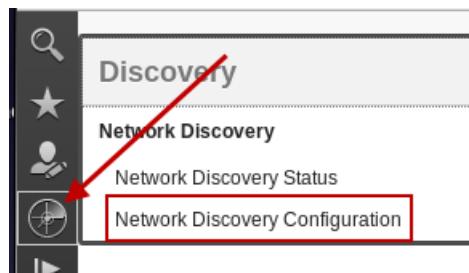
```
netcool@host1:~/Desktop
File Edit View Search Terminal Help
[netcool@host1 Desktop]$ itnm_status
Network Manager:
Domain: NOI_AGG_P
  ncp_ctrl          RUNNING  PID=3161  NOI_AGG_P
  ncp_store         RUNNING  PID=4160  NOI_AGG_P
  ncp_class         RUNNING  PID=4161  NOI_AGG_P
  ncp_model         RUNNING  PID=4990  NOI_AGG_P
  ncp_disco         RUNNING  PID=6745  NOI_AGG_P
  ncp_d_helpserv   RUNNING  PID=4162  NOI_AGG_P
  ncp_config        RUNNING  PID=4163  NOI_AGG_P
  ncp_poller_default RUNNING  PID=7306  NOI_AGG_P
  ncp_poller_admin  RUNNING  PID=7307  NOI_AGG_P
  nco_p_ncpmonitor RUNNING  PID=4164  NOI_AGG_P
  ncp_g_event       RUNNING  PID=6989  NOI_AGG_P
  ncp_webtool       RUNNING  PID=4165  NOI_AGG_P
  ncp_virtualdomain RUNNING  PID=7839  NOI_AGG_P
Apache Storm:
  supervisord       RUNNING  PID=4316
  storm_nimbus      RUNNING  PID=4325
  storm_supervisor  RUNNING  PID=4326
  zookeeper         RUNNING  PID=4324
Storm topologies:
  NMstormTopology   ACTIVE
```

All processes must be running.

Exercise 2 Discovering devices with Network Manager

You are currently logged in to Dashboard Application Services Hub as the **engineer** user. The engineer user is configured with access to Network Manager features. In this exercise, you discover the simulated routers with Network Manager.

1. Click the icon and select **Network Discovery Configuration**.



2. Examine the defined subnet.

Select	#	Address	Netmask
<input type="checkbox"/>	1	10.191.101.0	24

The subnet for the simulated routers is already defined.

3. Click the X to close the discovery configuration page.

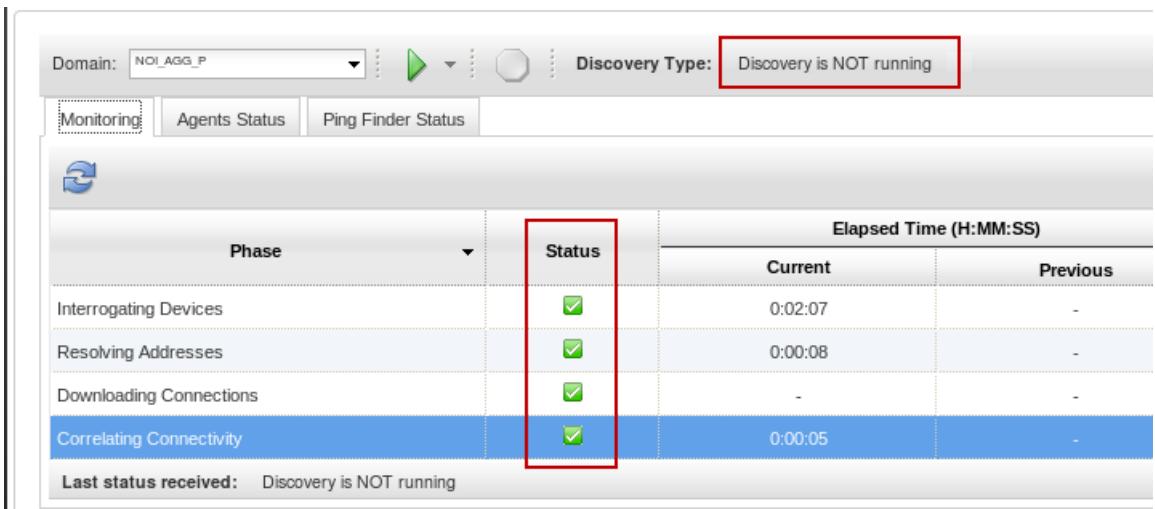
4. Click the icon and select Network Discovery Status.

5. Click the green arrow icon to start the discovery.

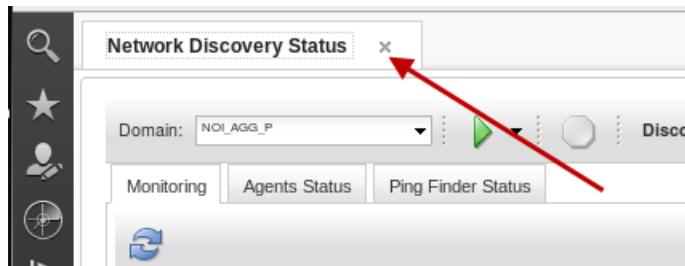
After a short time, the discovery starts.



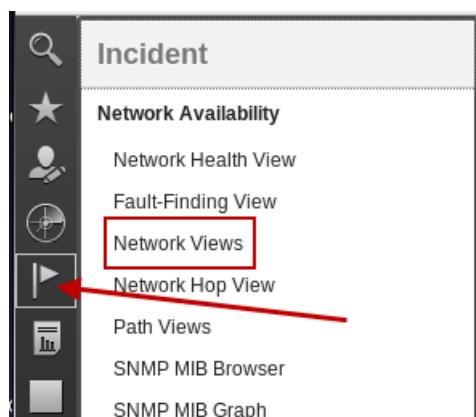
The discovery runs for approximately 2 minutes.



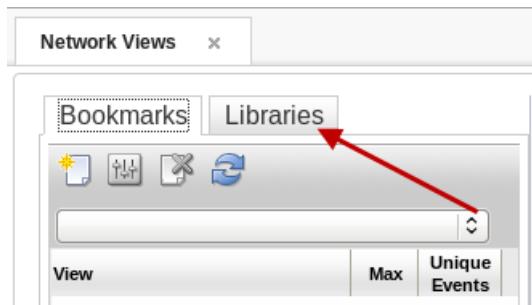
6. Click the X to close the discovery status page.



7. Click the icon and select Network Views.



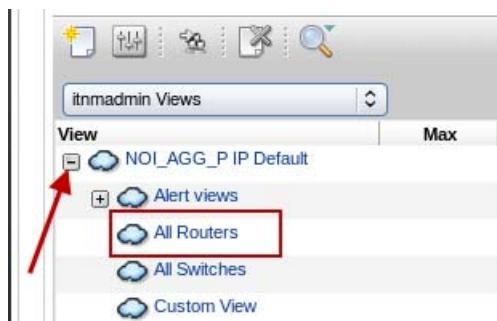
8. Click **Libraries**.



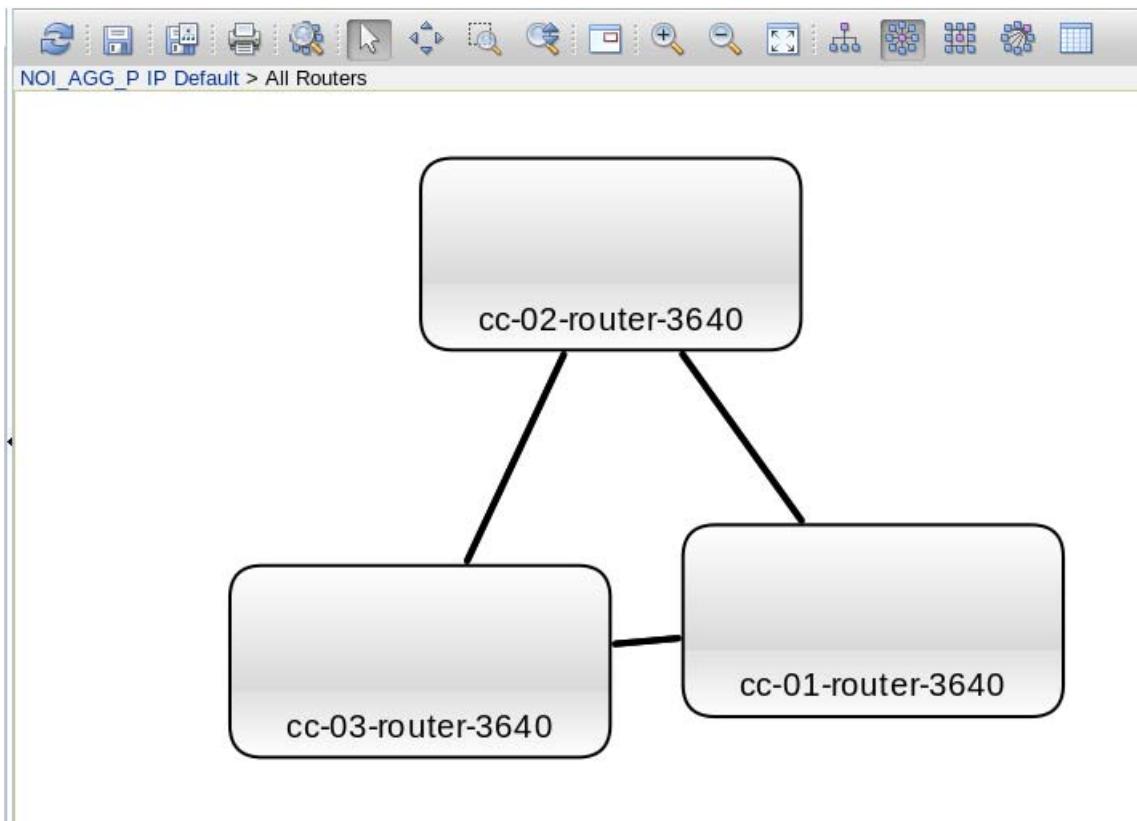
9. Click the arrow and select **itnmadmin Views**.



10. Expand the **NOI_AGG_P IP Default** container. Click **All Routers**.



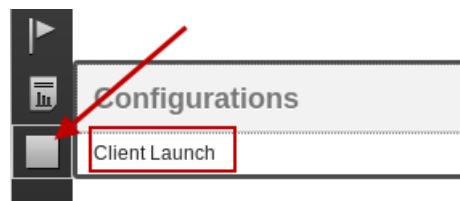
The network view contains the three simulated routers.



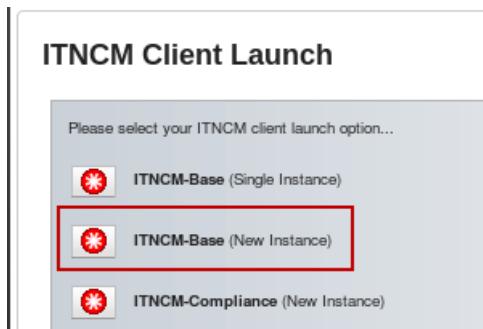
Exercise 3 Deleting customer CC devices

In this exercise, you remove the customer CC devices that you discovered in the previous exercises.

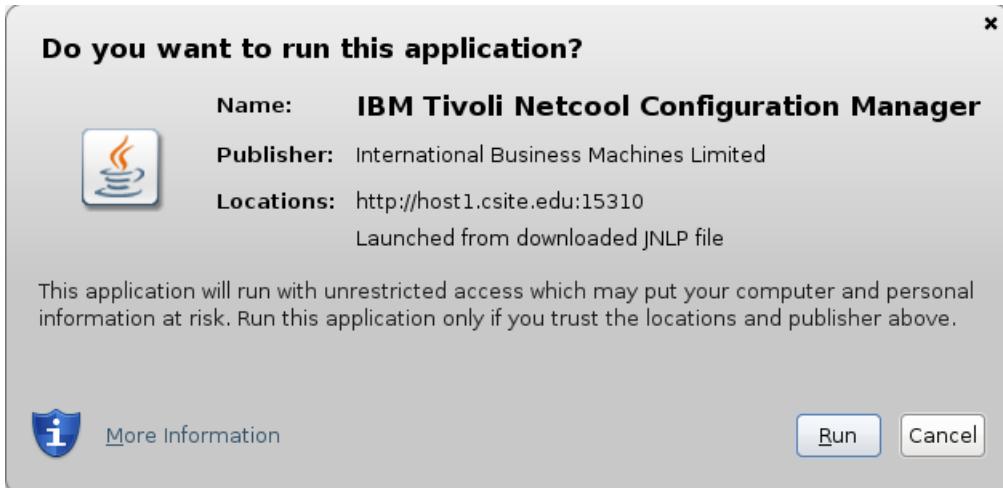
1. Start the Netcool Configuration Manager client from Dashboard Application Services Hub.
 - a. Click the icon and select **Client Launch**.



- b. Select **ITNCM-Base (New Instance)** to start a new Netcool Configuration Manager user interface client.

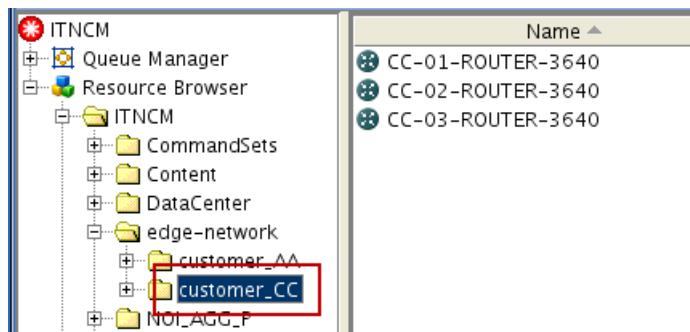


- c. Click **Run**.

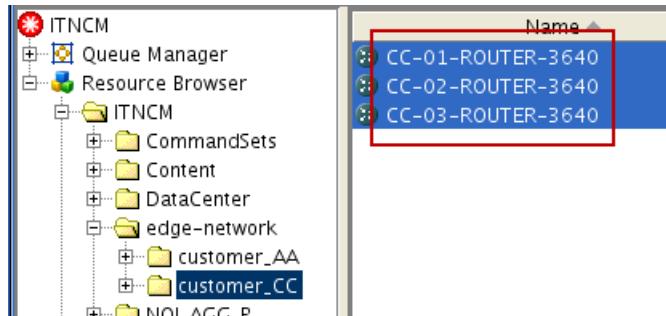


The Java Webstart client starts, connects to Netcool Configuration Manager and logs in as the **engineer** user.

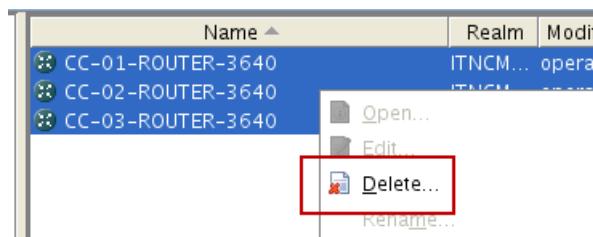
2. In the **Netcool Configuration Manager** interface, delete the three devices that you discovered in the Unit 3 exercises.
- a. Browse to the **ITNCM > edge-network > customer_CC realm**.



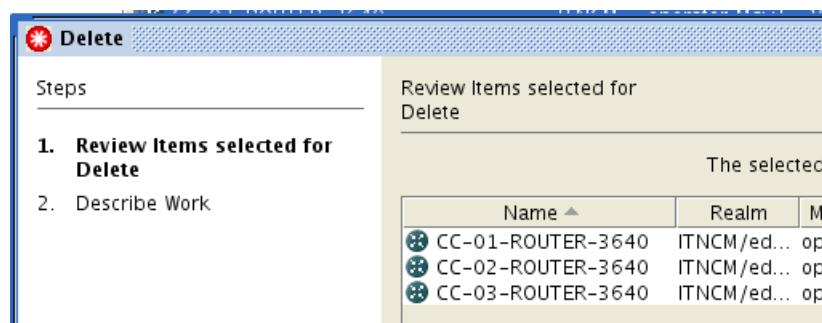
- b. Press and hold the Ctrl key to select the three devices in that realm.



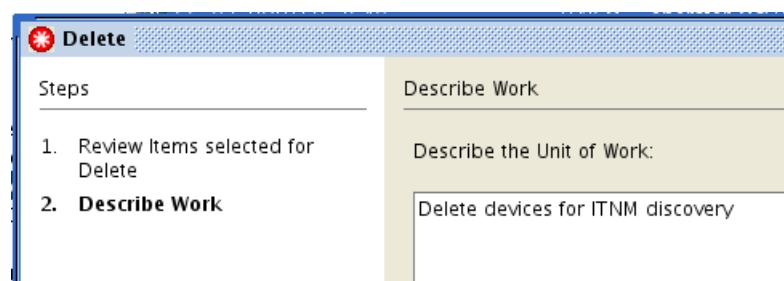
- c. Right-click the devices and click **Delete**.



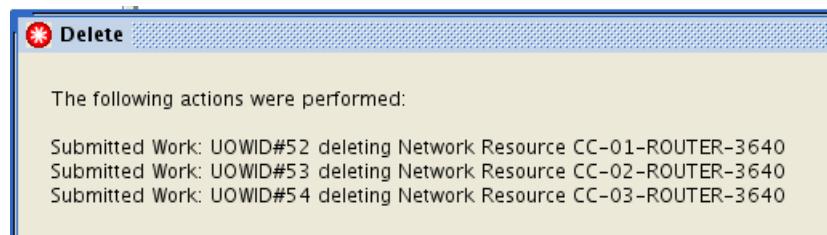
- d. Click **Next** in the Delete window.



- e. Enter the description **Delete devices for ITNM discovery** and click **Finish**.



- f. Click **Close** after the *units of work* are submitted.



Exercise 4 Verifying integration with Configuration Manager

Netcool Configuration Manager imports discovered devices periodically. The frequency of this import is configured in a property file.

1. Check the log file to verify the import.

- a. Change to the target directory.

```
cd /opt/IBM/ncm/logs
```

- b. Check the file.

```
tail Intelliden.log
```

```
.
```

```
.
```

```
.
```

```
2016/05/05,19:33:06.546,com.intelliden.nmentitymapping.NMEntityMappingCompon
ent$NMEntityMappingTimerTask,THR:72,WARN,NM Entity Mapping is running...
```

```
2016/05/05,19:33:06.675,com.intelliden.nmentitymapping.NMEntityMappingCompon
ent$NMEntityMappingTimerTask,THR:72,WARN,NM Entity Mapping returned 4
devices
```

This message indicates that Configuration Manager found four devices to import.



Important: You might need to repeat the tail command several times before the correct message appears.

2. Return to the configuration manager client.
3. Under Queue Manager, click **Work That is Finished**.

The screenshot shows the Queue Manager interface with the 'Work That is Finished' queue selected. The right pane displays a table of work items with the following data:

UOW ID	Type	Submitter	Request Type
37	UOW	operator	Configuration Change
38	UOW	operator	Configuration Synchronization
39	UOW	operator	Configuration Synchronization
40	UOW	administrator	Run Autodiscovery
41	UOW	administrator	Run Autodiscovery
42	UOW	administrator	Run Autodiscovery
43	UOW	administrator	Run Autodiscovery
44	UOW	administrator	Import Configuration
45	UOW	administrator	Import Configuration
46	UOW	administrator	Import Configuration



Important: The import process runs for several minutes. You might need to refresh the view several times before you see the appropriate units of work.

You see units of work that are labeled Run Autodiscovery, and other units of work that are labeled Import Configuration. When Tivoli Network Manager discovers the simulated routers, the IP addresses for the devices are added to a database table. Netcool Configuration Manager reads the addresses from the table and performs a discovery. For each discovered device, a unit of work is submitted to import the device configuration file.



Note: You see a unit of work for Autodiscovery with a FAILED status. Network Manager discovers four devices, but only three devices are routers. Netcool Configuration Manager receives all four devices addresses, but is not able to discover the device that is not a router.

4. Under Resource Browser, click NOI_AGG_P.

Name	Realm	Modified By	Modified At	Vendor	Type
10.191.101.126	ITNCM/NOI...	administrator	May 6, 2016...	Unknown	Router
cc-01-router-3640	ITNCM/NOI...	administrator	May 6, 2016...	Cisco	Router
cc-02-router-3640	ITNCM/NOI...	administrator	May 6, 2016...	Cisco	Router
cc-03-router-3640	ITNCM/NOI...	administrator	May 6, 2016...	Cisco	Router

Observe the entries for the imported routers. The device with address 10.191.101.126 is the GNS simulator UNIX image.



Important: You configure the realm that Configuration Manager uses for imported devices in a property file. In this example, the realm is defined as NOI_AGG_P. You can find the property file in the following location:

/opt/IBM/ncm/config/properties/rseries.properties

The following property setting defines the realm name:

NMEntityMappingComponent/importRealm=ITNCM/NOI_AGG_P

This file also defines the frequency for device imports. You define the frequency in minutes with the following property setting:

NMEntityMappingComponent/period=5

5. Click any entry to select it. Click the **Configurations** tab.

The screenshot shows the IBM Tivoli Netcool/OMNibus interface. On the left is a tree view of resources under 'ITNCM'. In the center, there are two tables. The top table is titled 'Configurations' and lists three entries: 'cc-01-router-3640', 'cc-02-router-3640', and 'cc-03-router-3640'. A red box highlights the first entry, 'cc-01-router-3640'. The bottom table is titled 'Imported Configuration' and lists one entry: 'Imported Configuration'. A red box highlights this entry. A red arrow points from the text in step 5 to the 'Configurations' tab at the bottom of the interface.

Name	Realm	Modified By	Modified At	Version
cc-01-router-3640	ITNCM/...	adminis...	May 6, 2016	Cisco
cc-02-router-3640	ITNCM/...	adminis...	May 6, 2016	Cisco
cc-03-router-3640	ITNCM/...	adminis...	May 6, 2016	Cisco

Name	Realm	Modified By	Modified At
Imported Configuration	ITNCM/NOI_...	administr...	May 6, 2016

The entry in the bottom view represents the configuration for the selected device.

6. Verify that traps are captured in Netcool/OMNibus from the *units of work*.

- a. Click the icon, and select **Event Viewer**.

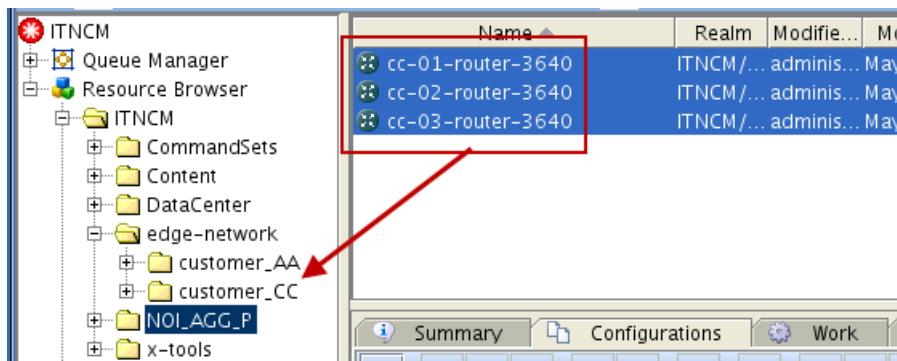
The screenshot shows the IBM Tivoli Netcool/OMNibus interface. On the left is a sidebar with various icons. One icon, which looks like a play button, is highlighted with a red box and has a red arrow pointing to it from the text in step 6a. To the right of the sidebar is a main panel titled 'Incident'. It contains sections for 'Network Availability' (with options like 'Network Health View', 'Fault-Finding View', 'Network Views', 'Network Hop View', 'Path Views', 'SNMP MIB Browser', 'SNMP MIB Graph', and 'Network Health Dashboard') and 'Events' (with options like 'Event Dashboard', 'Event Viewer', and 'Active Event List (AEL)'). The 'Event Viewer' option is also highlighted with a red box.

b. Observe the events.

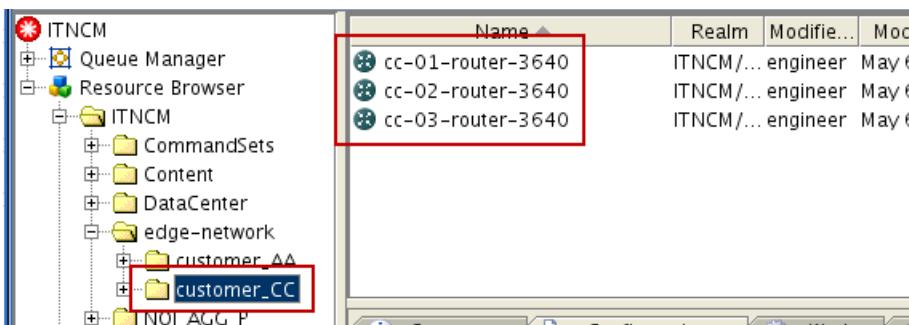
Event Viewer				
Sev	Ack	Node	Alert Group	Summary
Info	No	192.168.100.100	UOW trap	Import UOW '23' submitted by engineer is executing (1076836236) 124 days, 1 hr ago
Info	No	192.168.100.100	UOW trap	Import UOW '27' submitted by engineer is executing (1076840251) 124 days, 1 hr ago
Info	No	192.168.100.100	Resource Event	Manage Cisco Device 'CC-03-ROUTER-3640.localdomain'
Info	No	192.168.100.100	UOW trap	Apply Native Commandset UOW '35' submitted by engineer is executing (1078111250) 124 days, 1 hr ago
Info	No	192.168.100.100	UOW trap	Apply Native Commandset UOW '37' submitted by engineer is executing (1078111252) 124 days, 1 hr ago
Info	No	192.168.100.100	UOW trap	Apply Configuration UOW '28' submitted by engineer ready for execution, scheduled (1078111253) 124 days, 1 hr ago
Info	No	192.168.100.100	UOW trap	Synchronize From Device UOW '29' submitted by engineer ready for execution (1078111254) 124 days, 1 hr ago
Info	No	192.168.100.100	UOW trap	Synchronize From Device UOW '43' submitted by operator ready for execution (1078111255) 124 days, 1 hr ago
Info	No	192.168.100.100	Resource Event	Delete Cisco Device 'CC-03-ROUTER-3640'

The event records are created when Configuration Manager generates trap messages for various activities.

7. Return to the configuration manager client.
8. Move the devices to the **ITNCM > edge-network > customer_CC realm**. Open the **ITNCM > edge-network** realm. Press and hold the Ctrl key and select all three devices in the realm. Drag the selected devices into the **customer_CC** realm.



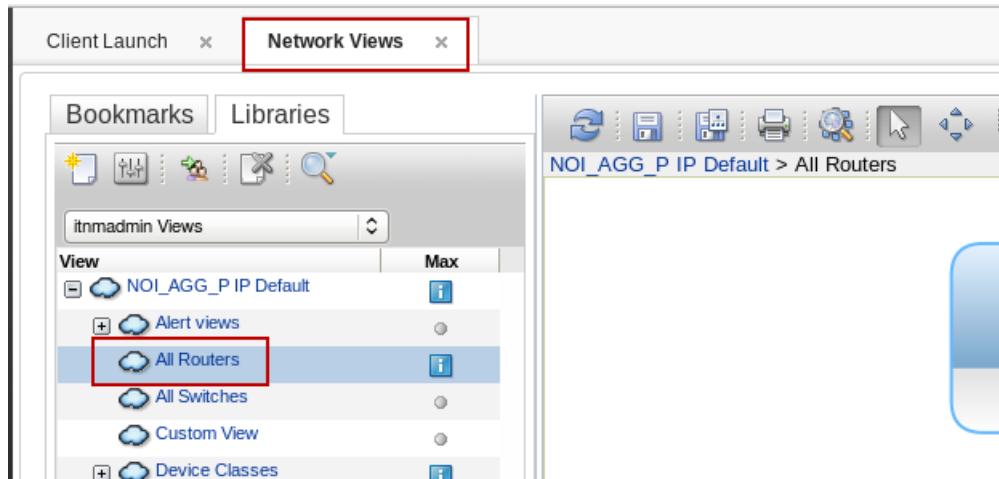
9. Verify that the devices appear in the **customer_CC** realm.



Exercise 5 Applying a policy to devices from Tivoli Network Manager

In this exercise, you apply a compliance policy to a device that you imported.

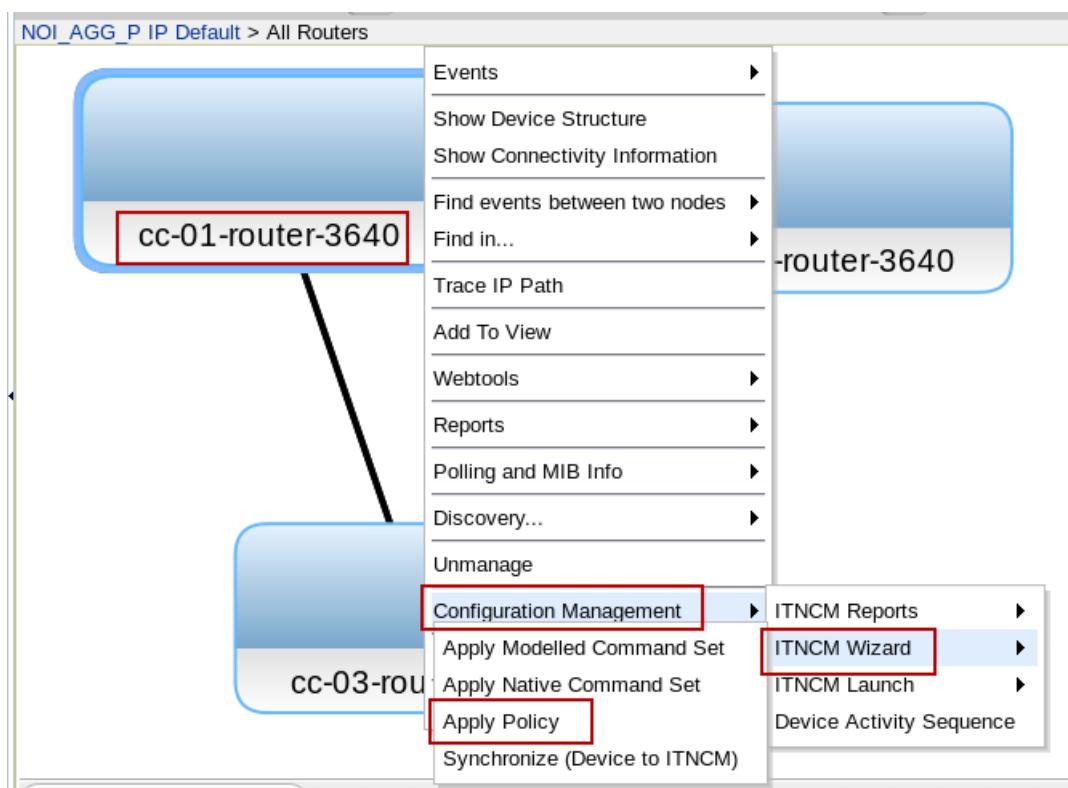
1. Return to the Firefox browser, and the Network Views page.



2. Apply the following policies to the cc-01-router-3640 through the network view.

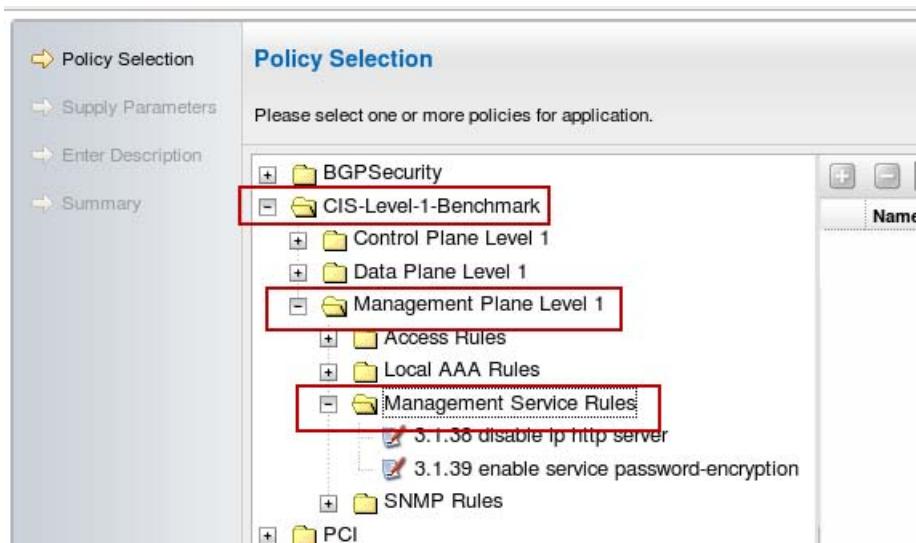
Field	Value
Network Device	cc-01-router-3640
Policy Realm	CIS-Level-1-Benchmark/Management Plane Level 1/ Management Service Rules
Policies	3.1.38 disable ip http server 3.1.39 enable service password-encryption
Parameters	Not applicable
Description	Test management service policies

- a. Right-click the **cc-01-router-3640** in the network view and select **Configuration Management > ITNCM Wizard > Apply Policy**.

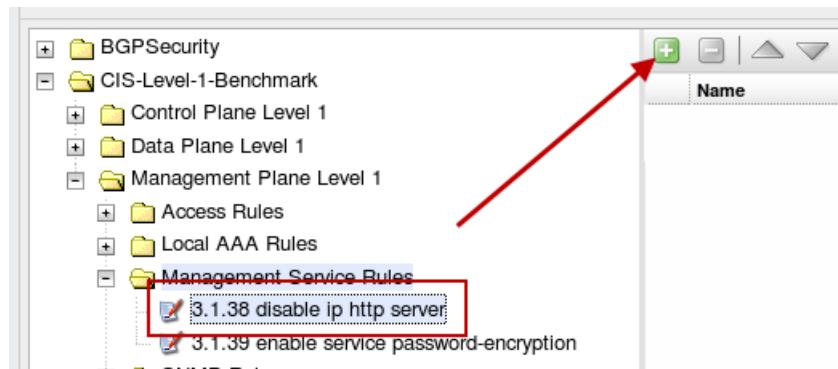


The policy wizard opens in a new Firefox tab.

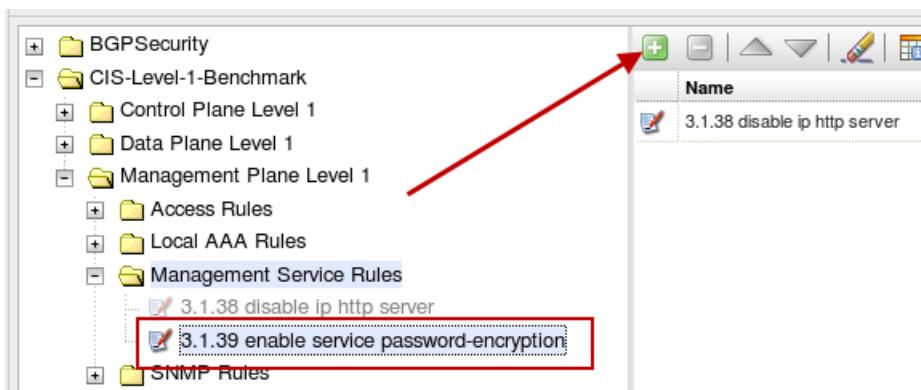
- b. Navigate to the policy realm **CIS-Level-1-Benchmark > Management Plane Level 1 > Management Service Rules**.



- c. Select the **3.1.38 disable ip http server** policy and click the *green plus sign* to add it to the list on the right.



- d. Select the **3.1.39 enable service password-encryption** policy and click the *green plus sign* to add it to the list on the right. Click **Next**.



- e. Click **Next**. No parameters are in these policies.

Supply Parameters

Please ensure each parameter is assigned a value. Selecting a table row moves focus to the input widget.

Resource	Parameter

There are no parameters.

- f. Enter the description **Test management service policies** and click **Next**.

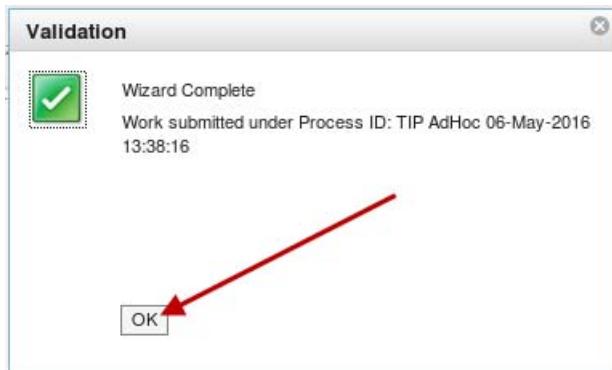
Enter Description

Please enter a description (290 character limit).

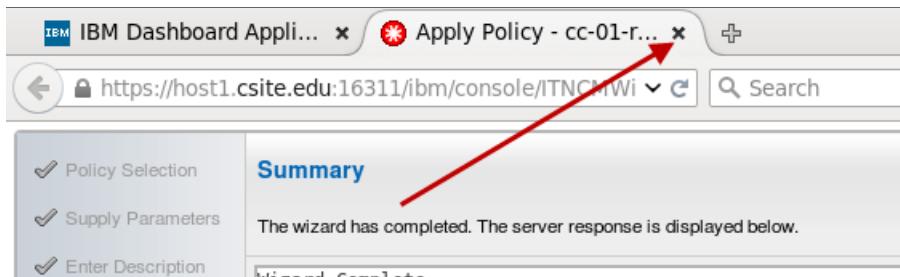
- g. Click **Yes** to confirm the submission.



- h. Click **OK**.



- Click the X to close the Firefox tab.



- Return to the Event Viewer page. Notice the new events that show the CC-01-ROUTER-3640 device is not compliant with these policies.

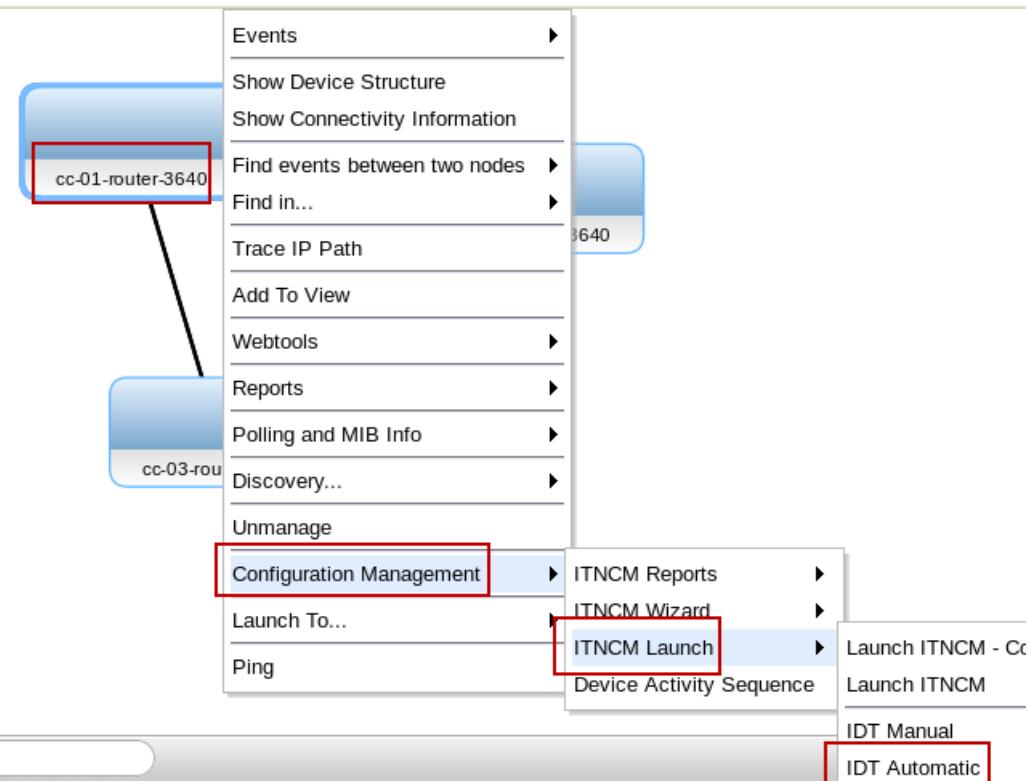
Sev	Ack	Node	Alert Group	Summary
	No	cc-01-router-3640	Policy Trap	cc-01-router-3640 is in violation of policy 3.1.38 disable ip http server
	No	cc-01-router-3640	Policy Trap	cc-01-router-3640 is in violation of policy 3.1.39 enable service password-encryption
	No	192.168.100.100	UOW trap	Autodiscovery UOW '59' submitted by administrator is executing (1093100194) 126 days

Note: It might take a few minutes for the events to appear.

Exercise 6 Applying a change to a device by using the device terminal

In this exercise, you apply a change by using the device terminal and you use Configuration Manager to synchronize the device.

1. Return to the Network Views page.
2. Right-click **cc-01-router-3640** and click **Configuration Management > ITNCM Launch > IDT Automatic**.



Note: A new instance of the configuration manager client starts, and the device terminal.

3. Enter the configuration mode and delete the exec banner with a **no banner exec** command and then exit the IDT session.

- a. Enter the configuration mode by entering the following command:

```
config t
```

```
cc-01-router-3640#term len 0
cc-01-router-3640#term width 100
cc-01-router-3640#config t
Enter configuration commands, one per line. End with
cc-01-router-3640(config) #
```

- b. Enter the following command to remove the banner:

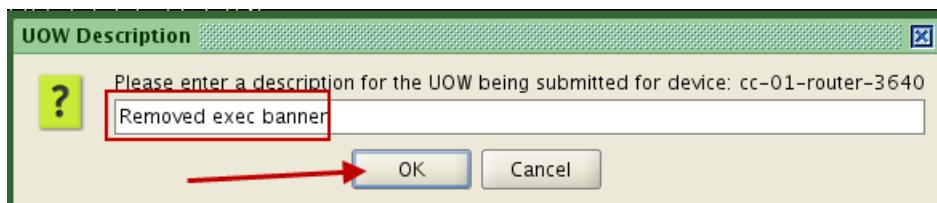
```
no banner exec
```

```
Enter configuration commands, one per line. End
cc-01-router-3640(config)#no banner exec
cc-01-router-3640(config) #
```

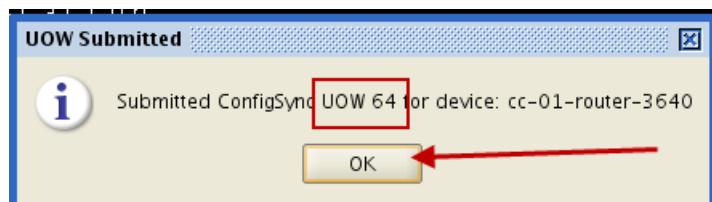
- c. Enter **exit** twice to exit the device.

```
Enter configuration commands, one per line.
cc-01-router-3640(config)#no banner exec
cc-01-router-3640(config)#exit
cc-01-router-3640#exit
```

- d. When the system prompts you, add the description **Removed exec banner**. Click **OK**.



- e. Note the unit of work number and click **OK** to close the window.

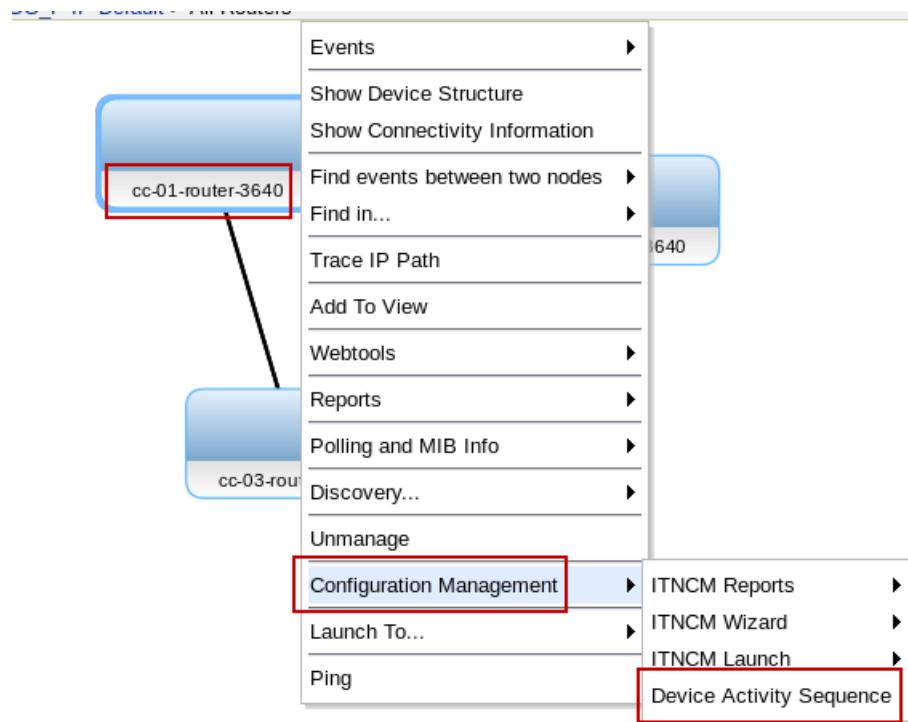


4. Close the device terminal when complete.

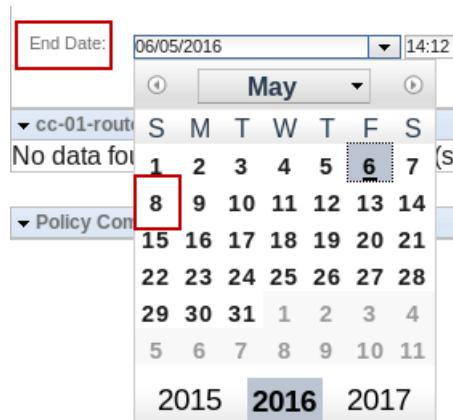
Exercise 7 Viewing device history in Activity Viewer

In this exercise, you review the recent actions on a device through the Activity Viewer.

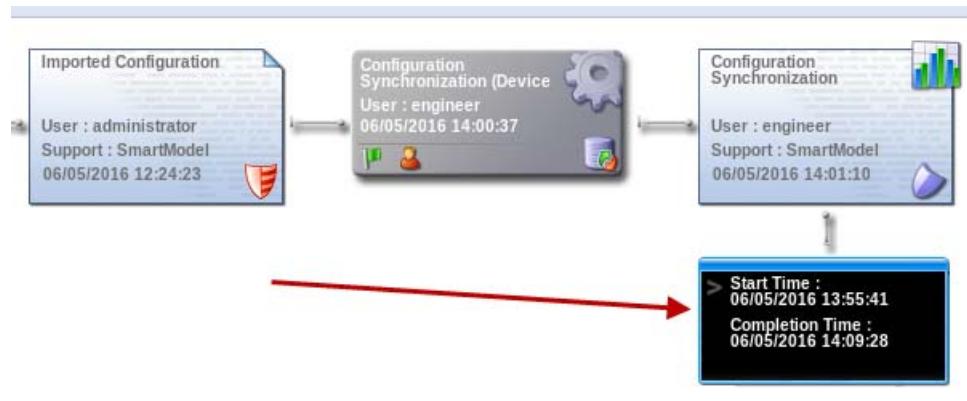
1. Return to the Network Views page. Right-click **cc-01-router-3640** and click **Configuration Management > Device Activity Sequence**.



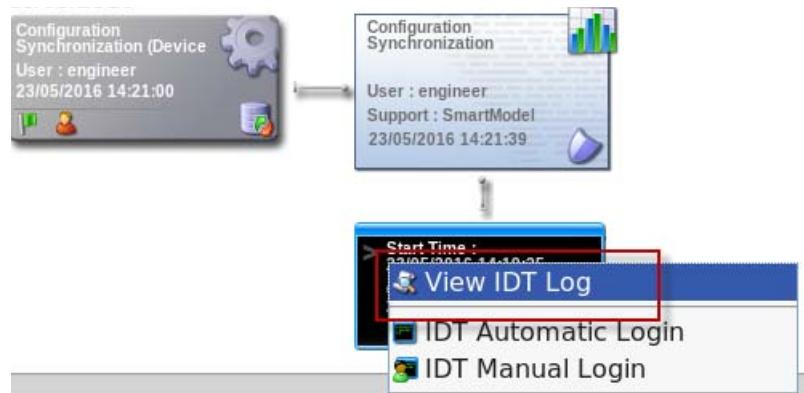
Important: If the ITNCM Activity Viewer is empty, modify the End Date to be two days in the future. Click **Search**.



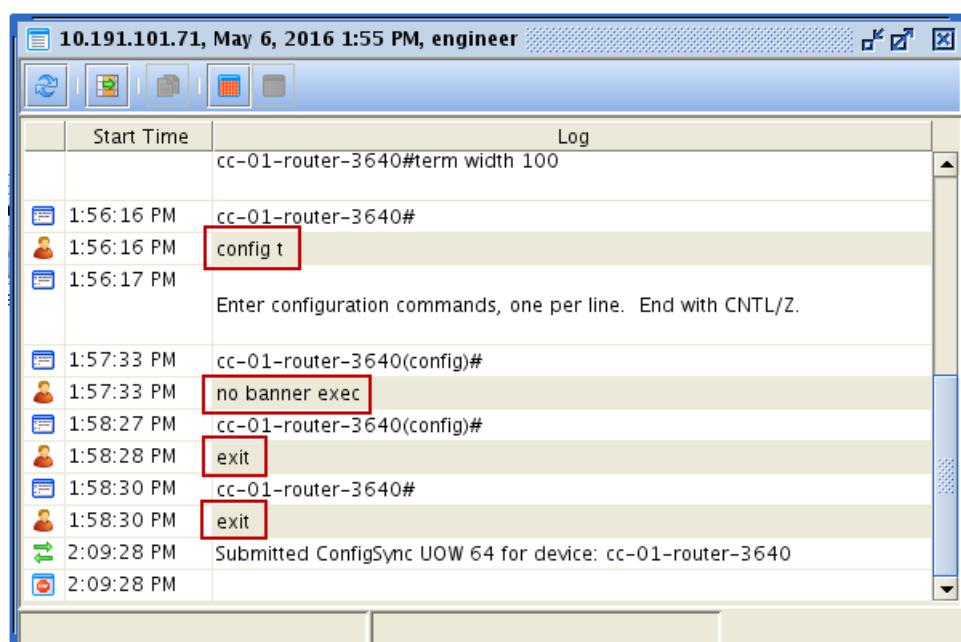
2. Review the device terminal log that was created for the **cc-01-router-3640** device in the previous exercise.
 - a. Find the device terminal icon on the right side of the viewer.



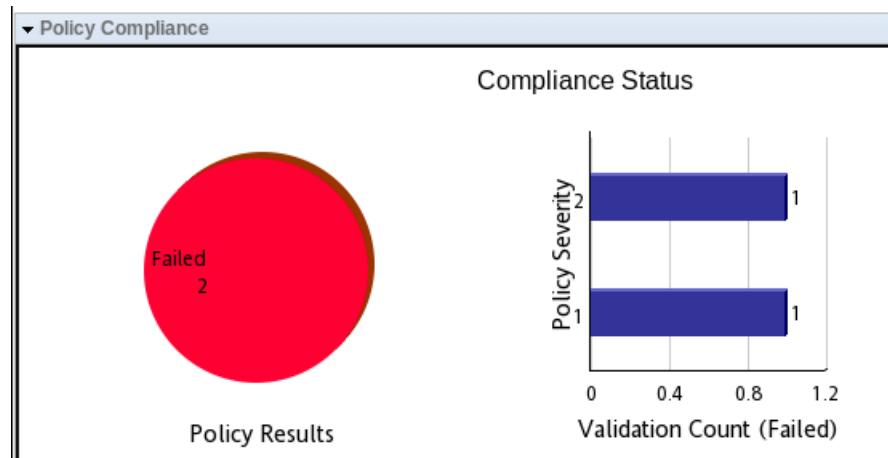
- b. Right-click the device terminal icon and select **View IDT Log**.



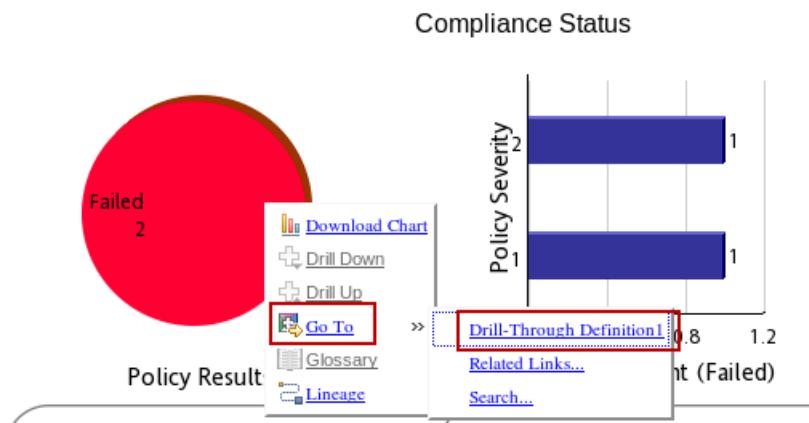
- c. Validate that the keystrokes that are submitted in the previous exercise are noted in the log. Close the window when you finish.



3. Review the specific compliance policies that failed on the **cc-01-router-3640** device.
 - a. Note the **Policy Compliance** charts in lower half of the Activity Viewer.



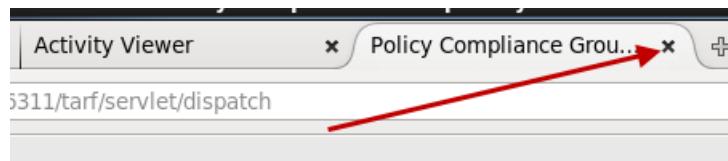
- b. Right-click the Policy Results pie chart (the red circle) and select the **Go To > Drill-Through Definition1** menu.



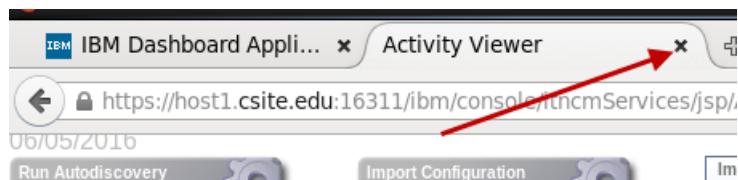
Note the two policies that were run against the device in a previous exercise.

IBM® Tivoli®			
Device Name	cc-01-router-3640	Policy Name	Policy Realm
Device Realm	ITNCM/edge-network/customer_CC	3.1.38 disable ip http server	CIS-Level-1-Benchmark/Management Plane Level 1/Management Service Rules/
Device VTMOS	Cisco/Router/3640/C3640-I-M-12.3(5b)		1 FAIL
		Policy Count	1
Device Name			
Device Name	cc-01-router-3640	Policy Name	Policy Realm
Device Realm	ITNCM/edge-network/customer_CC	3.1.39 enable service password-encryption	CIS-Level-1-Benchmark/Management Plane Level 1/Management Service Rules/
Device VTMOS	Cisco/Router/3640/C3640-I-M-12.3(5b)		2 FAIL
		Policy Count	1

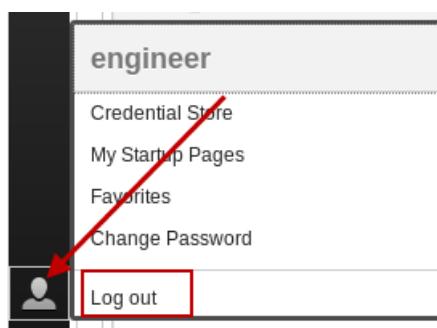
4. Click the X to close the policy report tab.



5. Click the X to close the Activity Viewer tab



6. Click the icon and select Log out.



7. Close the Firefox browser.

8. Close all open instances of the configuration manager client.



7 Authentication and authorization model exercises

The exercises in this unit demonstrate how to create users, groups and assign security attributes.

Exercise 1 Creating a group and a user

In this exercise, you create a security group. You create a user and assign the user to the group. The class image is configured to use an LDAP repository. Because you are using LDAP, you must create the group and user in LDAP first. Then you can assign Configuration Manager Security attributes.

1. Open a Firefox browser.



2. Log in as **smadmin** with password **object00**.

IBM Dashboard Application Services Hub

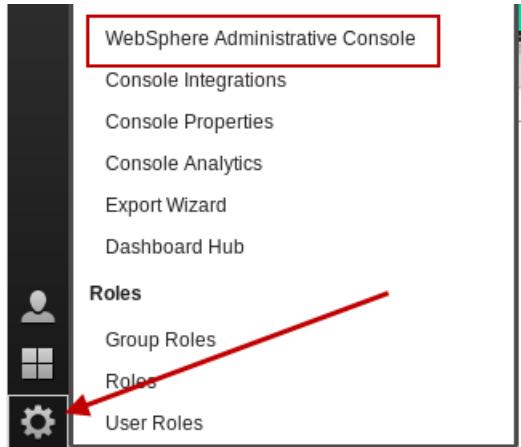
User ID
smadmin

Password

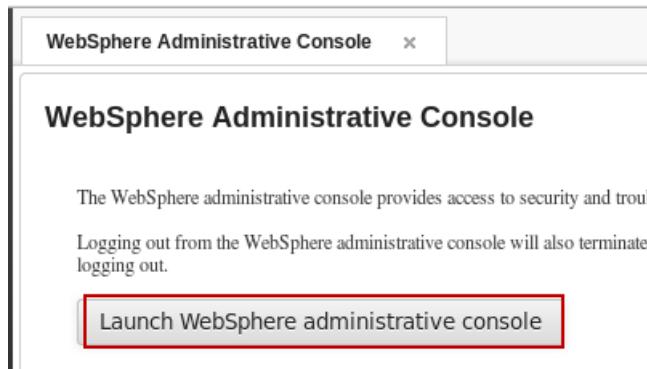
Go

Exercise 1 Creating a group and a user

3. Click the icon and select **WebSphere Administrative Console**.



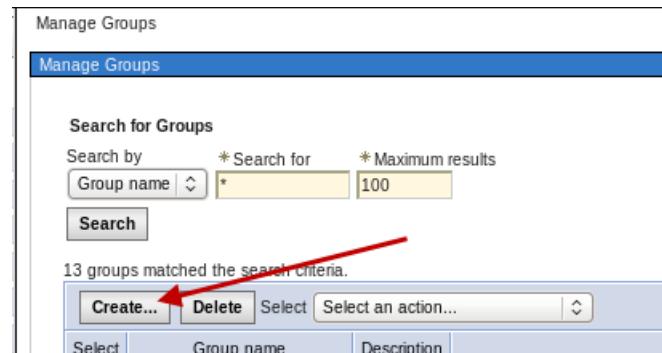
4. Click **Launch WebSphere administrative console**.



5. Expand **Users and Groups**. Click **Manage Groups**.



6. Click **Create**.



7. Enter the group name **Customer_CC** and the description **Manage Customer CC Devices**. Click **Create**.

The screenshot shows a 'Create a Group' dialog box. At the top, it says 'Create a Group'. Below that, there is a field labeled '* Group name' containing 'Customer_CC'. Underneath it is a 'Description' field containing 'Manage Customer CC Devices'.

8. Click **Close**.



9. Under Users and Groups, click **Manage Users**.

The screenshot shows a navigation menu on the left. Under the 'Users and Groups' section, the 'Manage Users' option is highlighted with a red box. To the right is a list of users with checkboxes next to their names.

User
Customer
ISQLWri
ImpactA
Intellider
Intellider

10. Click **Create**.

The screenshot shows a 'Manage Users' page. At the top, it says 'Search for Users'. Below that are search fields for 'User ID' (containing '*'), 'Search for' (containing '*'), and 'Maximum results' (containing '100'). There is a 'Search' button. Below the search area, it says '39 users matched the search criteria.' At the bottom, there is a toolbar with buttons for 'Create...', 'Delete', 'Select', and 'Select an action...'. A red arrow points to the 'Create...' button.

Exercise 1 Creating a group and a user

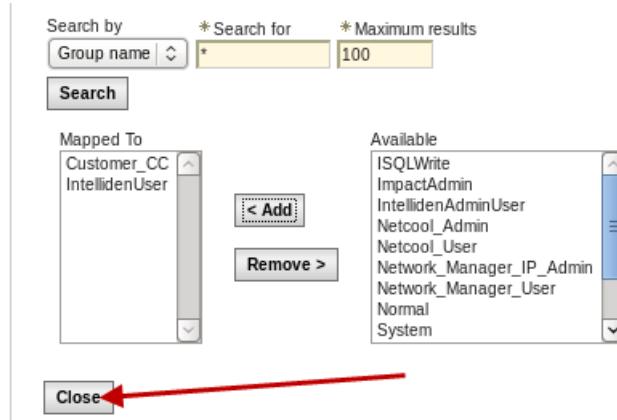
11. Create a user named **CC-user** with the password **object00**. Assign the user a first name of **CC** and a last name of **User** and email address of **cc-user@test.com**. Click the **Group Membership** tab.

12. Click **Search**.

13. Click **Customer_CC** to select it. Click **Add**.

14. Click **IntellidenUser** to select it. Click **Add**.

15. Click **Close**.



16. Click **Create**.

Manage Users

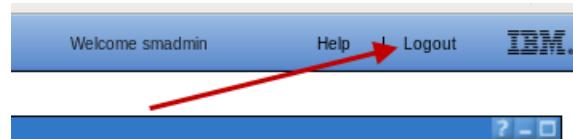
Create a User

* User ID CC-user	Group Membership
* First name CC	* Last name User
E-mail CC-user@test.com	
* Password *****	* Confirm password *****
<input type="button" value="Create"/> <input type="button" value="Cancel"/>	

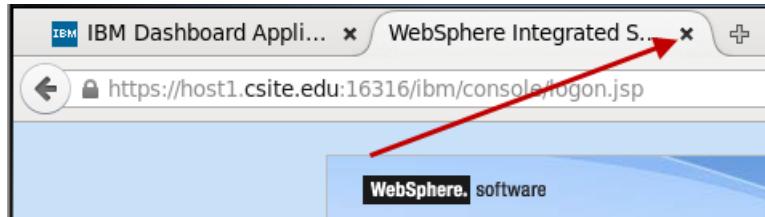
17. Click **Close**.



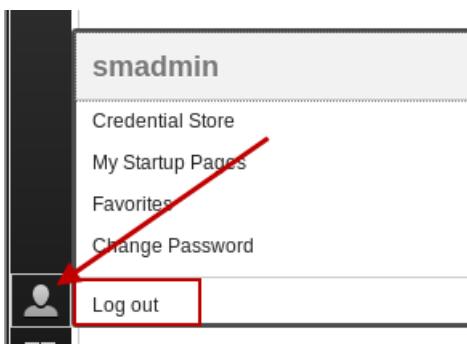
18. Click **Logout**.



19. Click the X to close the Firefox tab.



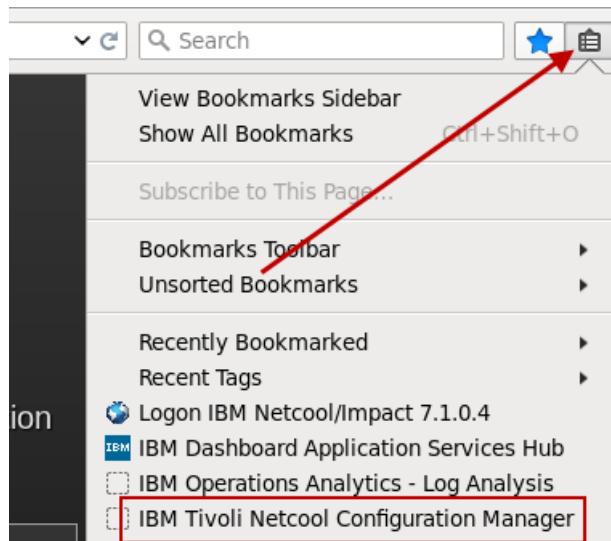
20. Click the icon and select Log out.



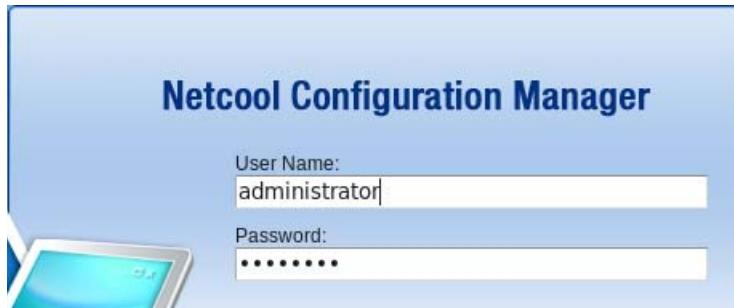
Exercise 2 Assigning security attributes

In this exercise, you create the same group name in Netcool Configuration Manager. You assign security attributes to the group.

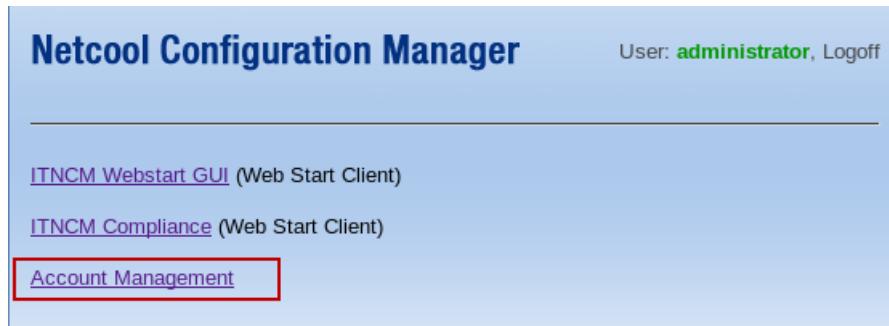
1. Use the Firefox browser to access the account management user interface.
 - a. Open the bookmarks and select **IBM Tivoli Netcool Configuration Manager**.



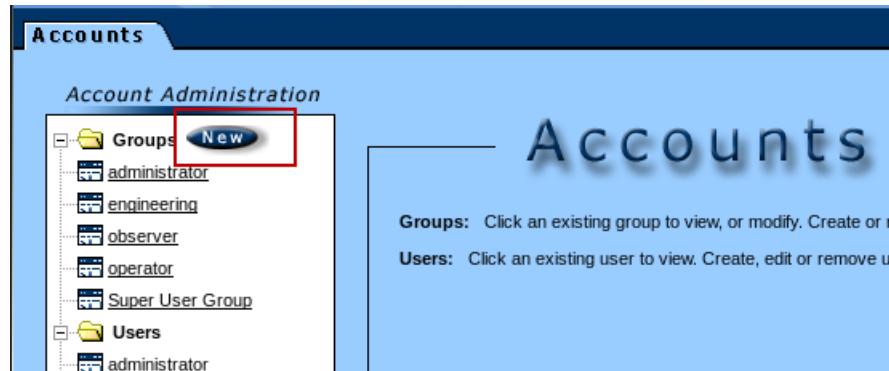
- b. Log In as **administrator** with password **object00**.



- c. Click **Account Management**.



2. Create a group and name it **Customer_CC**. Add the description **Manage Customer CC Devices** to the group.
a. Click **New** to create a group.



- b. Enter the group name **Customer_CC** and the description **Manage Customer CC Devices**.

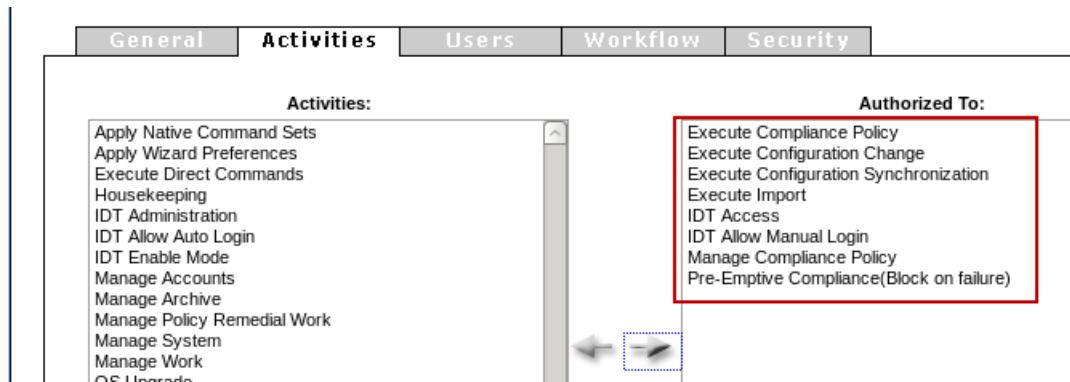
The image shows the 'New Group' dialog box. At the top is a navigation bar with tabs: General, Activities, Users, Workflow, and Security. The 'General' tab is selected. Below the tabs, there are two input fields: 'Group Name:' containing 'Customer_CC' and 'Description:' containing 'Manage Customer CC Devices'.

Exercise 2 Assigning security attributes

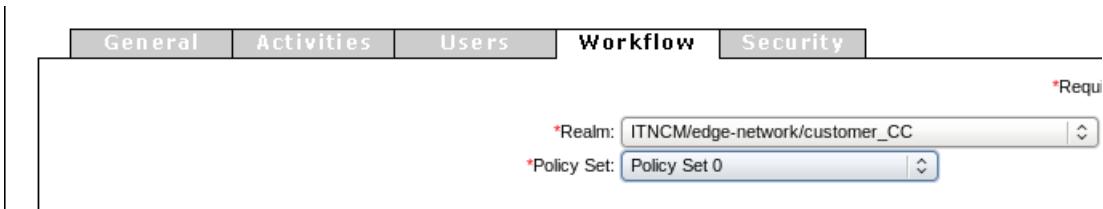
3. Add the following activities and workflow settings.

a. Click the **Activities** tab and add the following activities:

- ◆ Execute Compliance Policy
- ◆ Execute Configuration Change
- ◆ Execute Configuration Synchronization
- ◆ Execute Import
- ◆ IDT Access
- ◆ IDT Allow Manual Login
- ◆ Manage Compliance Policy
- ◆ Pre-Emptive Compliance (Block on failure)



b. Click the **Workflow** tab and set the **Realm** to **ITNCM/edge-network/customer_CC** and the **Policy Set** to **Policy Set 0**.



4. Define security settings so that the group can view and change devices only in the **ITNCM/edge-network/customer_CC** realm.

a. Click the **Security** tab. You are looking at the security settings for the realm structure.

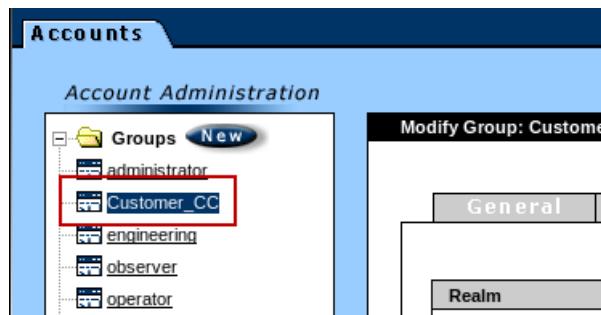
Disable the view rights for the entire realm structure by clearing the **View** check box for the **ITNCM** realm.

Realm	View	Add	Modify	Delete	All
ITNCM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ITNCM/CommandSets	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ITNCM/CommandSets/ModeledCommands	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ITNCM/CommandSets/NativeCommands	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- b. Scroll down and enable the view rights on the **ITNCM/edge-network/customer_CC** realm.

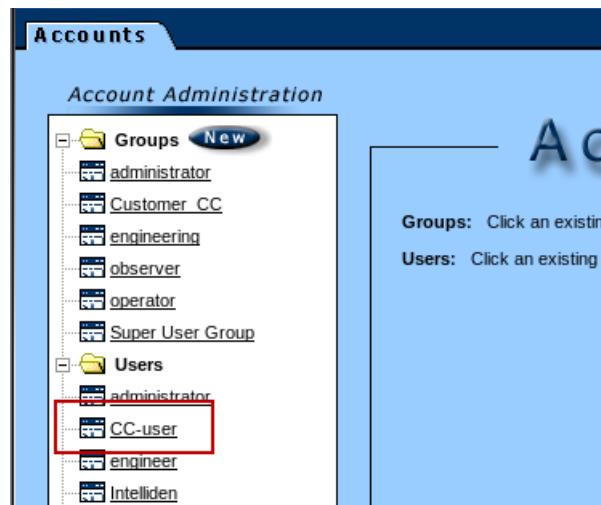
Realm	View	Add	Modify	Delete
ITNCM/edge-network	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ITNCM/edge-network/customer_AA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ITNCM/edge-network/customer_CC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ITNCM/x-tools	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ITNCM/x-tools/command-set-examples	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- c. Save the group by clicking **Create** in the lower right part of the window. Customer_CC is added to the list of available groups.



You maintain group names in LDAP and Netcool Configuration Manager. You maintain user names only in LDAP.

5. Scroll down and click **CC-user**.



Important: When you created the **CC-user** in the previous exercise, you assigned the user to the **IntellidenUser** group. Membership in the **IntellidenUser** group causes the user to appear here.

6. Enter **CC-user@test.com** and select the Groups tab.

User Name:	CC-user
First Name:	CC-user
Middle Initial:	(empty)
*Last Name:	CC-user
*E-mail:	CC-user@test.com
Telephone Number:	(empty)

7. Click **Customer_CC** and click the *right arrow* icon.

Groups:	administrator Customer_CC engineering observer operator
*Member of:	<no groups found>

8. Click **Save**.

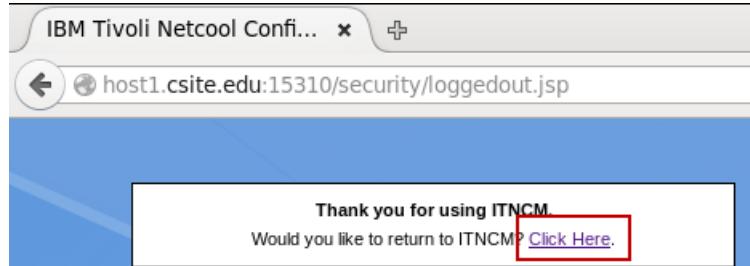
Groups:	administrator engineering observer operator Super User Group
*Member of:	Customer_CC

Save **Cancel**

9. Click the *running man* icon to log out.



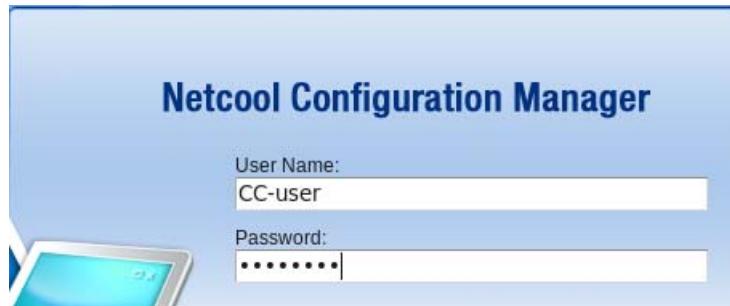
10. Select **Click Here** to return to the log in screen.



Exercise 3 Viewing the new user

In this exercise, you authenticate as the new user and note the permissions of the Customer_CC group.

1. Log in to Netcool Configuration Manager as the user **CC-user** with the password **object00**.

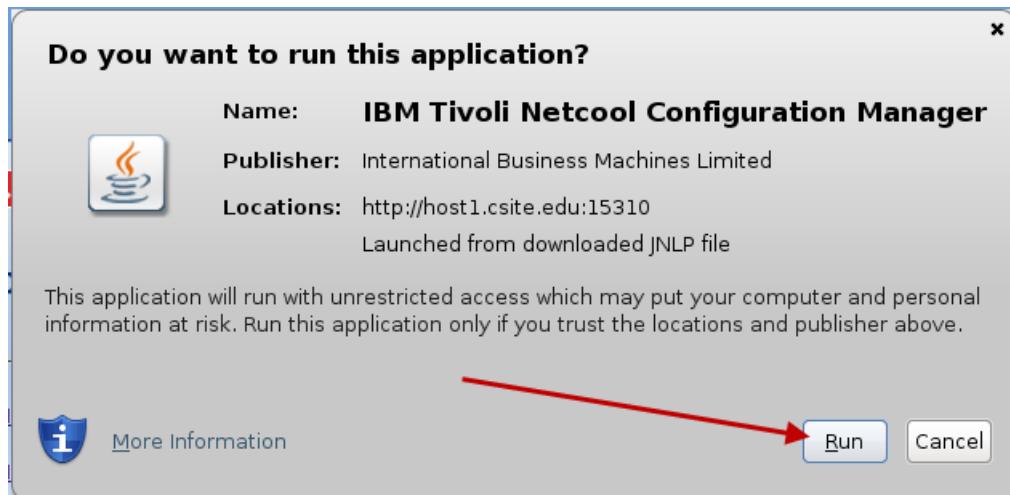


2. Click **ITNCM Webstart GUI**.



Exercise 3 Viewing the new user

3. Click Run.

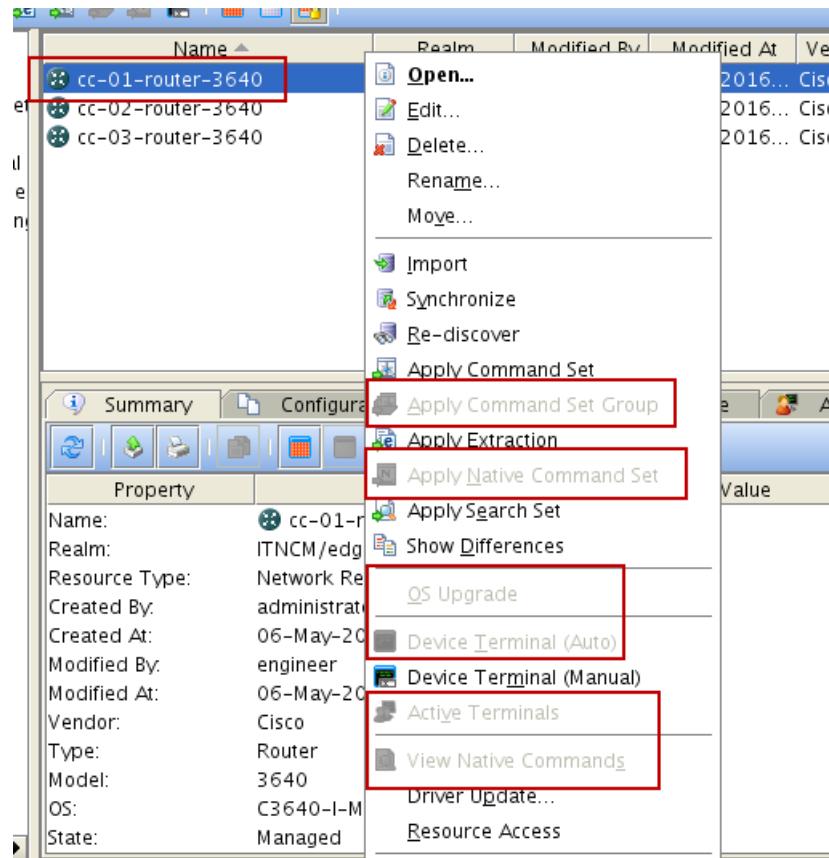


4. Expand the *resource browser*. Observe the realm structure.

Name	Realm	Modit
cc-01-router-3640	ITNCM/edge...	engine
cc-02-router-3640	ITNCM/edge...	engine
cc-03-router-3640	ITNCM/edge...	engine

The CC-user has access to only the **customer_CC** realm.

5. Right-click a device and note the items with no access rights.

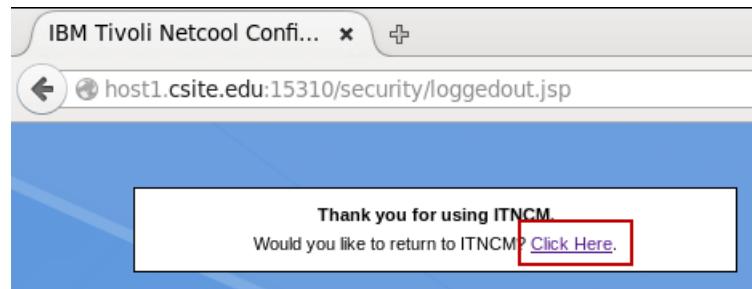


6. Close the configuration manager client.

7. Click **Logoff** to log out.



8. Select **Click Here** to return to the log in screen.



Leave the browser session as is. You return to it shortly.



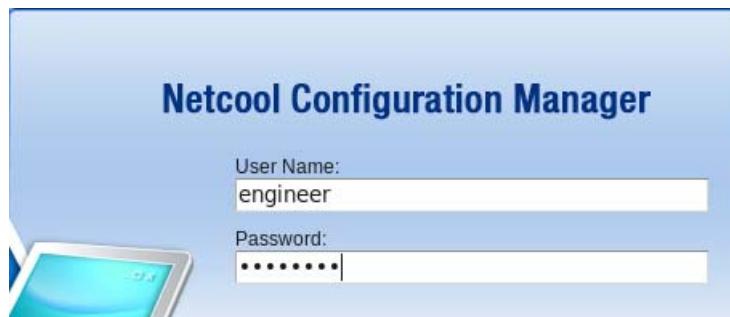
8 Device management exercises

The exercises in this unit demonstrate how to configure some of the Configuration Manager objects that you use for managing devices.

Exercise 1 Finding the actual model of a device

In this exercise, you view the actual model of two devices.

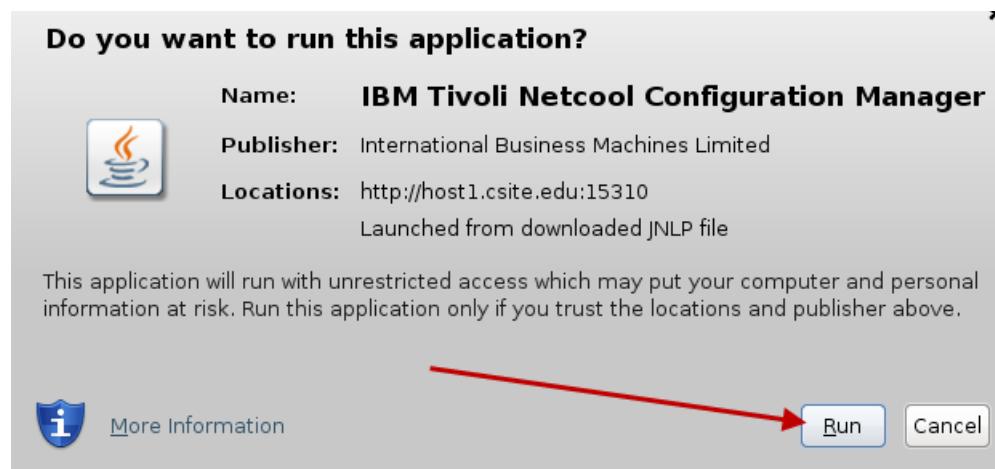
1. Log on to the user interface with the user name **engineer**. The password is **object00**.



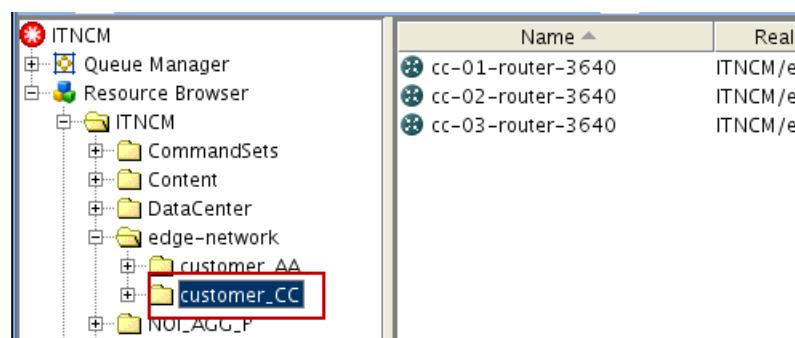
2. Click **ITNCM Webstart GUI**.



3. Click Run.



4. Click ITNCM > edge-network > customer_CC realm in the resource browser.



5. Click the cc-01-router-3640 device. Scroll down in the Summary tab to view the actual model of the router.

Name	Realm	Modified By	Modified At
cc-01-router-3640	ITNCM/edg...	engineer	May 6, 2016
cc-02-router-3640	ITNCM/edg...	engineer	May 6, 2016
cc-03-router-3640	ITNCM/edg...	engineer	May 6, 2016

Summary Configurations Work Hardware

Property	V
Modified By:	engineer
Modified At:	06-May-2016 21:14
Vendor:	Cisco
Type:	Router
Model:	3640
OS:	C3640-I-M-12.3(5b)
State:	Managed
Description:	VMADX
Permissions:	VMADX
Stale Config:	false
Driver State:	Optimal
Driver Type:	CLI
Support Level:	SmartModel
Actual Model:	3640 (R4700)
Driver Name:	cisco_router_36xx_c3640-ik9s-mz.123-6a_v20

8 Device management exercises

Exercise 1 Finding the actual model of a device

6. Middle-click the column headings about the network devices. Click **Actual Model** to add this column to the *resource browser*.

The screenshot shows the 'Resource Browser' pane with a tree view on the left and a table view on the right. The table has columns: Name, Realm, Modified By, Modified At, Vendor, Type, Model, OS, and Actual Model. The 'Actual Model' column is currently empty. A context menu is open over the 'Name' column, listing various properties like Name, Realm, Resource Type, etc., with 'Actual Model' being one of them.

7. View the actual model of the devices in this realm.

Name	Realm	Modified By	Modified At	Vendor	Type	Model	OS	Actual Model
cc-01-router-3640	ITNCM/ed...	engineer	May 6, 201...	Cisco	Router	3640	C3640-I-M-12...	3640 (R4700)
cc-02-router-3640	ITNCM/ed...	engineer	May 6, 201...	Cisco	Router	3640	C3640-I-M-12...	3640 (R4700)
cc-03-router-3640	ITNCM/ed...	engineer	May 6, 201...	Cisco	Router	3640	C3640-IK95-M...	3640 (R4700)

8. Find the actual model of the devices in the **customer_AA** realm.

- a. Click **ITNCM > customer_AA** realm in the *resource browser*.

The screenshot shows the 'Resource Browser' pane with a tree view on the left and a table view on the right. The tree view shows a folder structure under 'edge-network': 'customer_AA' and 'customer_CC'. The table on the right lists realms with columns: Name and Realm. The 'Actual Model' column is currently empty. A context menu is open over the 'Name' column, listing various properties like Name, Realm, Resource Type, etc., with 'Actual Model' being one of them.

- b. View the **Actual Model** column for the customer_AA devices.

Name	Realm	Modified By	Modified At	Vendor	Type	Model	OS	Actual Model
BRU-CPE-dca.gov	ITNCM/edg...	administrator	May 4, 201...	Cisco	Router	3640	C3640-I03...	3640 (R4700)
PAR-dca.gov	ITNCM/edg...	engineer	May 4, 201...	Cisco	Router	7206...	C7200-JK9...	7206VXR (NPE400)
NYC-dca.gov	ITNCM/edg...	engineer	May 4, 201...	Cisco	Router	7206...	C7200-JK9...	7206VXR (NPE400)
BRU-dca.gov	ITNCM/edg...	engineer	May 4, 201...	Cisco	Router	7206...	C7200-JK9...	7206VXR (NPE400)
LON-dca.gov	ITNCM/edg...	engineer	May 4, 201...	Cisco	Router	7206...	C7200-JK9...	7206VXR (NPE400)
WAS-dca.gov	ITNCM/edg...	engineer	May 4, 201...	Cisco	Router	7206...	C7200-JK9...	7206VXR (NPE400)
SYD-dca.gov	ITNCM/edg...	engineer	May 4, 201...	Cisco	Router	7206...	C7200-JK9...	7206VXR (NPE400)
MOS-dca.gov	ITNCM/edg...	engineer	May 4, 201...	Cisco	Router	7206...	C7200-JK9...	7206VXR (NPE400)
BRU-SW-dca.gov	ITNCM/edg...	engineer	May 4, 201...	Cisco	Router	3660	C3660-JK9...	3660 (R527x)
BRU-ACS-dca.gov	ITNCM/edg...	engineer	May 4, 201...	Cisco	Router	3640	C3640-I03...	3640 (R4700)

Exercise 2 Using an authentication resource

In this exercise, you edit an authentication resource. You also add a user name and password to a device. Finally, you verify that the change you made to the authentication resource is used by Netcool Configuration Manager.

1. Find the authentication resource that is used for devices in the customer_CC realm.

- a. Click the **customer_CC** realm.

Name	Realm	Modified By	Modified At	Vendor	Type
cc-03-router-36...	ITNCM/edg...	engineer	May 6, 201...	Cisco	Router
cc-02-router-36...	ITNCM/edg...	engineer	May 6, 201...	Cisco	Router
cc-01-router-36...	ITNCM/edg...	engineer	May 6, 201...	Cisco	Router

All of the devices in the customer_CC realm are Cisco routers. The customer_CC realm does not contain an authentication resource for Cisco routers. Look at the parent realm.

- b. The parent realm is named **edge-network**. Click the **edge-network** realm.

Name	Realm	Modified By	Modified At	Vendor
Cisco-Router-RAD	ITNCM/edg...	engineer	May 2, 201...	Cisco
customer_AA	ITNCM/edg...	engineer	May 2, 201...	
customer_CC	ITNCM/edg...	engineer	May 2, 201...	

The edge-network realm does not contain an authentication resource for Cisco routers.
Look at the parent realm.

- c. The parent realm is named **ITNCM**. Click the **ITNCM** realm.

The screenshot shows the ITNCM realm structure on the left and a table of resources on the right. The resources table has columns: Name, Realm, Modified By, and Modified At. The 'DevicePasswords' resource is highlighted with a red box in both the tree and the table.

Name	Realm	Modified By	Modified At
DevicePasswords	ITNCM	engineer	May 3, 201...
WorkDistribution	ITNCM	administrator	Feb 26, 20...
File Transfer	ITNCM	engineer	May 3, 201...
Cisco_36x_Device...	ITNCM	engineer	May 3, 201...
show_memory_flash	ITNCM	engineer	May 6, 201...
sequence_exec	ITNCM	engineer	May 6, 201...
12 Hour Work	ITNCM	engineer	May 6, 201...
36 Hour Work	ITNCM	engineer	May 6, 201...
Content	ITNCM	Installer	Feb 25, 20...

The ITNCM realm does contain an authentication resource that is named **DevicePasswords** for all devices, the VTMOS is `*//*/*`. Cisco routers in the **ITNCM > edge-network > customer_CC** realm resolve to this authentication resource.

2. Edit the authentication resource. Use the values in the following table to add a user name and password. Close the authentication resource when you finish.

Field	Value
User name	itncm
Password	object00
Enable Password	3n4bl3
Retry Count	0
Retry Delay	0
Ignore	False
Position	1

- a. Right-click the **DevicePasswords** resource and click **Edit**.

The screenshot shows the context menu for the 'DevicePasswords' resource in the ITNCM realm. The 'Edit...' option is highlighted with a red box.

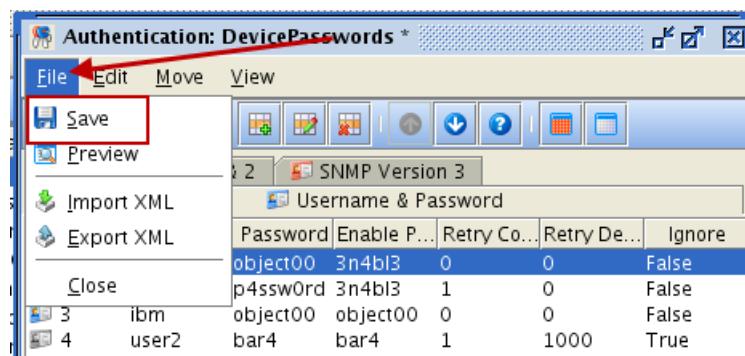
- b. Click **Edit > Add**.



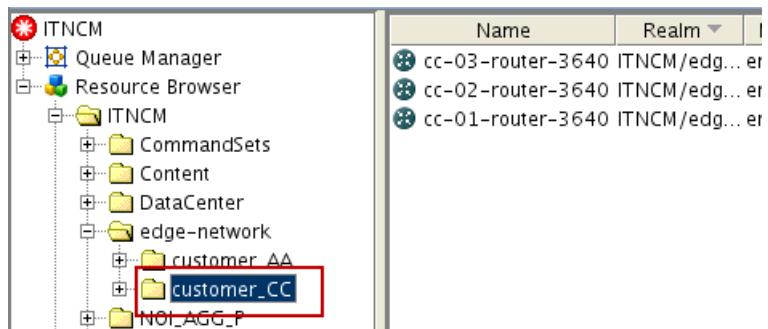
- c. Enter the values from the preceding table and click **OK**.



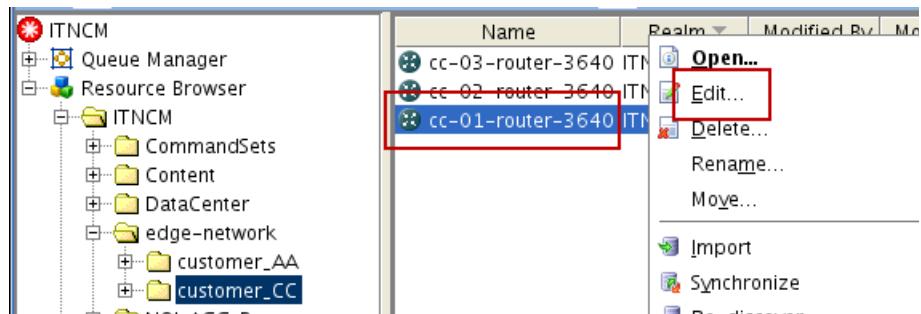
- d. Click **File > Save**. Close the authentication resource when you finish.



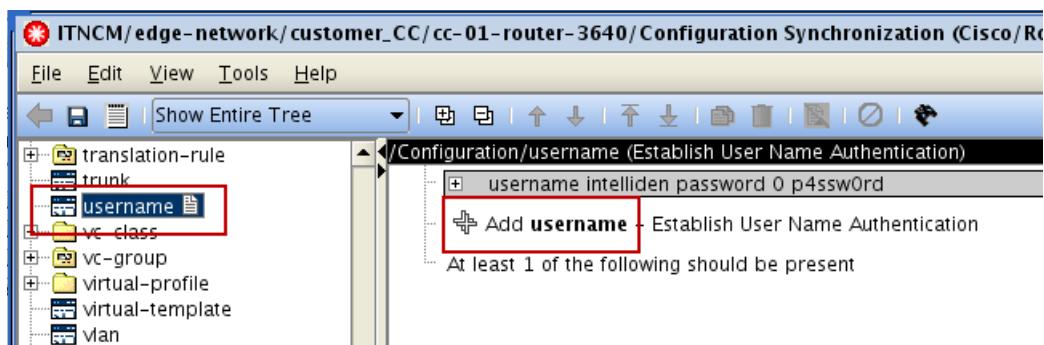
3. Edit the configuration of the cc-01-router-3640 device.
 - Add the user name **itncm** and the password **object00** to the configuration.
 - Use encryption level **0** for the password.
 - Mark these changes as **Added**.
 - Verify that the markup is adding the user name, password, and encryption level.
 - When you finish the configuration, save it and submit the change.
- a. Click **ITNCM > edge-network > customer_CC**.



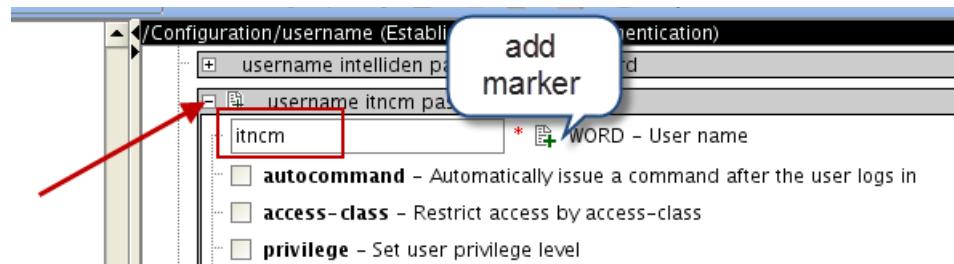
- b. Right-click **cc-01-router-3640** and click **Edit**.



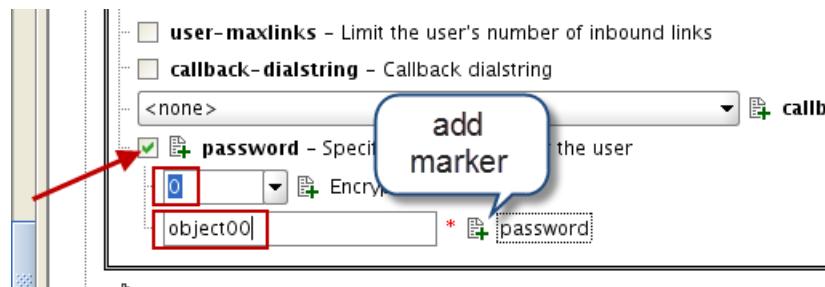
- c. Click the **username** object in the command tree. On the right side of the *configuration editor*, click **Add username**.



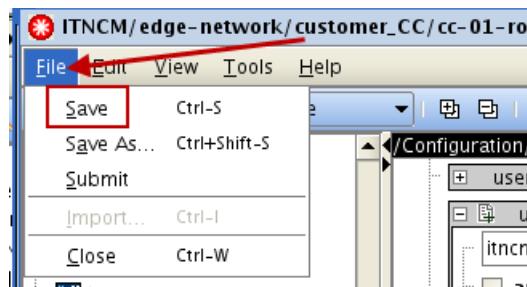
- d. Expand the new **username** object. Enter **itncm** in the **User name** field.



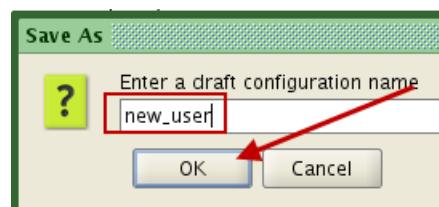
- e. Select the **password** field. Click **0** in the **Encryption** field. Enter **object00** in the **password** field. Verify that all of the fields you edit have the add marker next to them, the marker looks like a green plus symbol.



- f. Save the configuration. Click **File > Save**.



4. Name the configuration **new_user**.

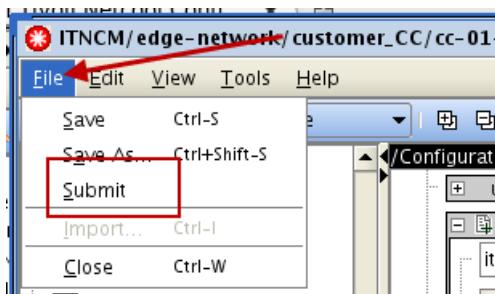


5. Submit the change. Use the following values to complete the wizard.

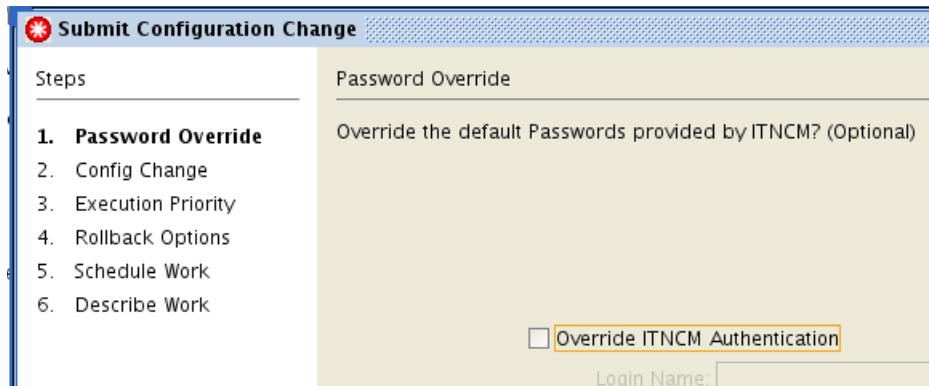
Field	Value
Password Override	Do not override
Config Change	Merge
Execution Priority	Medium

Field	Value
Schedule Work	Single Schedule > Immediate
Describe Work	Adding a new user

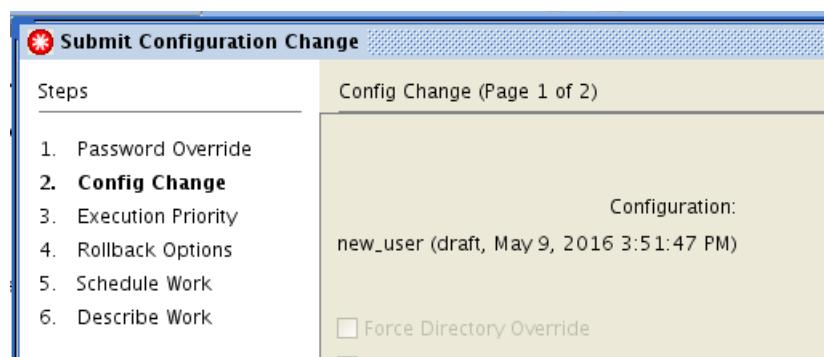
- a. Click **File > Submit**. The configuration change wizard starts.



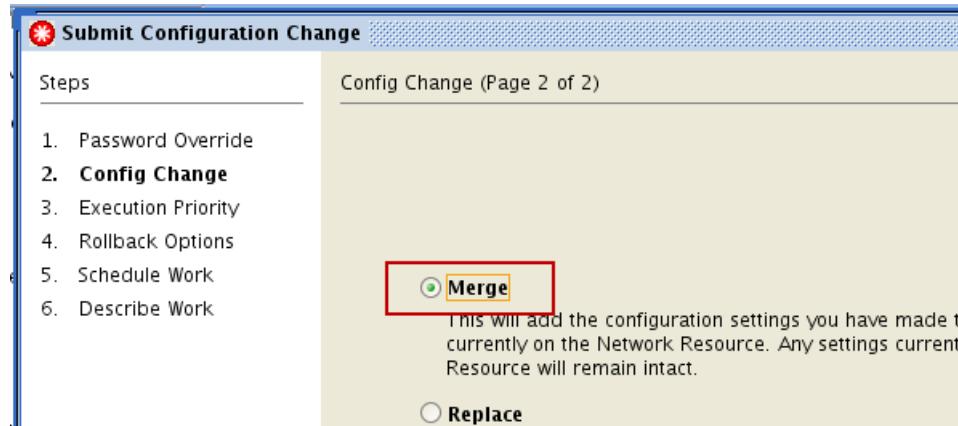
- b. Click **Next** in the Password Override window.



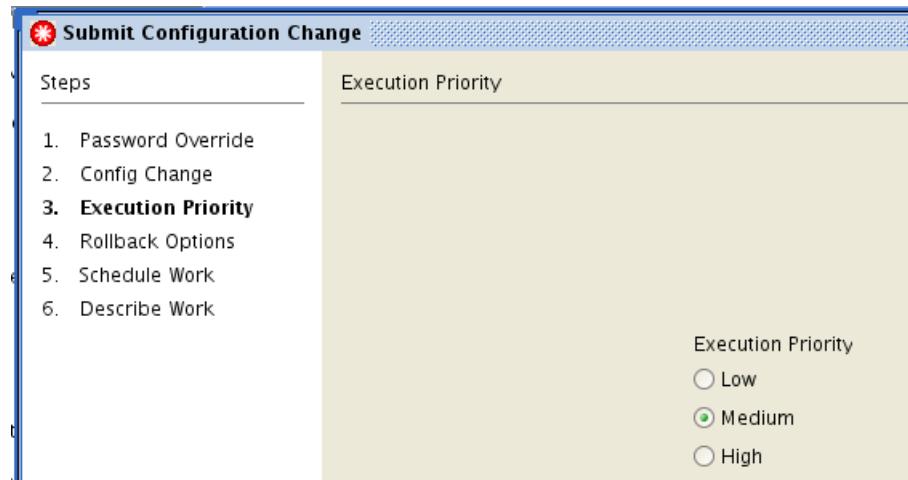
- c. Click **Next** in the Config Change window.



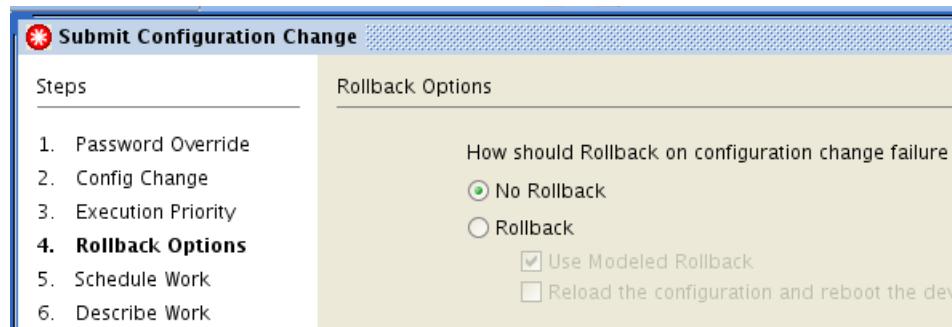
- d. Select **Merge** and click **Next** in the Config Change window.



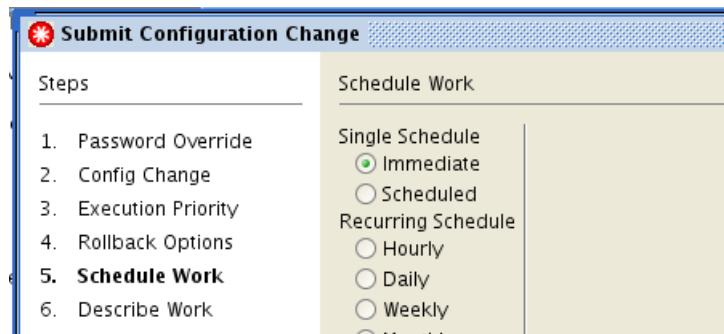
- e. Click **Next** in the Execution Priority window.



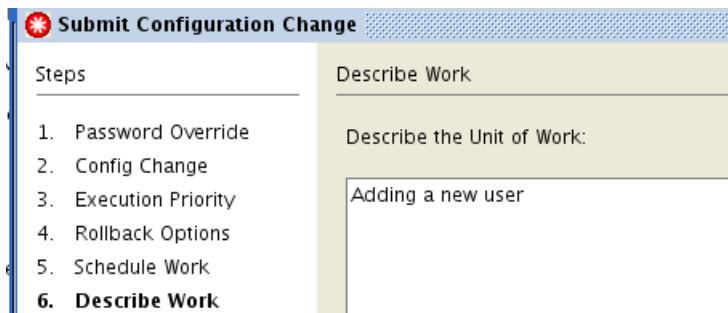
- f. Click **Next** in the Rollback Options window.



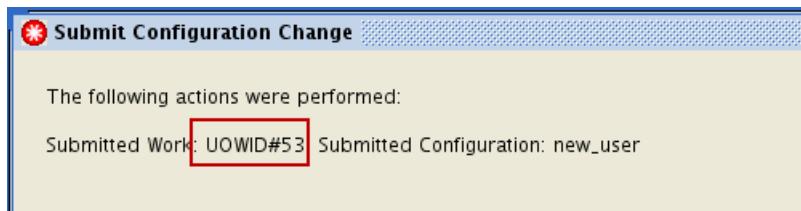
- g. Click **Next** in the Schedule Work window.



- h. Enter **Adding a new user** in the Describe Work window. Click **Finish**.

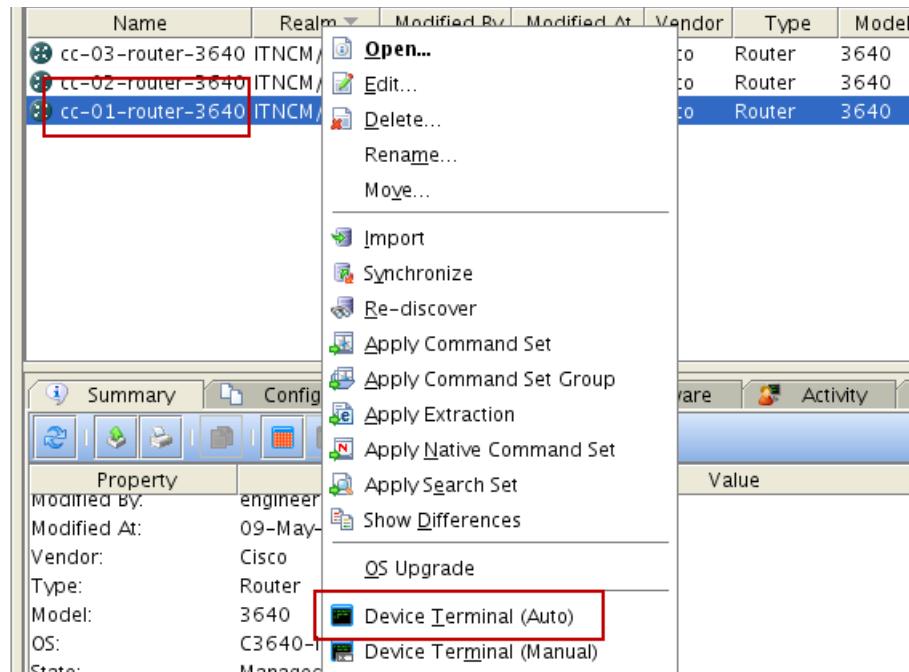


- i. Note the unit of work number and click **Close**.



After the unit of work finishes, log on to the cc-01-router-3640 router by using the automatic device terminal.

6. Right-click the cc-01-router-3640 device and click **Device Terminal (Auto)**.



7. Verify that the new user name is tried first and that the login is successful. Exit the device terminal when you finish.

The log in attempt is successful because you added the name and password to the router configuration.

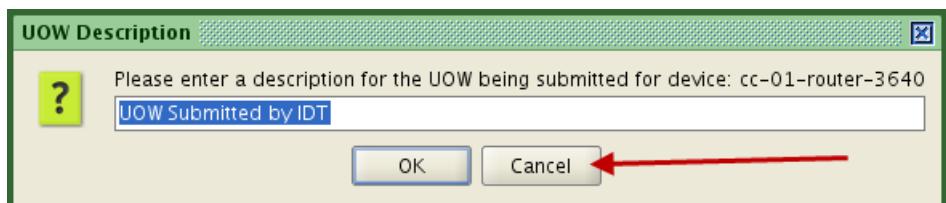
```
# #####
# #
##      Unauthorized access is prohibited. #
## #####
User Access Verification
Username: itncm
Password: 

cc-01-router-3640>en
Password:
cc-01-router-3640#terminal 0
cc-01-router-3640#term width 100
cc-01-router-3640#
```

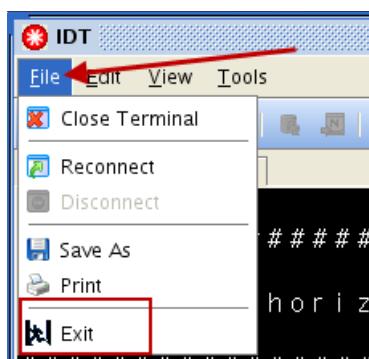
- a. Type **exit**.

```
cc-01-router-3640#terminal 0
cc-01-router-3640#term width 100
cc-01-router-3640#exit
```

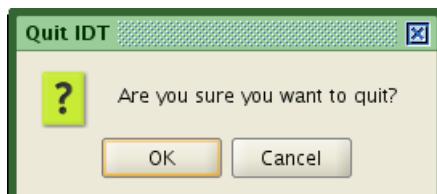
- b. Click **Cancel**.



- c. Click **File > Exit** to close the device terminal window.



- d. Click **OK** to confirm.



Exercise 3 Viewing a resource access document

In this exercise, you view the settings in a resource access document.

- Find the resource access document that is used for devices in the **customer_CC** realm.
 - Click the **customer_CC** realm.

Name	Realm	Modified By	M
cc-03-router-3640	ITNCM/edg...	engineer	Ma
cc-02-router-3640	ITNCM/edg...	engineer	Ma
cc-01-router-3640	ITNCM/edg...	engineer	Ma

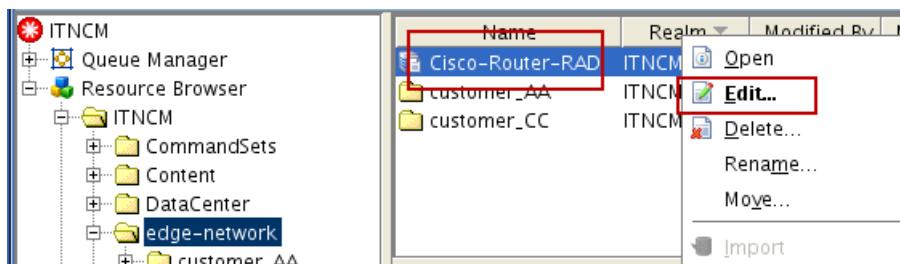
All of the devices in the customer_CC realm are Cisco routers. The customer_CC realm does not contain a resource access document for Cisco routers. Look at the parent realm.

- b. The parent realm is named **edge-network**. Click the **edge-network** realm.

Name	Realm	Modified By	Modified At	Vendor
Cisco-Router-RAD	ITNCM/edge... engineer	May 2, 201...		Cisco
customer_AA	ITNCM/edge... engineer	May 2, 201...		
customer_CC	ITNCM/edge... engineer	May 2, 201...		

The edge-network realm does contain a resource access document that is named **Cisco-Router-RAD** for Cisco routers (the VTMOS is Cisco/Router/*/*). Cisco routers in the **ITNCM > edge-network > customer_CC** realm resolve to this resource access document.

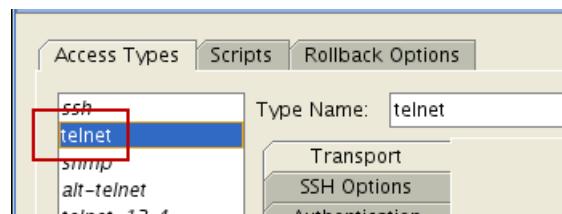
2. Open the resource access document named **Cisco-Router-RAD**. Use the **Edit** option to open the document.
- a. Right-click the resource access document named **Cisco-Router-RAD**. Click **Edit**.



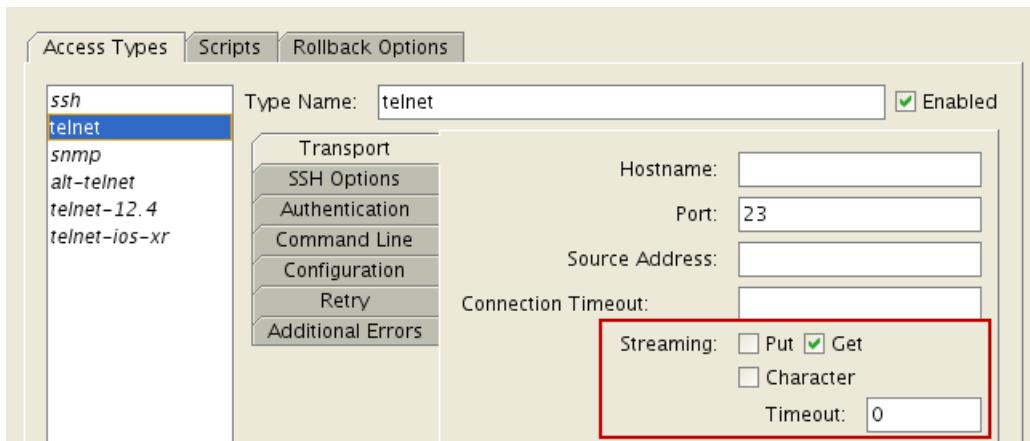
- b. Click all of the options in the **Access Type** tab. The only access type that is enabled is **telnet**.

Type Name:	Enabled
ssh	<input type="checkbox"/>
telnet	<input checked="" type="checkbox"/>
snmp	<input type="checkbox"/>
alt-telnet	<input type="checkbox"/>
telnet-12.4	<input type="checkbox"/>
telnet-ios-xr	<input type="checkbox"/>

3. The following steps describe how the **Cisco-Router-RAD** resource access document gets configurations from routers.
- Click **telnet** in the **Access Types** tab.

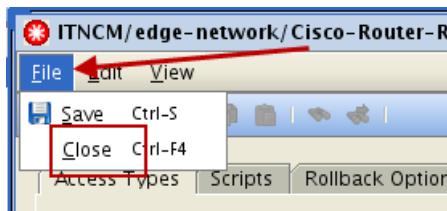


- Examine the **Streaming** options.

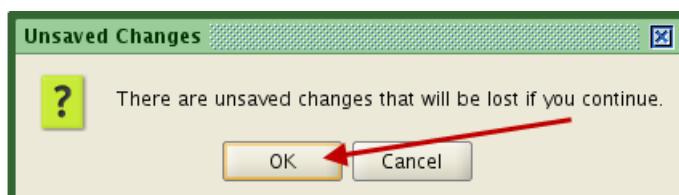


The **Get** option is selected. This setting means that configurations are obtained by streaming them through the telnet session. The **Put** option is cleared. This setting means that configurations are sent to devices with file transfer.

- Click **File** and select **Close** to close the resource access document.



- Click **OK** to confirm the close.

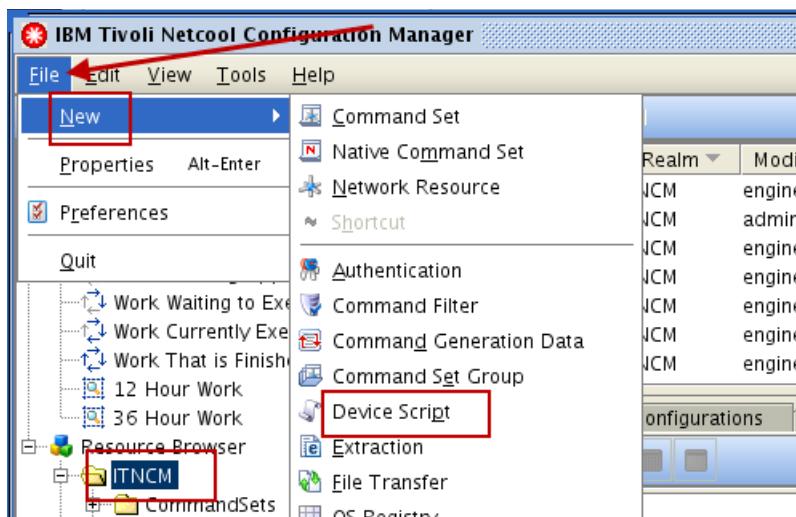


Exercise 4 Creating a device script resource

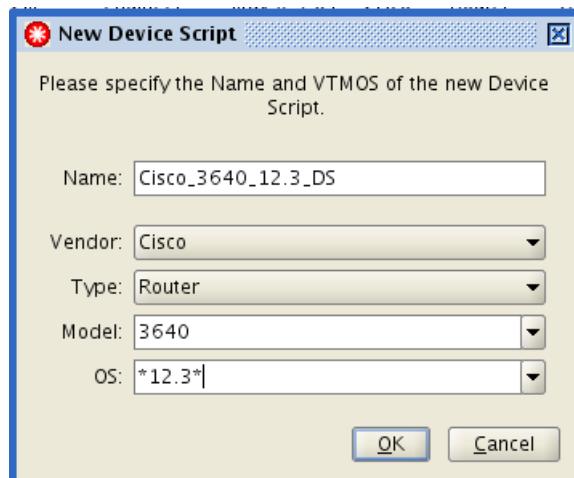
In this exercise, you create a device script resource for Cisco 3640 routers that use IOS version 12.3.

1. Create a device script resource in the **ITNCM** realm named **Cisco_3640_12.3_DS**. Use the following VTMOS settings. This device script uses an extra carriage return to respond to the request to overwrite NVRAM from 3640 routers that run IOS version 12.3.
 - Name: Cisco_3640_12.3_DS
 - Vendor: Cisco
 - Type: Router
 - Model: 3640
 - Operating System: *12.3*

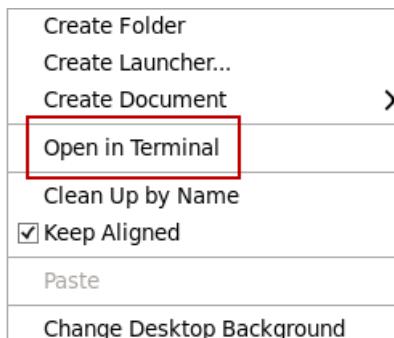
- a. Click the **ITNCM** realm. Click **File > New > Device Script**.



- b. Enter the following values in the New Device Script window and click **OK**.
- ◆ Name: **Cisco_3640_12.3_DS**
 - ◆ Vendor: **Cisco**
 - ◆ Type: **Router**
 - ◆ Model: **3640**
 - ◆ Operating System: ***12.3***



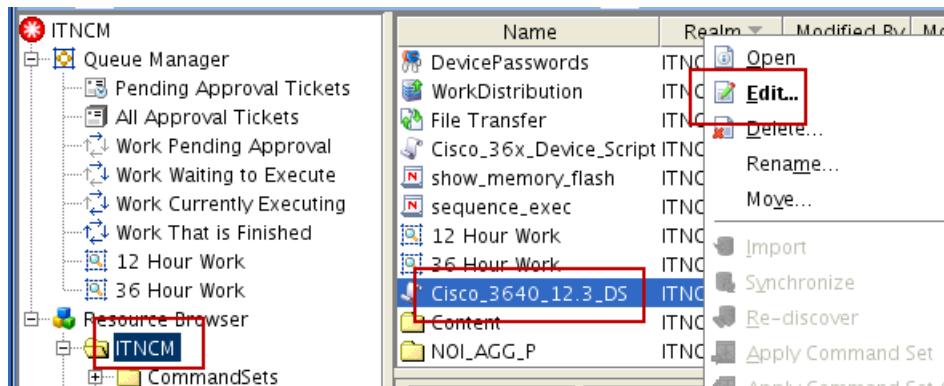
2. Edit the new device script to send an extra carriage return after the running configuration is copied to the startup configuration. The class image contains a device script excerpt in a text file that is named **/home/netcool/device_script_excerpt.txt** that you can copy and paste into the device script resource.
- a. Right-click the desktop and click **Open in Terminal**.



- b. Run the following command to open the **/home/netcool/device_script_excerpt.txt** file. Leave this file open.

```
gedit /home/netcool/device_script_excerpt.txt
```

- c. Return to the *configuration manager* user interface. Click the **ITNCM** realm. Right-click the new **Cisco_3640_12.3_DS** device script and click **Edit**.



- d. Scroll past halfway down in the device script. Find the following 10 lines:

```

### Disconnect
#disconnect.01.send=(something to do before disconnecting)
disconnect.errorResponse=Error disconnecting from device.

### Ftp file
ftp.01.send=copy ftp://$ftp_username$:$ftp_password$@$ftp_hostname$/ftp_filename$ running-config\r
ftp.02.wait=?
ftp.03.send=\r
ftp.04.wait=#\r
ftp.05.sleep=5000
ftp.06.send=copy running-config startup-config\r
ftp.07.wait=?
ftp.08.send=\r
ftp.09.wait=#
#ftp.01.send=copy tftp running-config\r
#ftp.02.wait=?
#ftp.03.send=$ftp_hostname$\r
#ftp.04.wait=?
#ftp.05.send=$ftp_filename$\r
#ftp.06.wait=?
#ftp.07.send=running-config\r
#ftp.08.send=\r
#ftp.09.wait=#
#ftp.10.sleep=5000
#ftp.11.send=copy running-config startup-config\r

```

- e. Remove those 10 lines from the device script.



```

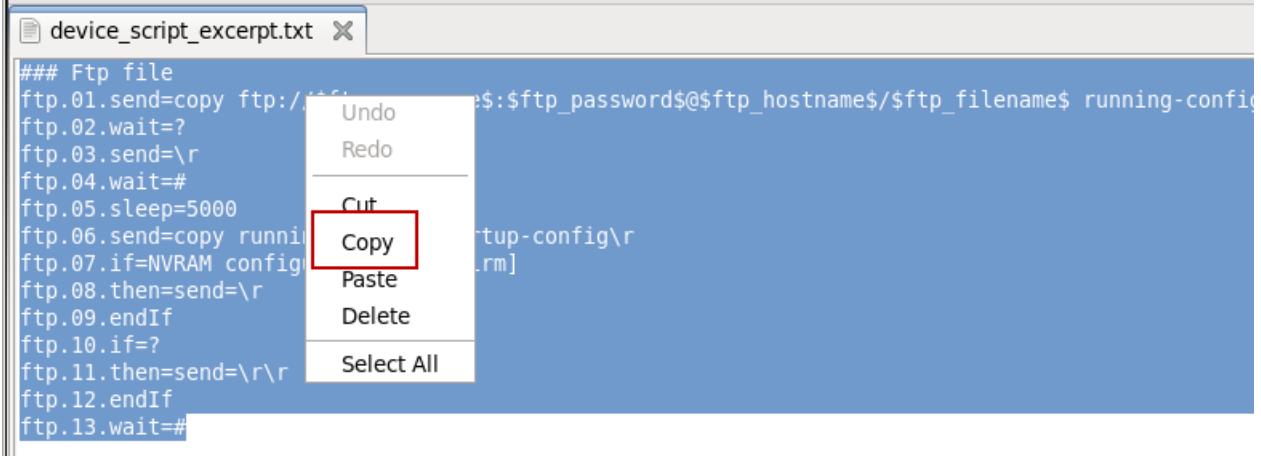
Device Script: Cisco_3640_12.3_DS
File Edit View
[Delete] [New] [Open] [Save] [Print] [Run] [Cancel] [Help]

### Disconnect
#disconnect.01.send=(something to do before disconnecting)
disconnect.errorResponse=Error disconnecting from device.

### Ftp file
ftp.01.send=copy ftp://$ftp_username$:$ftp_password@$ftp_hostname$/ftp_filename$ running-config\r
ftp.02.wait=?\r
ftp.03.send=\r
ftp.04.wait=#\r
ftp.05.sleep=5000\r
ftp.06.send=copy running-config startup-config\r
ftp.07.wait=?\r
ftp.08.send=\r
ftp.09.wait=#\r
#ftp.01.send=copy tftp running-config\r
#ftp.02.wait=?\r
#ftp.03.send=$ftp_hostname$\r

```

- f. Return to the gedit application. Copy the 14 lines from the text file.



```

device_script_excerpt.txt

### Ftp file
ftp.01.send=copy ftp://$ftp_username$:$ftp_password@$ftp_hostname$/ftp_filename$ running-config
ftp.02.wait=?\r
ftp.03.send=\r
ftp.04.wait=#\r
ftp.05.sleep=5000\r
ftp.06.send=copy running-config startup-config\r
ftp.07.if=NVRAM config\r
ftp.08.then=send=\r
ftp.09.endIf\r
ftp.10.if=?\r
ftp.11.then=send=\r\r
ftp.12.endIf\r
ftp.13.wait=#

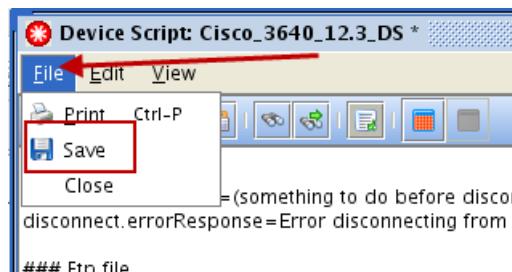
```

- g. Return to the device script. Paste the 14 lines from the text file into the device script.

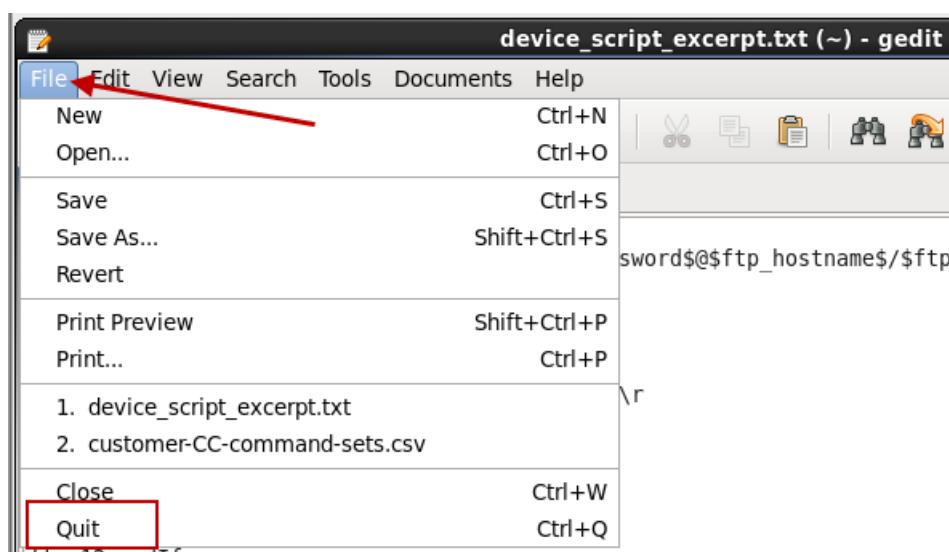
```
Device Script: Cisco_3640_12.3_DS *
File Edit View
H Print Ctrl-P Save Close
### Disconnect
#disconnect.01.send=(something to do before disconnecting)
disconnect.errorResponse=Error disconnecting from device.

### Ftp file
ftp.01.send=copy ftp://$ftp_username$:$ftp_password$@$ftp_hostname$/ftp_filename$ running-config\r
ftp.02.wait=?
ftp.03.send=\r
ftp.04.wait=#
ftp.05.sleep=5000
ftp.06.send=copy running-config startup-config\r
ftp.07.if=NVRAM configuration?[confirm]
ftp.08.then=send=\r
ftp.09.endif
ftp.10.if=?
ftp.11.then=send=\r\r
ftp.12.endif
ftp.13.wait=#
#ftp.01.send=copy tftp running-config\r
#ftp.02.wait=?
#ftp.03.send=$ftp_hostname$\r
```

- h. Click **File > Save** and **File > Close**.



- i. Click **File > Quit** to exit the gedit utility.



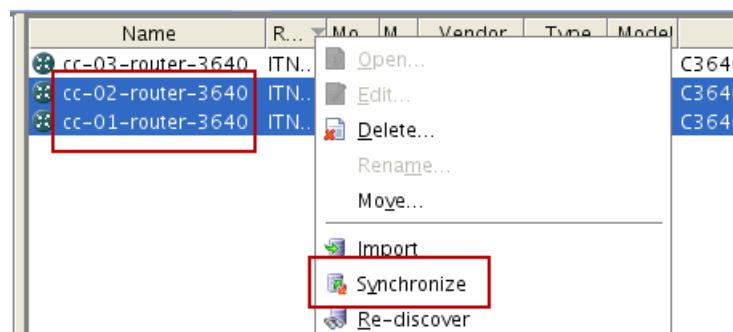
Exercise 4 Creating a device script resource

3. Synchronize the cc-01-router-3640 and cc-02-routers-3640 routers. Notice that cc-01-router-3640 uses IOS version 12.3 and cc-02-router-3640 uses IOS version 12.4.
- Click the **ITNCM > edge-network > customer_CC** realm.

The screenshot shows the ITNCM interface. On the left is a tree view of resources under 'Resource Browser'. Under 'edge-network', there are two realms: 'customer_AA' and 'customer_CC', with 'customer_CC' being selected and highlighted in red. On the right is a table listing three routers:

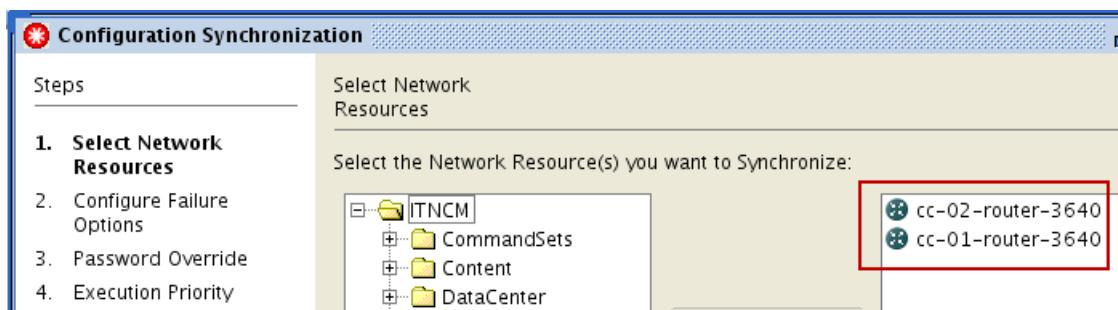
Name	R...	Mo...	M...	Vendor	Type	Model	OS
cc-03-router-3640	ITN...	en...	M...	Cisco	Router	3640	C3640-IK95-M-12.4(25c)
cc-02-router-3640	ITN...	en...	M...	Cisco	Router	3640	C3640-I-M-12.4(25c)
cc-01-router-3640	ITN...	en...	M...	Cisco	Router	3640	C3640-I-M-12.3(5b)

- Select the cc-01-router-3640 and cc-02-router-3640 routers. Right-click and select **Synchronize**.

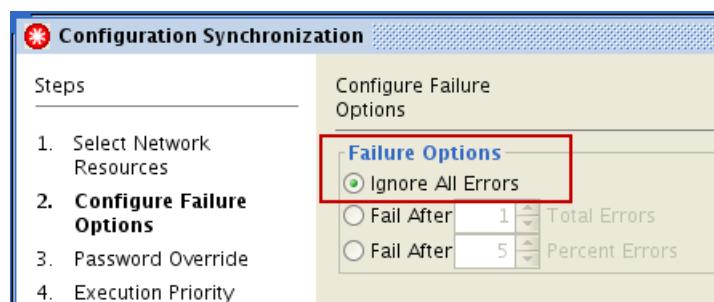


The synchronization wizard starts.

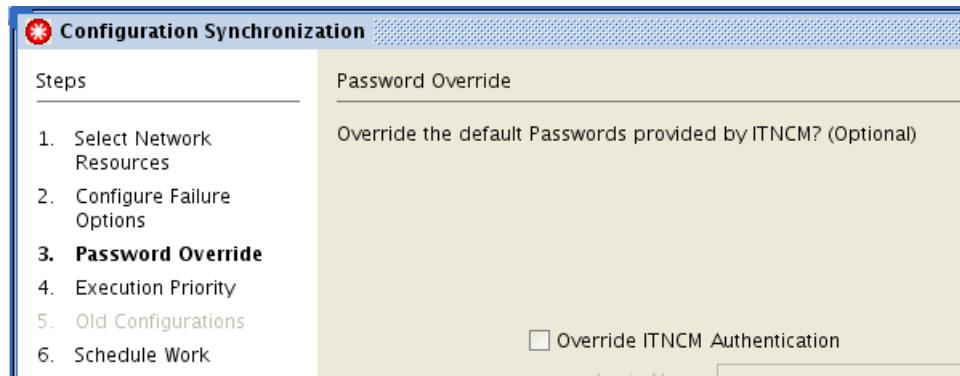
- These two routers are already selected. Click **Next**.



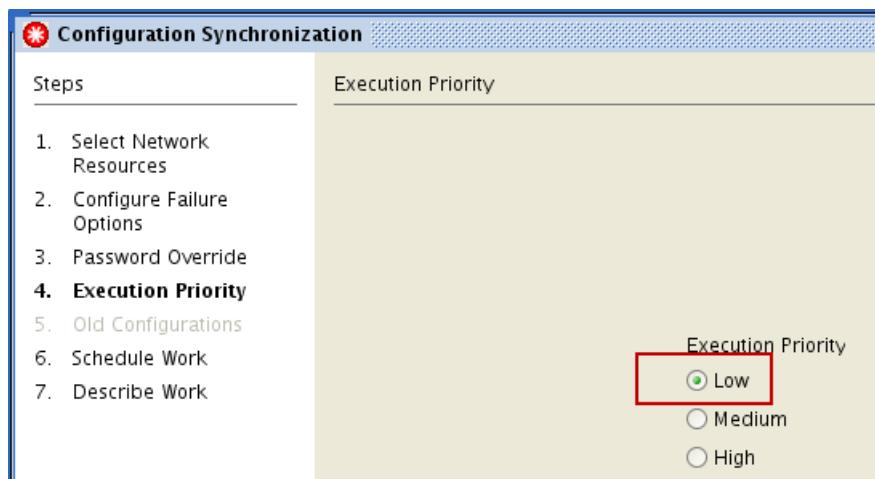
- Click **Next**.



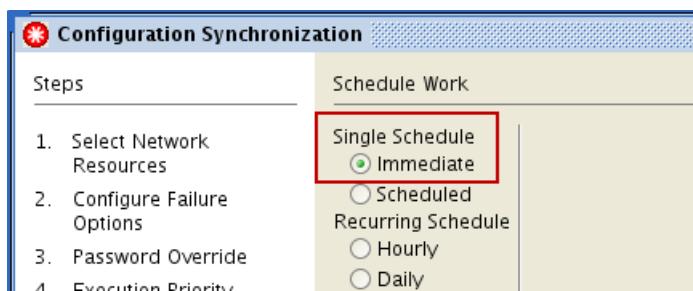
e. Do not override the default authentication. Click **Next**.



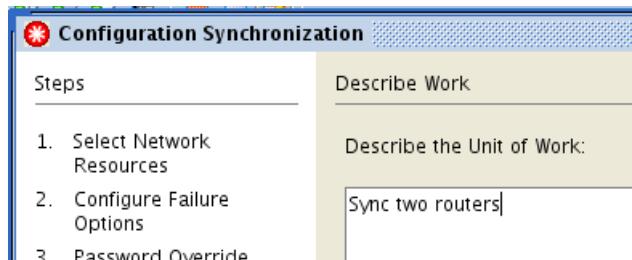
f. Click **Next**.



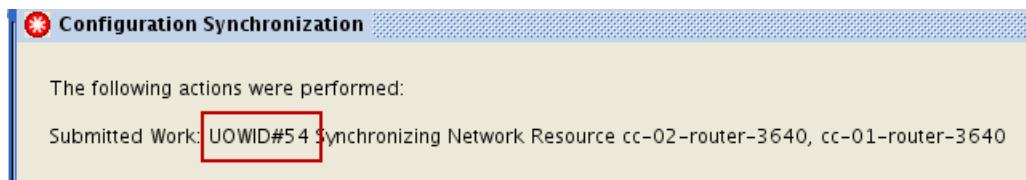
g. Select **Single Schedule > Immediate**. Click **Next**.



h. Enter **Sync two routers** and click **Finish**.



- Note the unit of work number and click **Close**.



- After the unit of work finishes, look at the work log for each of the routers you synchronized. Notice that the new device script is used to connect to the cc-01-router-3640 router. A different device script is used to connect to the cc-02-router-3640 router.
- Click **Work That is Finished** in the *queue manager*. Click the unit of work that synchronized the two routers.

UOW ID	Type	Submitter	Request Type	Status
48	UOW	engineer	Remove Network Resource	SUCCESS
49	UOW	engineer	Remove Network Resource	SUCCESS
50	UOW	engineer	Remove Network Resource	SUCCESS
51	UOW	administrator	Run Autodiscovery	FAILURE
52	UOW	engineer	Configuration Synchronization (...)	SUCCESS
53	UOW	engineer	Configuration Change	SUCCESS
54	UOW	engineer	Configuration Synchronization (...)	SUCCESS

- Click the **Resources** tab. Click the cc-01-router-3640 router.

Summary Results **Resources** Approvals Schedule Details

Name	Realm	Status	Failure	Service	Set...
cc-02-router-3640	ITNC...	Up	None	W...	
cc-01-router-3640	ITNC...	Up	None	W...	

```

atomic resource 'cc-01-router-3640' (VT**)
match: Cisco/Router/**/*
(8) Using DeviceScript resource
'ITNCM/Cisco_3640_12.3_DS' for atomic resource
'cc-01-router-3640' (VTMOS match:
Cisco/Router/3640/*12.3*)
(9) <<< Operation Finished in 0 seconds
(radCheck): 2016/05/09 19:54:31.644 GMT+00:00
(10) >>> Operation Started on Worker Server

```

Notice in the work log that the **Cisco_3640_12.3_DS** device script is used to connect to this router.

- Click the cc-02-router-3640 router.

Summary Results **Resources** Approvals Schedule Details

Name	Realm	Status	Failure	Service	Set...
cc-02-router-3640	ITNC...	Up	None	W...	
cc-01-router-3640	ITNC...	Up	None	W...	

```

match: Cisco/Router/**/*
(8) Using DeviceScript resource
'ITNCM/Cisco_36x_Device_Script' for atomic resource
'cc-02-router-3640' (VTM* match:
Cisco/Router/36*/*)
(9) <<< Operation Finished in 0 seconds
(radCheck): 2016/05/09 19:54:31.624 GMT+00:00

```

Notice in the work log that a different device script is used to connect to this router.

Exercise 5 Viewing a file transfer resource

In this exercise, you view a file transfer resource.

1. Find the file transfer resource that is used for devices in the customer_CC realm.
 - a. Click the **customer_CC** realm.

The screenshot shows the ITNCM interface. On the left, the Resource Browser tree is expanded to show the ITNCM realm, which contains CommandSets, Content, DataCenter, edge-network, customer_AA, and customer_CC. The customer_CC folder is selected and highlighted in blue. On the right, a table lists three Cisco routers: cc-03-router-3640, cc-02-router-3640, and cc-01-router-3640. The columns are Name, R..., Mo..., M..., Vendor, and Type. All three routers are listed as Cisco routers.

Name	R...	Mo...	M...	Vendor	Type
cc-03-router-3640	ITN...	en...	M...	Cisco	Route
cc-02-router-3640	ITN...	en...	M...	Cisco	Route
cc-01-router-3640	ITN...	en...	M...	Cisco	Route

All of the devices in the customer_CC realm are Cisco routers. The customer_CC realm does not contain a file transfer resource for Cisco routers. Look at the parent realm.

- b. The parent realm is named **edge-network**. Click the **edge-network** realm.

The screenshot shows the ITNCM interface. On the left, the Resource Browser tree is expanded to show the ITNCM realm, which contains CommandSets, Content, DataCenter, and edge-network. The edge-network folder is selected and highlighted in blue. On the right, a table lists three realms: Cisco-Router-RAD, customer_AA, and customer_CC. The columns are Name, R..., Mo..., M..., and Vendor. Cisco-Router-RAD is listed as a Cisco router, while customer_AA and customer_CC are listed as M... (Management).

Name	R...	Mo...	M...	Vendor
Cisco-Router-RAD	ITN...	en...	M...	Cisco
customer_AA	ITN...	en...	M...	
customer_CC	ITN...	en...	M...	

The edge-network realm does not contain a file transfer resource for Cisco routers. Look at the parent realm.

- c. The parent realm is named **ITNCM**. Click the **ITNCM** realm.

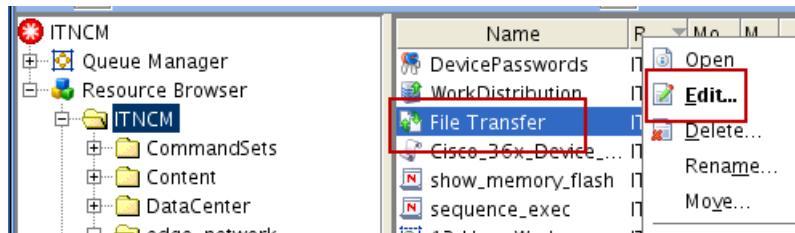
The screenshot shows the ITNCM interface. On the left, the Resource Browser tree is expanded to show the ITNCM realm, which contains CommandSets, Content, DataCenter, and edge-network. The ITNCM folder is selected and highlighted in blue. On the right, a table lists various resources: DevicePasswords, WorkDistribution, File Transfer, Cisco_36x_Device, show_memory_flash, sequence_exec, and test. The File Transfer resource is highlighted with a red box. The columns are Name, R..., Mo..., M..., Vendor, Type, and Model. The File Transfer resource is listed as ITN... en... M...*, Router, 36*, and *.*. The Cisco_36x_Device resource is listed as ITN... en... M... Cisco, Router, 36*, and *.*. The show_memory_flash and sequence_exec resources are also listed.

Name	R...	Mo...	M...	Vendor	Type	Model
DevicePasswords	ITN...	en...	M...*	*	*	*
WorkDistribution	ITN...	ad...	F...*	*	*	*
File Transfer	ITN...	en...	M...*	*	*	*
Cisco_36x_Device	ITN...	en...	M... Cisco	Router	36*	*.*
show_memory_flash	ITN...	en...	M... Cisco	Router	*	*
sequence_exec	ITN...	en...	M... Cisco	Router	36*	*12.3*
test	ITN...	an...	M...			

The ITNCM realm does contain a file transfer resource named **File Transfer** for all devices. Cisco routers in the **ITNCM > edge-network > customer_CC** realm resolve to this file transfer resource.

2. Open the file transfer resource named **File Transfer**. Use the **Edit** option to open the document.

 - a. Right-click the file transfer resource and Click **Edit**.



- b. Enter the FTP user name as **tncm_ftp**, the password as **object00**, the FTP host name as **host1.csuite.edu**, and the FTP directory as **/home/tncm_ftp**.

Name:	ftpInfo
Host:	host1.csuite.edu
Username:	tncm_ftp
Password:	object00
Path:	/home/tncm_ftp
<input type="checkbox"/> Passive Mode	

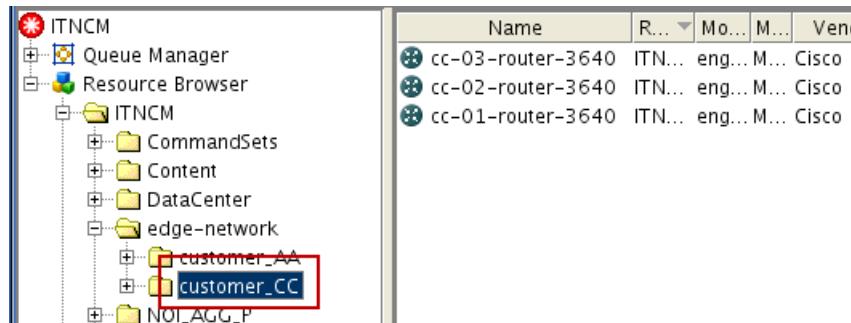
- c. Close the file transfer resource.

Exercise 6 Working with security sets

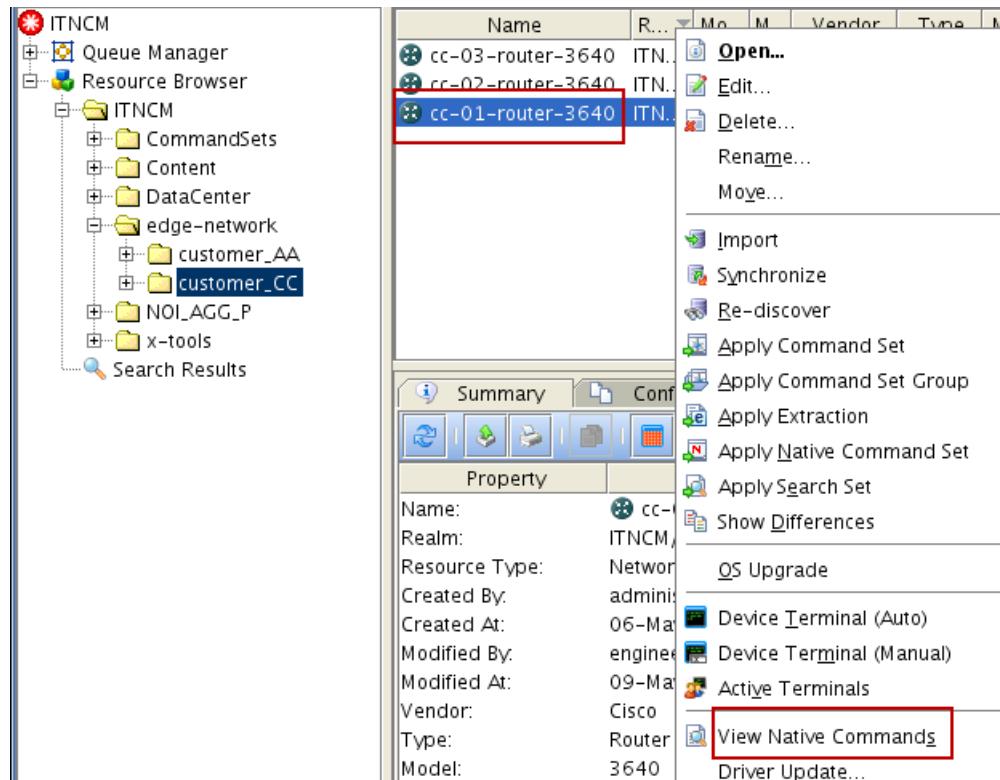
In this exercise, you create and test a security set. The security set you create prevents users in the Customer_CC group from viewing the user password information in a device configuration.

1. Use the **View Native Commands** option to view the configuration of **cc-01-router-3640**.

 - a. Click the **ITNCM > edge-network > customer_CC** realm.



- b. Right-click the **cc-01-router-3640** device and select **View Native Commands**.



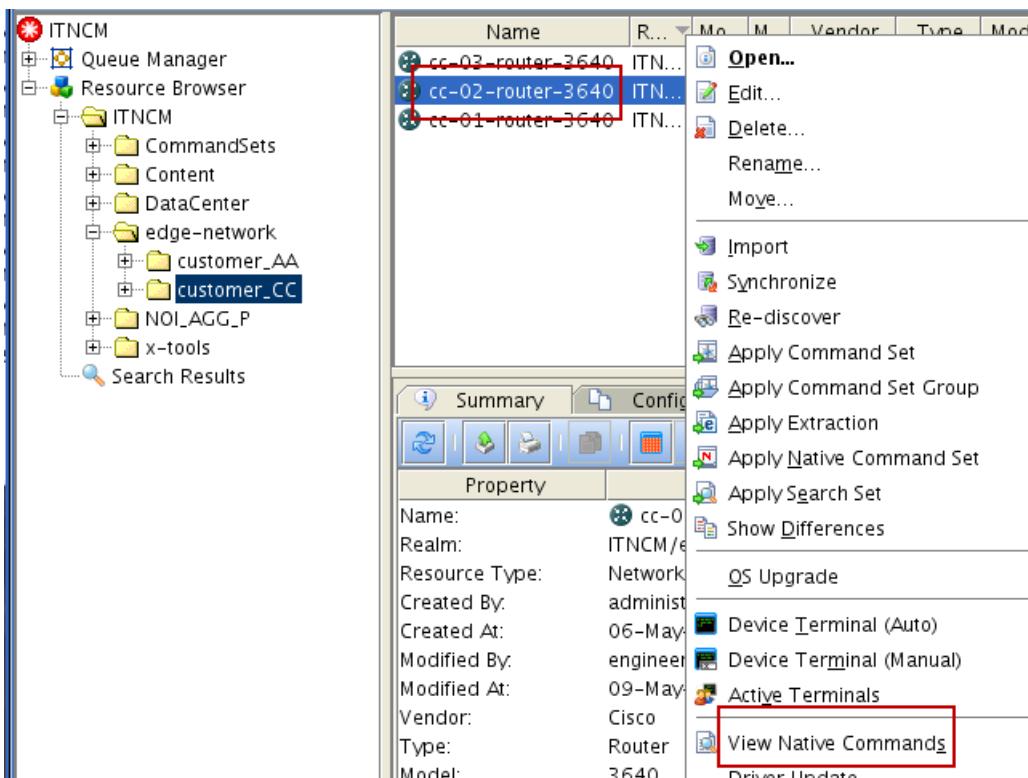
2. Find out which commands in the configuration show user password information. The security set must block any commands that show user password information. Scroll down in the configuration. The two commands that show user password information are **username** and **enable secret**. The security set must block these two commands. Close the configuration when you finish.

```

00012: no logging console
00013: enable secret 5 $1$TXVP$9wwXnF4/IkK9p83E9.Vrz1
00014: !
00015: username intelliden password 0 p4ssw0rd
00016: username itncm password 0 object00
00017: memory-size iomem 25
00018: aaa new-model

```

3. Use the **View Native Commands** option to view the configuration of cc-02-router-3640. Right-click the cc-02-router-3640 device and click **View Native Commands**.



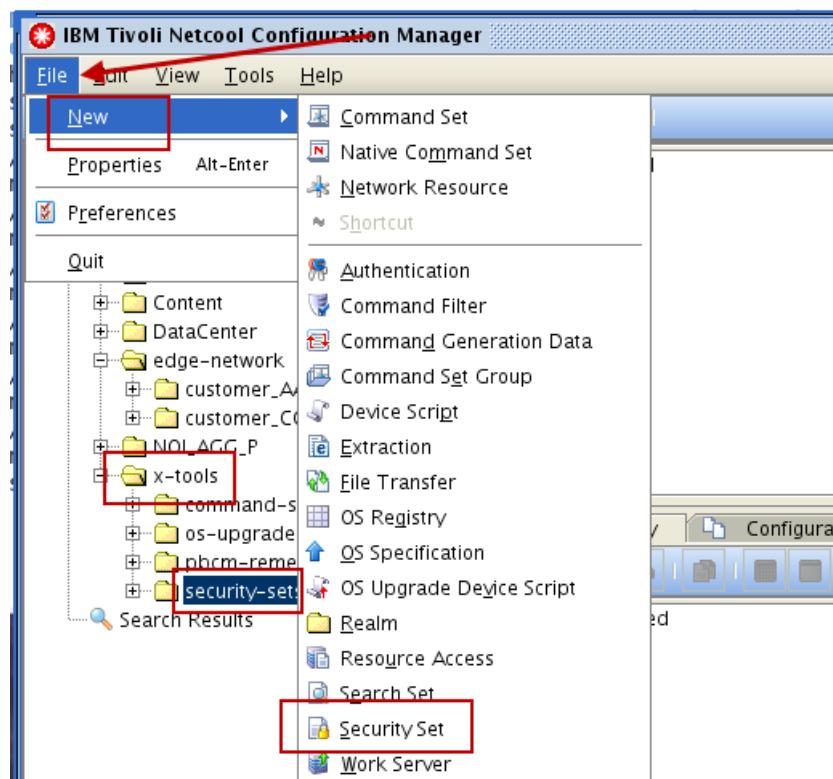
4. Find out which commands in the configuration show user password information. The security set must block any additional commands that show user password information. Scroll down in the configuration. The two commands that show user password information are **enable password** and **username**. The security set must block these two commands. Close the configuration when you finish.

```

00012: no logging console
00013: enable password 7 0558085B23401D
00014: !
00015: aaa new-model
00027: !
00028: username intelliden password 7 0831185D1A0E550516
00029: !
00030: !

```

5. Create a security set in the **ITNCM > x-tools > security-sets** realm. Use the following parameters to create the security set. Save and close the security set when you finish.
 - Name the security set **no_passwords**.
 - Use **Cisco/Router/* /*** as the VTMOS.
 - Configure the security set to block the **username**, **enable secret**, and **enable password** commands from a configuration. Block all rights (VMAD) to these three commands.
 - Remember to use the **securityMarkup** keyword to permit users to see the entire configuration except for these three commands.
 - Use correct XML formatting and close each XML tag.
- a. Click the **ITNCM > x-tools > security-sets** realm. Click **File > New > Security Set**.

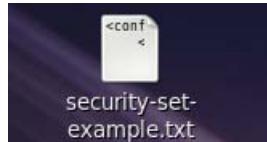


- b. Enter **no_passwords** as the name. Choose **Cisco** as the vendor. Choose **Router** as the type. Choose ***** as the model. Choose ***** as the OS. Click **OK**.



6. Add the following seven lines to the security set. In this example, the lines are wrapped to fit the page. The XML content for this security set is contained in the **security-set-example.txt** document that is on the desktop. Edit the **security-set-example.txt** and copy and paste the XML into the **no_password** security set. Be sure to completely overwrite the default XML that is in the **no_password** security set.

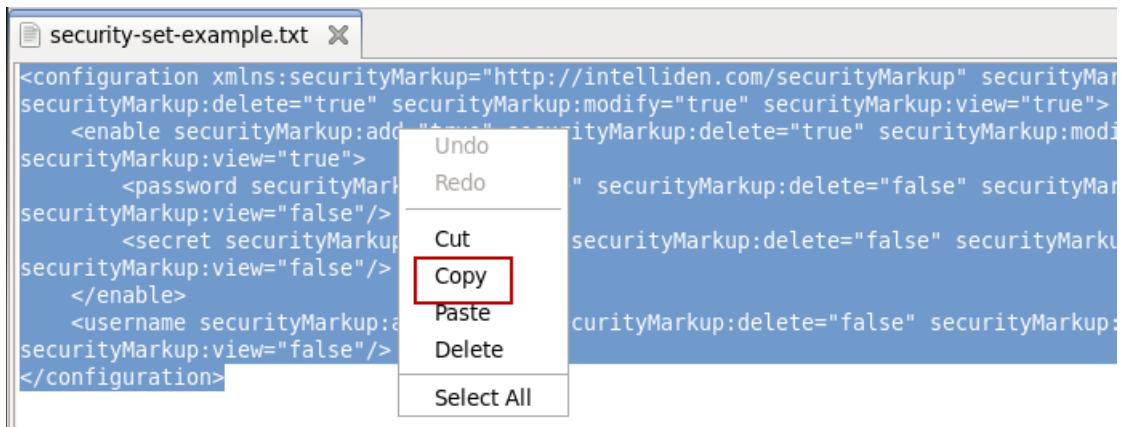
- a. Double-click the **security-set-example.txt** document that is on the desktop.



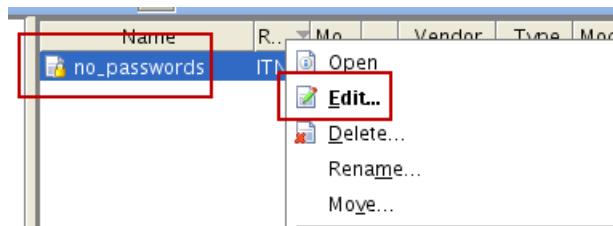
- b. Click **Display**.



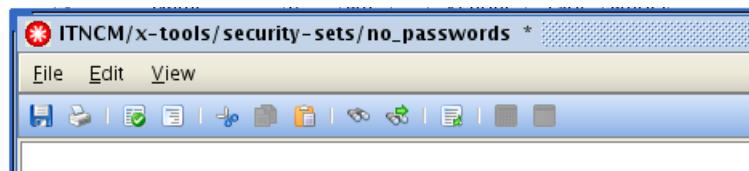
- c. Copy all of the text in the document.



- d. Right-click the **no_passwords** security set. Click **Edit**.



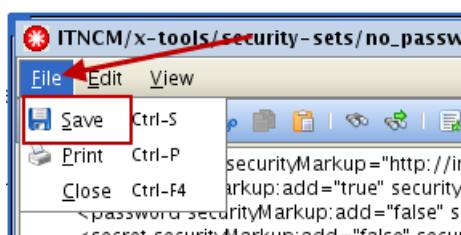
- e. Remove the default text in the **no_passwords** security set.



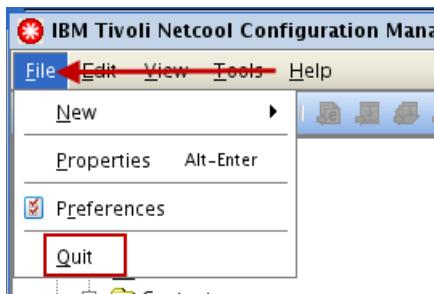
- f. Paste the XML content into the **no_passwords** security set.



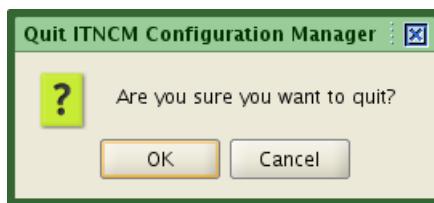
- g. Click **File > Save** and **File > Close**.



7. Exit the user interface.
 - a. Click **File > Quit**.



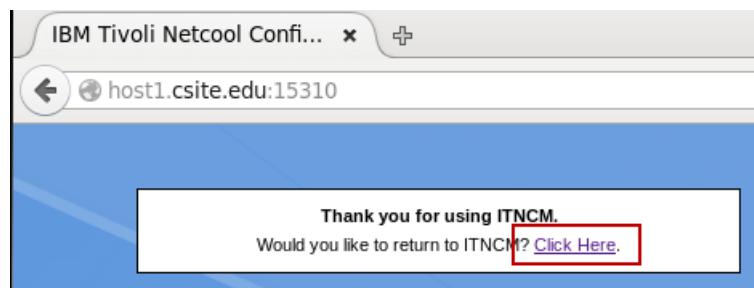
- b. Click **OK**.



8. Return to the Firefox browser and click **Logoff**.



- a. Select **Click Here**.



- b. Enter **administrator** and **object00** for the user name and password. Click **Login**.



9. Click Account Management.

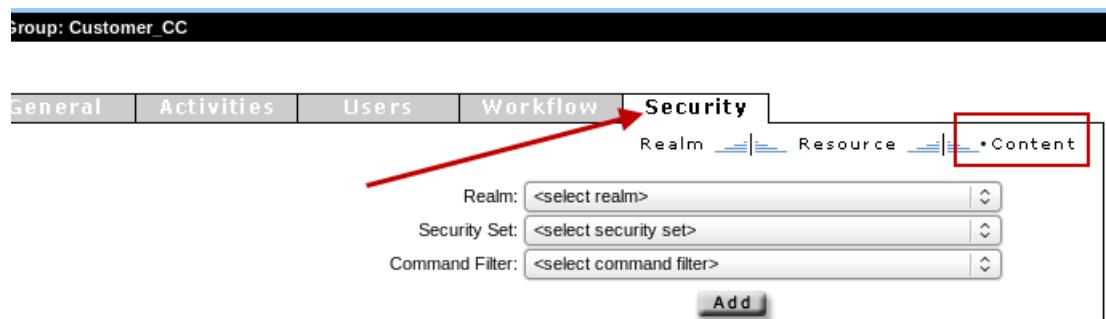


10. Click the **Customer-CC** group.

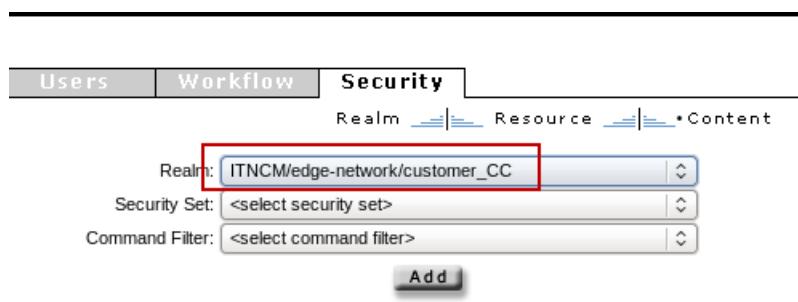


11. Use the Security tab to apply the **no_passwords** security set to the **ITNCM > edge-network > customer-CC** realm. Save the change.

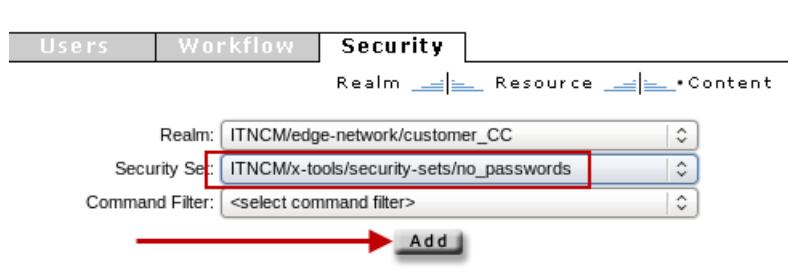
a. Click **Security > Content**.



b. Choose **ITNCM/edge-network/customer-CC** in the **Realm** field.



- c. Choose **ITNCM/xtools/security-sets/no_passwords** in the **Security Set** field. Click **Add**.



- d. Confirm that you applied the security set to the correct realm and click **Save**.

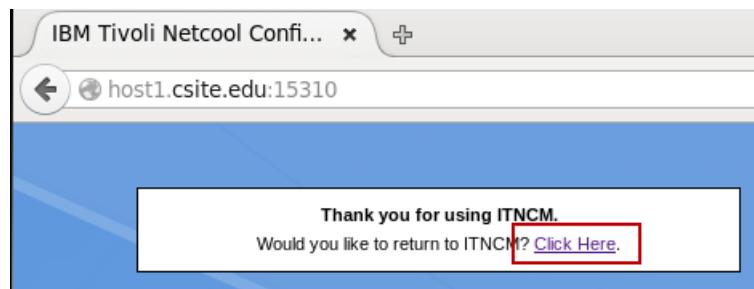
Realm	Resource	Resource Type	Delete	Status
ITNCM/edge-network/customer_CC	ITNCM/x-tools/security-sets/no_passwords	SecuritySet		

A red arrow points from the 'Save' button on the page to the 'Save' button in the bottom right corner of the table.

- e. Click the *running man* icon to log out of account management.

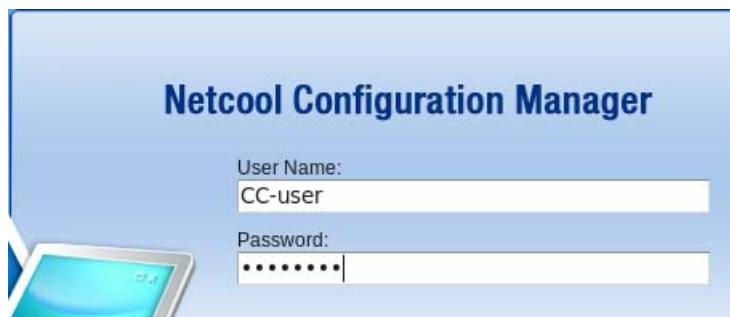


- f. Select **Click Here**.



12. Log In to the user interface with the user name **CC-user**. The password is **object00**.

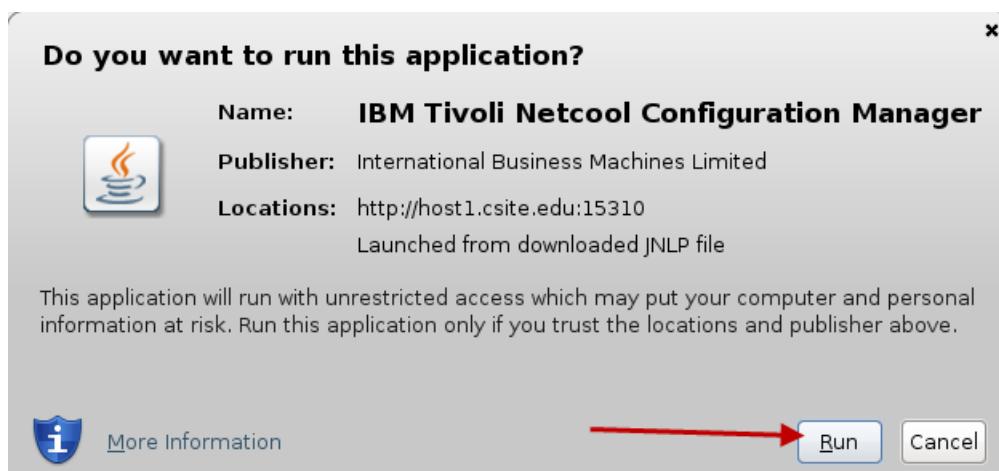
- Enter **CC-user** and **object00** as the user name and password. Click **Login**.



- Click **ITNCM Webstart GUI**.

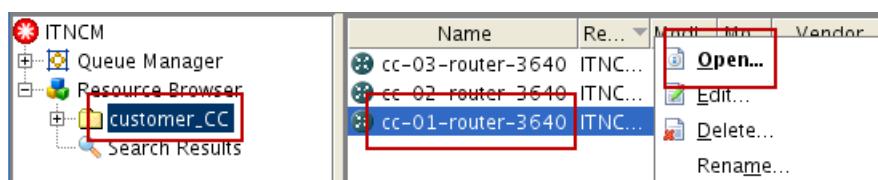


- Click **Run**.

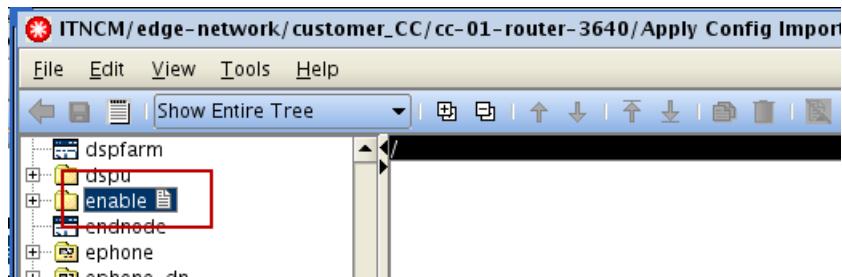


13. Open the configuration of the cc-01-router-3640 device. Verify that the security set successfully blocks the enable passwords and the user name parts of the configuration. Close the configuration when you finish.

- Click **customer_CC** realm in the *resource browser*. Right-click the **cc-01-router-3640** device and click **Open**.

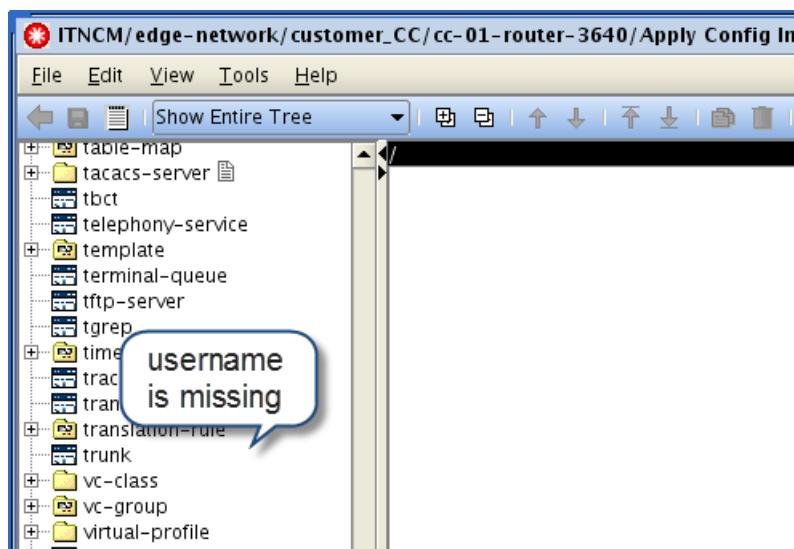


- b. Scroll down and click the **enable** command.



The **enable** command is shown, but it is empty. It is empty because the subcommands **password** and **secret** are blocked.

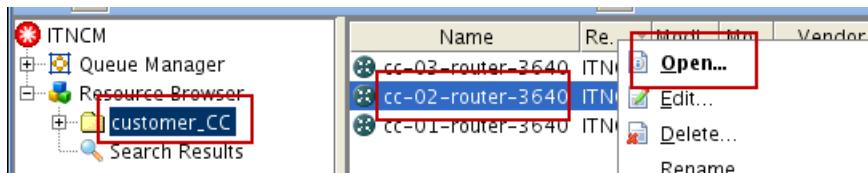
- c. Scroll down and click the **username** command.



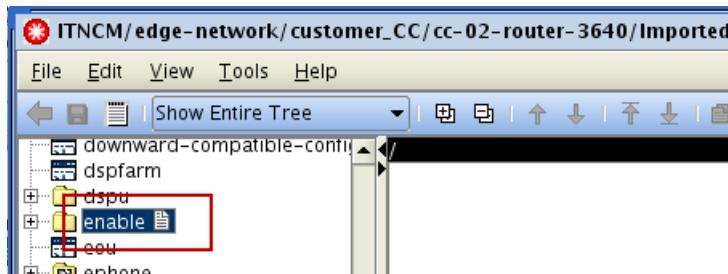
The **username** command is missing from the tree. It is missing because the **username** command is blocked. Close the configuration.

14. Open the configuration of the cc-02-router-3640 device. Verify that the security set successfully blocks the enable passwords and the username parts of the configuration. Close the configuration when you finish.

- a. Click **customer_CC** realm in the *resource browser*. Right-click the **cc-02-router-3640** device and click **Open**.

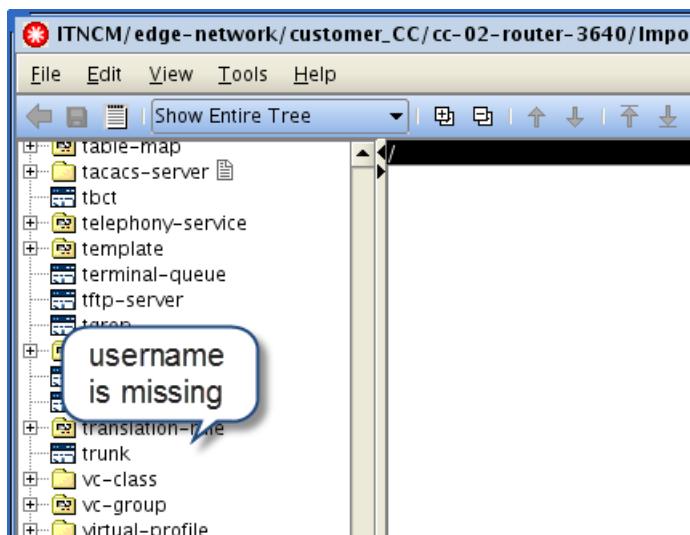


- b. Scroll down and click the **enable** command.



The **enable** command is shown, but it is empty. It is empty because the subcommands **password** and **secret** are blocked.

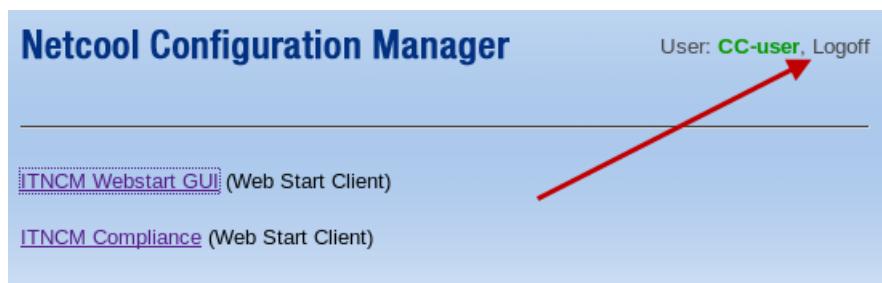
- c. Scroll down and click the **username** command.



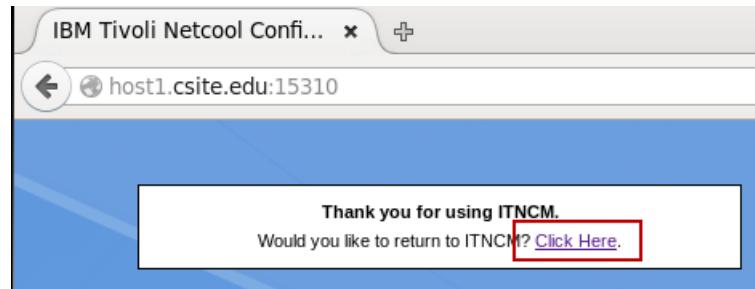
The **username** command is missing from the tree. It is missing because the **username** command is blocked. Close the configuration.

15. Close the configuration manager client.

16. Return to the Firefox browser and click **Logoff**.



17. Select **Click Here**.



Leave the browser session as is. You return to it shortly.



9 Using workflow and scheduling exercises

In this unit you learn how to schedule *units of work*, and create recurring *units of work*.

Exercise 1 Scheduling work

In this exercise, you create and schedule a unit of work.

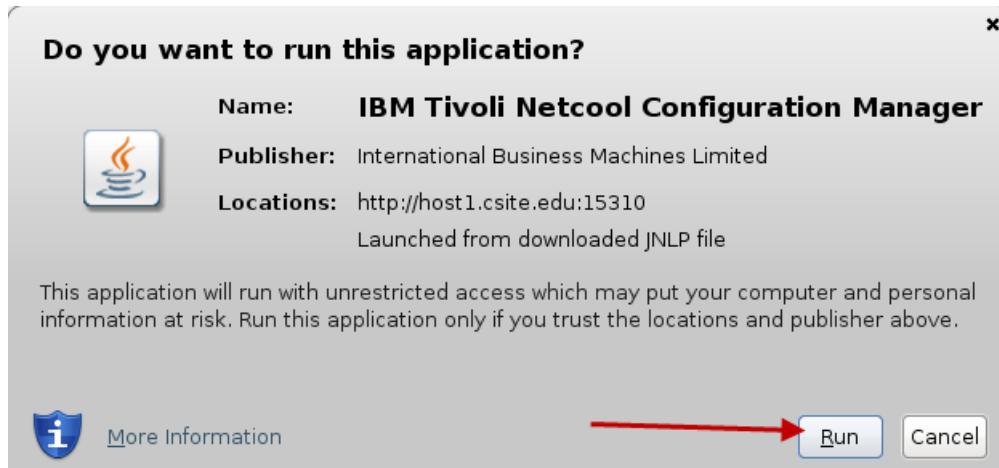
1. Log on to the Netcool Configuration Manager user interface with the user name **operator**. The password is **object00**.
 - a. Enter **operator** and **object00** as the user name and password. Click **Login**.



- b. Click **ITNCM Webstart GUI**.

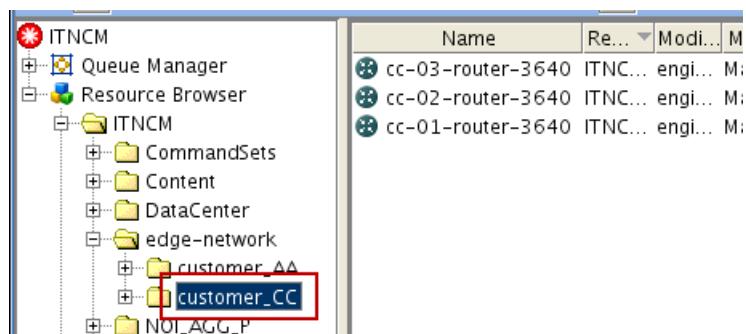


- c. Click Run.

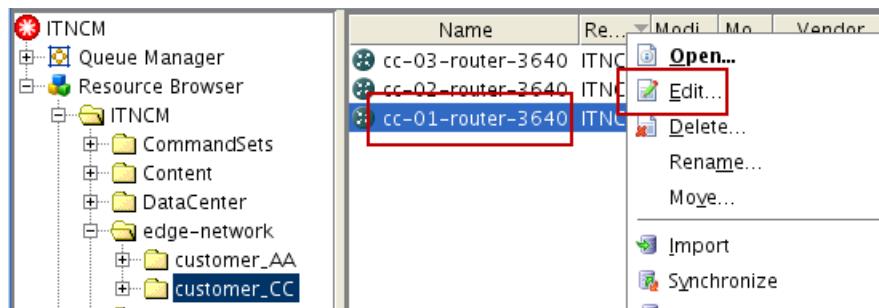


2. Edit the configuration of the cc-01-router-3640 device.

- a. Find the **cc-01-router-3640** device in the *resource browser*. Click **ITNCM > edge-network > customer_CC**.



- b. Right-click **cc-01-router-3640** and click **Edit**.

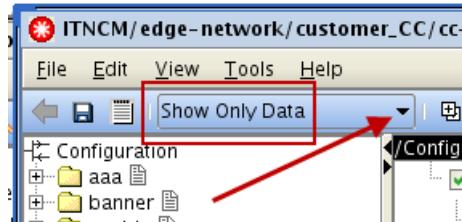


3. Change the **exec-timeout** of the **line vty 0 4** to 10 minutes. When you finish, save it and submit the change. Name the configuration **vty_timeout**. Use the following values to complete the wizard.

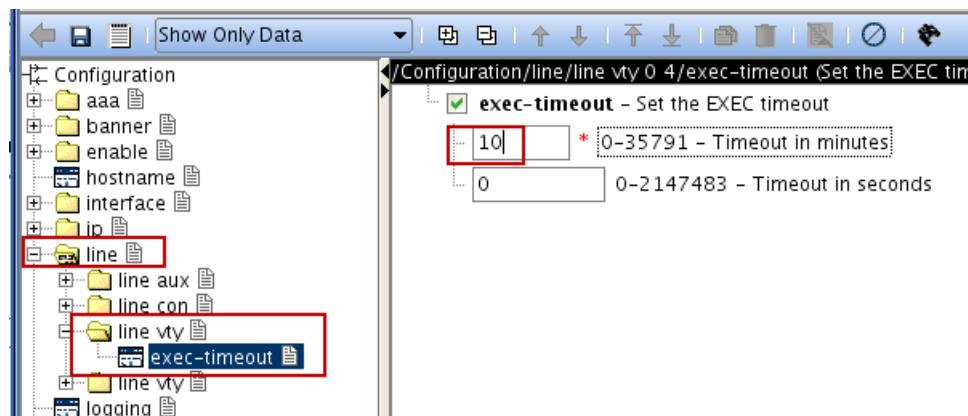
Field	Value
Password Override	Do not override
Execution Priority	Medium

Field	Value
Schedule Work	Select Single Schedule . Schedule the start time for 12:00 AM tomorrow morning. Schedule the end time for 2:00 AM tomorrow morning.
Describe Work	Changing the vty timeout

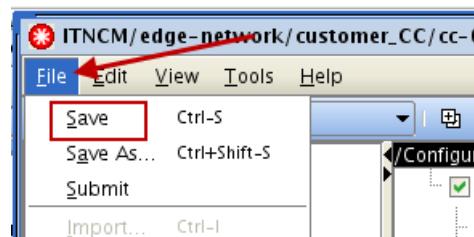
- a. Change the display to **Show Only Data**.



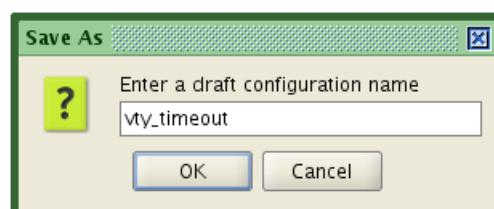
- b. Expand the **line > line vty > exec-timeout** object in the command tree. On the right side of the *configuration editor*, change **15** to **10** in the **Timeout in minutes** field.



- c. Click **File > Save**.



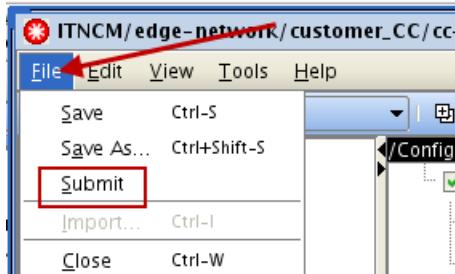
- d. Enter **vty_timeout** as the name of the configuration and click **OK**.



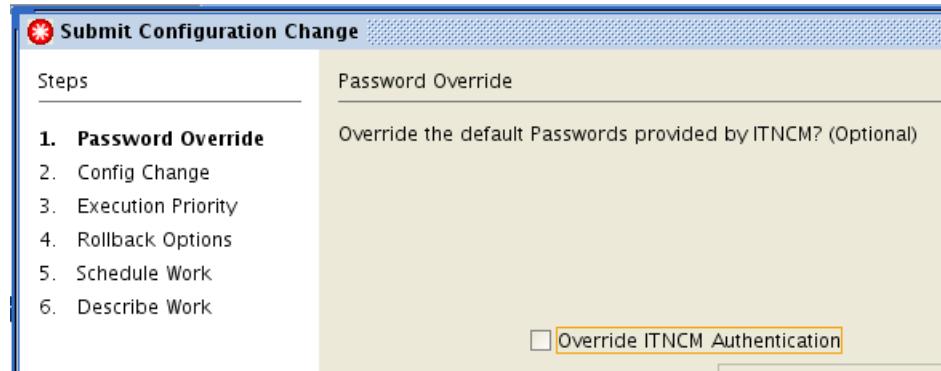
9 Using workflow and scheduling exercises

Exercise 1 Scheduling work

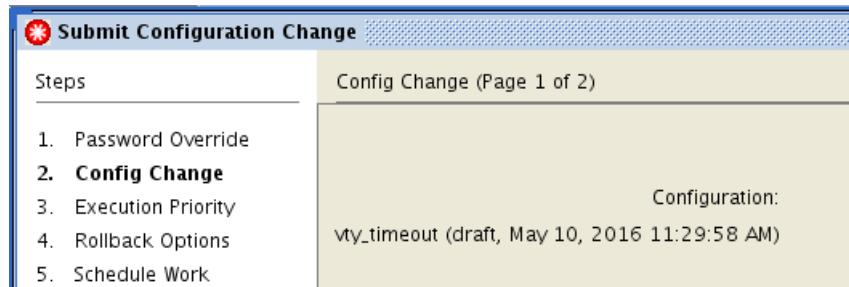
- e. Submit the configuration. Click **File > Submit**. The configuration change wizard starts.



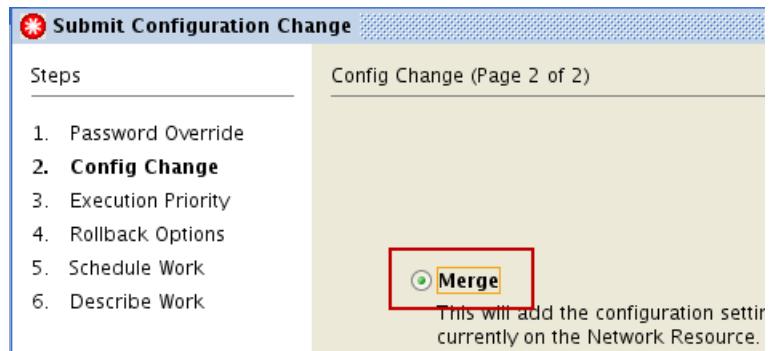
- f. Click **Next** in the Password Override window.



- g. Click **Next** in the Config Change window.



- h. Select **Merge** and click **Next** in the Config Change window



- i. Click **Next** in the Execution Priority window.

The window title is "Submit Configuration Change". The left panel shows steps 1 through 6. Step 3, "Execution Priority", is highlighted. The right panel shows the "Execution Priority" section with three radio buttons: "Low" (unchecked), "Medium" (checked), and "High" (unchecked).

- j. Click **Next** in the Rollback Options window.

The window title is "Submit Configuration Change". The left panel shows steps 1 through 5. Step 4, "Rollback Options", is highlighted. The right panel shows the "Rollback Options" section with three radio buttons: "No Rollback" (checked), "Rollback" (unchecked), and "Use Modeled Rollback" (unchecked). A note above the buttons says "How should Rollback on configuration changes be handled?"

- k. Click **Single Schedule > Scheduled** in the Schedule Work window. Enter 12:00 AM *tomorrow* as the start time. Enter 2:00 AM *tomorrow* as the stop time. Click **Next**.

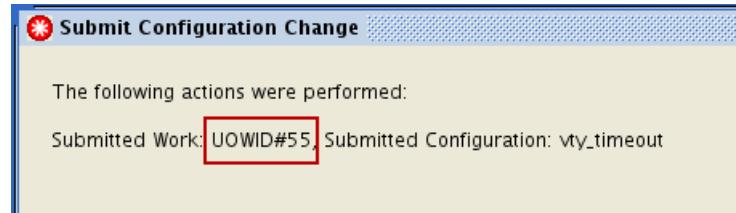
The window title is "Submit Configuration Change". The left panel shows steps 1 through 6. Step 5, "Schedule Work", is highlighted. The right panel shows the "Schedule Work" section. Under "Single Schedule", the "Scheduled" radio button is selected (highlighted with a red box). Under "Recurring Schedule", all other options are unchecked. The "Scheduled Start" field shows "12:00 AM" and "11-May-2016" (with a calendar icon). The "Scheduled End" field shows "2:00 AM" and "11-May-2017" (with a calendar icon).

- l. Enter **Changing the vty timeout** in the Describe Work window. Click **Finish**.

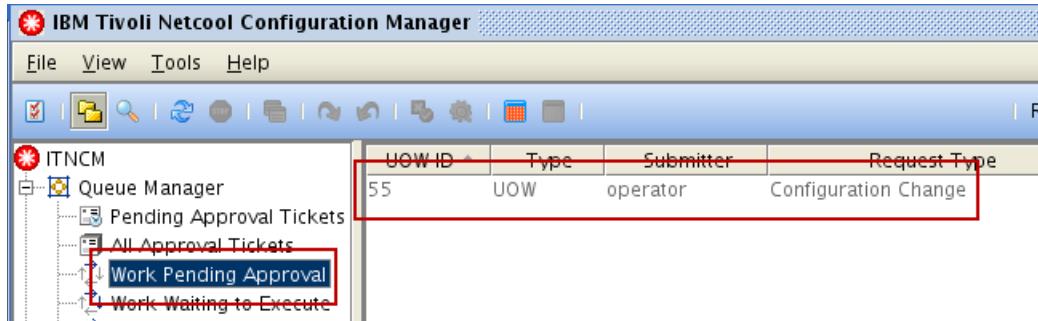
The window title is "Submit Configuration Change". The left panel shows steps 1 through 4. The right panel shows the "Describe Work" section with a text input field containing "Changing the vty timeout".

Exercise 1 Scheduling work

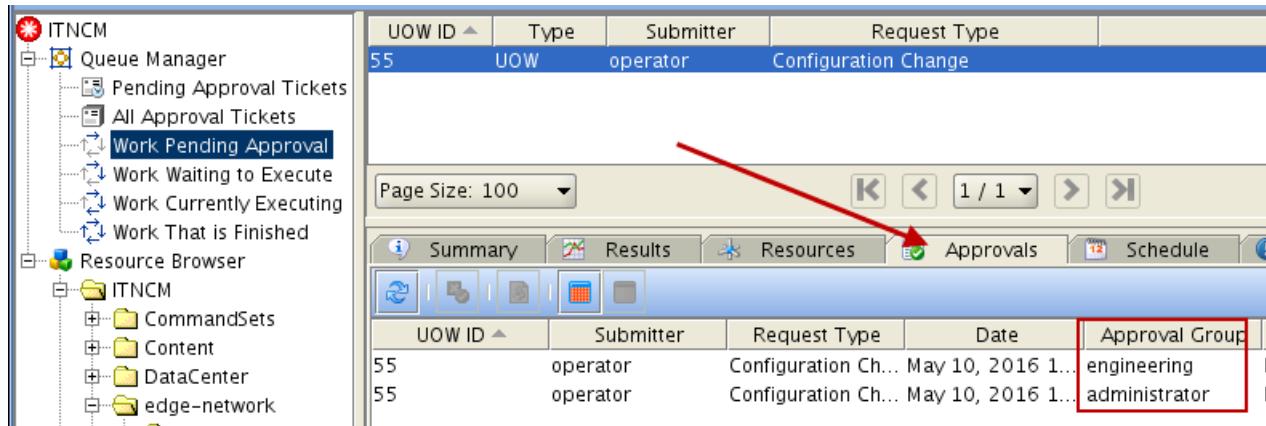
- m. Note the unit of work number and click **Close**.



4. Find the unit of work that you created. Click the **Work Pending Approval** queue in the *queue manager*. The unit of work must be approved before it is processed.

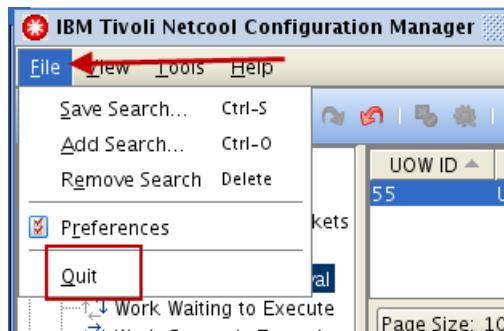


5. Find out what groups can approve the unit of work that you created. Click the unit of work that you created. Click the **Approvals** tab. In the **Approval Group** column, you can see the groups that can approve this unit of work.



6. Log out of the user interface.

- a. Click **File > Quit**.



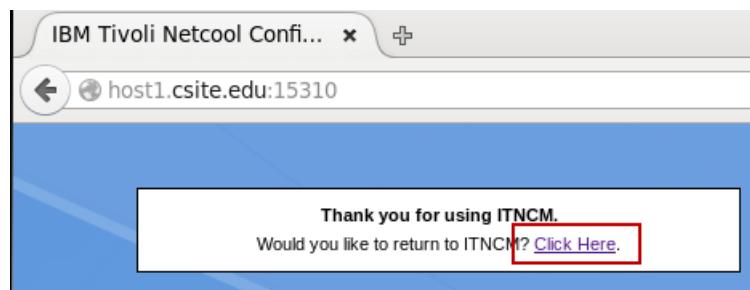
b. Click **OK**.



c. Return to the Firefox browser. Click **Logoff**.

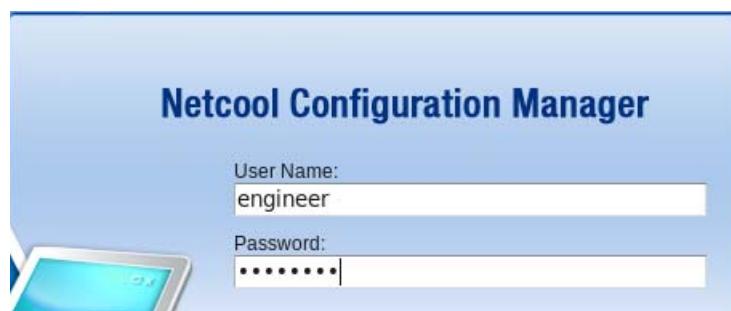


d. Select **Click Here**.



7. Log in to the user interface with the user name **engineer**. The password is **object00**.

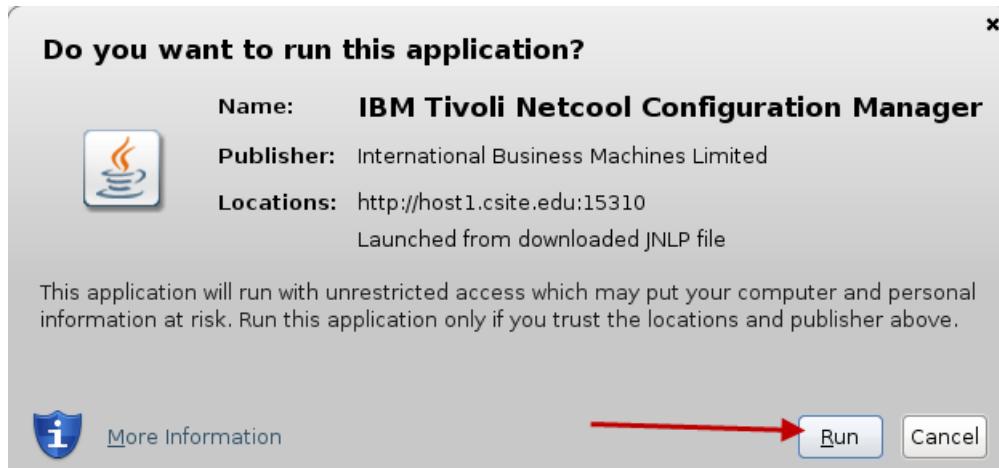
a. Enter **engineer** and **object00** as the user name and password. Click **Login**.



b. Click **ITNCM Webstart GUI**.



- c. Click Run.



8. Find the approval ticket for the unit of work you created and approve it. Enter **Change OK** as the reason for approval.
- Click **Pending Approval Tickets** in the *queue manager*. The approval ticket for the unit of work that you created as the operator user is in this queue.

UOW ID	Submitter	Request Type	
55	operator	Configuration Change	Ma

- b. Right-click the approval ticket and click **Approve/Reject**.

- c. Enter **Change OK** as the reason for approval. Click **Approve**.

Approve or Reject Tickets

You have requested to approve or reject the following tickets:

55/engineering

Enter the reason for approval or rejection:

Change OK

- Find the unit of work that you just approved. Click **Work Waiting to Execute** in the queue manager. The unit of work is in this queue because it is scheduled for tomorrow.

UOW ID	Type	Submitter	Request Type
55	UOW	operator	Configuration Change

Exercise 2 Creating a recurring unit of work

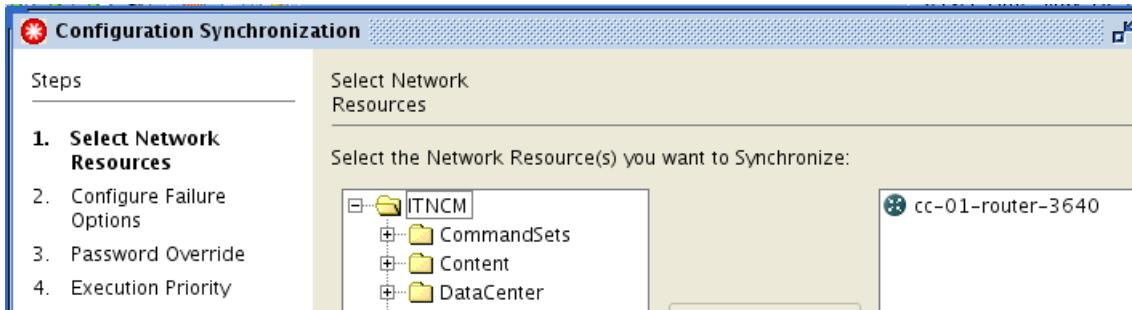
In this exercise, you create a recurring unit of work.

- Select the cc-01-router-3640 in the customer_CC realm. Synchronize it. Use the following values to complete the wizard.

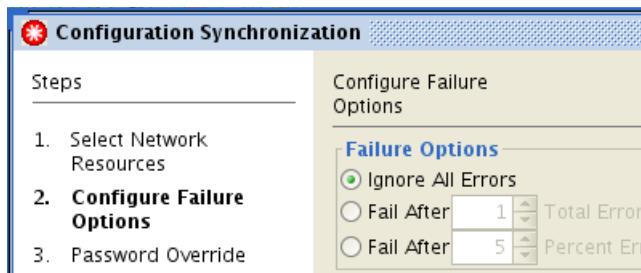
Field	Value
Select Network Resources	Leave cc-01-router-3640 selected
Configure Failure Options	Ignore All Errors
Password Override	Do not override
Execution Priority	Low
Schedule Work	Set the window size to 2 hours. Use a weekly schedule. Configure the unit of work to run at 12:00 AM every Thursday morning.
Describe Work	Synchronization of a single router

- As the **engineer** user, right-click the **ITNCM > edge-network > customer_CC > cc-01-router-3640** device. Click **Synchronize**. The Configuration Synchronization wizard starts.

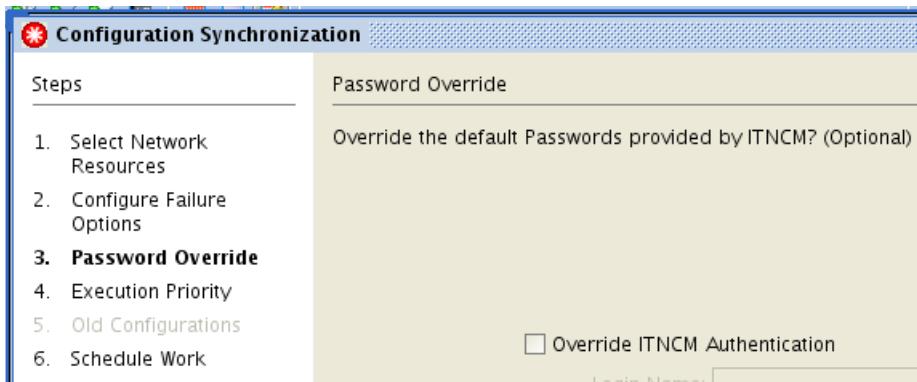
- b. Click **Next** in the Select Network Resources window.



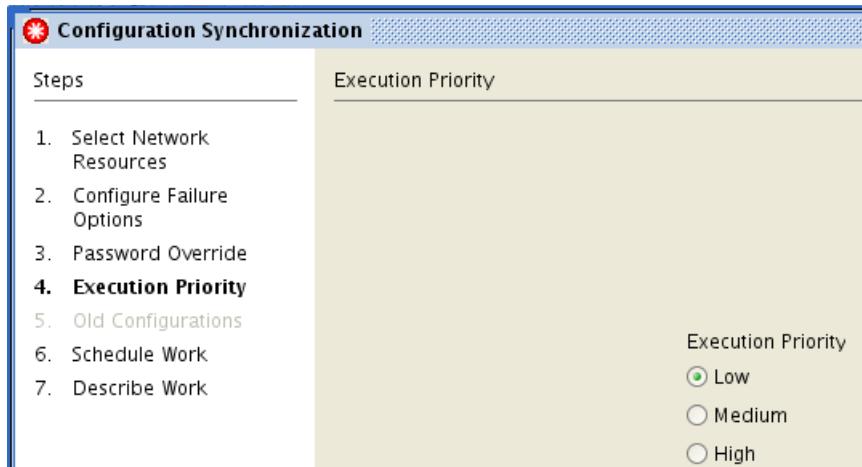
- c. Click **Next** at the Configure Failure Options window.



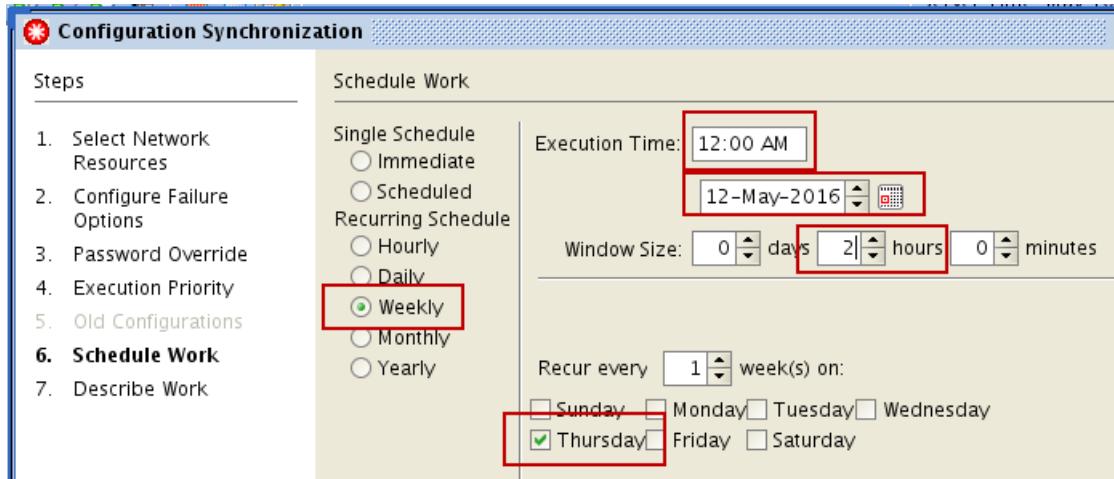
- d. Click **Next** in the Password Override window.



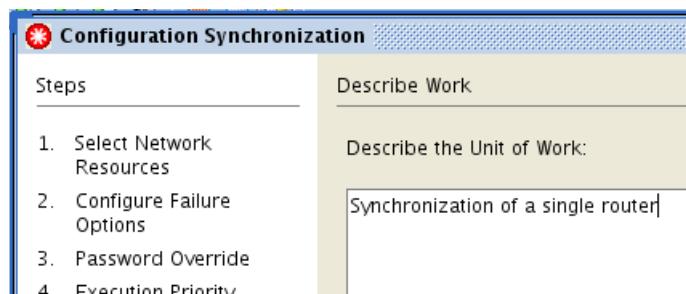
- e. Click **Next** in the Execution Priority window.



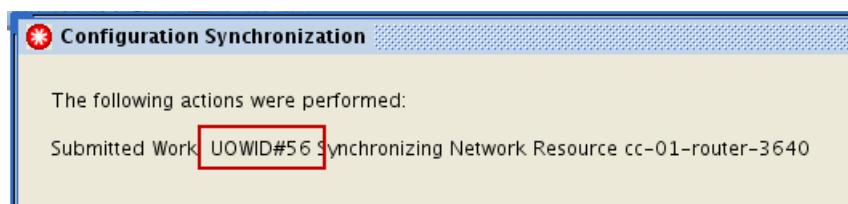
- f. Click **Recurring Schedule > Weekly** in the Schedule Work window. Enter **12:00 AM** next Thursday in the **Execution Time** field. Enter **2 hours** in the **Window Size** field. Schedule the unit of work to recur every **1 week on Thursday**. Click **Next**.



- g. Enter **Synchronization of a single router** in the Describe Work window. Click **Finish**.



- h. Note the unit of work number and click **Close**.



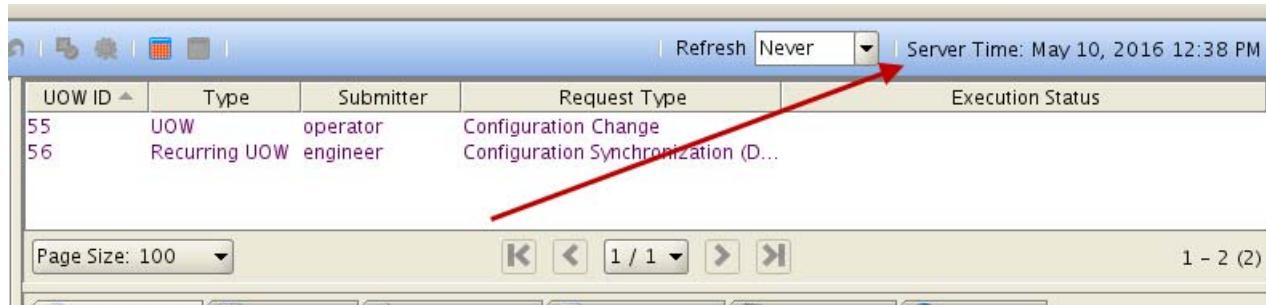
2. Find the recurring unit of work that you created. Click **Work Waiting to Execute** in the queue manager. The recurring unit of work is in this queue.

UOW ID	Type	Submitter	Request Type
55	UOW	operator	Configuration Change
56	Recurring UOW	engineer	Configuration Synchronization

Exercise 3 Working with time zones

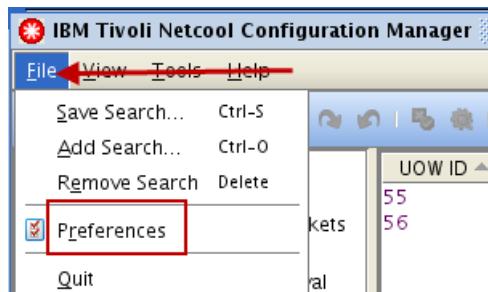
In this exercise, you compare the time zone of the user interface to the zone of the guest operating system.

- Find the **Server Time** in the user interface. Note the time. Look in the upper-right corner of the user interface. This time is shown to the user.

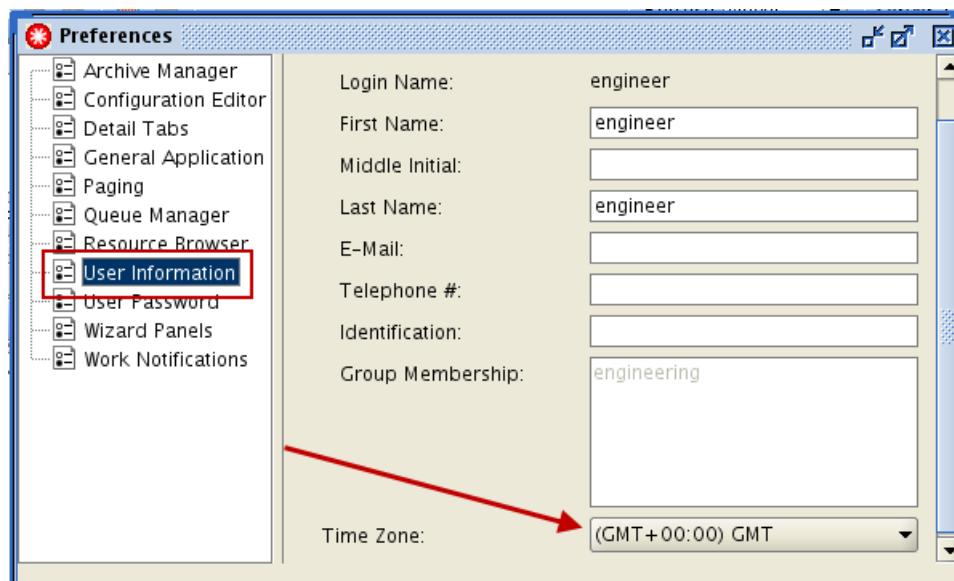


- Find the time zone that you are using in the user interface.

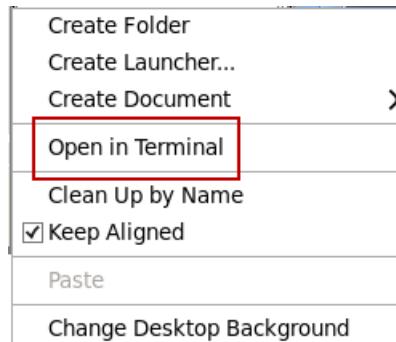
- Click **File > Preferences**.



- Click **User Information**. The engineer user is using the GMT time zone.



3. Open a terminal window in the guest operating system. Use the **date** command to show the system time. Compare it to the server time you found in the user interface.
 - a. Right-click the desktop of the guest system and click **Open in Terminal**.



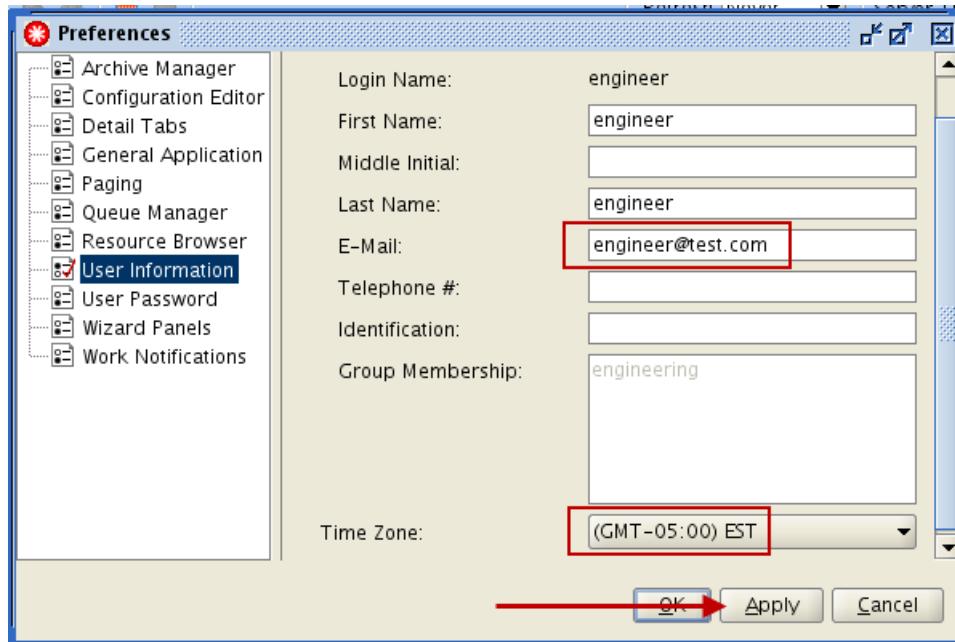
- b. Enter the command **date**. The output of this command is the operating system time.

```
date
```

```
netcool@host1:~/Desktop
File Edit View Search Terminal Help
[netcool@host1 Desktop]$ date
Tue May 10 12:42:29 UTC 2016
[netcool@host1 Desktop]$
```

The engineer user sees the same time as the server.

4. Enter **engineer@test.com** for the email address. Select **(GMT-05:00) EST** and click **Apply**.



5. Close the preferences window.

9 Using workflow and scheduling exercises

Exercise 3 Working with time zones

The time that the user sees is now set to Eastern Standard Time.



Leave the user interface as is. You return to it shortly.



10 UOW management exercises

In this unit, you learn how Configuration Manager processes *units of work*.

Exercise 1 Finding a worker server resource

In this exercise, you view a worker server resource.

1. Find the worker server resource that is used for devices in the **customer_CC** realm.
 - a. Click the **customer_CC** realm.

Name	Re...	Modi...	Mo...	Vendor
cc-03-router-3640	ITNC...	engi...	Ma...	Cisco
cc-02-router-3640	ITNC...	engi...	Ma...	Cisco
cc-01-router-3640	ITNC...	engi...	Ma...	Cisco

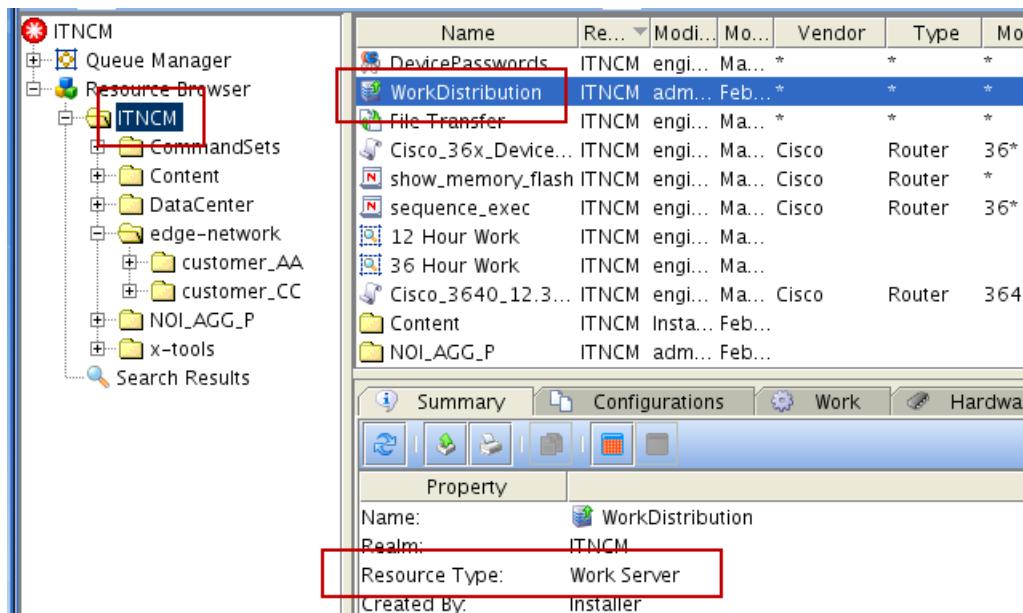
All of the devices in the **customer_CC** realm are Cisco routers. The **customer_CC** realm does not contain a worker server resource for Cisco routers. Look at the parent realm.

- b. The parent realm is named **edge-network**. Click the **edge-network** realm.

Name	Re...	Modi...	Mo...	Vendor
Cisco-Router-RAD	ITNC...	engi...	Ma...	Cisco
customer_AA	ITNC...	engi...	Ma...	Cisco
customer_CC	ITNC...	engi...	Ma...	Cisco

The **edge-network** realm does not contain a worker server resource for Cisco routers. Look at the parent realm.

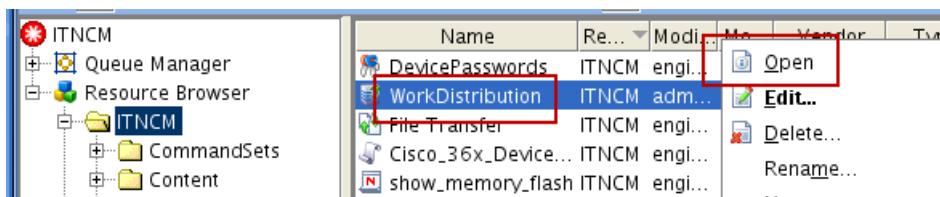
- c. The parent realm is named **ITNCM**. Click the **ITNCM** realm.



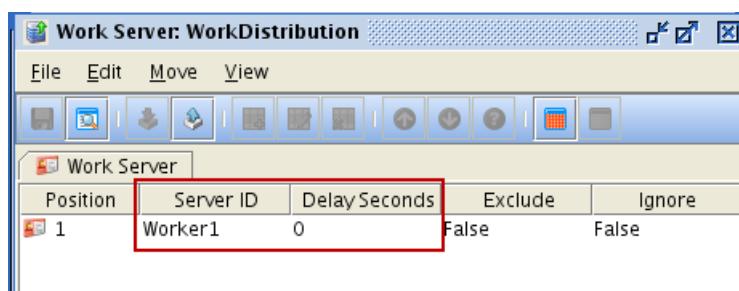
The ITNCM realm contains a worker server resource that is named **WorkDistribution** for all devices. Devices in the customer_CC realm resolve to this worker server resource.

2. Open the worker server resource.

- a. Right-click the **WorkDistribution** resource. Click **Open**.



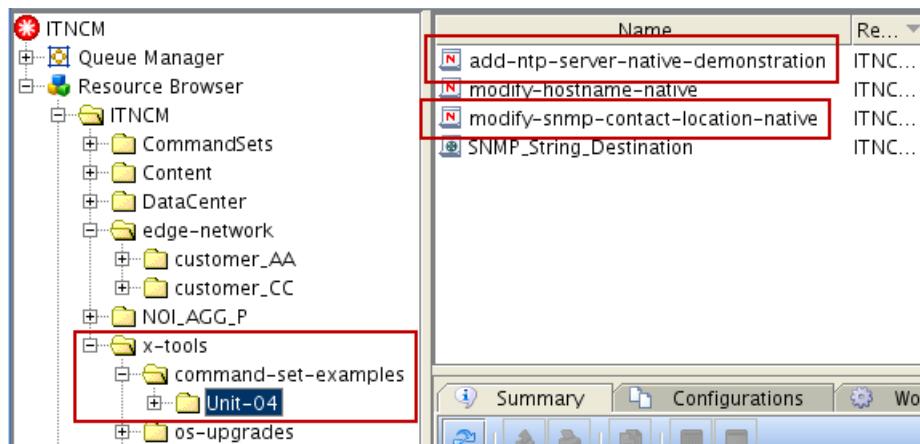
- b. The resource contains only one worker server. The server name is **Worker1**. The delay setting is **0**. Close the resource when you finish.



Exercise 2 Splitting a unit of work

In this exercise, you submit a unit of work and split it into smaller units of work.

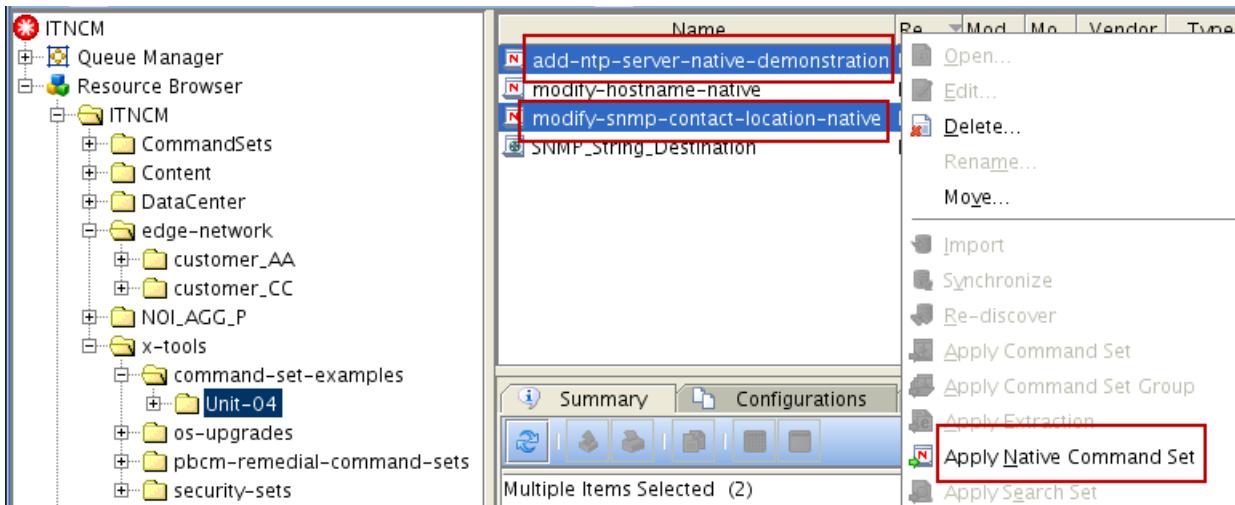
- Find the **modify-snmp-contact-location-native** and **add-ntp-server-native-demonstration** native command sets in the **TNCM/x-tools/command-set-examples/Unit-04** realm. Click the **ITNCM/x-tools/command-set-examples/Unit-04** realm in the **resource browser**.



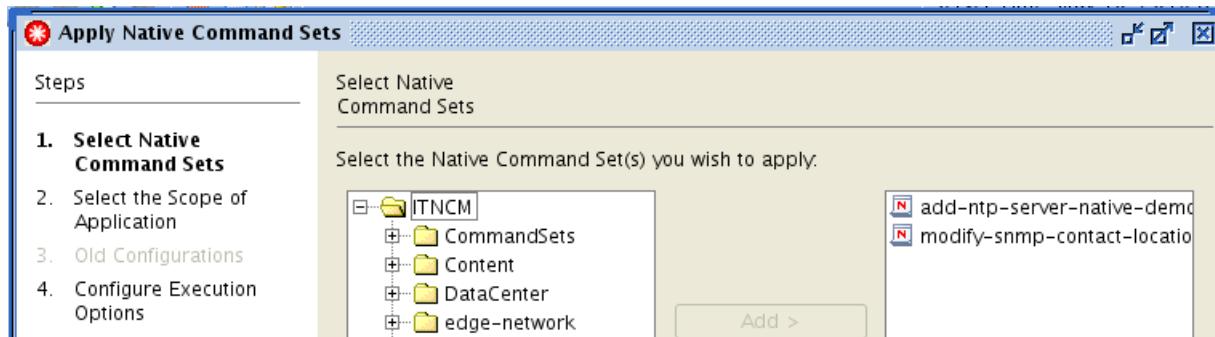
- Apply the **modify-snmp-contact-location-native** and **add-ntp-server-native-demonstration** native command sets. The Apply Command Sets wizard starts. Use the following values to complete the wizard. When you finish, notice that the work is split into multiple units of work.

Field	Value
Select Command Sets	Leave modify-snmp-contact-location-native and add-ntp-server-native-demonstration as the selected command sets
Scope of Application	Apply the Command Sets to specific Network Resources
Scope of Application	Add all of the devices in the customer_CC and customer_AA realm to the unit of work.
Execution Options	Apply Device at a time
Rollback Options	Default
Enter Parameters	Defaults
Password Override	Do not override
Execution Priority	Medium
Schedule Work	Single Schedule > Immediate
Resources per UOW	Select two resources per unit of work
Describe Work	Applying native command set

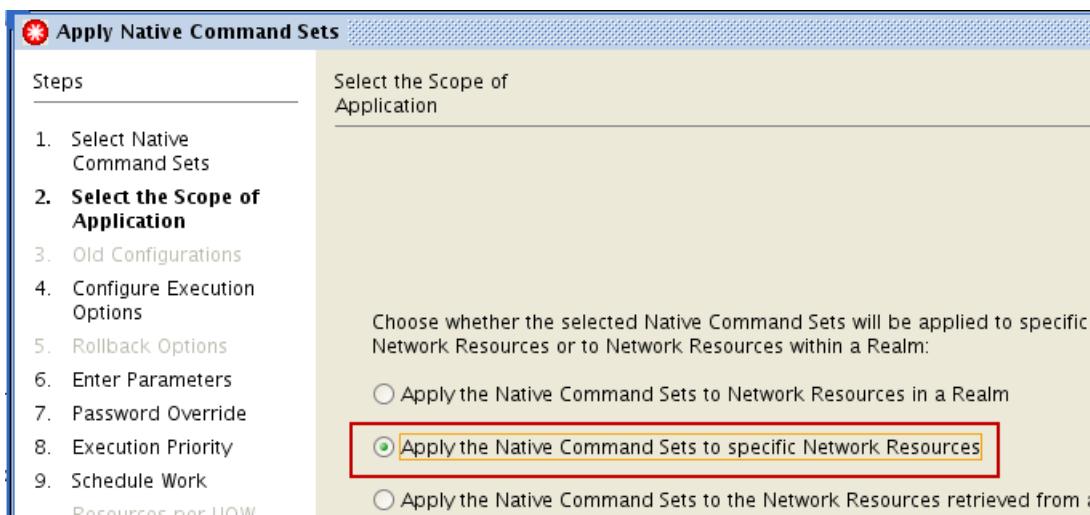
- a. Select the **modify-snmp-contact-location-native** and **add-ntp-server-native-demonstration** native command sets. Right-click and select **Apply Native Command Set**. The Apply Command Sets wizard starts.



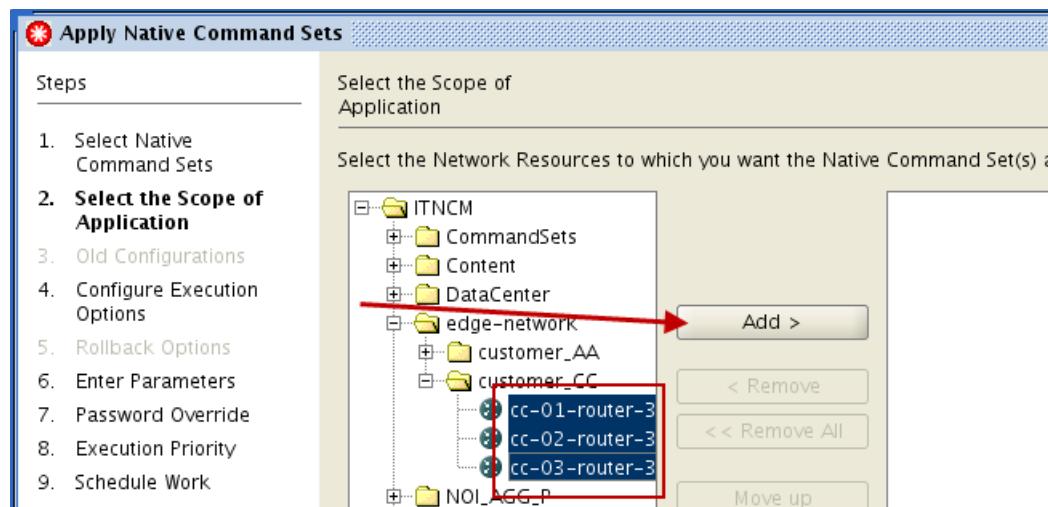
- b. Click **Next** in the Select Native Command Sets window.



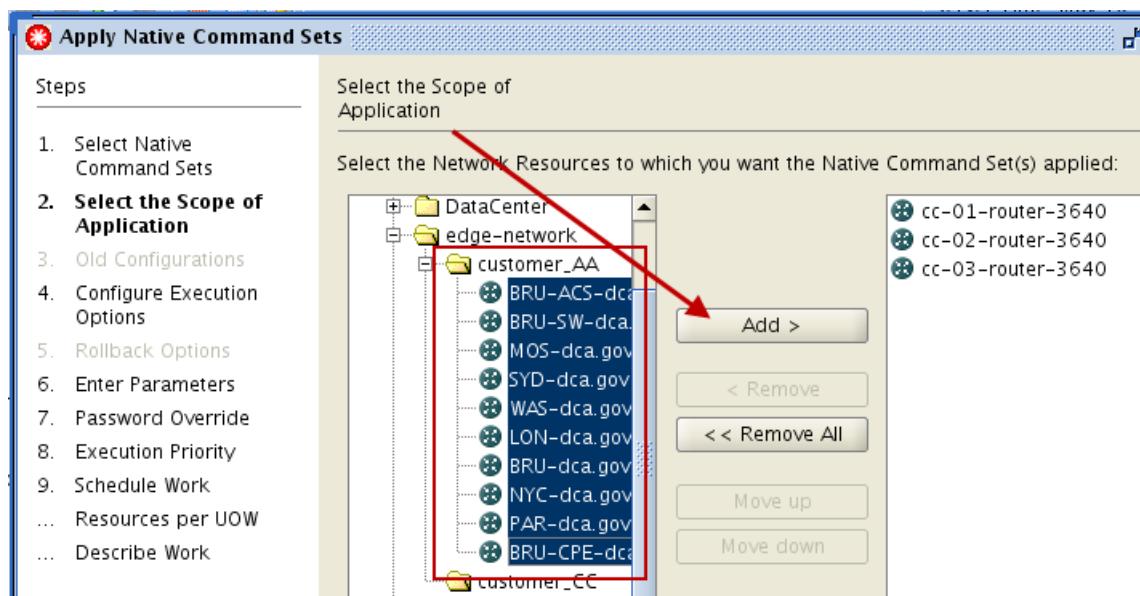
- c. Select **Apply the Native Command Sets to specific Network Resources** in the Select the Scope of Application window. Click **Next**.



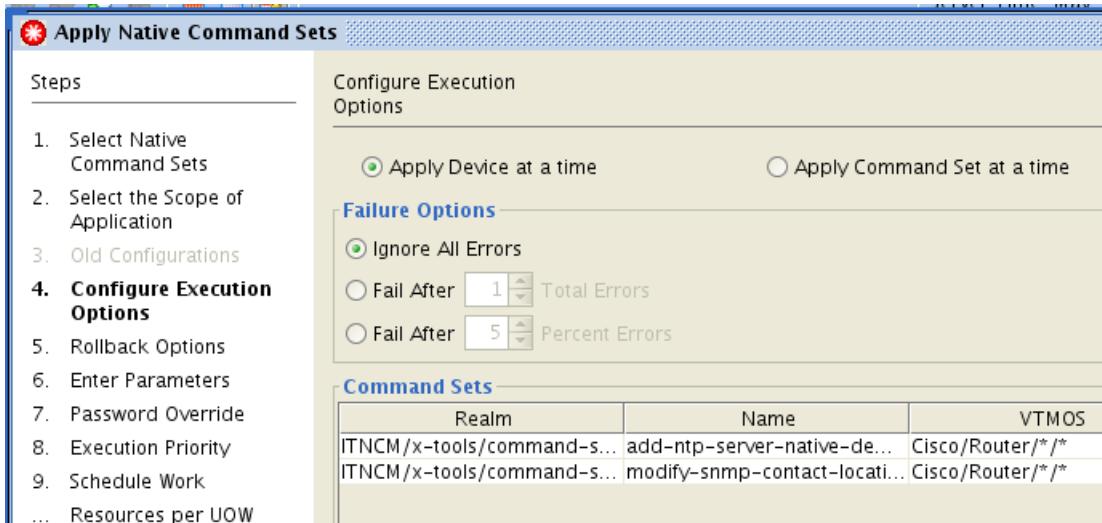
- d. Expand the **edge-network > customer_CC realm**. Select all of the devices in the customer_CC realm and click **Add**.



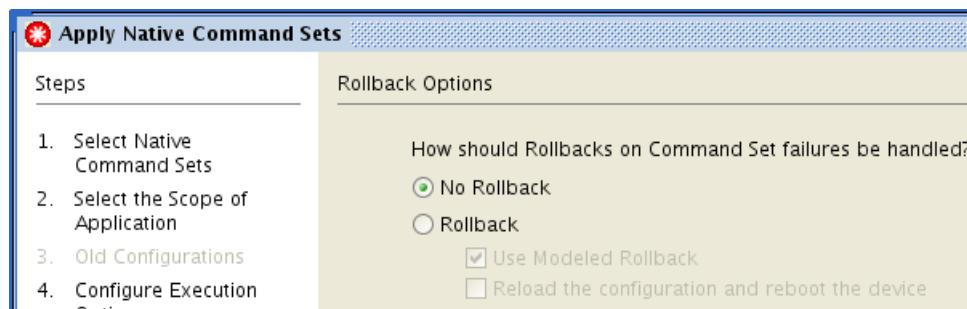
- e. Expand the **edge-network > customer_AA realm**. Select all of the devices in the customer_AA realm and click **Add**. Click **Next**.



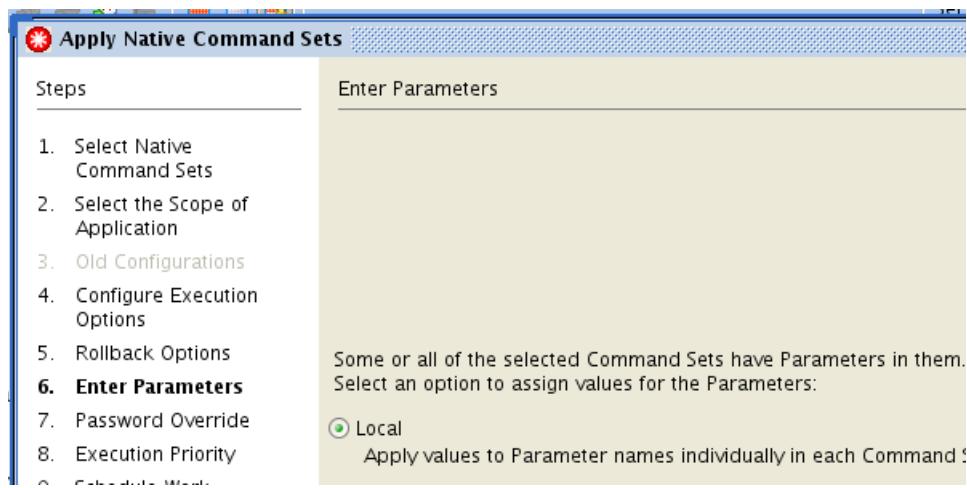
f. Click **Next** in the Configure Execution Options window.



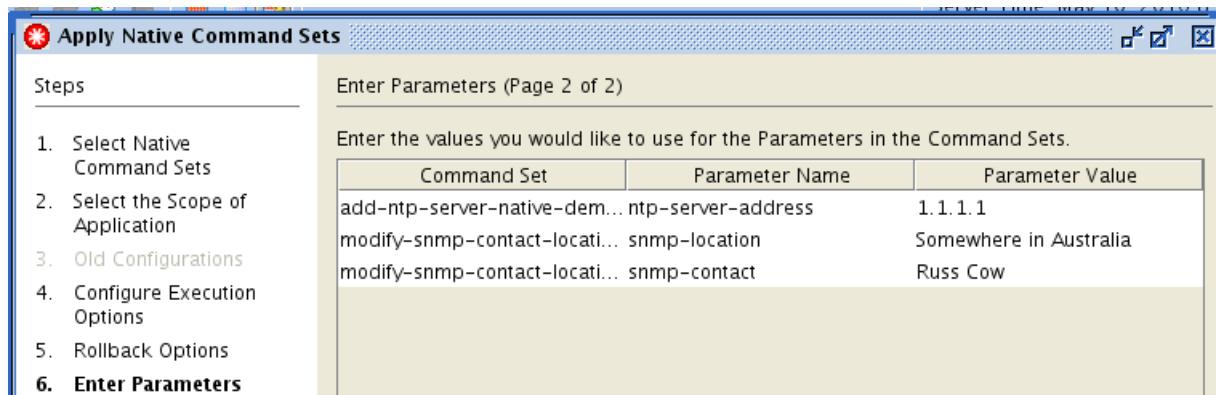
g. Click **Next** in the Rollback Options window



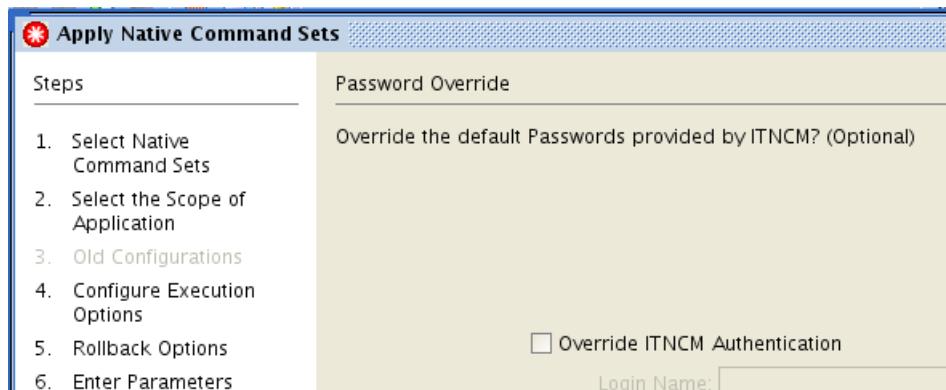
h. Click **Next** in the Enter Parameters window.



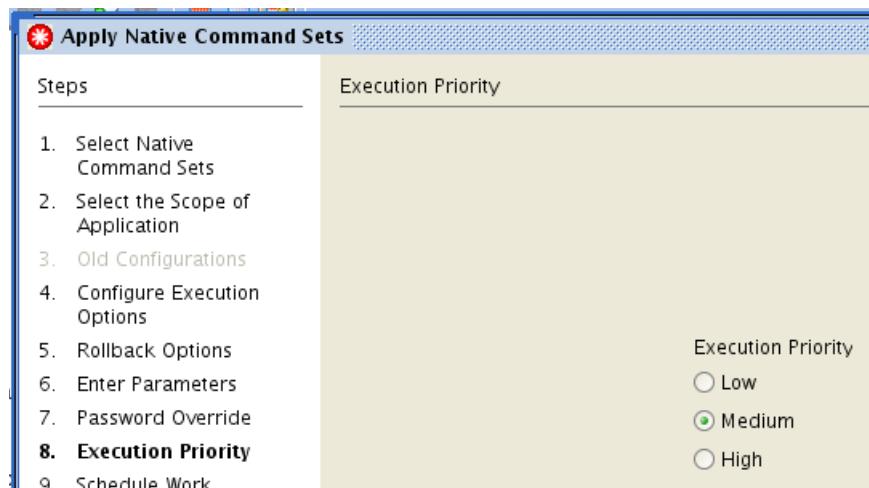
- i. Leave the default parameter values and click **Next** in the Enter Parameters window.



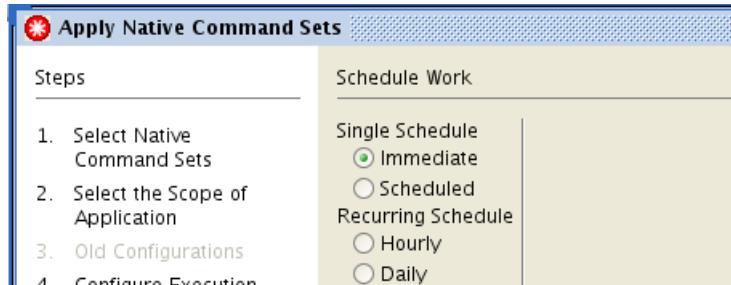
- j. Click **Next** in the Password Override window.



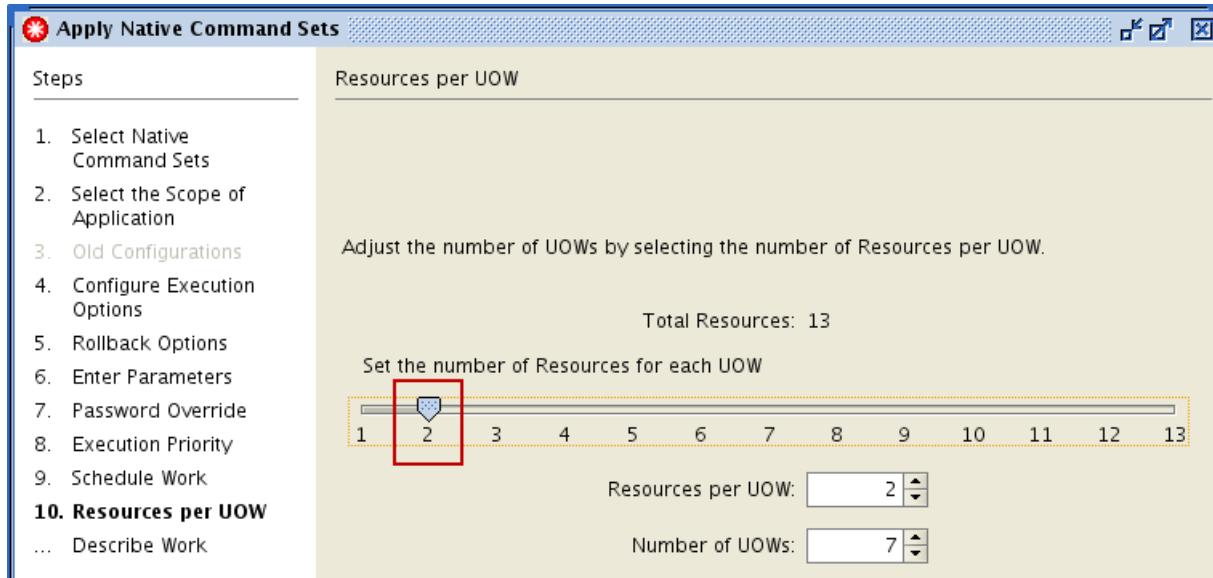
- k. Click **Next** in the Execution Priority window.



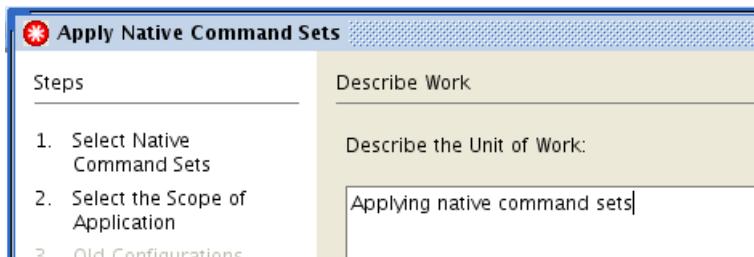
- I. Click **Next** in the Schedule Work window.



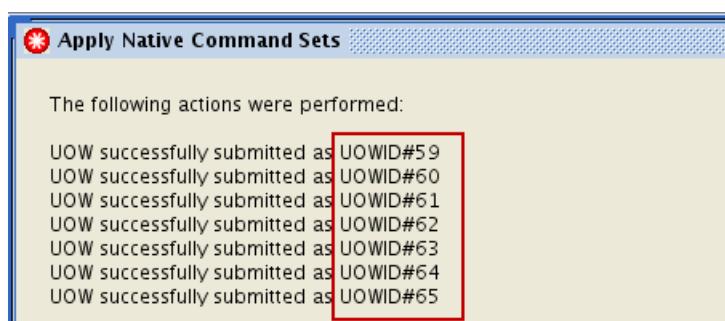
- m. Move the **Set the number of Resources for each UOW** slide control to 2. Click **Next**.



- n. Enter **Applying native command sets** in the Describe Work window. Click **Finish**.



- o. Notice that multiple *units of work* are created. Click **Close**.

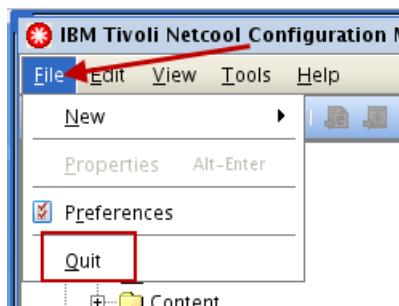


Exercise 3 Enabling the scheduling alert

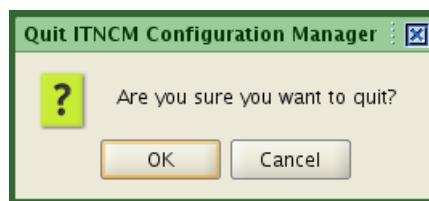
In this exercise, you enable the schedule alert feature in the unit of work wizard. This feature determines whether there are any other units of work in the system that might affect the current unit of work.

1. Log out of the user interface.

- a. Click **File > Quit**.



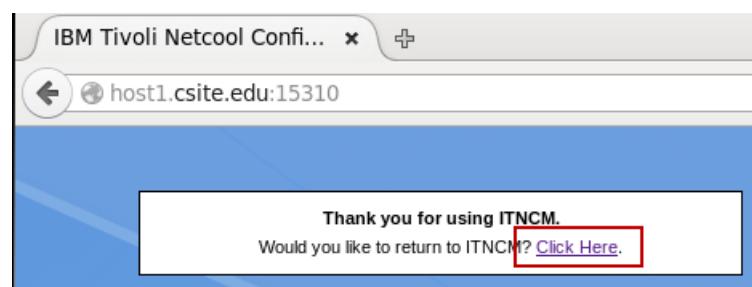
- b. Click **OK**.



- c. Return to the Firefox browser. Click **Logoff**.



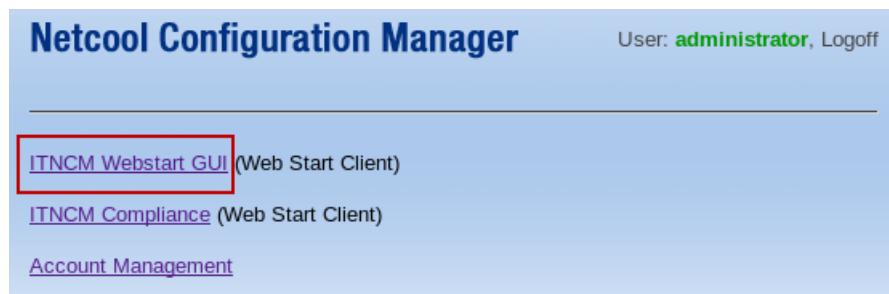
- d. Select **Click Here**.



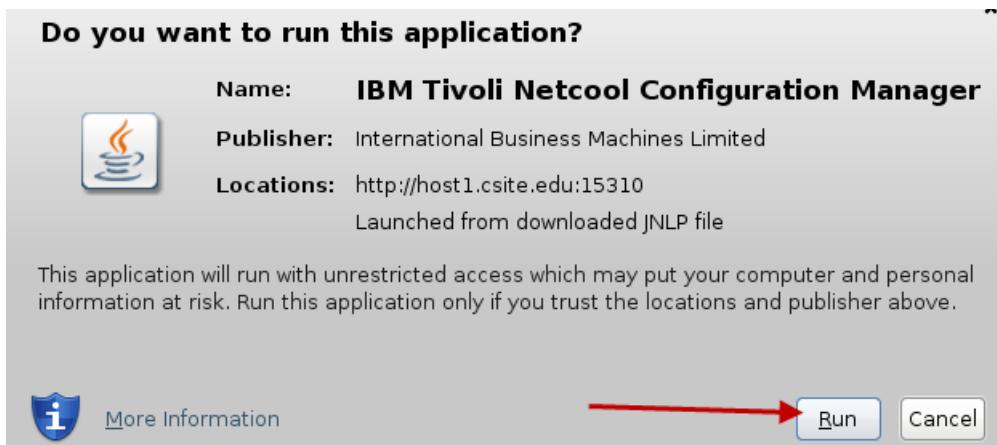
2. Log in to the user interface with the user name **administrator**. The password is **object00**.
 - a. Enter **administrator** and **object00** as the user name and password. Click **Login**.



- b. Click **ITNCM Webstart GUI**.

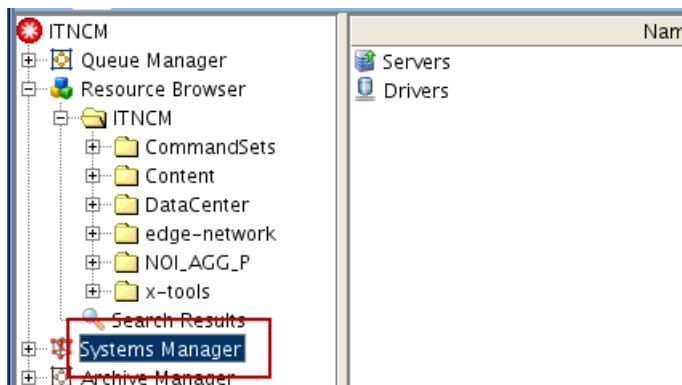


- c. Click **Run**.

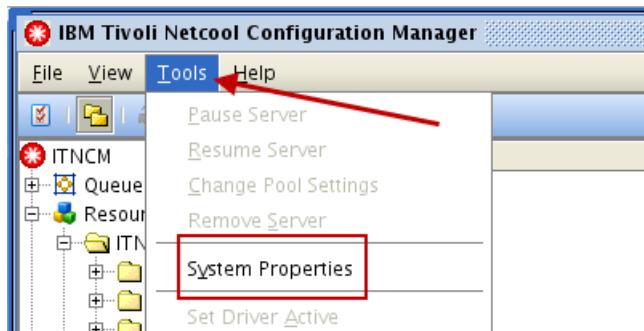


3. Open the System Properties.

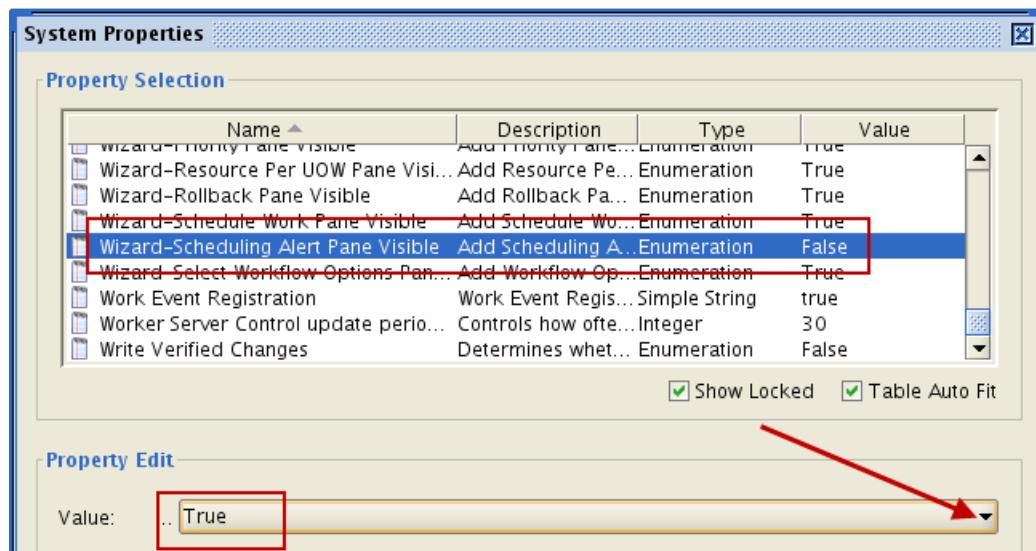
- a. Click the **Systems Manager** object.



b. Click Tools > System Properties.



4. Find the property named **Wizard-Scheduling Alert Pane Visible** in the system properties window. Set the value of this property to *true*.
 - a. Scroll down in the list of system properties. Click the property named **Wizard-Scheduling Alert Pane Visible**. Change the value to *true*.



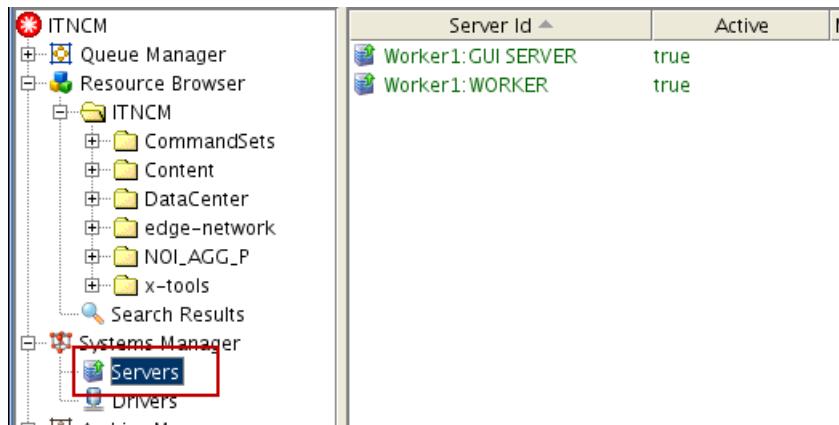
b. Click **Update**, then click **Close**.



Exercise 4 Viewing system servers

In this exercise, you view the servers that are running in your environment. You can view the servers because you are logged in as an administrative user.

- Find the Servers folder in the Systems Manager. Click **Systems Manager > Servers**.



- Two servers are listed. One server is a presentation server (GUI Server). The other server is a worker server.

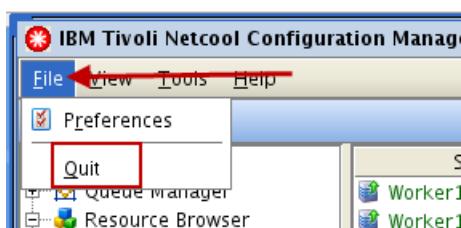
Server Id	Active	M
Worker1:GUI SERVER	true	
Worker1:WORKER	true	

- The maximum normal pool size for the worker server is set to 4.

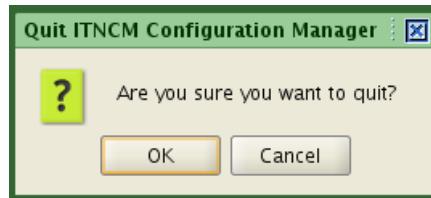
Server Id	Active	Max Normal Pool Size	Max I
Worker1:GUI SERVER	true	2	
Worker1:WORKER	true	4	

- Log out of the user interface.

- Click **File > Quit**.



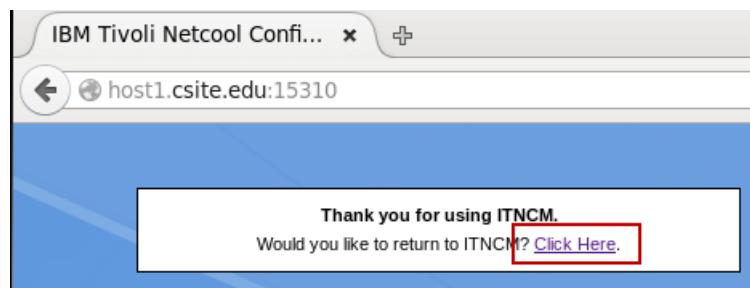
b. Click **OK**.



c. Return to the Firefox browser. Click **Logoff**.



d. Select **Click Here**.



Leave the browser session as is. You return to it shortly.



11 IBM device terminal exercises

The exercises in this unit demonstrate how to use the IBM Device Terminal to make changes to devices.

Exercise 1 Using the IBM device terminal

In this exercise, you create an access list by using the IBM device terminal. After you add the access list, you view the keystrokes that you entered.

1. Log in to the user interface with the user name **engineer**. The password is **object00**.
 - a. Enter **engineer** and **object00** as the user name and password. Click **Login**.

Netcool Configuration Manager

User Name:
engineer

Password:
.....

- b. Click **ITNCM Webstart GUI**.

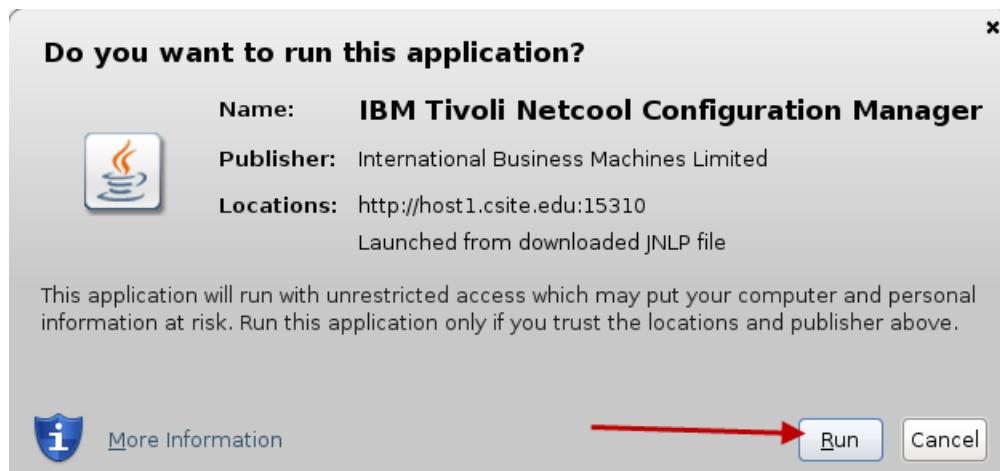
Netcool Configuration Manager

User: engineer, Logoff

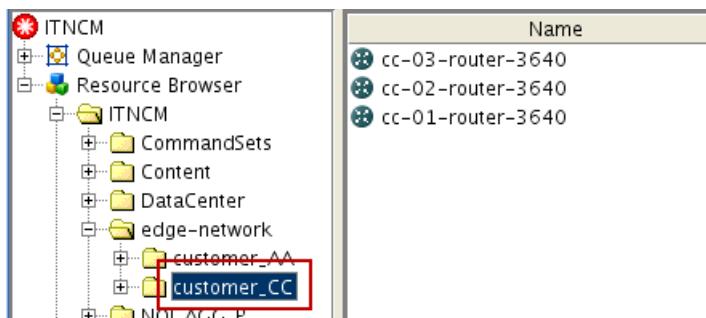
[ITNCM Webstart GUI](#) (Web Start Client)

[ITNCM Compliance](#) (Web Start Client)

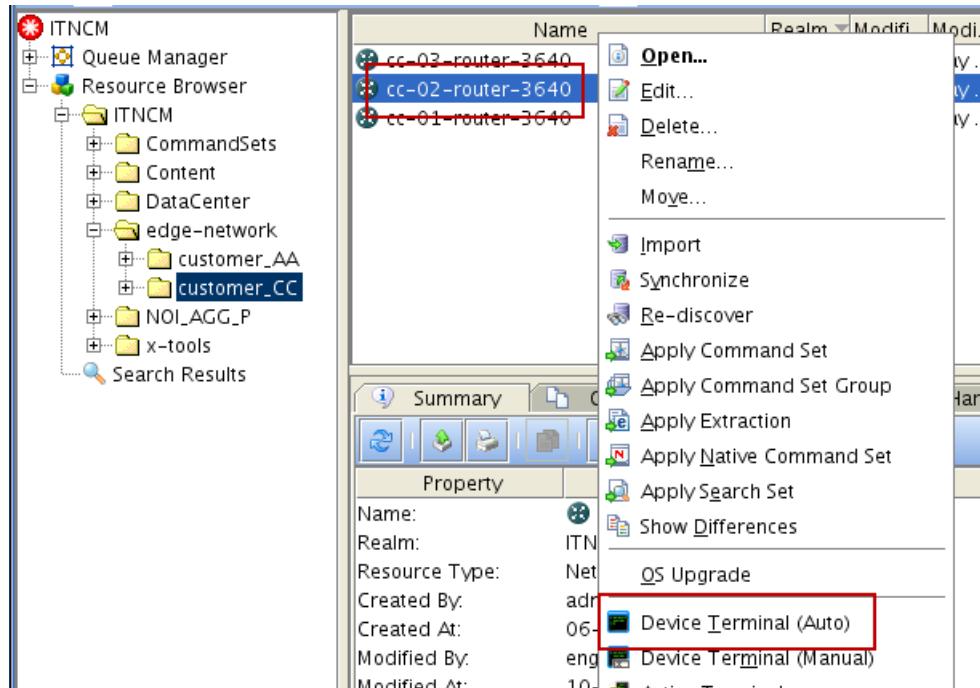
- c. Click **Run**.



2. Use the device terminal in automatic mode to access the cc-02-router-3640 device. Enter all of the following commands to configure an access list on the device. These commands add an IP address to interface FastEthernet3/0, create an access list that prevents IP spoofing, and apply the access list to interface FastEthernet3/0. When you finish, accept the default unit of work description (UOW Submitted by IDT). Close the device terminal window.
a. Click **ITNCM > edge-network > customer_CC** realm in the *resource browser*.



- b. Right-click the **cc-02-router-3640** device. Click **Device Terminal (Auto)**.



The device terminal logs you in and enters enable mode.

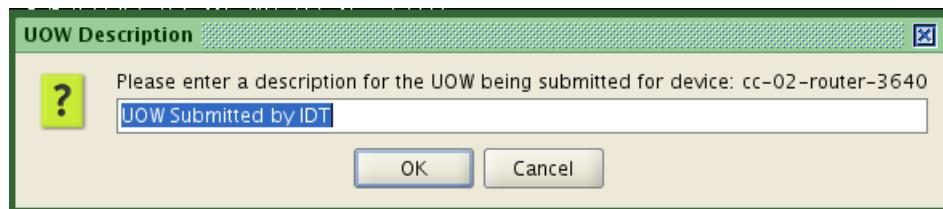
```
User Access Verification

Username: intelliiden
Password:
Use Netcool Configuration Manager to make changes
cc-02-router-3640>en
Password:
cc-02-router-3640#term len 0
cc-02-router-3640#term width 100
cc-02-router-3640#
```

- c. Enter these commands one line at a time.

```
conf t
interface FastEthernet3/0
ip address 9.57.77.146 255.255.0.0
no shut
exit
ip access-list ext antispoof-wan
deny ip 9.57.0.0 0.0.255.255 any
permit ip any any
exit
int FastEthernet3/0
ip access-group antispoof-wan in
exit
exit
exit
```

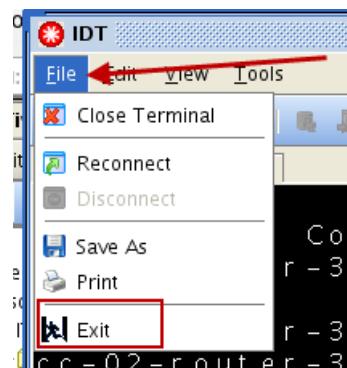
- d. When you type **exit** in the last command, the device terminal disconnects from the device. Click **OK** to accept the default unit of work description.



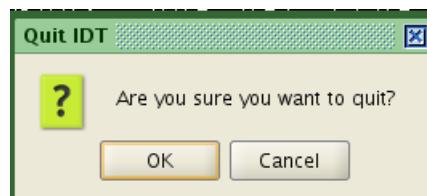
- e. Note the unit of work number and click **OK** to confirm the unit of work.



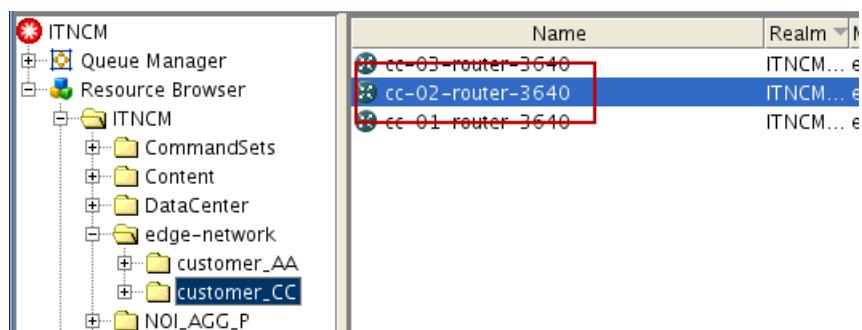
- f. Click **File > Exit** to close the device terminal window.



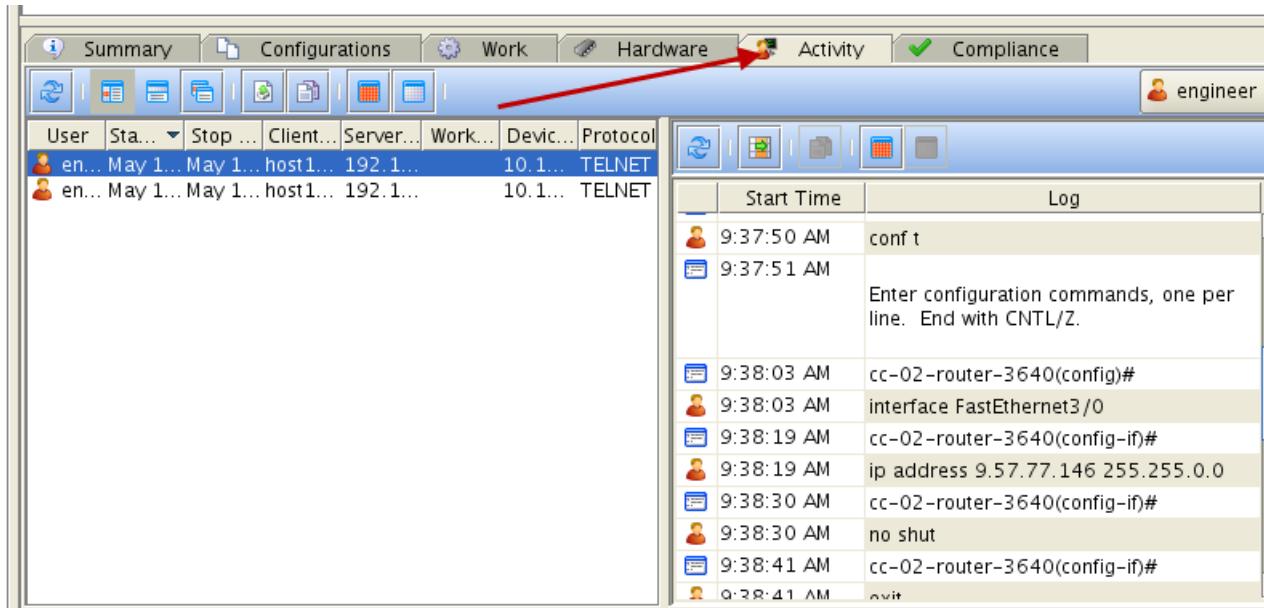
- g. Click **OK** to close the device terminal window.



3. Find and view the keystroke log for the device terminal session you just finished. Use the **Activity** tab in the *resource browser* to find the keystroke log.
a. Click the **cc-02-router-3640** device in the **ITNCM > edge-network > customer_CC realm**.



- b. Click the **Activity** tab. Find the keystroke log for the device terminal session that you just finished. The commands that you entered and the response of the device is shown in the keystroke log.

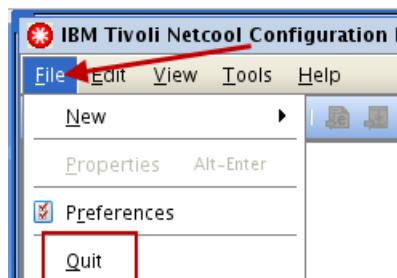


Exercise 2 Viewing the synchronization filter

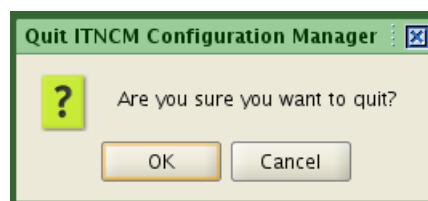
In this exercise, you view the regular expression filter. This filter caused the device terminal to synchronize the configuration change you made in the preceding exercise.

1. Log out of the user interface.

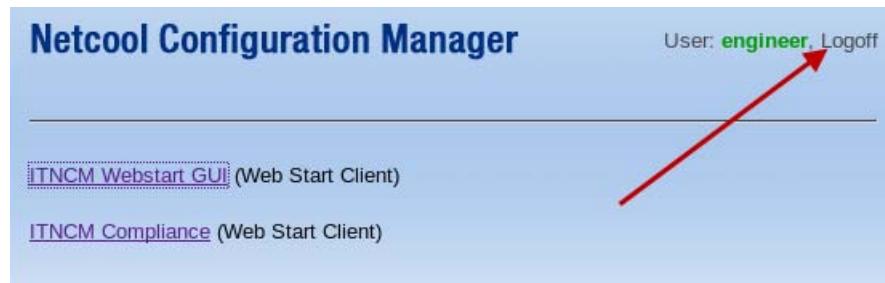
- a. Click **File > Quit**.



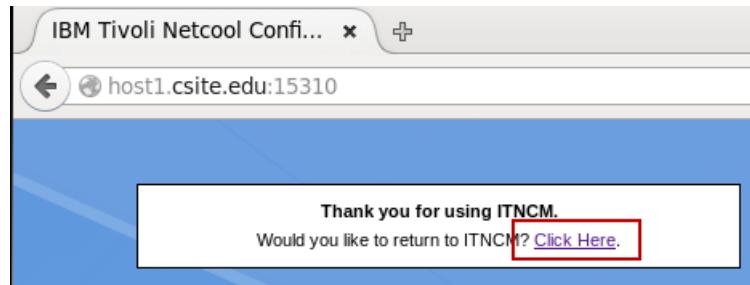
- b. Click **OK**.



- c. Return to the Firefox browser. Click **Logoff**.



- d. Select **Click Here**.



2. Log in to the user interface with the user name **administrator**. The password is **object00**.

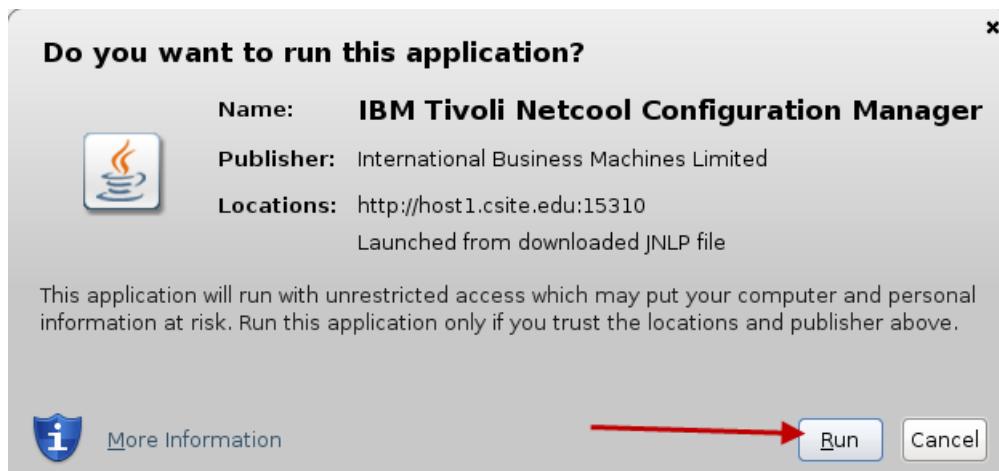
- a. Enter **administrator** and **object00** as the user name and password. Click **Login**.



- b. Click **ITNCM Webstart GUI**.

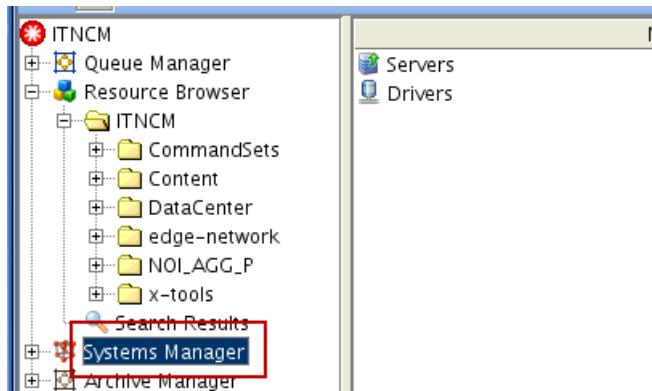


- c. Click Run.

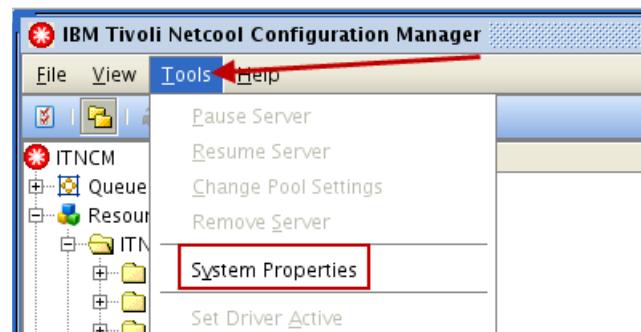


3. Click the Systems Manager and open the System Properties. Look for the following properties:

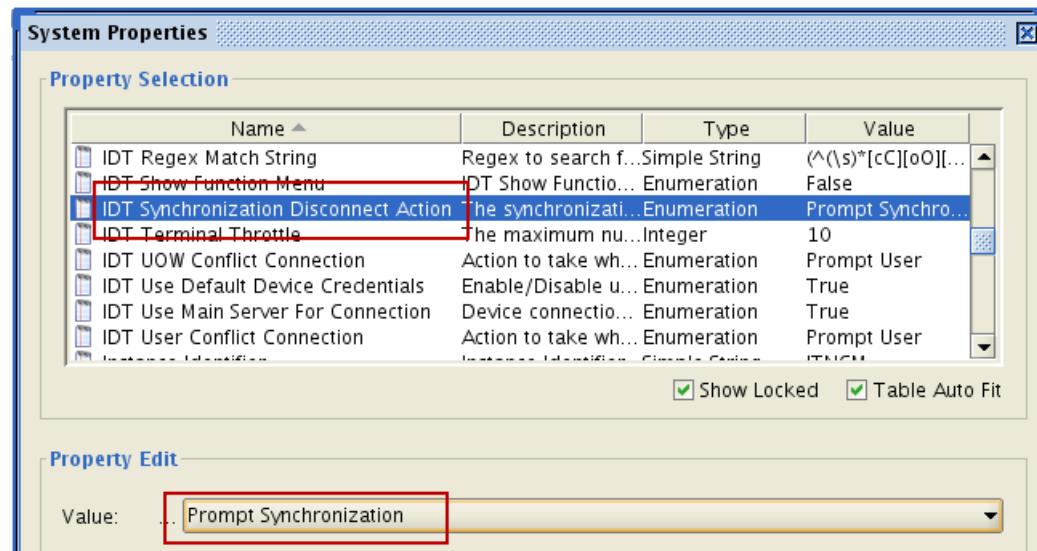
- **IDT Synchronization Disconnect Action**
 - **IDT Regex Match String**
- a. Click the **Systems Manager** object.



- b. Click Tools > System Properties.

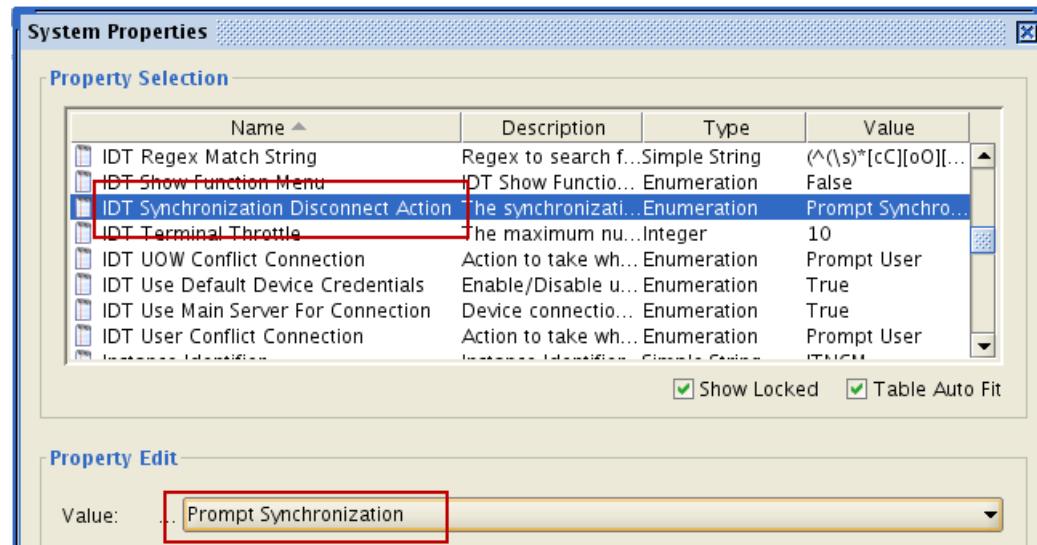


- c. Scroll down in the list of properties and find the property named **IDT Synchronization Disconnect Action**.



The property is set to **Prompt Synchronization**. This property causes the terminal session to prompt for a synchronization unit of work every time that the session ends.

- d. Click the arrow and select **Regex Match Synchronization**. Click **Update**.



This property causes the terminal session to prompt for a synchronization unit of work when a user command matches a regular expression definition.

- e. Find the property named **IDT Regex Match String**.

The screenshot shows the 'System Properties' window with the 'Property Selection' tab active. A table lists various properties with their names, descriptions, types, and values. The 'IDT Regex Match String' property is highlighted with a red box and selected. In the 'Property Edit' tab, the 'Value' field contains a complex regular expression string, also enclosed in a red box.

Name	Description	Type	Value
IDT Device Output Limit	The maximum number of lines to output from a command.	Integer	55000
IDT Display UOW Confirmation	Display a confirmation message when a unit of work is completed.	Enumeration	True
IDT Inactivity Timeout Period	Number of minutes before a session times out.	Integer	15
IDT Regex Match String	Regex to search for during a configuration session.	Simple String	<code>(^(\s)*[cC][oO][nN][fF][iI]?[gG]?[uU]?[rR]?[aA]?[tT]?[iI]?[oO]?[nN]?(\s)*[tT][eE]?[rR]?[mM]?[iI]?[nN]?[aA]?[lL]?(\s)*) (^(\s)*[cC][oO][pP][yY](\s*)) (^(\s)*[eE][rR][aA][sS][eE](\s*)) (^(\s)*[cC][lL][eE][aA][rR](\s*)) (^(\s)*[rR][eE][iL][oO][aA][dD](\s*)) (^(\s)*[sS][eE][tT](\s*)) (^(\s)*[wW][rR][iI][tT][eE](\s*))</code>
IDT Show Function Menu	IDT Show Function Menu	Enumeration	False
IDT Synchronization Disconnect Action	The synchronization disconnect action.	Enumeration	RegEx Match Sync
IDT Terminal Throttle	The maximum number of lines to throttle.	Integer	10
IDT UOW Conflict Connection	Action to take when a conflict occurs.	Enumeration	Prompt User
IDT Use Default Device Credentials	Enable/Disable using default device credentials.	Enumeration	True
IDT Use Main Server For Connection	Device connection type.	Enumeration	True

Show Locked Table Auto Fit

Property Edit

Value: `(^(\s)*[cC][oO][nN][fF][iI]?[gG]?[uU]?[rR]?[aA]?[tT]?[iI]?[oO]?[nN]?(\s)*[tT][eE]?[rR]?[mM]?[iI]?[nN]?[aA]?[lL]?(\s)*)|(^(\s)*[cC][oO][pP][yY](\s*))|(^(\s)*[eE][rR][aA][sS][eE](\s*))|(^(\s)*[cC][lL][eE][aA][rR](\s*))|(^(\s)*[rR][eE][iL][oO][aA][dD](\s*))|(^(\s)*[sS][eE][tT](\s*))|(^(\s)*[wW][rR][iI][tT][eE](\s*))`

The property is set to the following values:

`(^(\s)*[cC][oO][nN][fF][iI]?[gG]?[uU]?[rR]?[aA]?[tT]?[iI]?[oO]?[nN]?(\s)*[tT][eE]?[rR]?[mM]?[iI]?[nN]?[aA]?[lL]?(\s)*)|(^(\s)*[cC][oO][pP][yY](\s*))|(^(\s)*[eE][rR][aA][sS][eE](\s*))|(^(\s)*[cC][lL][eE][aA][rR](\s*))|(^(\s)*[rR][eE][iL][oO][aA][dD](\s*))|(^(\s)*[sS][eE][tT](\s*))|(^(\s)*[wW][rR][iI][tT][eE](\s*))`

This regular expression string tests for the presence of any of the following terms:

- configuration
- terminal
- copy
- erase
- clear
- reload
- set
- write

Each of these terms is a command that causes a change to the router configuration. If any of these commands are used during the terminal session, the user is prompted for a synchronization *unit of work*.

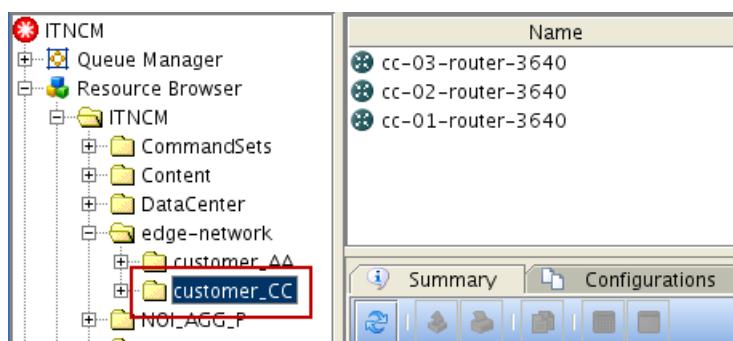
- f. Close the system properties window.

Exercise 3 Creating a command filter

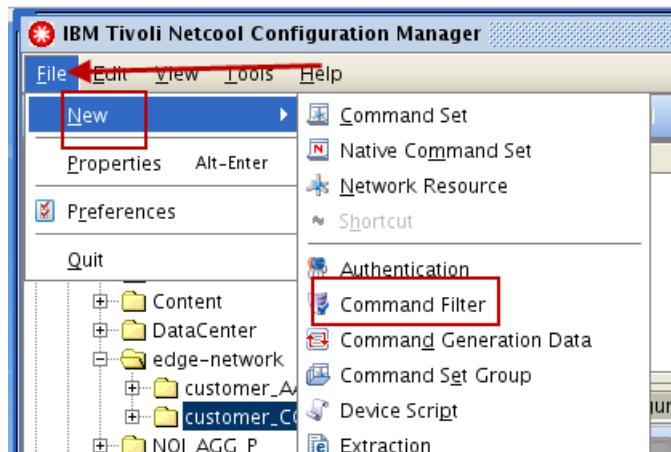
In this exercise, you create and configure a command filter.

1. Create a command filter named **no_erase_squeeze** in the **ITNCM > edge-network** realm. Use the following values when you create the command filter.

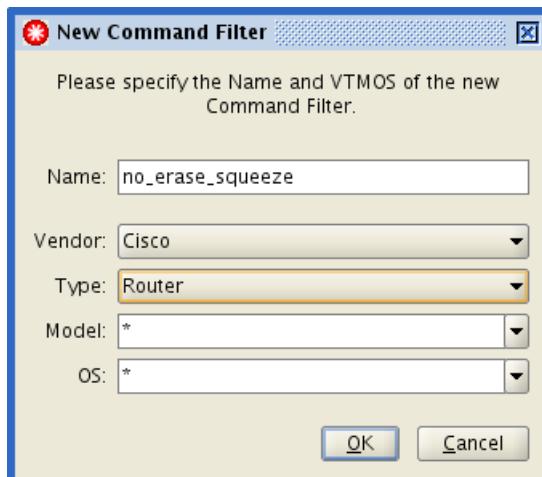
- Vendor: **Cisco**
 - Type: **Router**
 - Model: *
 - OS: *
- a. Click **ITNCM > edge-network**.



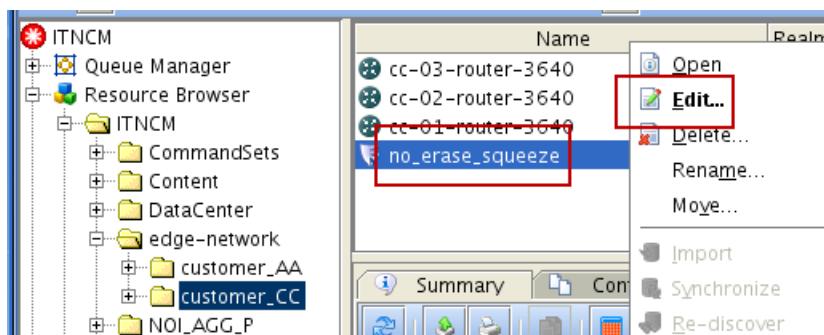
- b. Click **File > New > Command Filter**.



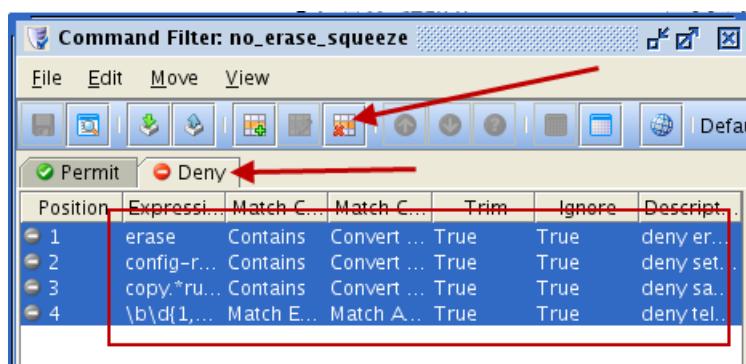
- c. Enter **no_erase_squeeze** as the name. Enter **Cisco** as the vendor. Enter **Router** as the type. Choose ***** as the model. Leave ***** as the OS. Click **OK**.



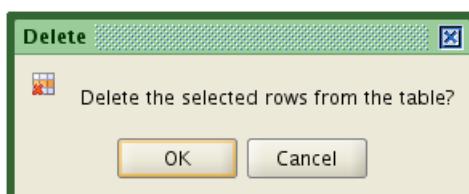
2. Edit the new command filter. Delete all of the default entries in the **Deny** tab.
- Right-click the **no_erase_squeeze** command filter in the **edge-network** realm and click **Edit**.



- Click the **Deny** tab. Select all of the entries and click the **Delete** icon.

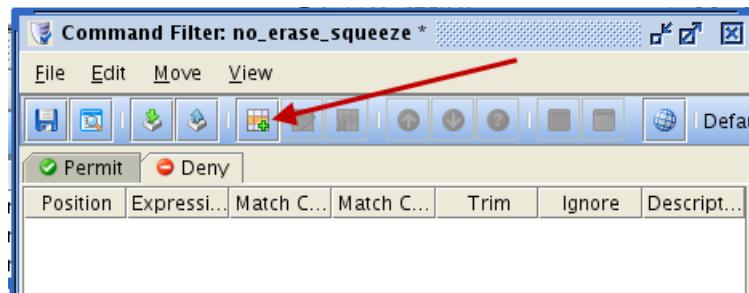


- Click **OK** to confirm.

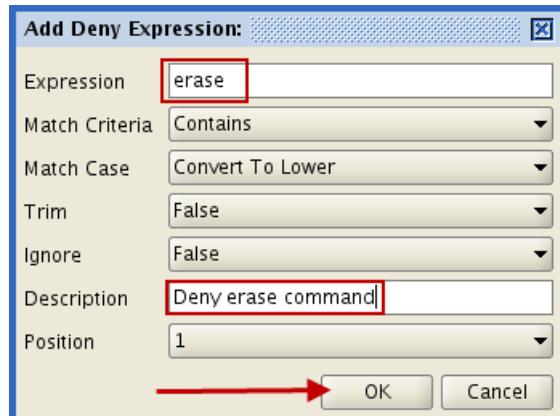


3. Add an entry in the command filter to deny the expression **erase**. Use the following values when you create the squeeze entry. Keep the command filter open.
 - Expression: **erase**
 - Match Criteria: **Contains**
 - Match Case: **Convert To Lower**
 - Trim: **False**
 - Ignore: **False**
 - Description: **Deny erase command**
 - Position: **1**

a. Click the **Add** icon in the command filter.



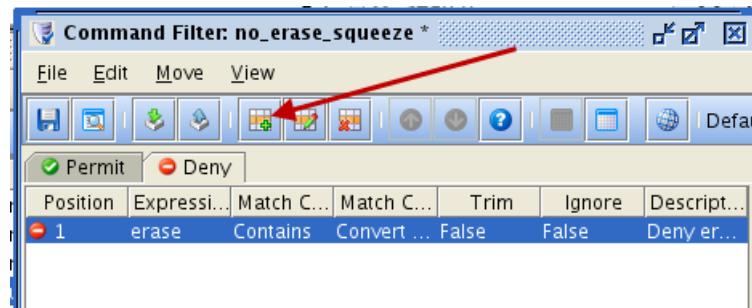
b. Enter the values in the Add Deny Expression window and click **OK**.



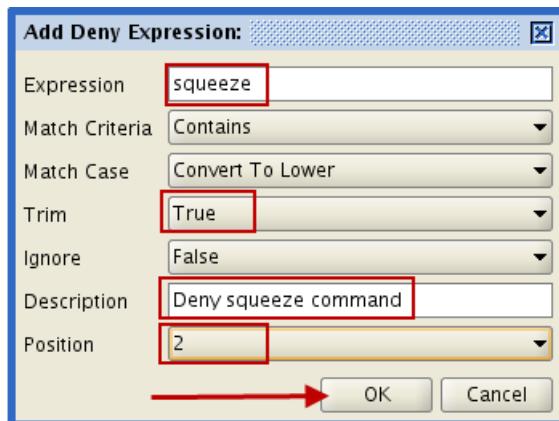
4. Add an entry in the command filter to deny the expression **squeeze**. Use the following values when you create the squeeze entry. Keep the command filter open.

- Expression: **squeeze**
- Match Criteria: **Contains**
- Match Case: **Convert To Lower**
- Trim: **True**
- Ignore: **False**
- Description: **Deny squeeze command**
- Position: **2**

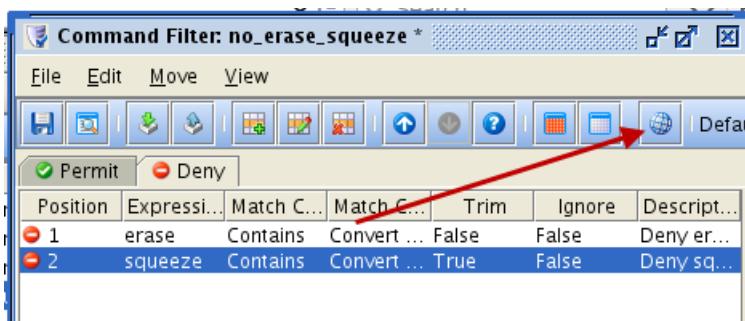
- a. Click the **Add** icon in the command filter.



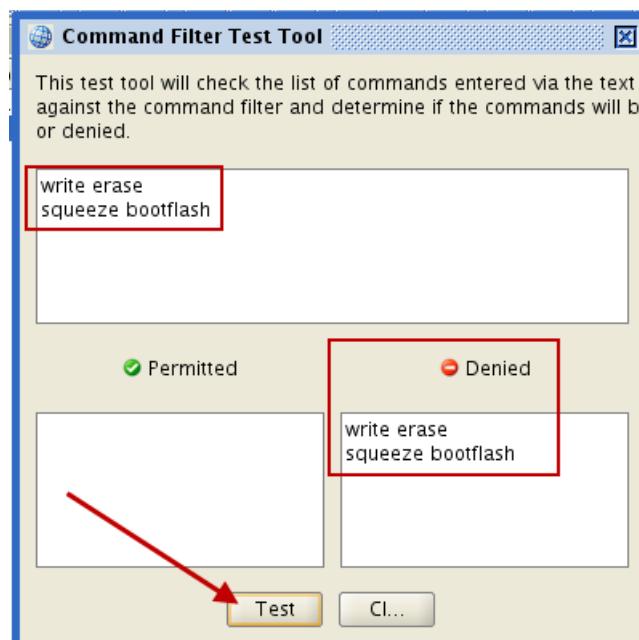
- b. Enter the values in the Add Deny Expression window and click **OK**.



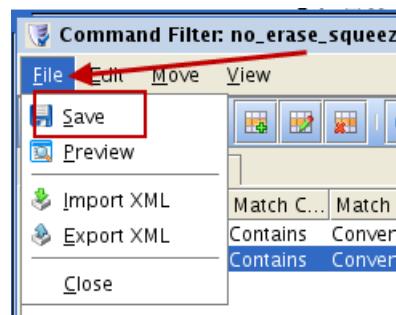
5. Test the command filter. Use the commands **write erase** and **squeeze bootflash** to test the command filter. Save and close the command filter when you are done.
 - a. Click the **Run Test Tool** icon.



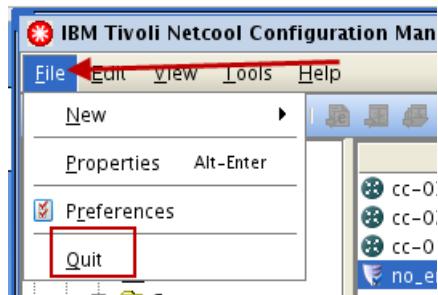
5. Test the command filter. Use the commands **write erase** and **squeeze bootflash** to test the command filter. Save and close the command filter when you are done.
 - b. Enter the commands **write erase** and **squeeze bootflash** in the top of the test tool. Click the **Test** icon. The test denies both commands. Close the test tool.



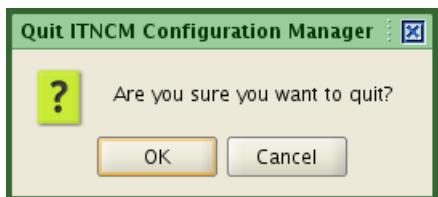
5. Test the command filter. Save and close the command filter.
 - c. Click **File > Save**. Close the command filter.



6. Click **File > Quit.**



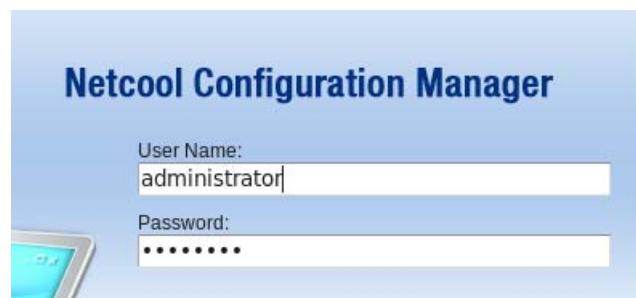
7. Click File > Quit.



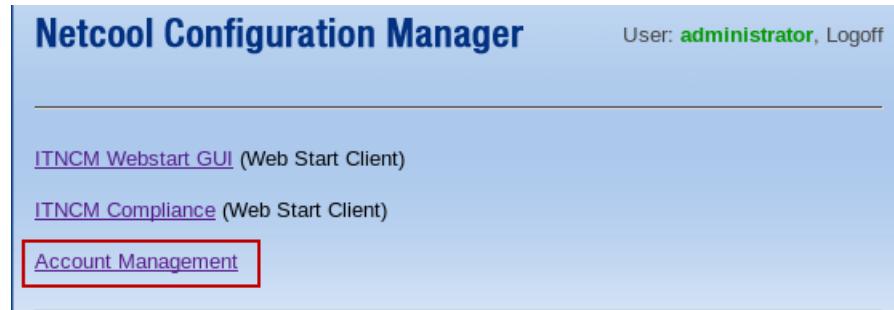
Exercise 4 Applying and testing the new command filter

In this exercise, you apply the new command filter to the engineering group.

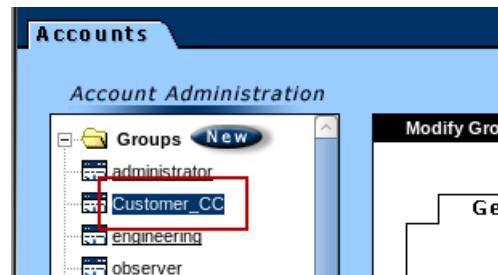
1. Return to the Firefox browser.
2. Log in as **administrator** with password **object00**.



3. Click Account Management.



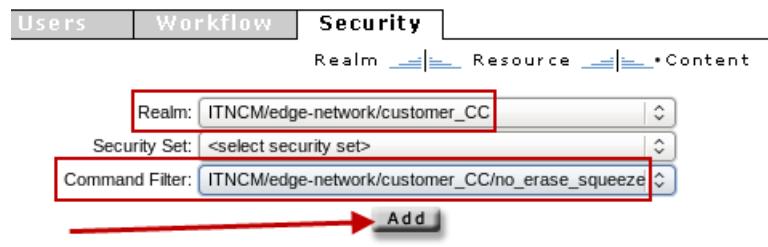
4. Configure content security for the Customer_CC group. Add the command filter named **no_erase_squeeze** to the **ITNCM/edge-network/customer_CC** realm. Save the entry after you add it.
- Click **Customer-CC**.



- Click **Security > Content**.



- Choose **ITNCM/edge-network/customer_CC** in the **Realm** field.
- Choose **ITNCM/xtools/command-filter/no_erase_squeeze** in the **Command Filter** field.
- Click **Add**.



- d. Click **Save**. Confirm that the lock icon is closed. Close the browser window when you are done.

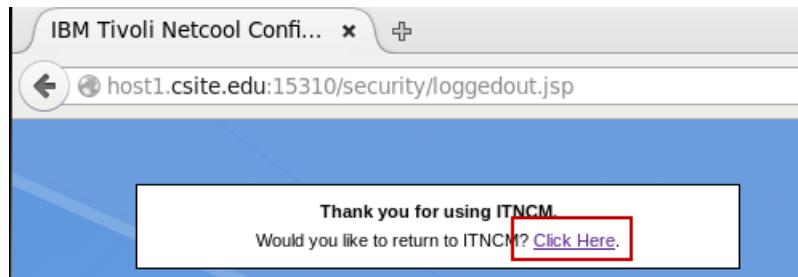
Realm	Resource	Resource Type	Delete	Status
ITNCM/edge-network/customer_CC	ITNCM/x-tools/security-sets/no_passwords	Security Set		
ITNCM/edge-network/customer_CC	ITNCM/edge-network/customer_CC/no_erase_squeeze	CommandFilter		

Save **Remove** **Cancel**

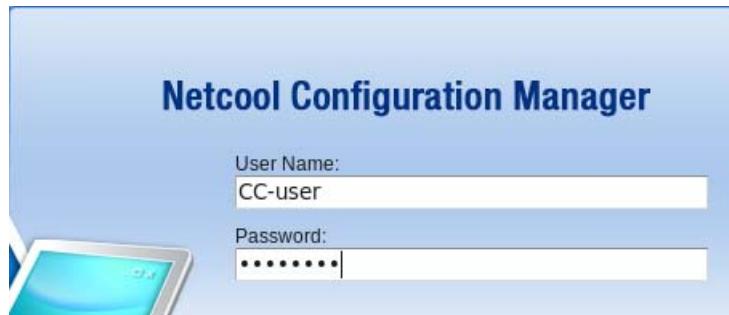
- e. Click the *running man* icon to log out.



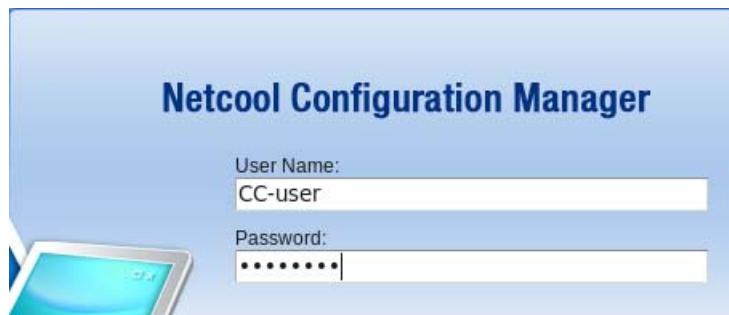
- f. Select **Click Here**.



5. Log In to the user interface with the user name **CC-user**. The password is **object00**.
- Enter **CC-user** and **object00** as the user name and password. Click **Login**.



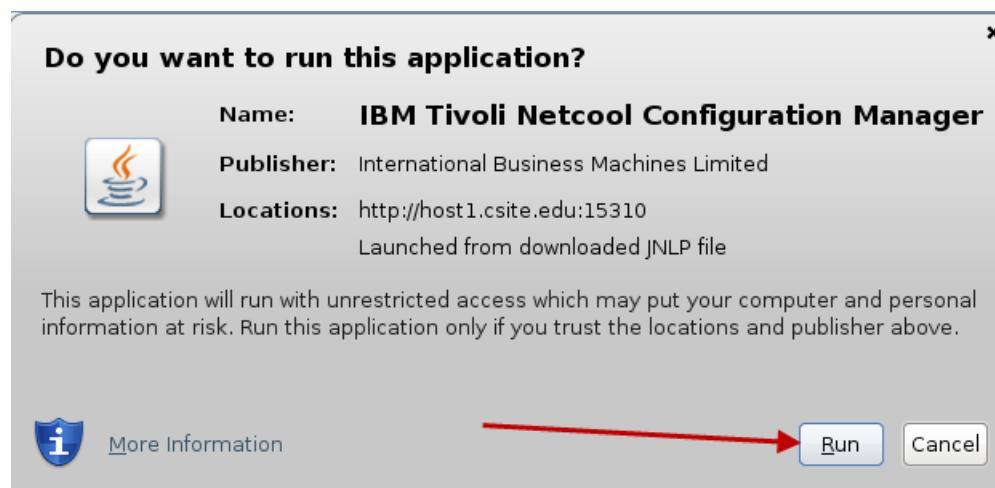
- Enter **CC-user** and **object00** as the user name and password. Click **Login**.



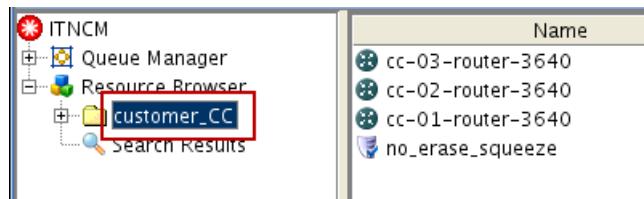
- Click **ITNCM Webstart GUI**.



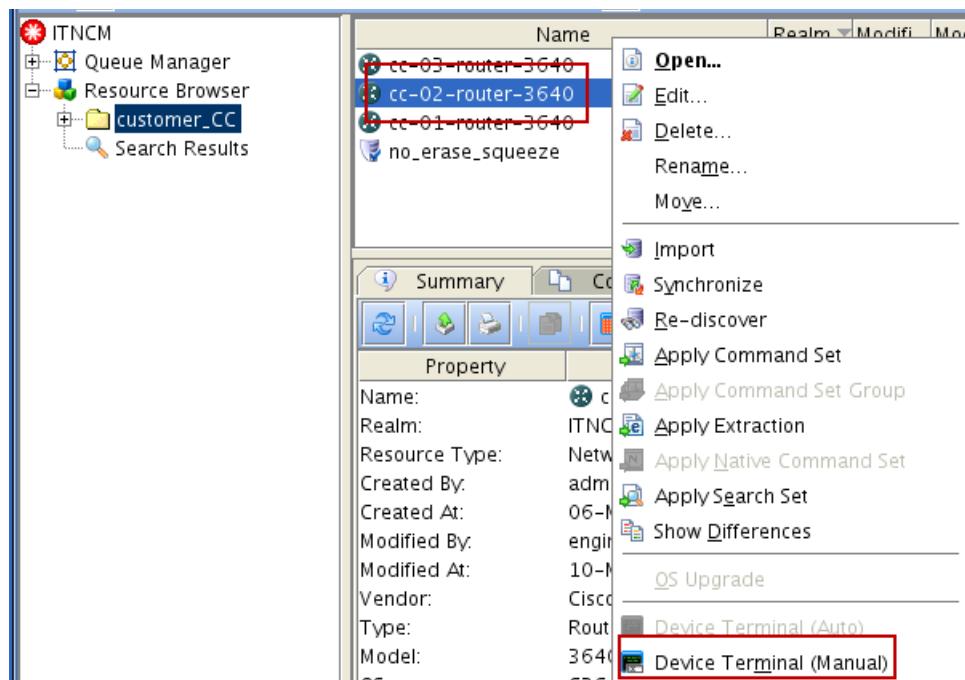
- Click **Run**.



6. Use the device terminal in manual mode to access the cc-01-router-3640 device. Authenticate with the user name **intelliden**, password of **p4ssw0rd**, a four and a zero, and enable password of **3n4bl3**, a three, a four, a lowercase L, and a three.
- Click **customer_CC** realm in the *resource browser*.



- Right-click the **cc-02-router-3640** device. Click **Device Terminal (Manual)**.



The device terminal takes you to the login prompt.

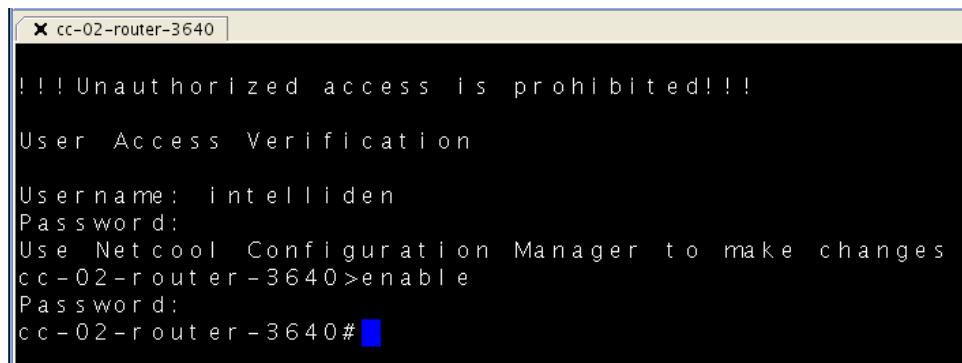
- Authenticate with user name **intelliden** and password **p4ssw0rd**, a four and a zero.

```

x cc-02-router-3640
!!! Unauthorized access is prohibited!!!
User Access Verification
Username: intelliden
Password:
Use Netcool Configuration Manager to make changes to t
cc-02-router-3640>

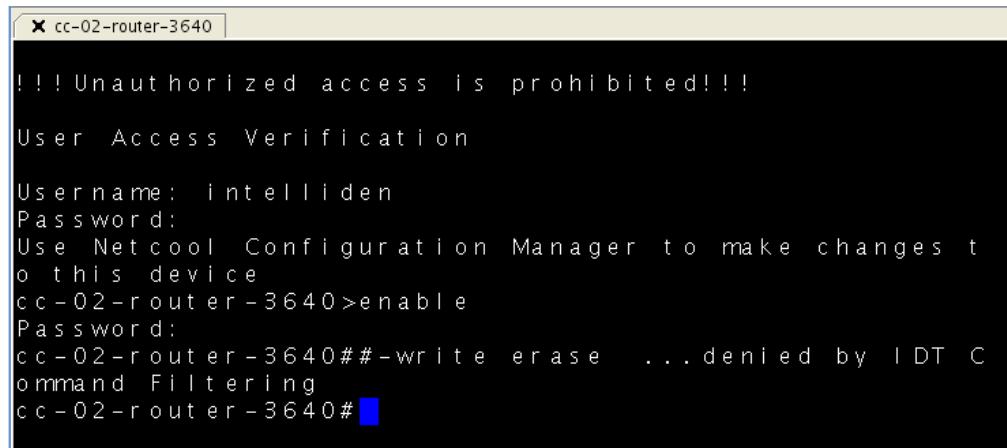
```

- d. Enter the enable mode for the device by entering command **enable** and supplying the password **3n4bl3**, a three, a four, a lowercase L, and a three, when prompted.



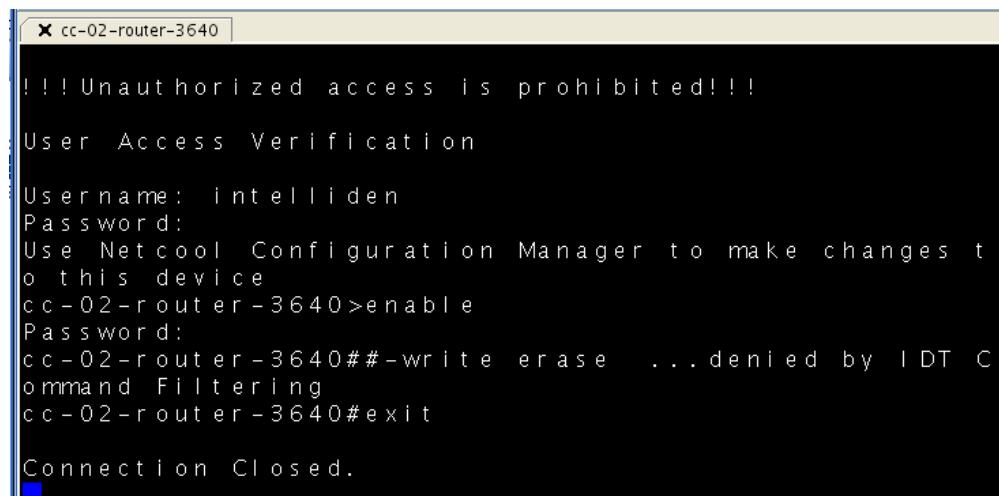
```
cc-02-router-3640
!!! Unauthorized access is prohibited!!!
User Access Verification
Username: intelliden
Password:
Use Netcool Configuration Manager to make changes
cc-02-router-3640>enable
Password:
cc-02-router-3640#
```

- e. Enter the command **write erase**. After you enter the command, the device terminal prints a message that the command is denied.



```
cc-02-router-3640
!!! Unauthorized access is prohibited!!!
User Access Verification
Username: intelliden
Password:
Use Netcool Configuration Manager to make changes to this device
cc-02-router-3640>enable
Password:
cc-02-router-3640##-write erase ... denied by IDT Command Filtering
cc-02-router-3640#
```

- f. Enter **exit** to close the terminal session.

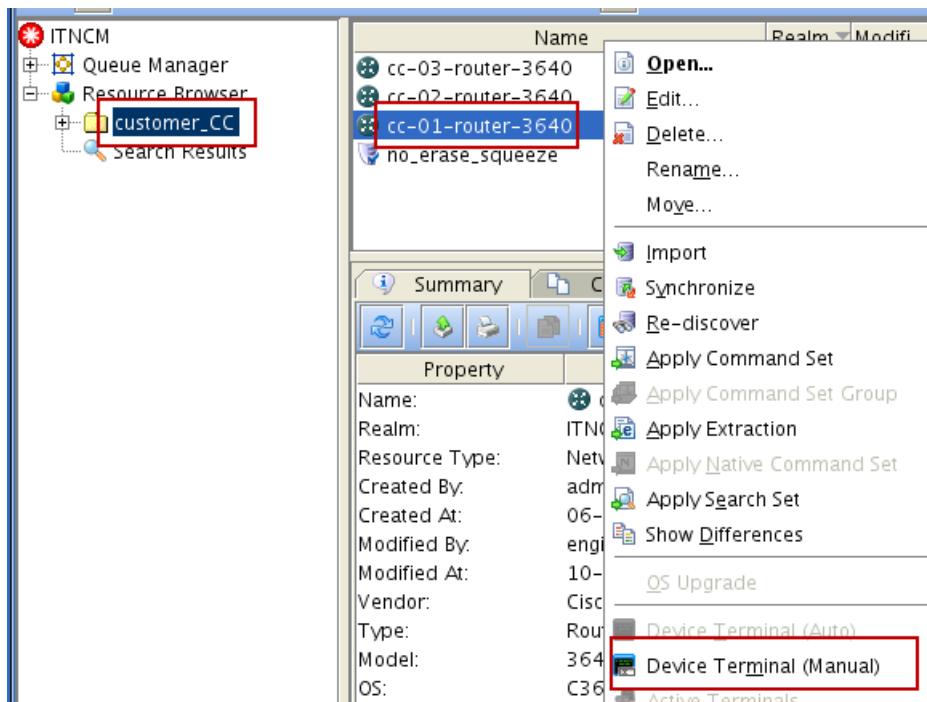


```
cc-02-router-3640
!!! Unauthorized access is prohibited!!!
User Access Verification
Username: intelliden
Password:
Use Netcool Configuration Manager to make changes to this device
cc-02-router-3640>enable
Password:
cc-02-router-3640##-write erase ... denied by IDT Command Filtering
cc-02-router-3640#exit
Connection Closed.
```

You do not see a prompt for a synchronization unit of work, which is because you changed the IDT synchronization property in the previous unit.

- g. Close the terminal window.

7. Right-click the **cc-01-router-3640** device. Click **Device Terminal (Manual)**.

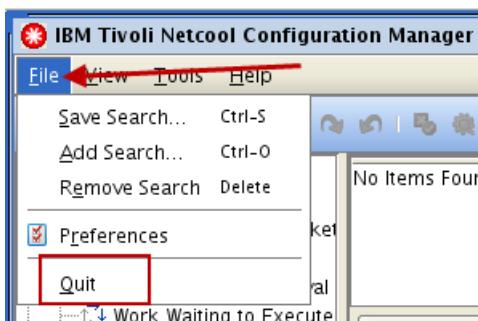


8. Observe the message. Click **Cancel**.

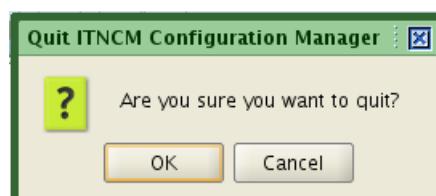


You receive a message about active units of work for the same device, which is because you enabled the Wizard Scheduling Alert property in a previous exercise.

9. Click **File > Quit**.



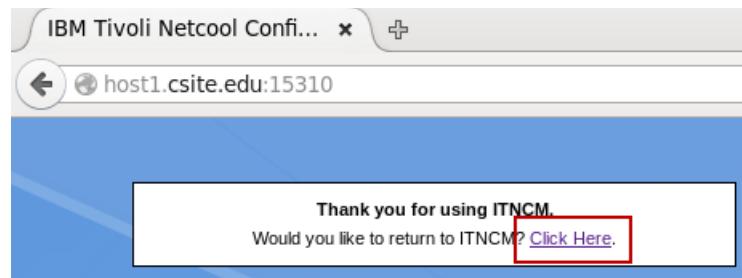
10. Click **OK**.



11. Return to the Firefox browser and click Logoff.



12. Select **Click Here**.



Leave the browser session as is. You return to it shortly.



12 Advanced command sets exercises

The exercises in this unit demonstrate how to create, test, and apply modeled command sets.

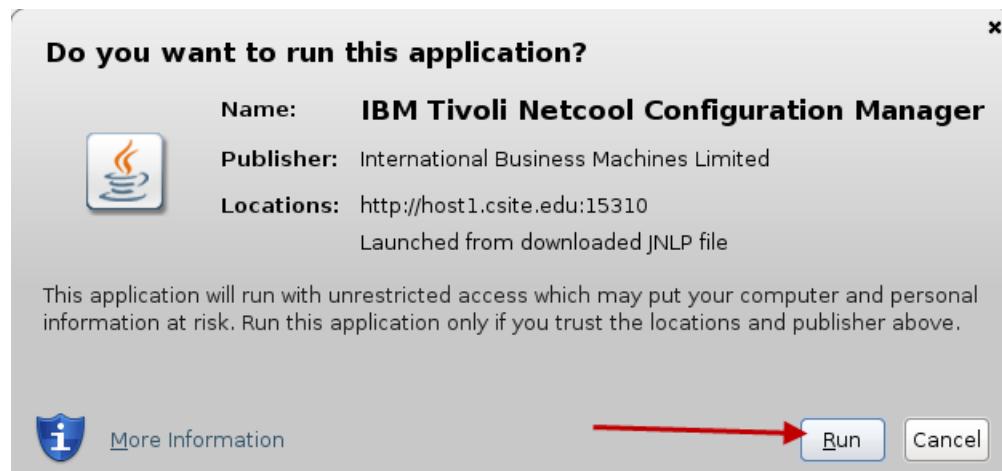
Exercise 1 Creating a modeled command set to add commands

In this exercise, you create a modeled command set to add configuration commands to a device.

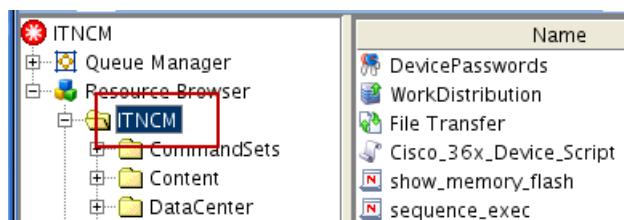
1. Log in to the user interface with the user name **engineer**. The password is **object00**.
 - a. Enter **engineer** and **object00** as the user name and password. Click **Login**.

- b. Click **ITNCM Webstart GUI**.

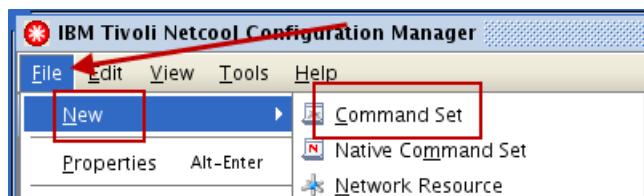
- c. Click **Run**.



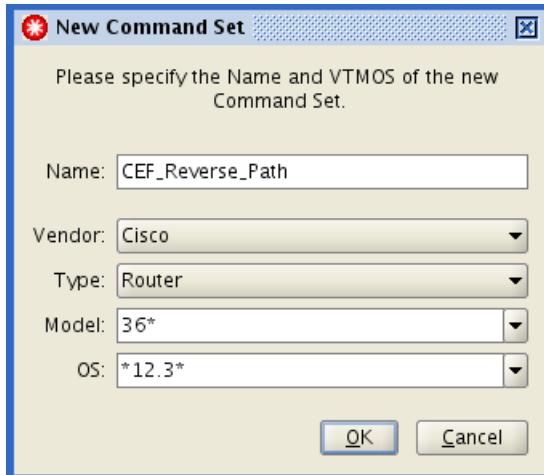
2. Create a new modeled command set named **CEF_Reverse_Path** in the **ITNCM** realm. Use the following VT莫斯 settings for the command set:
- Vendor: **Cisco**
 - Type: **Router**
 - Model: **36***
 - OS: ***12.3***
- a. Click the **ITNCM** realm in the *resource browser*.



- b. Click **File > New > Command Set**.



- c. Enter **CEF_Reverse_Path** into the **Name** field. Choose the VTMOS settings and click **OK**.

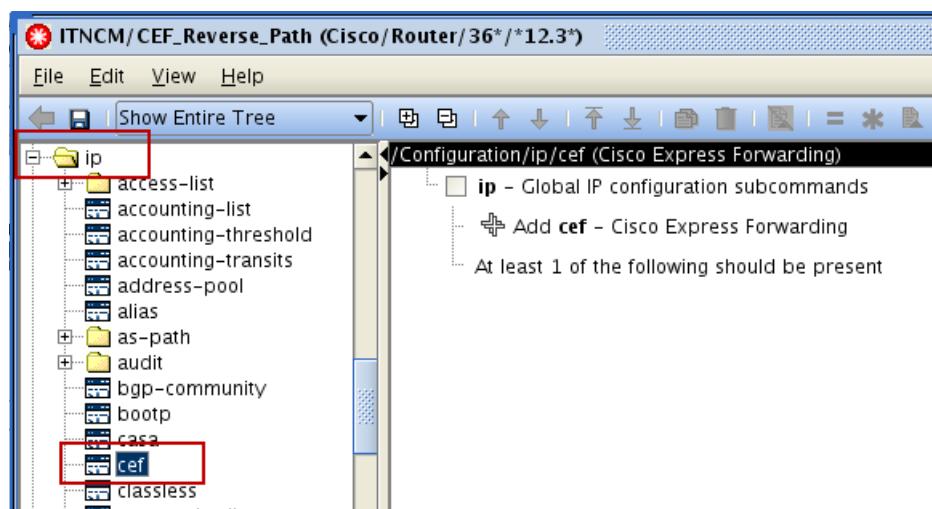


3. Configure the new **CEF_Reverse_Path** command set to perform the following tasks. Save and close the command set when you finish.
 - Enable Cisco Express Forwarding (CEF) globally. The command to enable CEF is **ip cef**. Mark this command as **Added**. Verify that the markup adds the **ip cef** command.
 - Add the command **ip verify unicast reverse-path** to a Fast Ethernet interface. Make the number of the Fast Ethernet interface a parameterized value. Use **0/0** as the default value for the interface parameter. Name the parameter **FE_interface_number**. Mark these commands as **Added**. Verify that the markup adds the **ip verify unicast reverse-path** command.

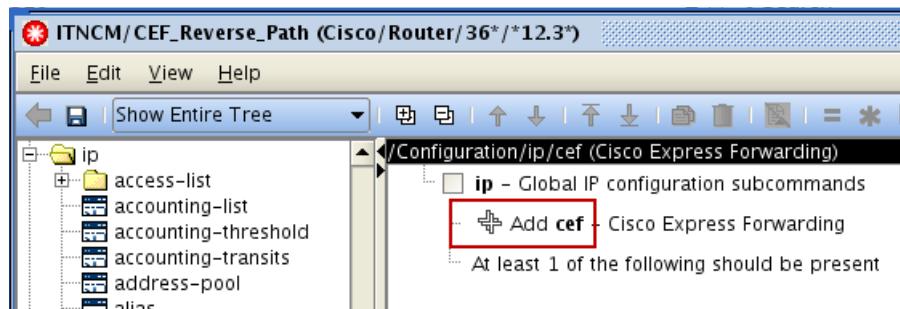
- a. Right-click the new **CEF_Reverse_Path** command set in the **ITNCM** realm and click **Edit**.



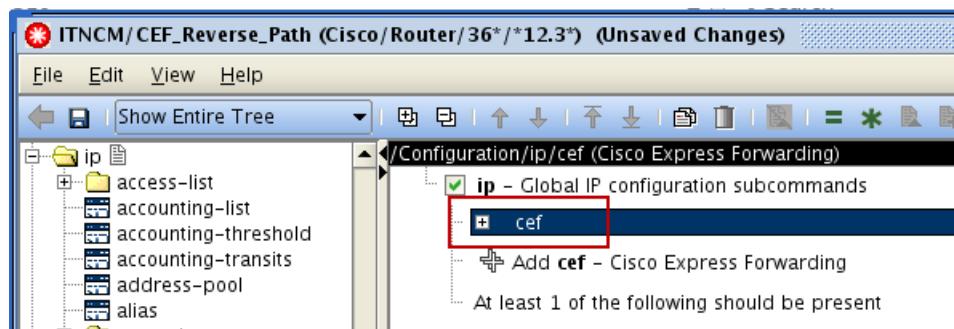
- b. Expand the **ip > cef** object.



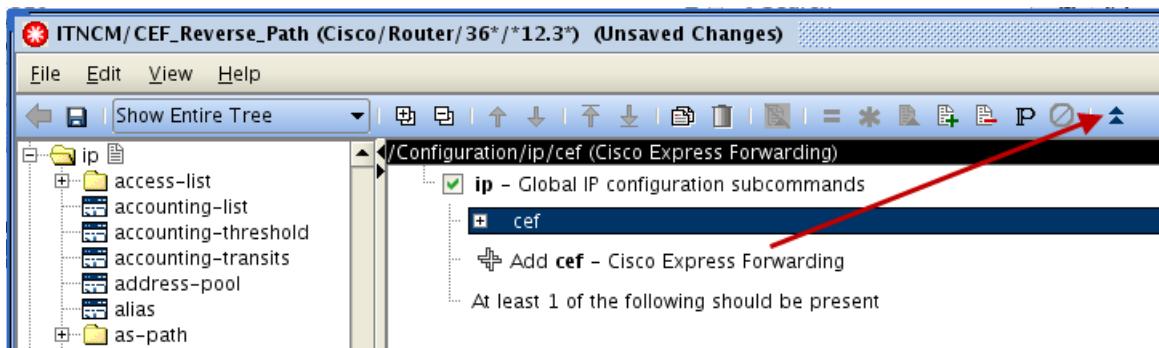
- c. Click the **Add cef** icon. A new **cef** command object is added.



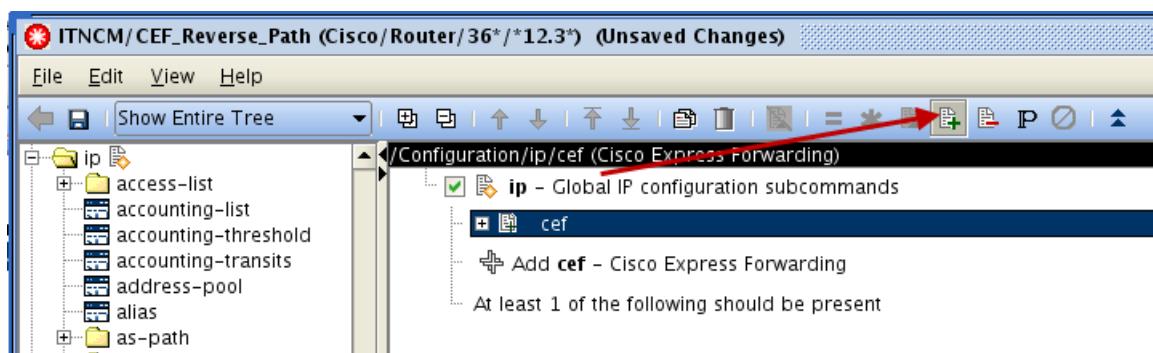
- d. Click new the **cef** command object to select it.



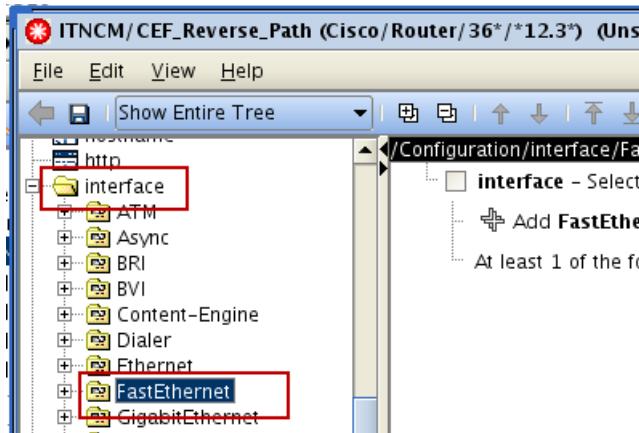
- e. Click the **Show Modify** icon.



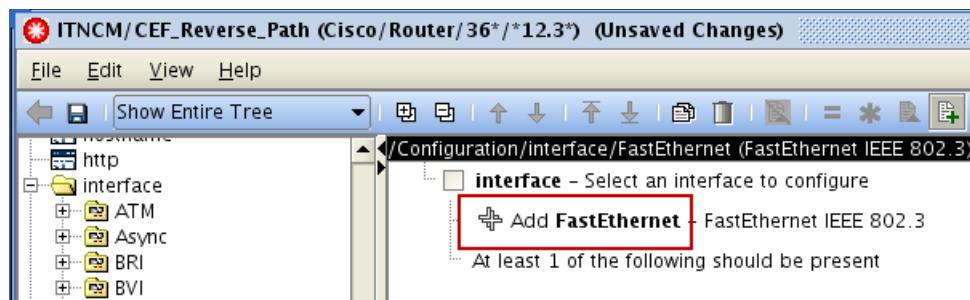
- f. Click the **Mark as Added** icon.



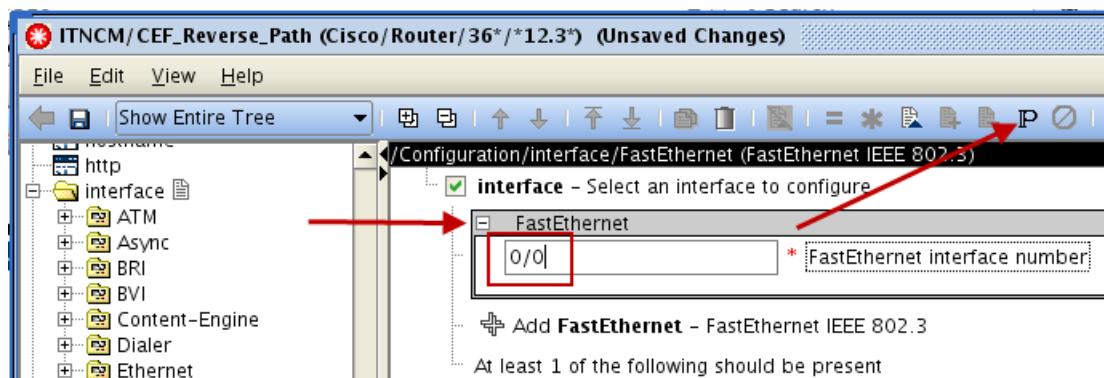
- g. Click the **interface > FastEthernet** object.



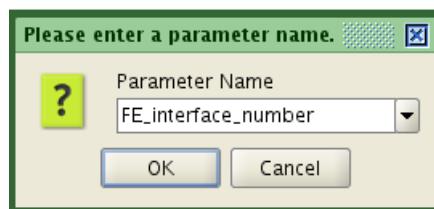
- h. Click the **Add FastEthernet** icon. An interface command object is added.



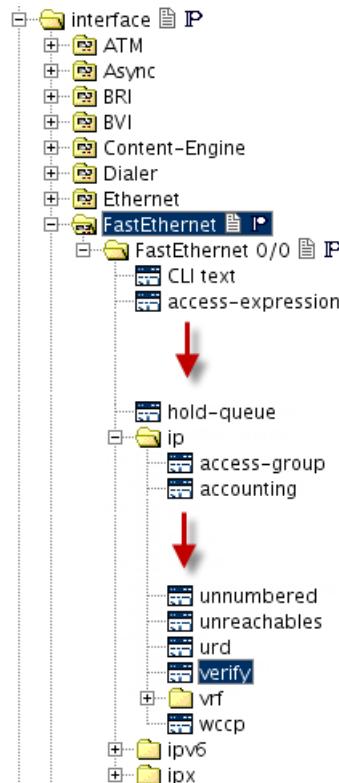
- i. Expand the new **FastEthernet** command object. Enter **0/0** in the **FastEthernet interface number** field. Click the **Mark as Parameter** icon. You are prompted to name the parameter.



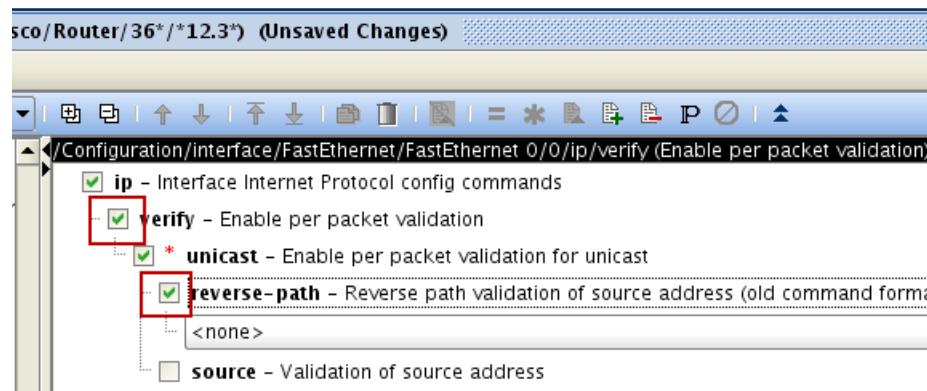
- j. Name the parameter **FE_interface_number**. Click **OK**.



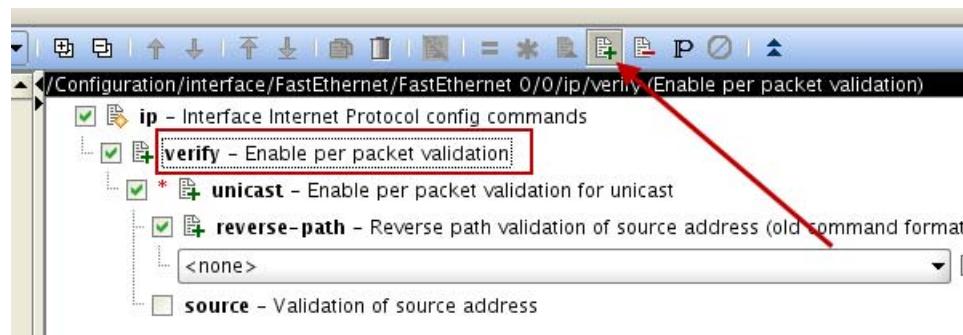
- k. Expand the interface > FastEthernet > FastEthernet 0/0 > ip > verify object.



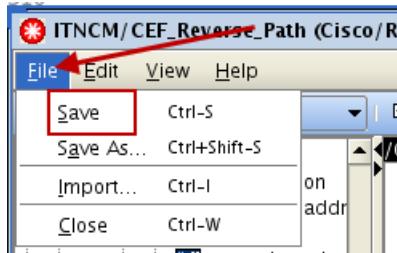
- l. Select **verify**. The **unicast** command is automatically selected. Select **reverse-path**.



- m. Click the **verify** object and click the **Mark as Added** icon. The **unicast** and **reverse-path** objects are automatically tagged with the add markup.



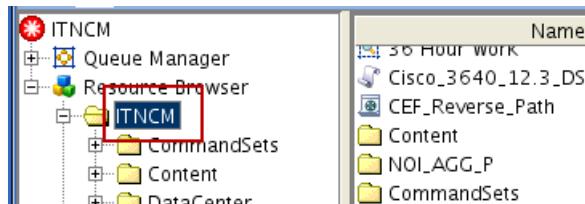
- n. Click **File > Save** to save the command set. Close the command set.



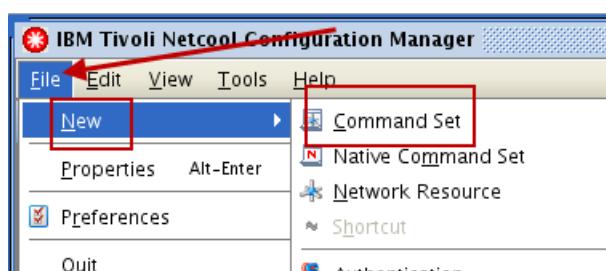
Exercise 2 Creating a modeled command set to modify commands

In this exercise, you create a modeled command set to replace and delete configuration commands that are already on a device.

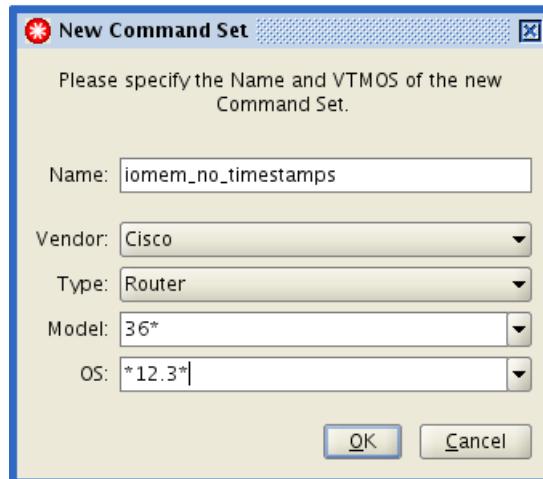
1. Create a new modeled command set named **iomem_no_timestamps** in the **ITNCM** realm. Use the following VTMOS settings for the command set:
 - Vendor: **Cisco**
 - Type: **Router**
 - Model: **36***
 - OS: ***12.3***
- a. Click the **ITNCM** realm in the *resource browser*.



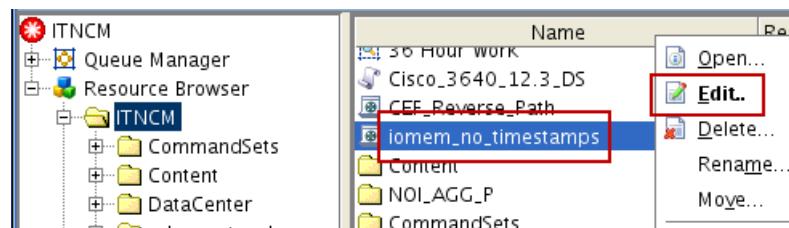
- b. Click **File > New > Command Set**.



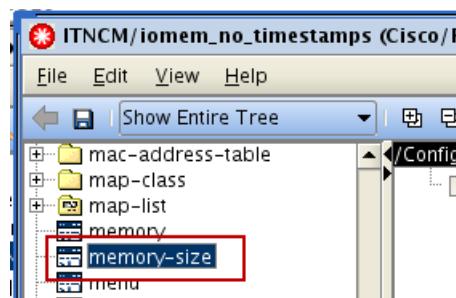
- c. Enter **iomem_no_timestamps** into the **Name** field. Choose the VTMOS settings and click **OK**.



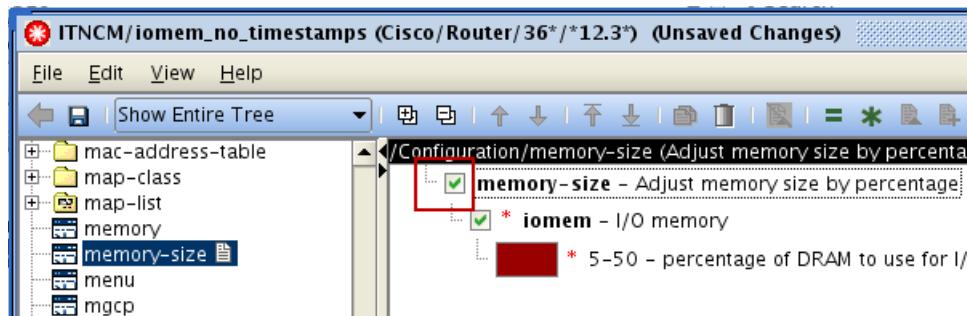
2. Configure the new **iomem_no_timestamps** command set to perform the following tasks. Save and close the command set when you finish.
- Change the **memory-size iomem** setting to **25**. The command set must match any current value of **memory-size iomem** and replace it with the value **25**. Mark this command as **Modify**. Verify that the markup modifies the **memory-size iomem** value.
 - Disable all service timestamp messages. Remove all forms of the command **service timestamps**. Mark the commands as **Deleted**. Verify that the markup deletes all the **service timestamps** commands.
- a. Right-click the new **iomem_no_timestamps** command set in the **ITNCM** realm and click **Edit**.



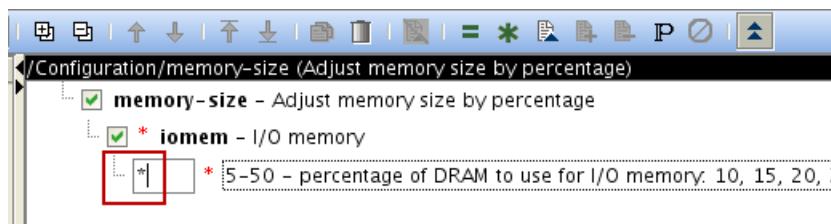
- b. Click the **memory-size** object in the command tree.



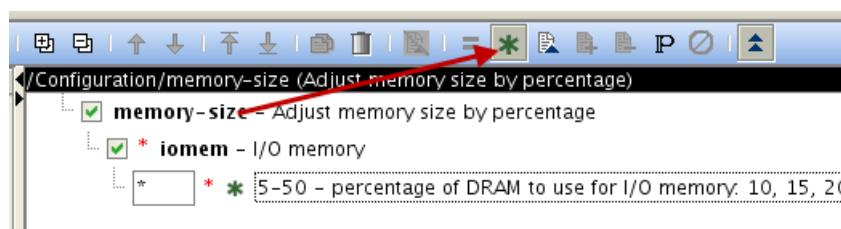
- c. Select the **memory-size** command.



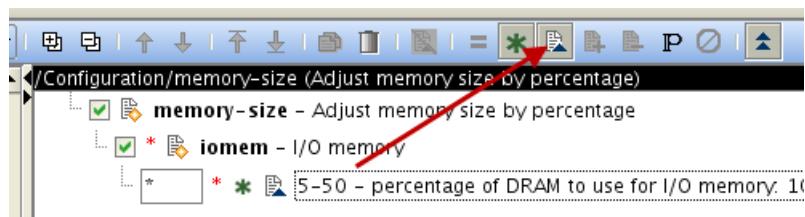
- d. Enter * in the **percentage of DRAM** field.



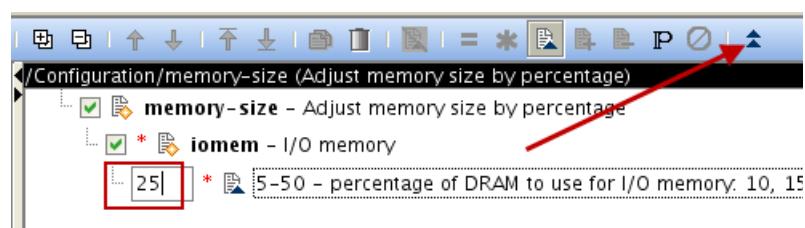
- e. Click the **Wildcard** icon.



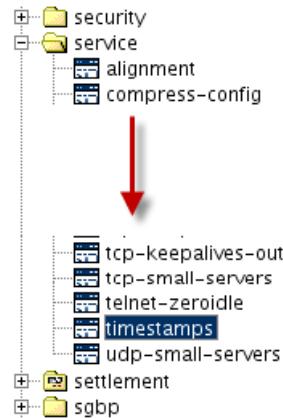
- f. Click the **Modify** icon. This view is the *match* window.



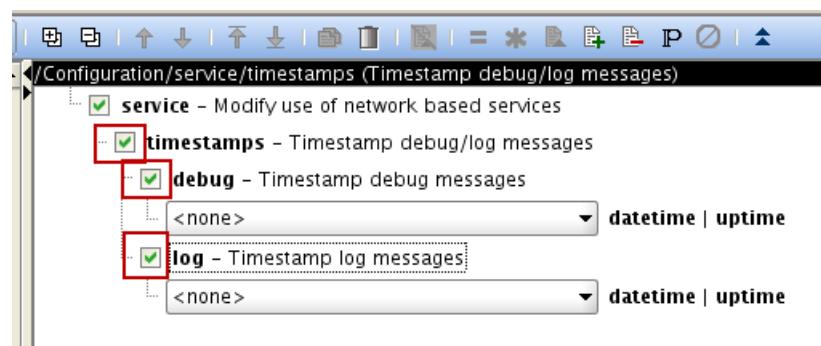
- g. Click the **Show Modify** icon and enter **25** in the **percentage of DRAM** field. This view is the *replace* window.



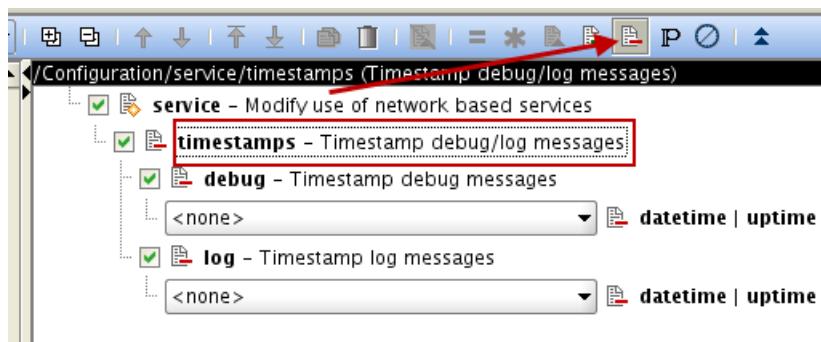
- h. Click the **service > timestamps** object in the command tree.



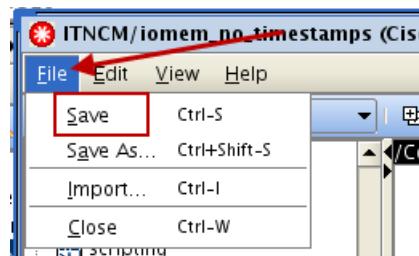
- i. Select **timestamps**. After you select **timestamps**, select **debug** and **log**.



- j. Click the **timestamps** object. Click the **Deleted** icon. The **debug** and **log** objects are automatically tagged with the delete markup.



- k. Click **File > Save** to save the command set. Close the command set.



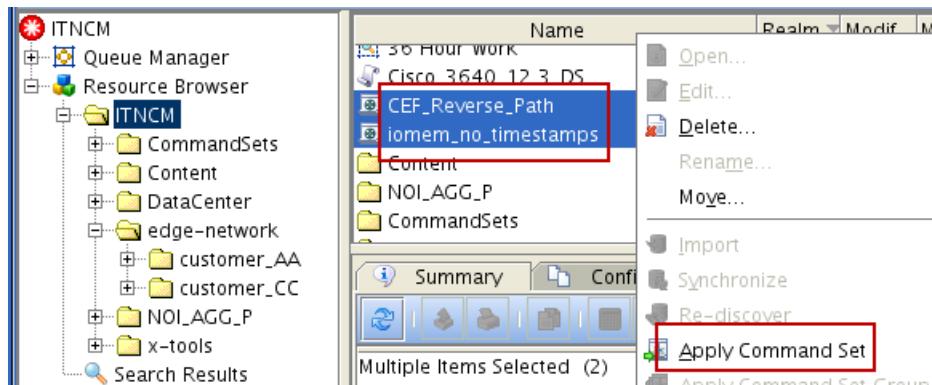
Exercise 3 Testing the command sets

In this exercise, you test the command sets by running them in report only mode.

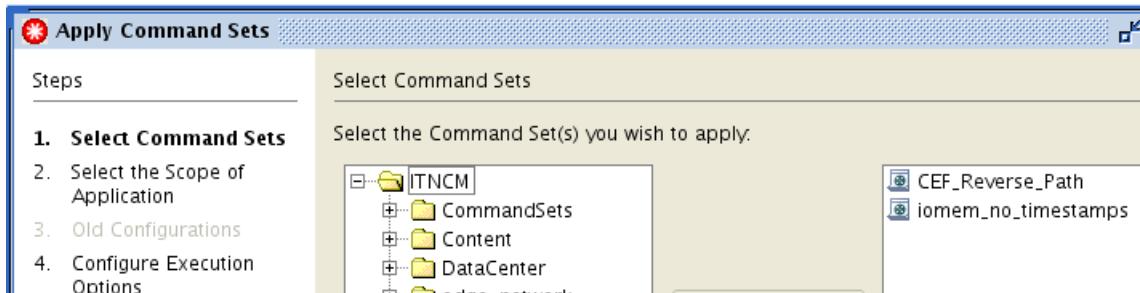
1. Apply both command sets in report only mode. The Apply Command Sets wizard starts. Use the following values to complete the wizard.

Field	Value
Select Command Sets	Leave CEF_reverse_path and iomem_no_timestamps as the selected command sets
Scope of Application	Network resources in a realm
Select the Realm	customer_CC
Execution Mode	Report only mode
Enter Parameters page 1	local
Enter Parameters page 2	Use 0/0 as the value of the FE_interface_number parameter.
Password Override	Do not override
Execution Priority	Medium
Schedule Work	Single Schedule > Immediate
Describe Work	Modeled command sets applied in report only mode

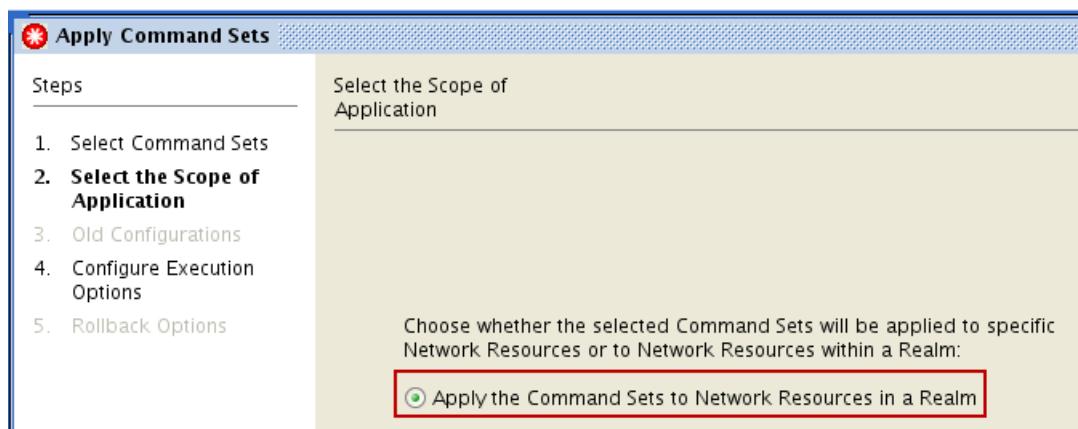
- a. Press the Ctrl key and select the **CEF_reverse_path** and **iomem_no_timestamps** command sets. Right-click the command sets and click **Apply Command Set**. The Apply Command Sets wizard starts.



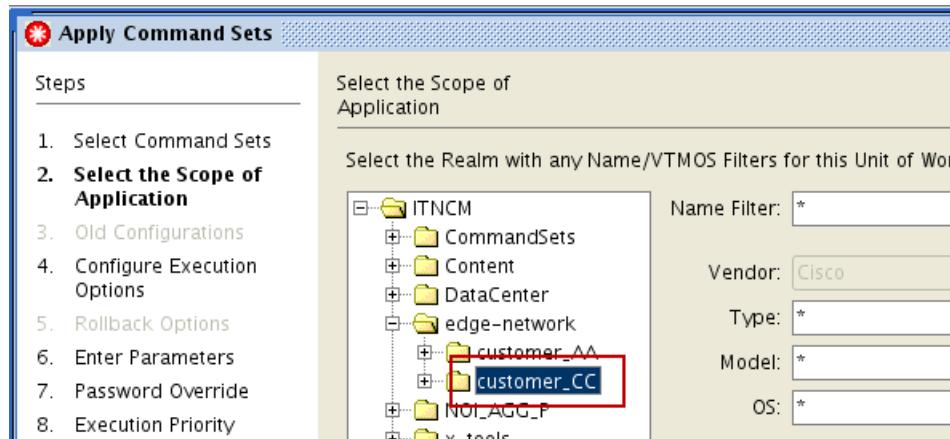
- b. Click **Next** in the Select Command Sets window.



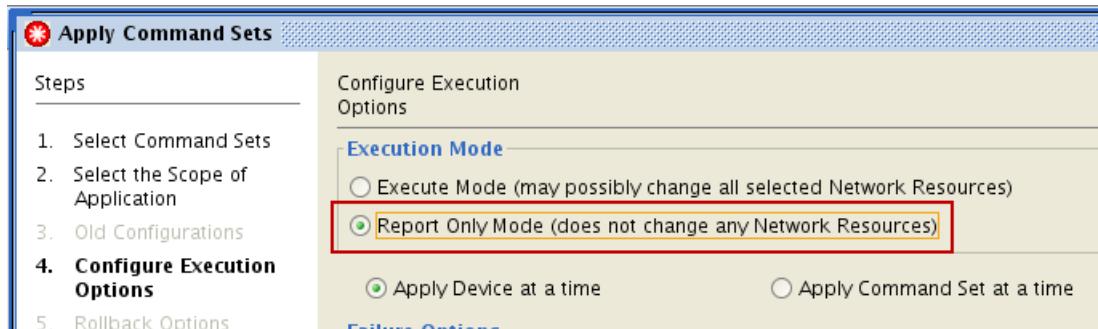
- c. Click **Next** in the Select the Scope of Application window.



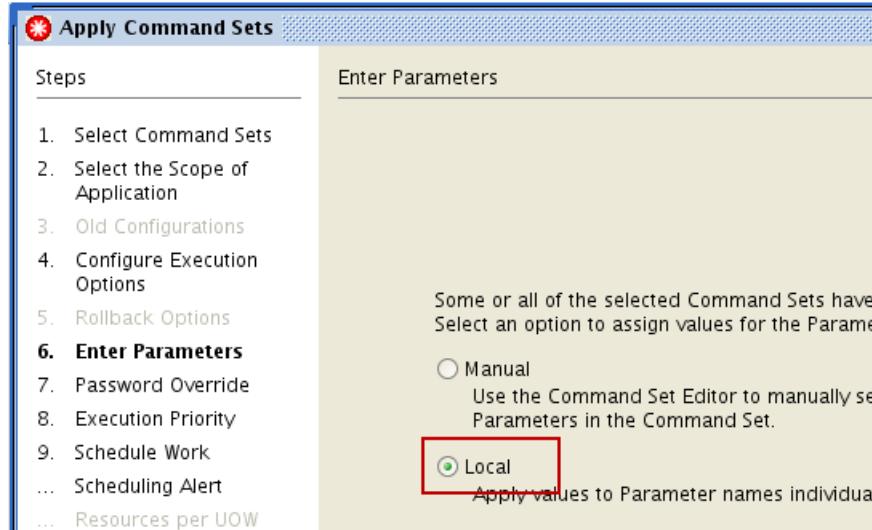
- d. Click **edge-network > customer_CC** in the Select the Realm field. Click **Next**.



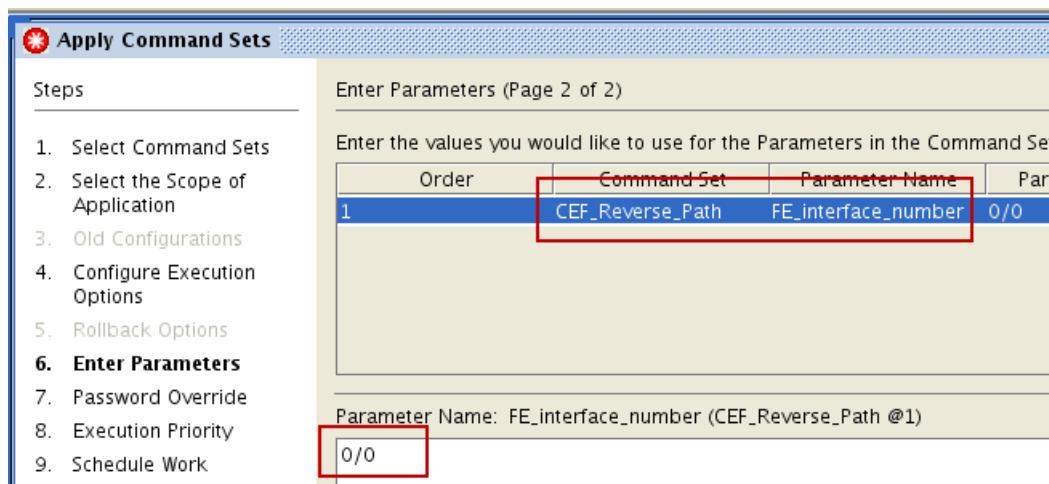
- e. Click **Report Only Mode** in the Configure Execution Options window. Click **Next**.



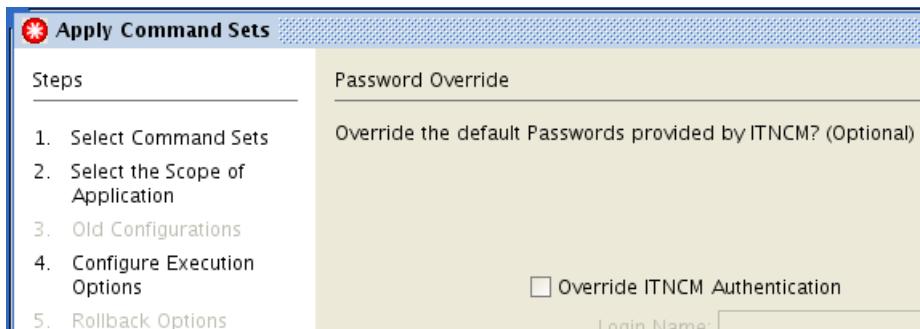
- f. Click **Local** in the Enter Parameters window. Click **Next**.



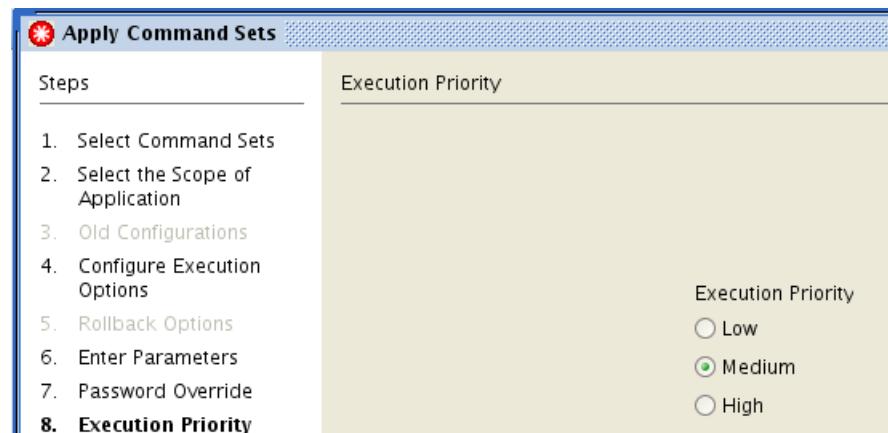
- g. Click the **FE_interface_number** parameter in the Enter Parameters (Page 2 of 2) window. Leave **0/0** in the **Parameter Name** field. Click **Next**.



- h. Click **Next** in the Password Override window.



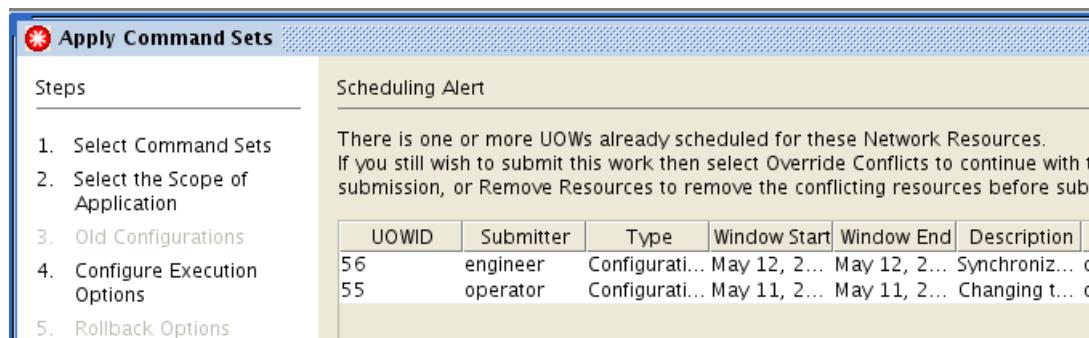
- i. Click **Next** in the Execution Priority window.



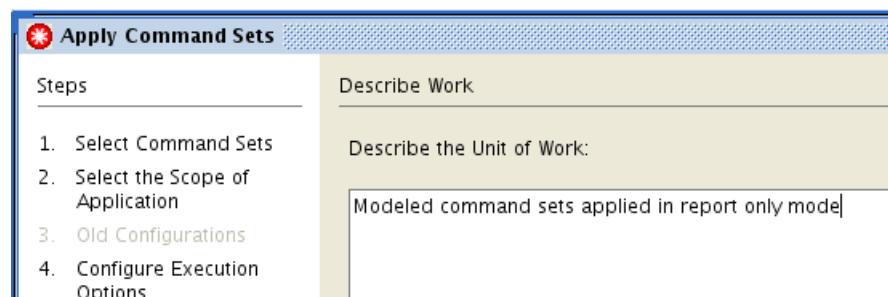
- j. Click **Next** in the Schedule Work window.



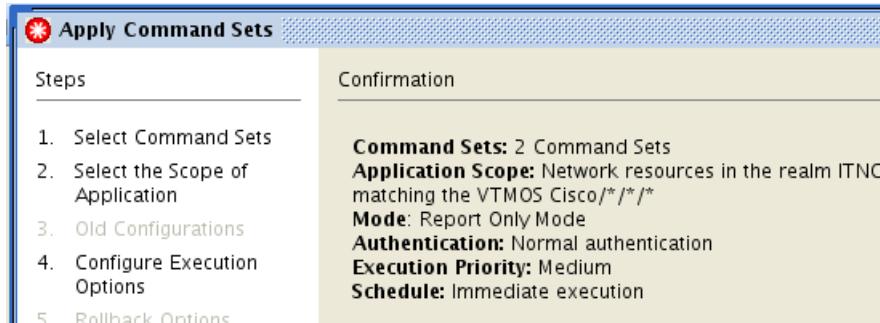
- k. Note the scheduling alert that is generated since other *units of work* are scheduled for one or more devices in the UOW your are submitting. Click **Next** to override the alert in the Scheduling Alert window.



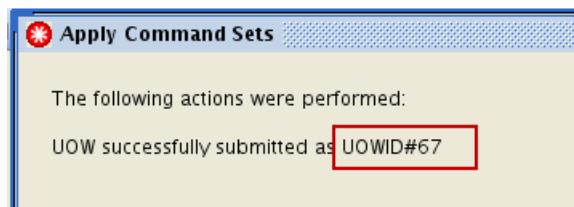
- l. Enter **Modeled command sets applied in report only mode** in the Describe Work window. Click **Next**.



- m. Click **Finish** in the Confirmation window.



- n. Note the unit of work number and click **Close**.



2. Use the work log in the unit of work to verify the result of the command sets for each device in the **customer_CC** realm. The work log shows the configuration changes that are made to each device when the command set is applied in execute mode.
- Find the unit of work in the queue manager that applied the command sets in read only mode. Click the unit of work.

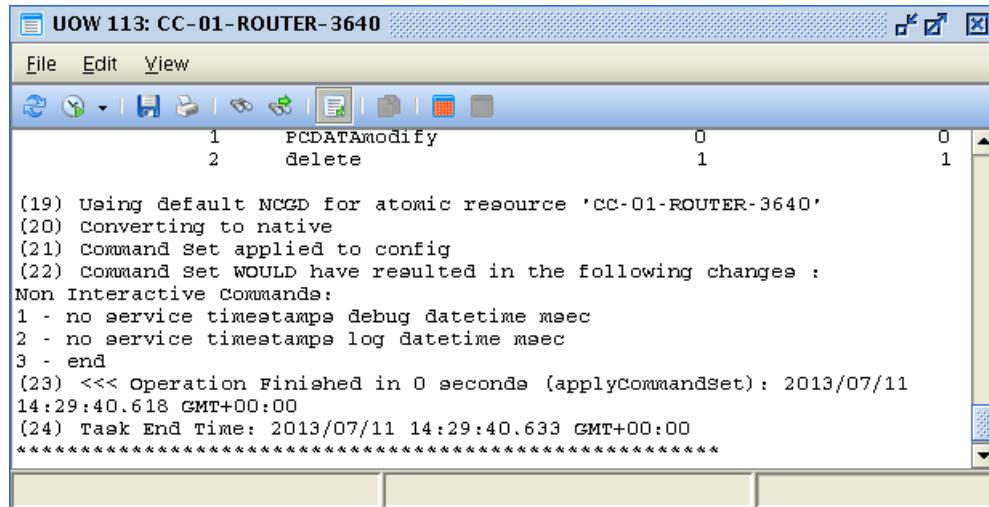
	UOW ID	Type	Submitter	Request Type
60	UOW	engineer	Native Command Set	
61	UOW	engineer	Native Command Set	
62	UOW	engineer	Native Command Set	
63	UOW	engineer	Native Command Set	
64	UOW	engineer	Native Command Set	
65	UOW	engineer	Native Command Set	
66	UOW	engineer	Configuration Synchronization (...)	
67	UOW	engineer	Command Set (Report Only)	

- Click the **Resources** tab in the unit of work. Click each device and scroll down in the work log to find the result of the command set.

The log output in the bottom pane includes:

- (21) Command Set applied to config
- (22) Command Set WOULD have resulted in the following changes :
- Non Interactive Commands:
- 1 - no service timestamps debug datetime msec
- 2 - no service timestamps log datetime msec
- 3 - end
- (23) <<< Operation Finished in 0 seconds
- (applyCommandSet): 2016/05/10 19:16:15.082
- GMT+00:00
- (24) Task End Time: 2016/05/10 19:16:15.95
- GMT+00:00

- c. Check the logs for cc-01-router-3640. No memory size changes are made. The command **memory-size iomem** is already set to 25, and the command set is not going change a value to the same value.



The screenshot shows a software window titled "UOW 113: CC-01-ROUTER-3640". The window has a menu bar with "File", "Edit", and "View". Below the menu is a toolbar with various icons. The main area displays a log of commands and their results:

Line Number	Action	Value 1	Value 2	Value 3
1	PCDATA modify	0	0	0
2	delete	1	1	1

Log output:

```
(19) Using default NCGD for atomic resource 'CC-01-ROUTER-3640'
(20) converting to native
(21) Command Set applied to config
(22) Command Set WOULD have resulted in the following changes :
Non Interactive Commands:
1 - no service timestamps debug datetime msec
2 - no service timestamps log datetime msec
3 - end
(23) <<< Operation Finished in 0 seconds (applyCommandSet): 2013/07/11
14:29:40.618 GMT+00:00
(24) Task End Time: 2013/07/11 14:29:40.633 GMT+00:00
*****
```

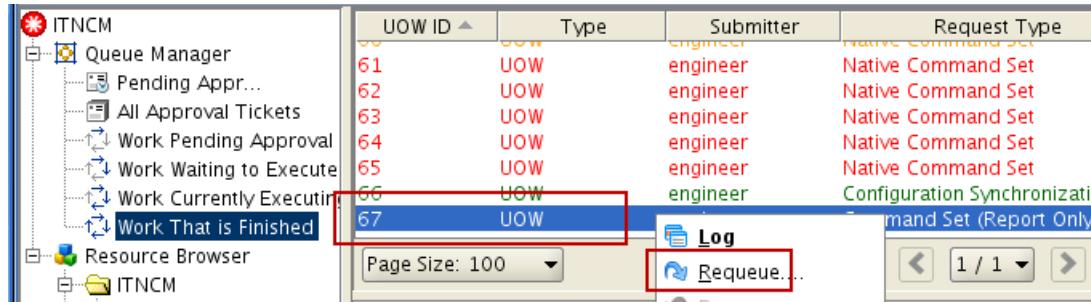
Exercise 4 Applying command sets

In this exercise, you apply two modeled command sets.

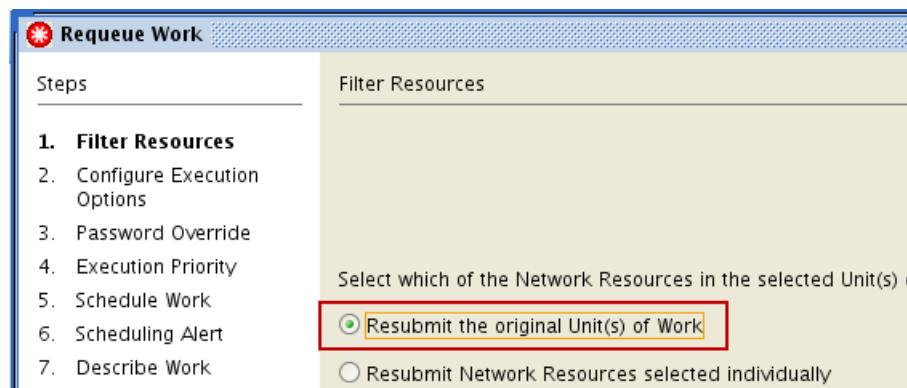
- Find the command set unit of work that ran in the previous exercise and requeue it. Use the following values to complete the wizard.

Field	Value
Filter Resources	Resubmit the original Unit(s) of Work
Configure Execution Options	Execute Mode
Password Override	Do not override
Execution Priority	Medium
Schedule Work	Single Schedule > Immediate
Scheduling Alert	Override Conflicts
Describe Work	Modeled command sets applied

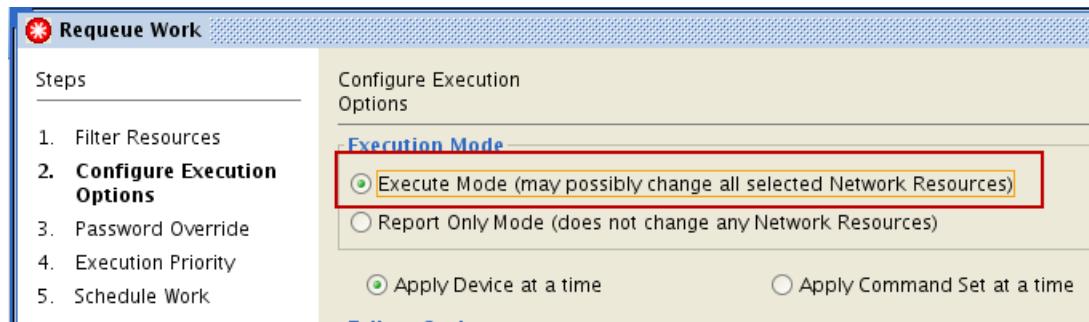
- Find and right-click the most recent unit of work. Select **Requeue**.



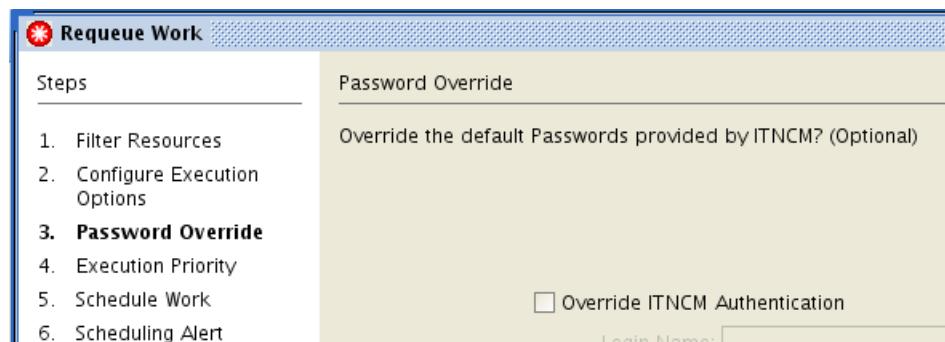
- In the Filter Resources window, select **Resubmit the original Unit(s) of Work**. Click **Next**.



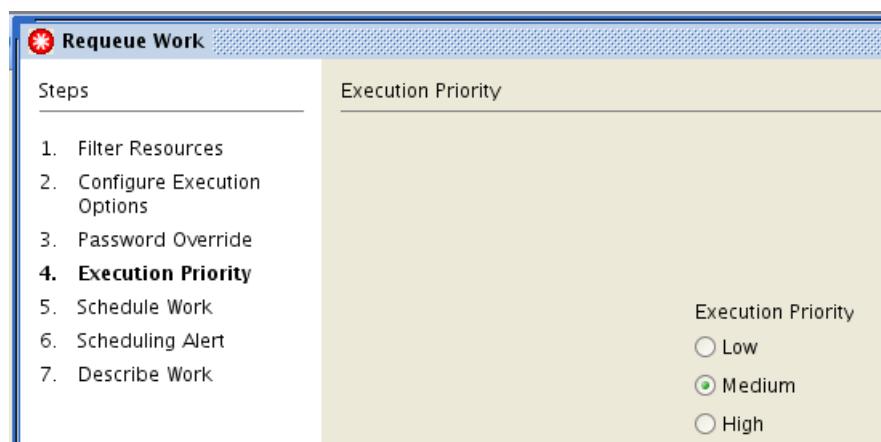
- c. In the Configure Execution Options window, select the **Execute Mode**. Click **Next**.



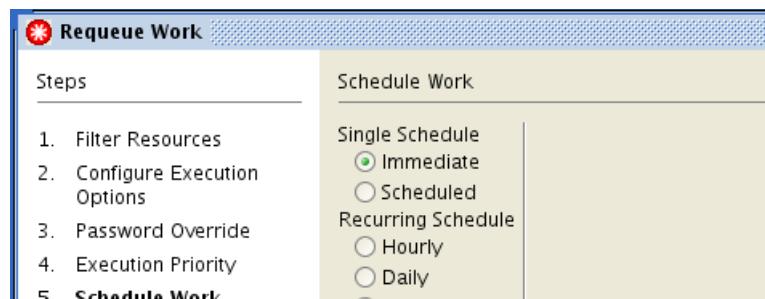
- d. In the Password Override window, click **Next**.



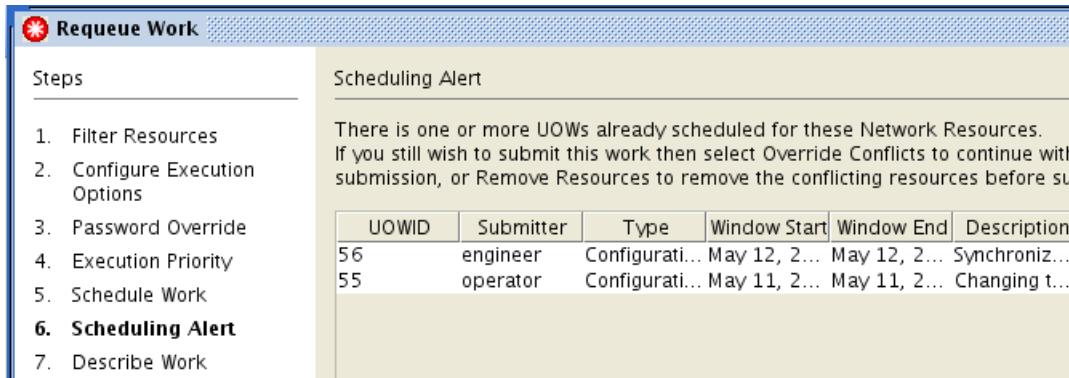
- e. In the Execution Priority window, click **Next**.



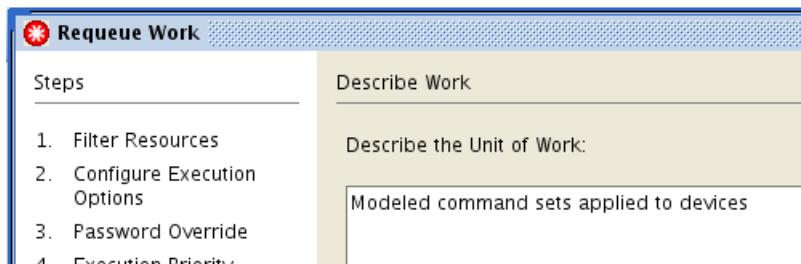
- f. In the Schedule Work window, click **Next**.



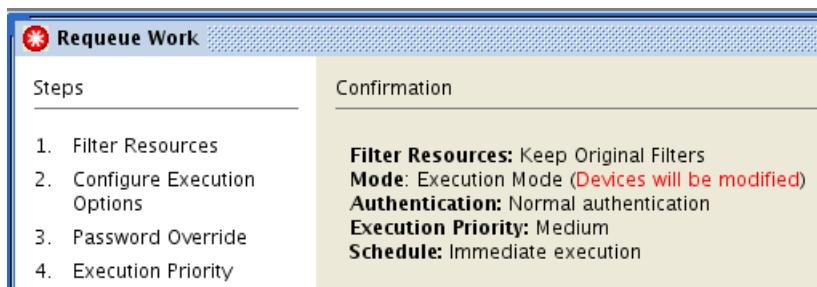
- g. Click **Next** at the Scheduling Alert window.



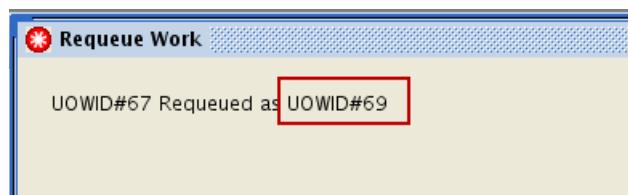
- h. In the Describe Work window, enter **Modeled command sets applied to devices**. Click **Next**.



- i. In the Confirmation window, click **Finish**.

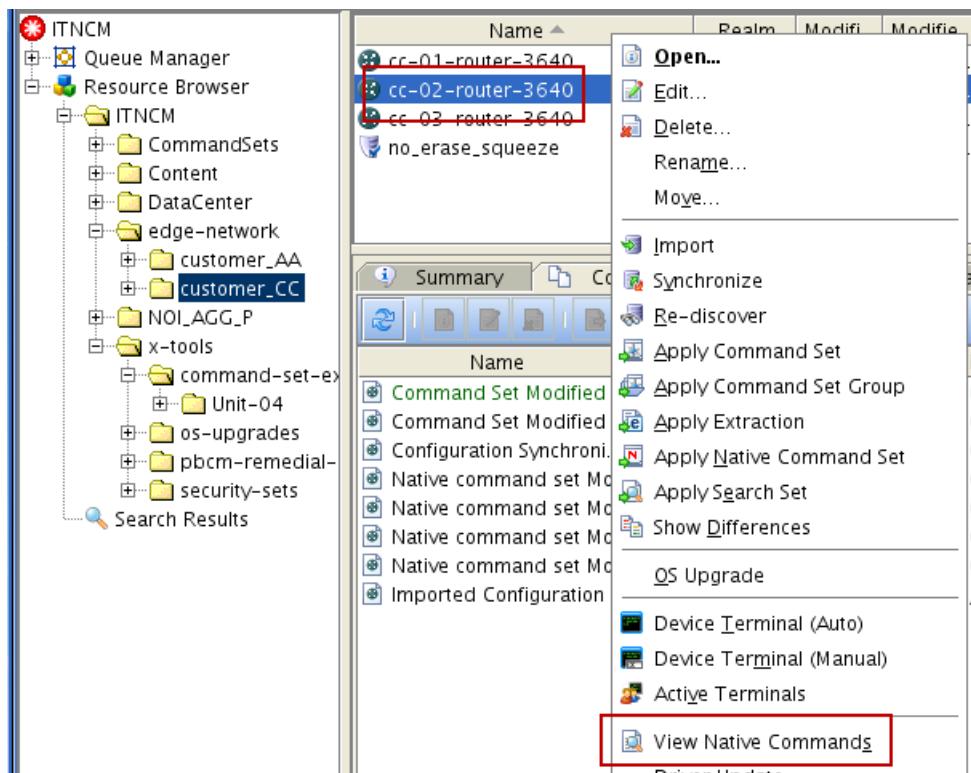


- j. Note the unit of work number and click **Close**.



Wait for the unit of work to finish.

2. Use the **View Native Commands** feature to verify that the command sets are successfully applied to the devices in the **customer_CC** realm. Verify the following configuration items:
 - All service timestamps are disabled
 - The value of memory-size iomem is set to **25** for devices with a memory-size iomem command defined
 - **IP CEF** is enabled globally
 - Interface FastEthernet0/0 has the **ip verify unicast reverse-path** feature enabled
 - a. Click the **customer_CC** realm in the *resource browser*. Right-click the device that is named **cc-02-router-3640** and click **View Native Commands**.



- b. Scroll down in the configuration to view the new configuration items.

```

00001: version 12.4
00002: no service timestamps debug uptime
00003: no service timestamps log uptime
00004: service password-encryption
00005: service sequence-numbers

00019: aaa session-id common
00020: memory-size iomem 25
00021: !
00022: !
00023: ip cef
00024: no ip domain lookup

00036: interface FastEthernet0/0
00037:   description Customer_CC_uplink_TelecomA
00038:   ip address 10.191.101.75 255.255.255.0
00039:   ip verify unicast reverse-path
00040:   speed 100
00041:   full-duplex
00042: !

```

- c. Close the window when complete.
- d. View the configuration of the **cc-01-router-3640** and **cc-03-router-3640** devices by using the **View Native Commands** feature. Verify that the changes in the command sets are applied to those devices.

Leave the user interface as is. You return to it shortly.



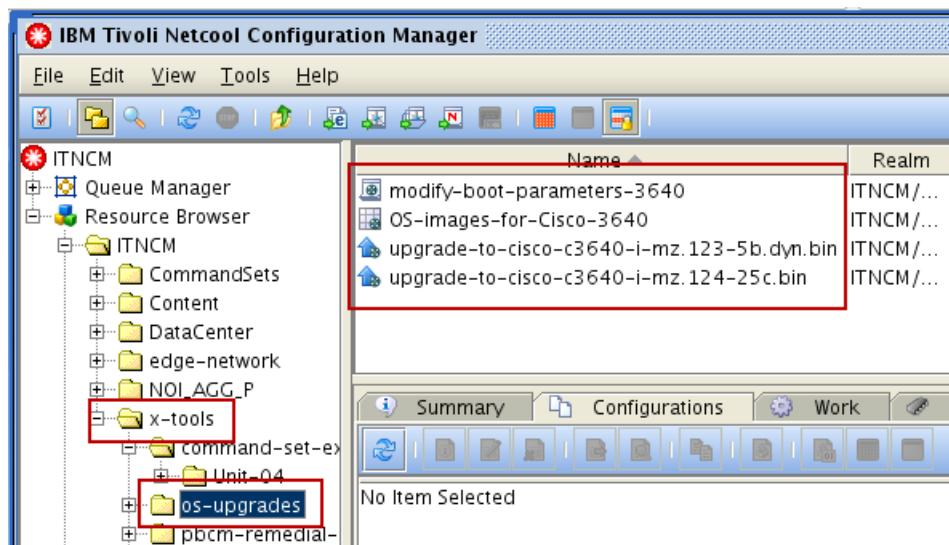
13 Device OS upgrade manager exercises

In the exercises for this unit, you work with two Netcool Configuration Manager resources. The operating system upgrade process requires these resources. The first resource is a catalog of IOS images. The second resource is the upgrade template for the upgrade of a device to a specific IOS image.

Exercise 1 Modifying an operating system registry

In this exercise, you modify the operating system registry.

1. View the existing operating system upgrade resources in the **ITNCM > x-tools > os-upgrades** realm. Click the **ITNCM > x-tools > os-upgrades** realm.



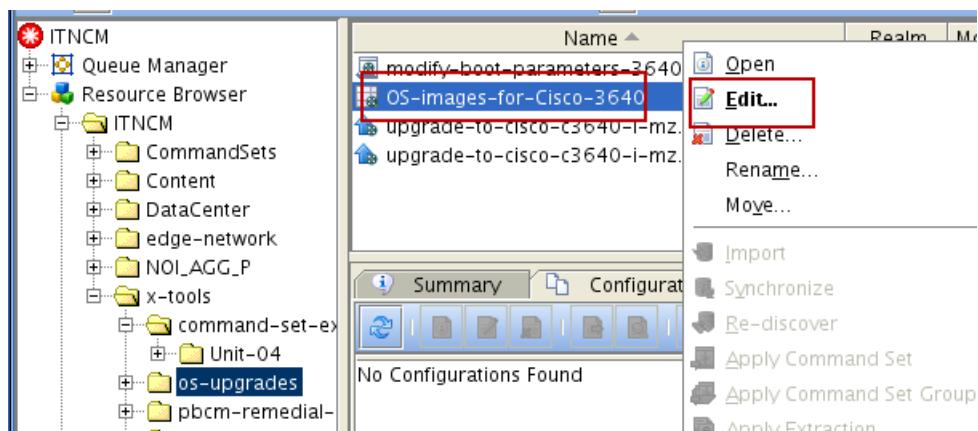
The realm contains the following resources:

- **OS-images-for-Cisco-3640:** This operating system registry is a catalog of images that are compatible with Cisco 3640 devices.
- **modify-boot-parameters-3640:** You use this command set to modify the boot commands in the device configuration. The command set points to the new image that is copied to the device.
- **upgrade-to-cisco-c3640-i-mz-124-25c.bin:** This operating system specification is an upgrade template. You select and apply it to a Cisco 3640 router to upgrade it to a specific version of 12.4 Cisco IOS.

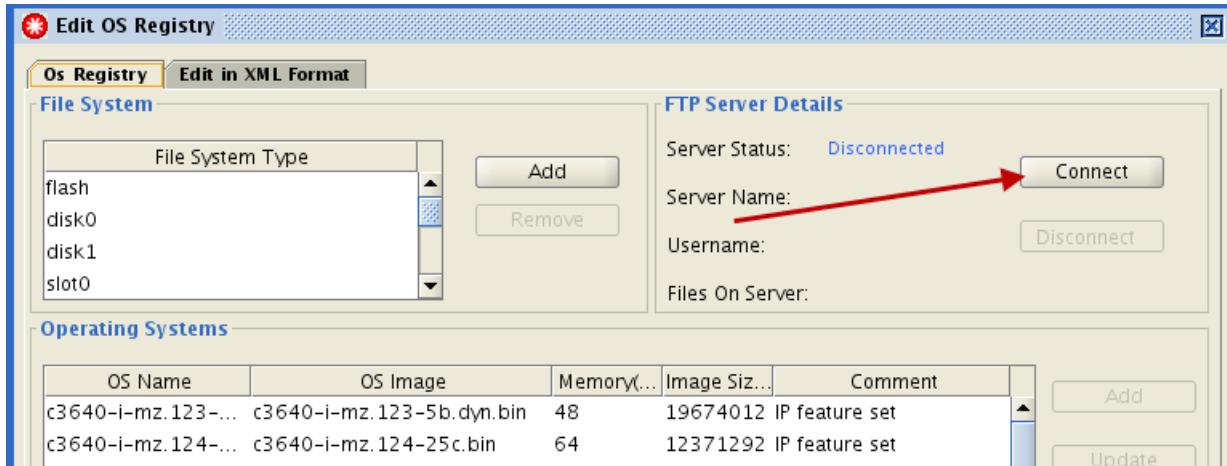
2. Edit the **OS-images-for-Cisco-3640** operating system registry. Use the following attributes to add another operating system image to the registry. Save and close the registry when you finish.

- File transfer resource: **File Transfer**
- FTP server name: **10.191.101.126**
- FTP user name: **virtuser**
- FTP user password: **object00**
- FTP server path: **../../opt/images**
- Operating system image: **c3640-ik9s-mz.124-25c.bin**
- Operating system required **RAM: 128 MB**
- Operating system comment: **12.4 IPSec features**

- a. Right-click the **OS-images-for-Cisco-3640** operating system registry and click **Edit**.

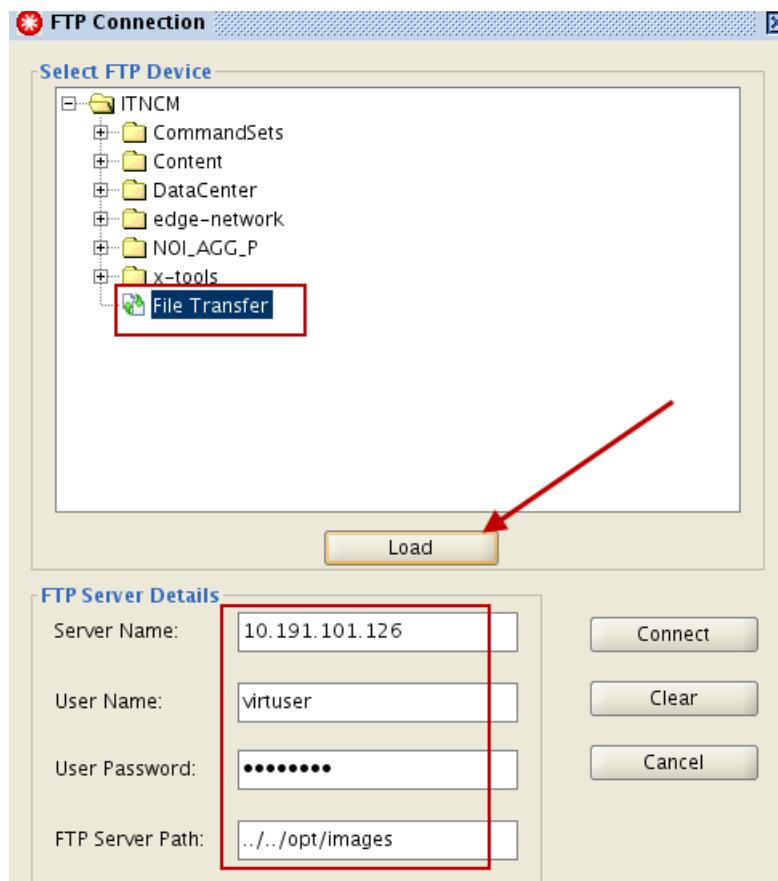


- b. Click the **Connect** button to enter the FTP server details.



- c. Click the **File Transfer** resource in the **Select FTP Device** window. Click the **Load** button.
The FTP Server Details are automatically completed. If they are not automatically completed, manually enter the following values:

- ◆ FTP server name: **10.191.101.126**
- ◆ FTP user name: **virtuser**
- ◆ FTP user password: **object00**
- ◆ FTP server path: **../../opt/images**



- d. Click the **Connect** button.

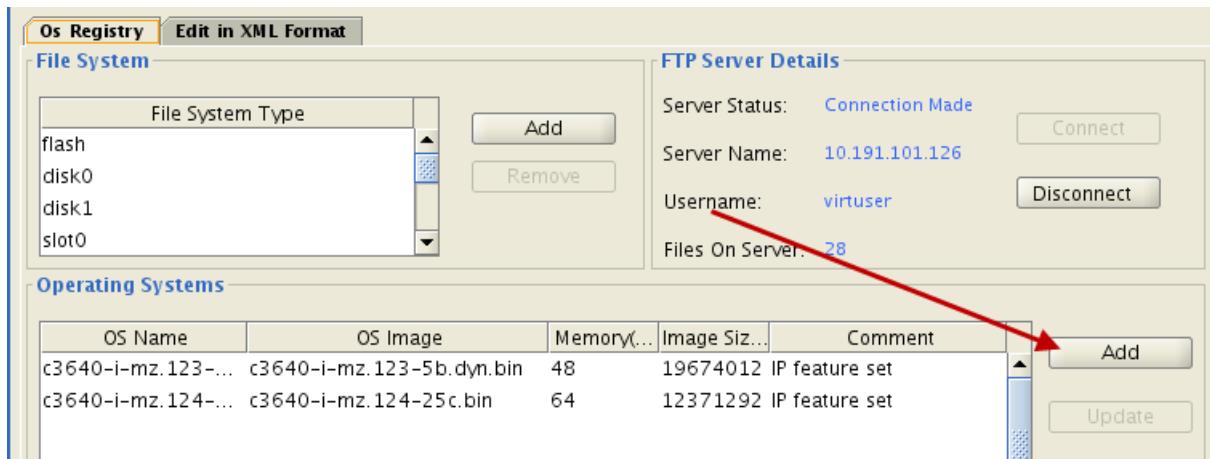


The FTP Connection window closes and you return to the operating system registry.



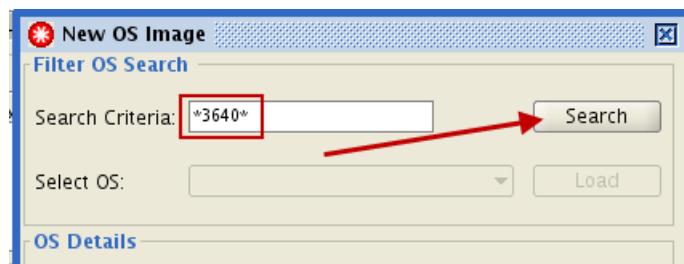
Note: You connect to the GNS image. The GNS image contains the Cisco IOS images.

- e. Click the **Add** button.

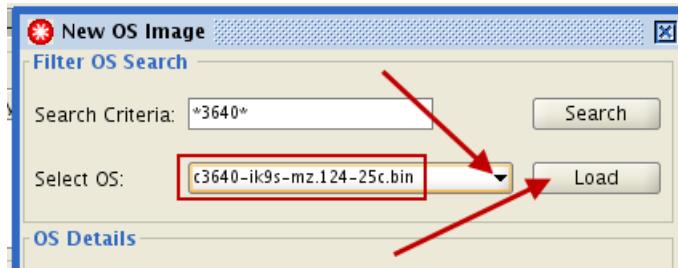


The New OS Image window opens.

- f. Enter ***3640*** in the **Search Criteria** field. Click **Search**.

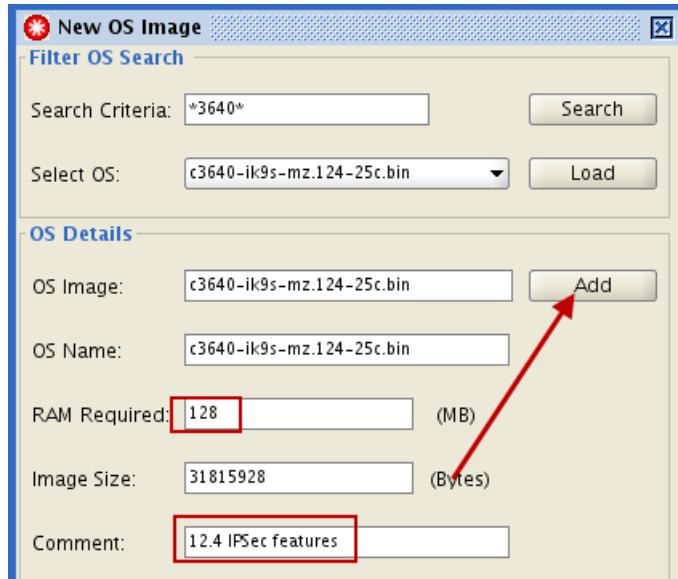


- g. Select the **c3640-ik9s-mz.124-25c.bin** image from the list of search results. Click **Load**.



Most of the fields are completed for you after you click Load.

- h. Enter **128** in the **RAM Required** field. Enter **12.4 IPSec features** in the **Comment** field. Click the **Add** icon. Close the New OS Image window when you finish.



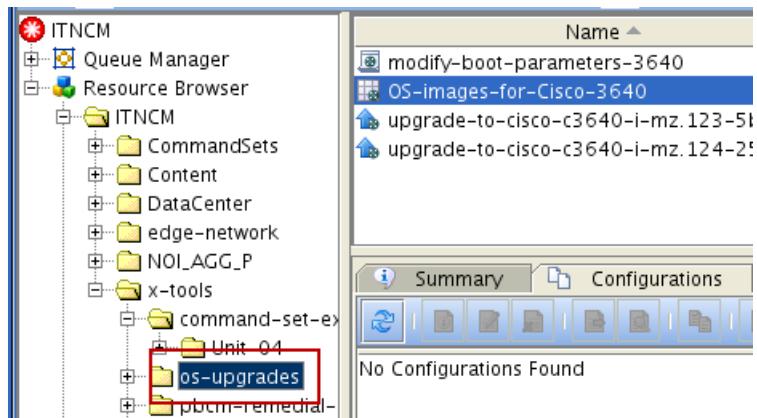
- i. Click the **Save** icon. After you save the registry, click the **Exit** icon.

OS Name	OS Image	Memory...	Image Siz...	Comment
c3640-i-mz.123-...	c3640-i-mz.123-5b.dyn.bin	48	19674012	IP feature set
c3640-i-mz.124-...	c3640-i-mz.124-25c.bin	64	12371292	IP feature set
c3640-ik9s-mz.12...	c3640-ik9s-mz.124-25c.bin	128	31815928	12.4 IPSec features

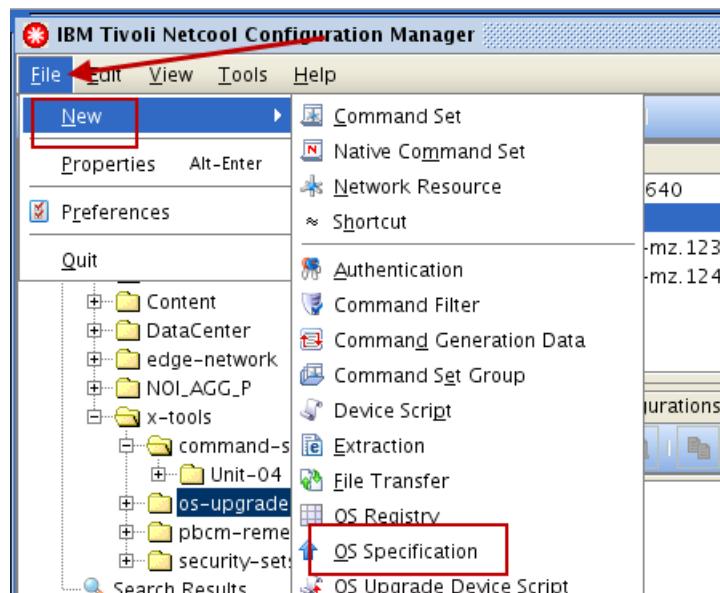
Exercise 2 Creating an operating system specification

In this exercise, you create and configure a new operating system specification. The new specification uses the new entry in the operating system registry.

1. Start the OS Specification wizard to create an operating system specification. Create the specification in the **os-upgrades** realm.
 - a. Click **ITNCM > x-tools > os-upgrades** in the *resource browser*.



- b. Click **File > New > OS Specification**. The OS Specification wizard starts.



2. Use the values in the following table to complete the Network Resource Discovery wizard.

Field	Value
Name	upgrade-to-cisco-c3640-ik9s-mz.124-25c
Vendor	Cisco
Type	Router
Model	3640
OS	*
OS Registry	ITNCM > x-tools > os-upgrades > OS-images-for-Cisco-3640
Target OS	c3640-ik9s-mz.124-25c.bin
File system	Flash
Erase All	Yes
Boot Command Set	ITNCM > x-tools > os-upgrades > modify-boot-parameters-3640
Parser	Device Content Parser
Describe Work	This OS specification upgrades to c3640-ik9s-mz.124-25c.bin and applies a command set to change the boot parameters on the device

a. Enter the following values in the Select VTMOS window. When you finish, click **Next**.

- ◆ Name: **upgrade-to-cisco-c3640-ik9s-mz.124-25c**
- ◆ Vendor: **Cisco**
- ◆ Type: **Router**
- ◆ Model: **3640**
- ◆ OS: *

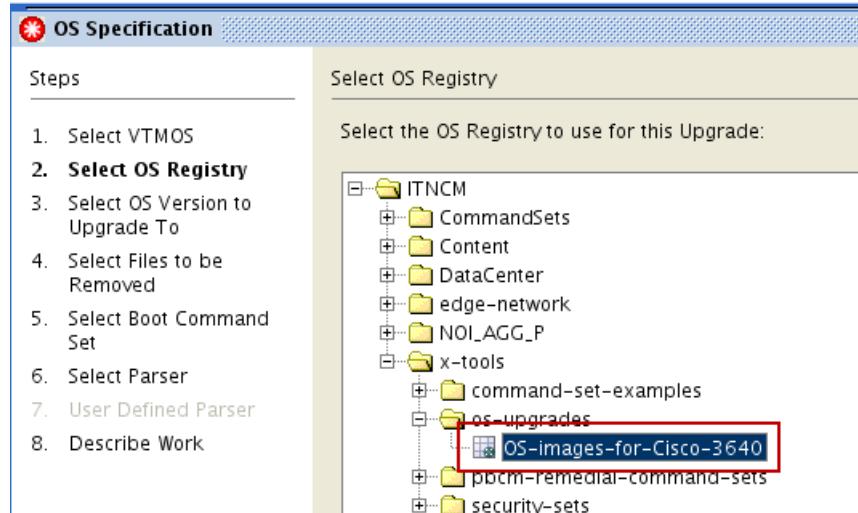
The screenshot shows the 'OS Specification' interface. On the left, a sidebar titled 'Steps' lists the following sequence:

1. Select VTMOS
2. Select OS Registry
3. Select OS Version to Upgrade To
4. Select Files to be Removed
5. Select Boot Command Set
6. Select Parser
7. User Defined Parser
8. Describe Work

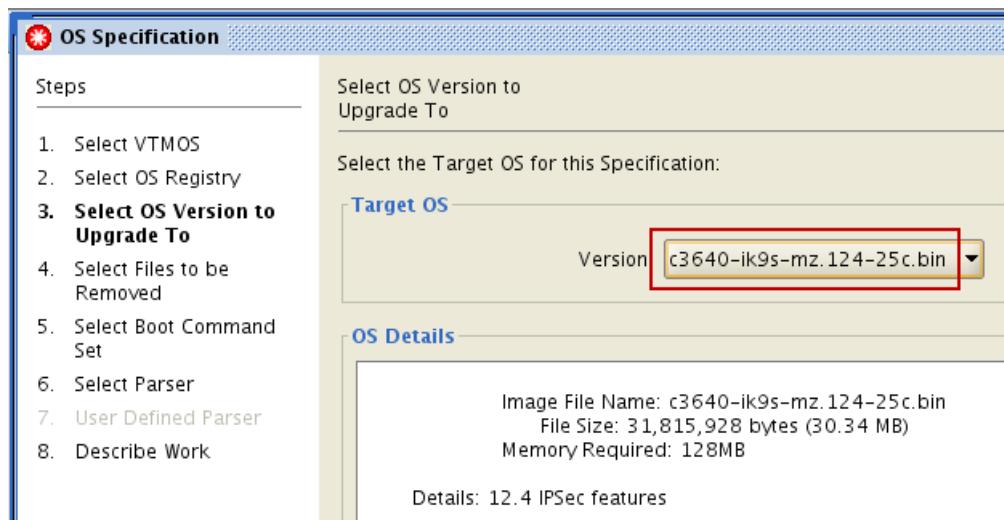
The main panel is titled 'Select VTMOS' and contains the following form fields:

Name:	upgrade-to-cisco-c3640-ik9s-mz.124-25c
Vendor:	Cisco
Type:	Router
Model:	3640
OS:	*

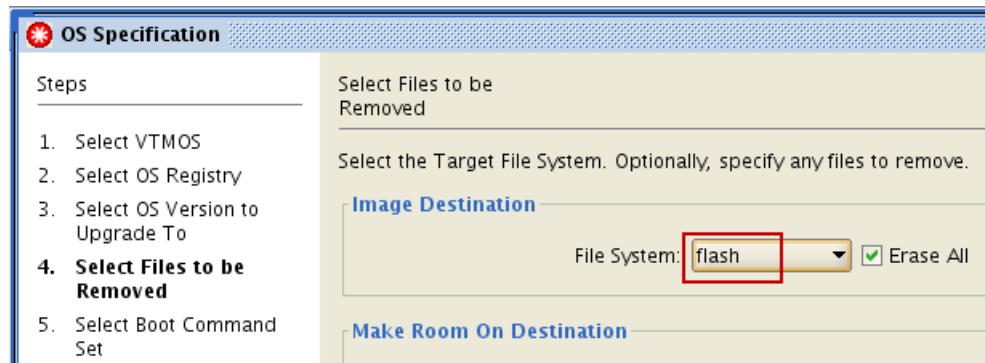
- b. Click ITNCM > x-tools > os-upgrades > OS-images-for-Cisco-3640. Click Next.



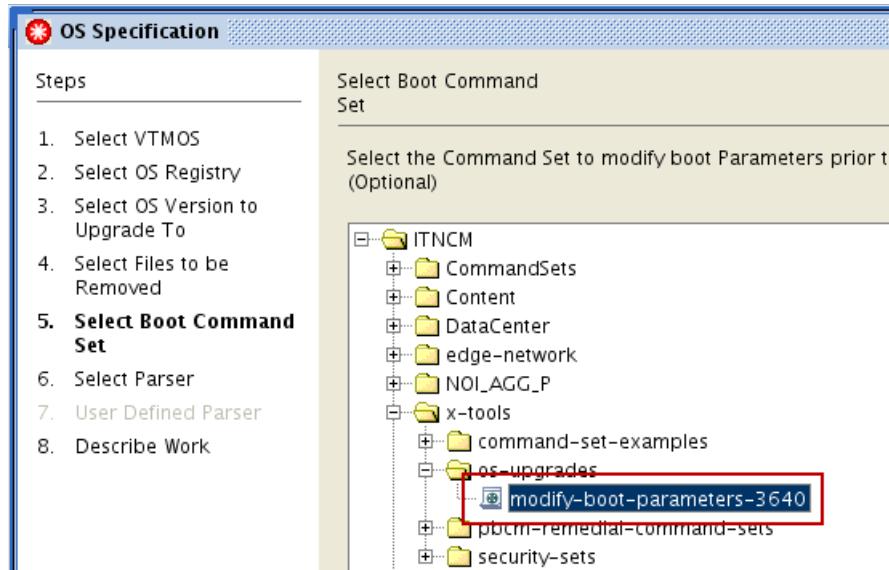
- c. Select c3640-ik9s-mz.124-25c.bin in the Target OS field. Click Next.



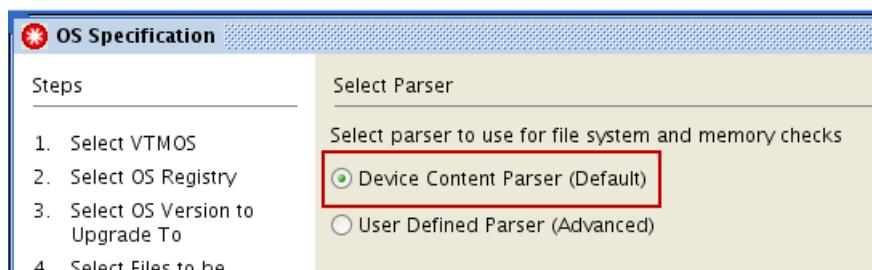
- d. Select Flash in the File System field. Verify that Erase All is selected. Click Next.



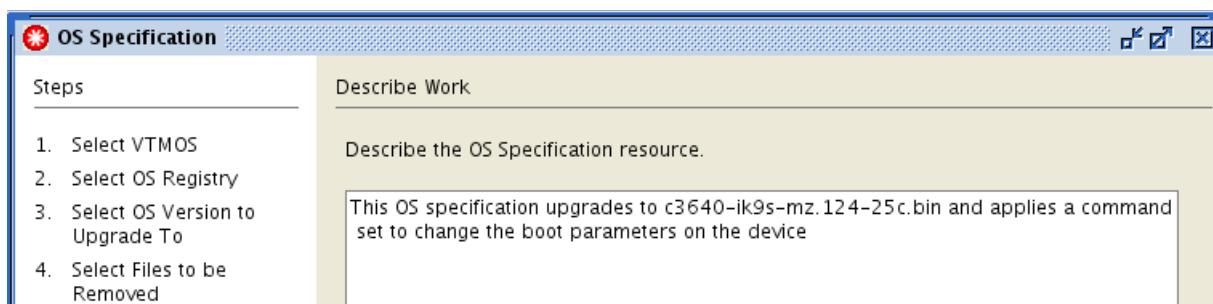
- e. Click **ITNCM > x-tools > os-upgrades > modify-boot-parameters-3640**. Click **Next**.



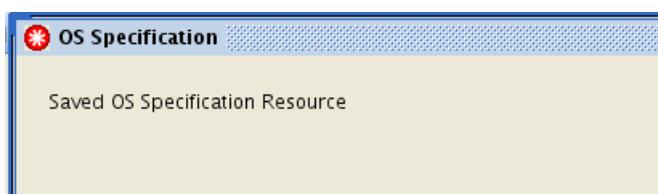
- f. Click **Device Content Parser**. Click **Next**.



- g. Enter **This OS specification upgrades to c3640-ik9s-mz.124-25c.bin and applies a command set to change the boot parameters on the device** as the description.



- h. Click **Close**.



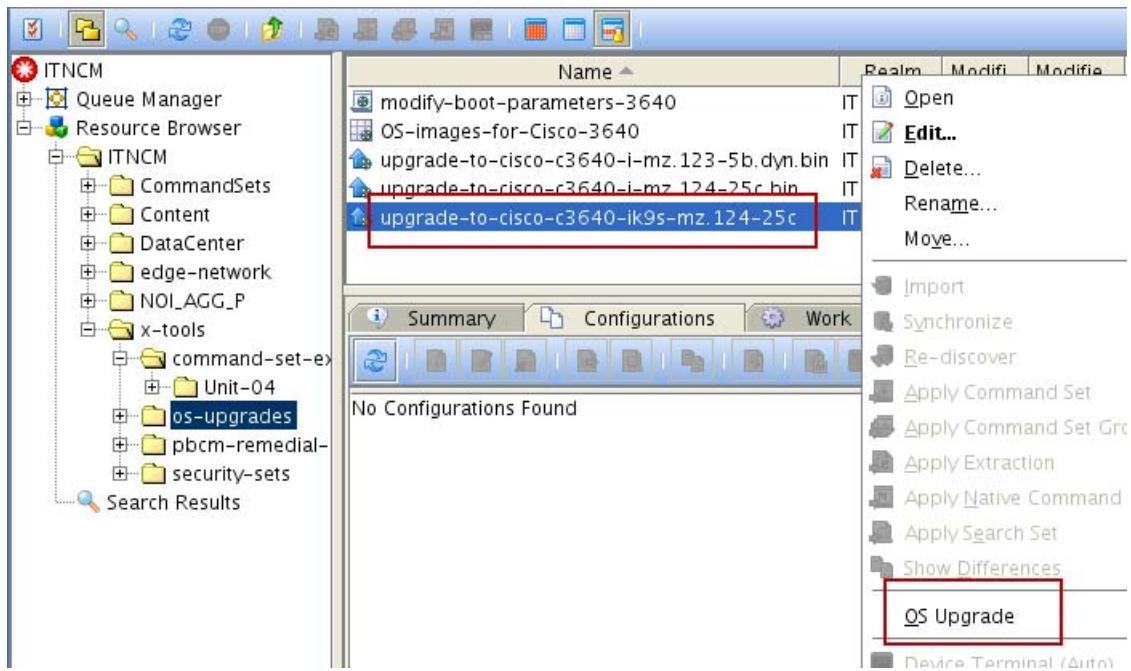
Exercise 3 Testing the network for upgrade compatibility

In this exercise, you use the operating system specification to analyze network devices. This analysis determines whether you can accomplish a successful upgrade.

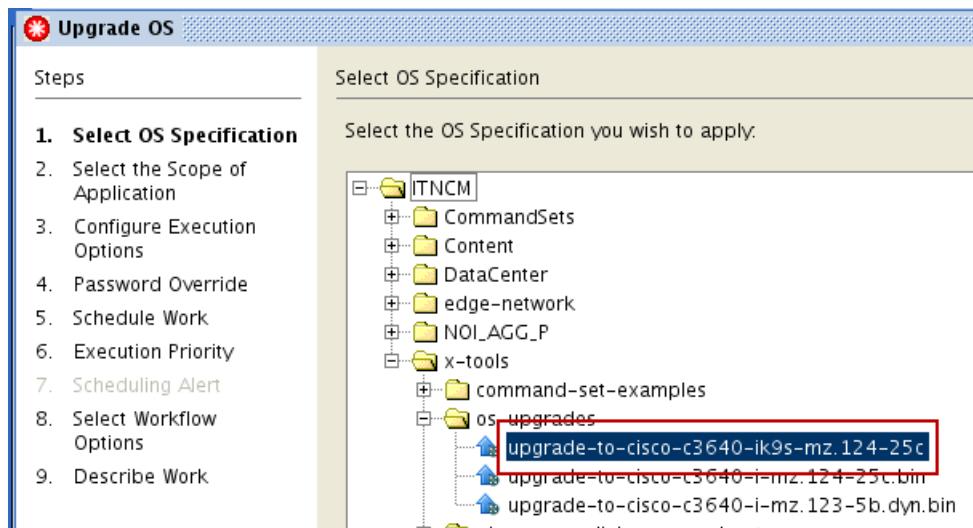
1. Use the **upgrade-to-cisco-c3640-ik9s-mz.124-25c** operating system specification to analyze the devices in the **customer_CC** realm. Apply the specification in report only mode. When you apply the specification, the Upgrade OS wizard starts. Use the following values to complete the wizard.

Field	Value
Select OS Specification	Leave upgrade-to-cisco-c3640-ik9s-mz.124-25c as the selected specification
Scope of Application	Apply the OS Specification to Network Resources in a Realm
Select the Realm	ITNCM > edge-network > customer_CC
Execution Mode	Report only mode
Password Override	Do not override
Schedule Work	Single Schedule > Immediate
Execution Priority	Medium
Workflow options	Do not synchronize device
Describe Work	upgrade test

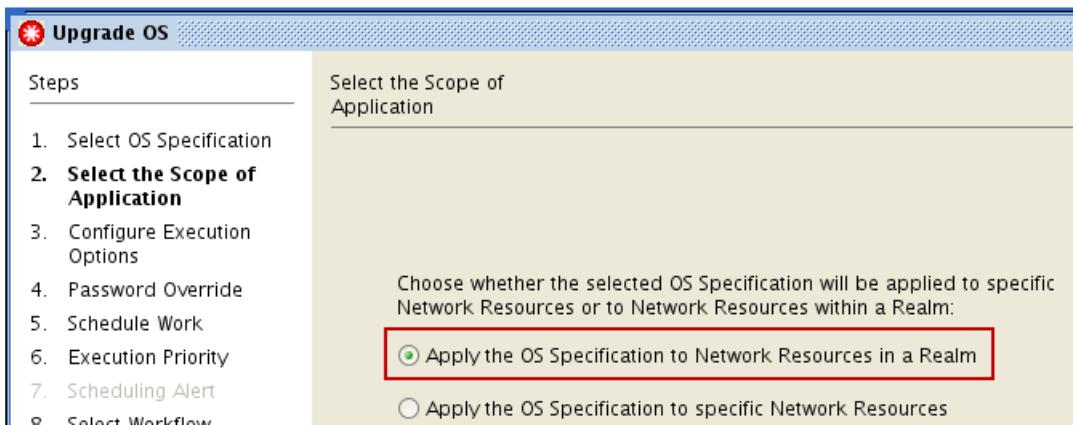
- a. Right-click the **upgrade-to-cisco-c3640-ik9s-mz.124-25c** operating system specification and click **OS Upgrade**. The Upgrade OS wizard starts.



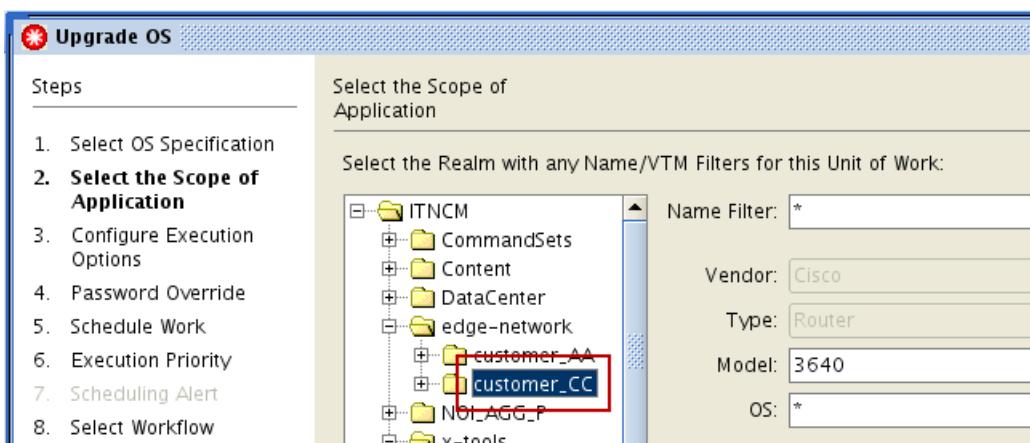
- b. Leave **upgrade-to-cisco-c3640-ik9s-mz.124-25c** as the selected specification and click **Next**.



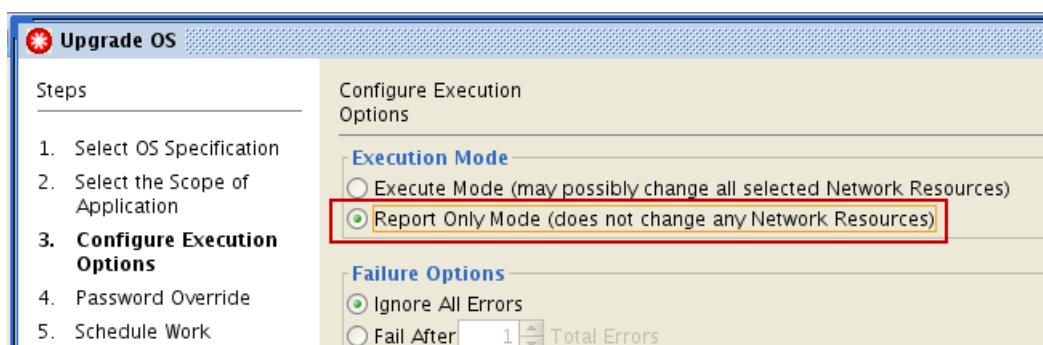
- c. Click **Apply the OS Specification to Network Resources in a Realm** and click **Next**.



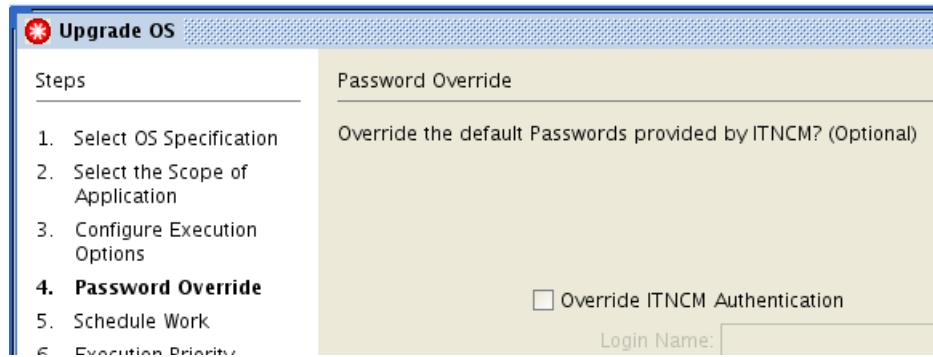
- d. Click **ITNCM > edge-network > customer_CC** and click **Next**.



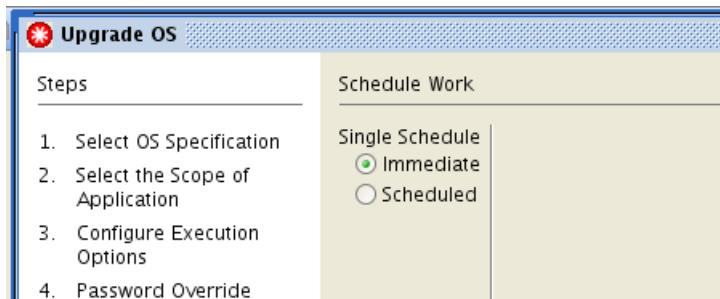
- e. Select **Report Only Mode** and click **Next**.



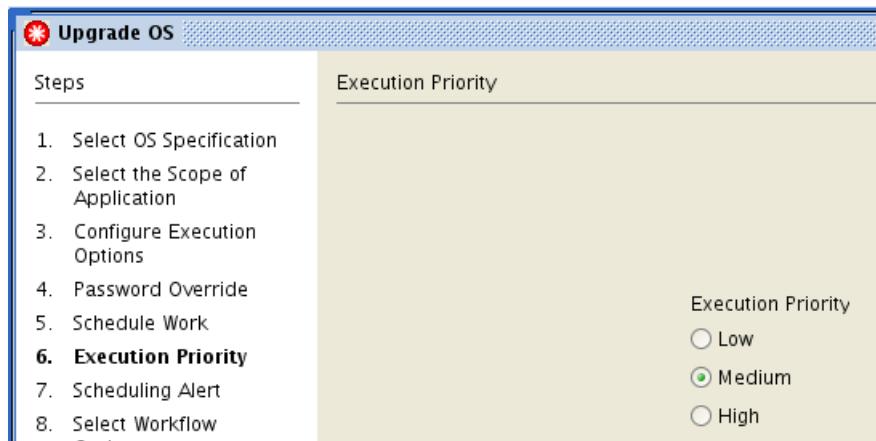
f. Click **Next** in the Password Override window.



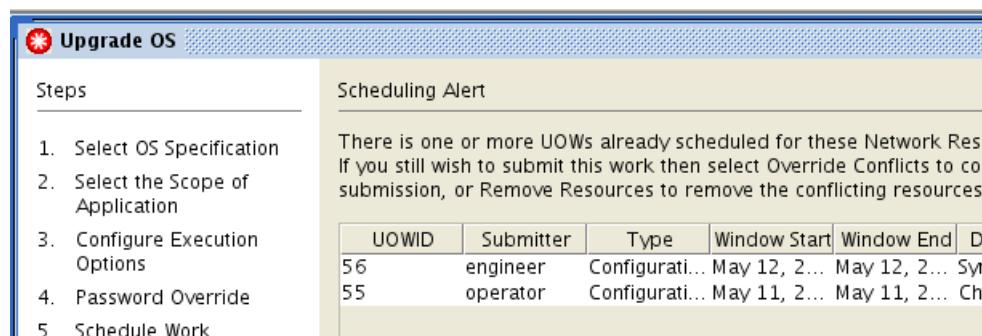
g. Click **Next**.



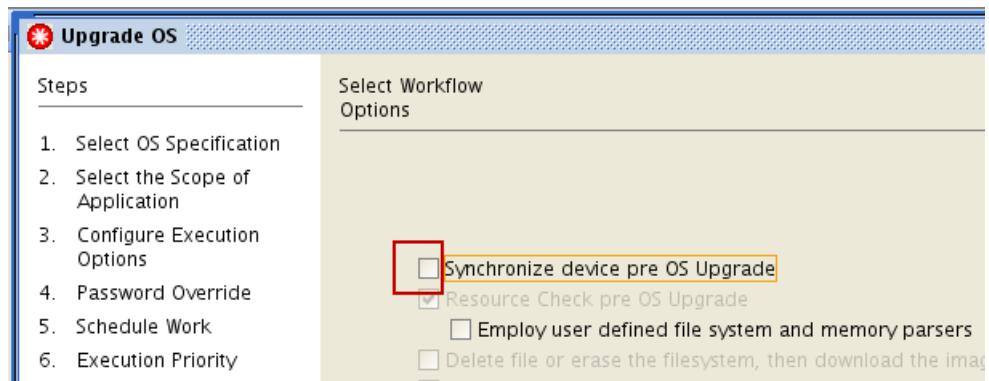
h. Click **Next**.



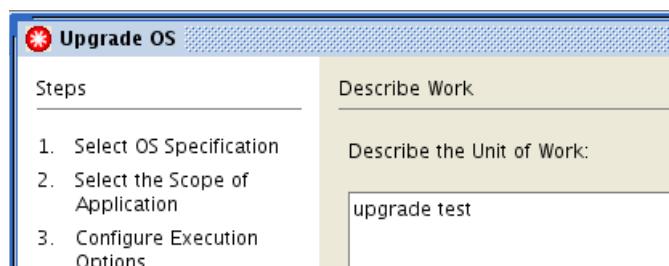
i. Click **Next** in the **Scheduling Alert** window.



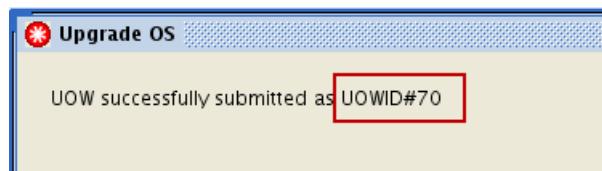
- j. Clear the **Synchronize device pre OS Upgrade** option and click **Next**.



- k. Enter **upgrade test** as the work description and click **Finish**.



- l. Note the unit of work number and click **Close**.



Exercise 4 Viewing the upgrade results

In this exercise, you view the unit of work log to see the operating system upgrade report.

1. Find the unit of work in the queue manager that applied the upgrade in read only mode. Click **Queue Manager > Work That is Finished**. The unit of work that applied the upgrade in read only mode is the most recent. It has the execution status of **FAILURE**.

The screenshot shows the IBM Tivoli Netcool Configuration Manager interface. On the left, there's a tree view under 'ITNCM' with 'Queue Manager' expanded, showing 'Pending Approval Tickets', 'All Approval Tickets', 'Work Pending Approval', 'Work Waiting to Execute', 'Work Currently Executing', and 'Work That is Finished'. The 'Work That is Finished' item is highlighted with a red box. On the right, a table lists units of work (UOW) with columns: UOW ID, Type, Submitter, Request Type, and Execution Status. Row 70 is highlighted with a red box and shows the following data:

UOW ID	Type	Submitter	Request Type	Execution Status
63	UOW	engineer	Native Command Set	FAILURE
64	UOW	engineer	Native Command Set	FAILURE
65	UOW	engineer	Native Command Set	FAILURE
66	UOW	engineer	Configuration Synchronization (...)	SUCCESS
67	UOW	engineer	Command Set (Report Only)	SUCCESS
68	UOW	engineer	Command Set (Report Only)	SUCCESS
69	UOW	engineer	Command Set	SUCCESS
70	UOW	engineer	OS Upgrade (Report Only Mode)	FAILURE

2. Look at the work log for the cc-01-router-3640 device.

- a. Click the unit of work and click the **Resources** tab.

The screenshot shows a detailed view of the work log for the cc-01-router-3640 device. A large black arrow points from the previous screenshot to this one, indicating the transition. The main table displays various units of work (UOW) with columns: UOW ID, Resources, Type, Request Type, Execution Status, and Submitter. Row 117 is selected and highlighted with a red box. Below the table is a navigation bar with 'Page Size: 100' and a page indicator '1 / 1'. At the bottom, there are tabs for 'Summary', 'Results', 'Resources' (which is highlighted with a blue box), 'Approvals', 'Schedule', and 'Details'. There are also several small icons in a row below the tabs.

- b. Click the **cc-01-router-3640** device in the **Resources** tab. Scroll down in the work log. The upgrade fails because the device does not have enough memory to perform the upgrade.

The screenshot shows the 'Results' tab selected in the top navigation bar. Below it, a table lists three devices: cc-03-router-3640, cc-02-router-3640, and cc-01-router-3640. The cc-01-router-3640 row is highlighted with a red box. To the right, a large red box highlights the work log area. The log details the upgrade process, which failed due to insufficient RAM memory on the device. The log entries are:

```
(23) Status: Upgrading source OS [tftp://255.255.255/unknown] to target os [flash:c3640-ik9s-mz.124-25c.bin].  
(24) Retrieving free memory  
(25) RAM Memory available: 36,864K  
(26) RAM Memory needed: 131,072K  
(27) Operation failed with failure category [Device Error]  
(28) [Caused by: Free RAM memory on device is less than needed memory  
(OperationFailedException)]  
(29) Task End Time: 2016/05/10 21:04:06.89  
GMT+00:00  
*****
```

The other devices fail for the same reason.

Leave the user interface as is. You return to it shortly.



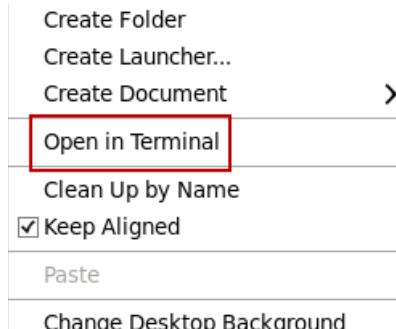
14 Out-of-band change (OOBC) daemon exercises

The exercises in this unit demonstrate how Configuration Manager identifies out-of-band device changes.

Exercise 1 Starting the out-of-band change daemon and making an out-of-band change

In this exercise, you start the out-of-band change daemon. When the daemon is running, you make an out-of-band change that generates a *unit of work*.

1. Open a terminal window. Right-click the desktop of the guest system and click **Open in Terminal**.



2. Start the out-of-band change daemon. It is in the `/opt/OutOfBandChange/run1` directory. Use the following command to start the out-of-band change daemon:

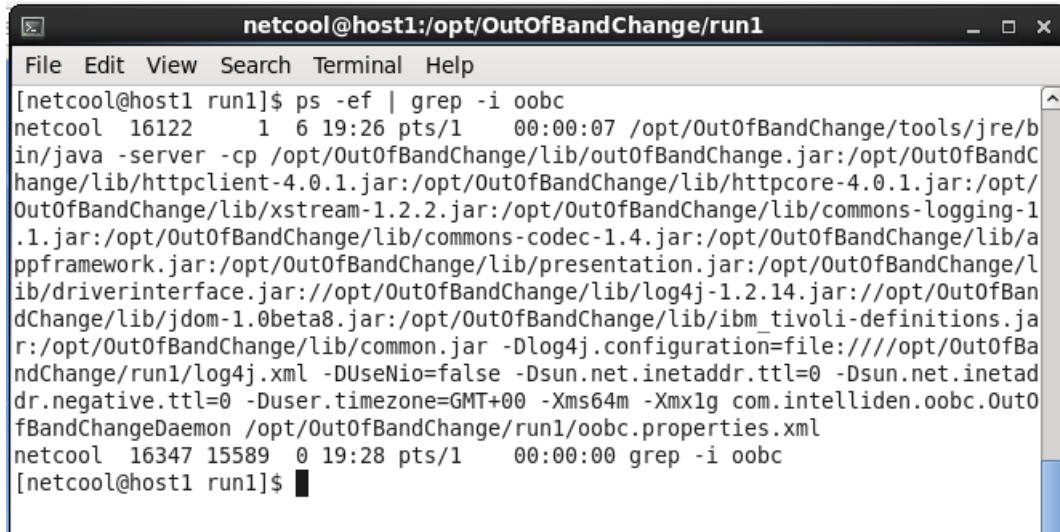
```
/opt/OutOfBandChange/run1/oobc.sh start
```

```
netcool@host1:/opt/OutOfBandChange/run1
File Edit View Search Terminal Help
[netcool@host1 run1]$ /opt/OutOfBandChange/run1/oobc.sh start
nohup: redirecting stderr to stdout
Started OOBC daemon: 16122
[netcool@host1 run1]$
```

Exercise 1 Starting the out-of-band change daemon and making an out-of-band change

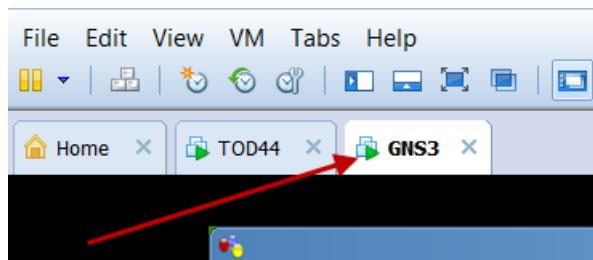
3. Confirm that the out-of-band change daemon is running. Use the following command to search for the running process of the daemon:

```
ps -ef | grep -i oobc
```

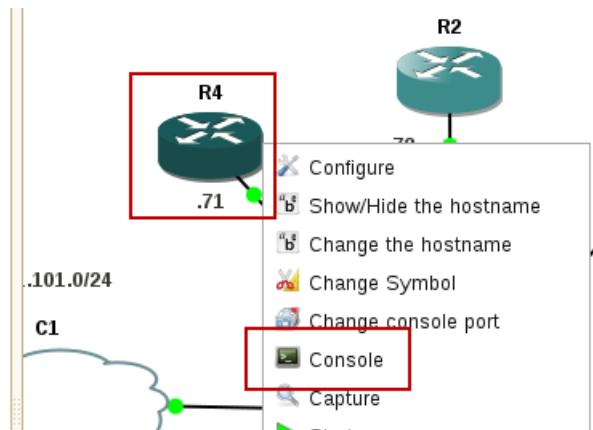


```
[netcool@host1 run1]$ ps -ef | grep -i oobc
netcool 16122 1 6 19:26 pts/1 00:00:07 /opt/OutOfBandChange/tools/jre/bin/java -server -cp /opt/OutOfBandChange/lib/outOfBandChange.jar:/opt/OutOfBandChange/lib/httpclient-4.0.1.jar:/opt/OutOfBandChange/lib/httpcore-4.0.1.jar:/opt/OutOfBandChange/lib/xstream-1.2.2.jar:/opt/OutOfBandChange/lib/commons-logging-1.1.jar:/opt/OutOfBandChange/lib/commons-codec-1.4.jar:/opt/OutOfBandChange/lib/appframework.jar:/opt/OutOfBandChange/lib/presentation.jar:/opt/OutOfBandChange/lib/driverinterface.jar://opt/OutOfBandChange/lib/log4j-1.2.14.jar://opt/OutOfBandChange/lib/jdom-1.0beta8.jar:/opt/OutOfBandChange/lib/ibm_tivoli-definitions.jar:/opt/OutOfBandChange/lib/common.jar -Dlog4j.configuration=file:///opt/OutOfBandChange/run1/log4j.xml -DUseNio=false -Dsun.net.inetaddr.ttl=0 -Dsun.net.inetaddr.negative.ttl=0 -Duser.timezone=GMT+00 -Xms64m -Xmx1g com.intelliden.oobc.OutOfBandChangeDaemon /opt/OutOfBandChange/run1/oobc.properties.xml
netcool 16347 15589 0 19:28 pts/1 00:00:00 grep -i oobc
[netcool@host1 run1]$
```

4. Click the GNS3 VMware image tab that is running the simulated network. The VMware image is named **GNS3**.



5. In the network simulator, right-click the device that is labeled **R4** and click **Console**. This action accesses the router with the console port. The changes that you make with the console port are considered out-of-band changes.



6. Press Enter in the console. Type **enable**. You are prompted for a password. The password is **3n4bl3**.

```
Dynamips(0): R4, Console port
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
Connected to Dynamips VM "R4" (ID 0, type c3600) - Console port
Press ENTER to get the prompt.

cc-01-router-3640>enable
Password:
cc-01-router-3640#
```

7. Enter the following four commands. Close the console window when you finish.

```
# config t
# service nagle
# exit
# exit
```

```
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
Connected to Dynamips VM "R4" (ID 0, type c3600) - Console port
Press ENTER to get the prompt.

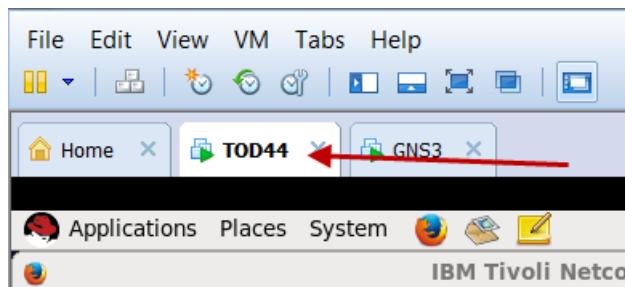
cc-01-router-3640>enable
Password:
cc-01-router-3640#config t
Enter configuration commands, one per line. End with CNTL/Z.
cc-01-router-3640(config)#service nagle
cc-01-router-3640(config)#exit
cc-01-router-3640#exit
```

8. Close the console window.

Exercise 2 Verifying the device synchronization

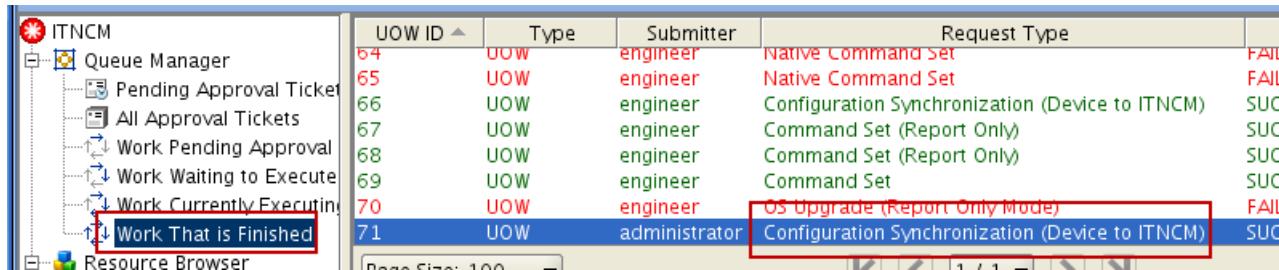
In this exercise, you look at the unit of work and out-of-band change daemon log files to verify that the change was synchronized.

1. Click the **TOD44** VMware image tab that is running Netcool Configuration Manager.



Exercise 2 Verifying the device synchronization

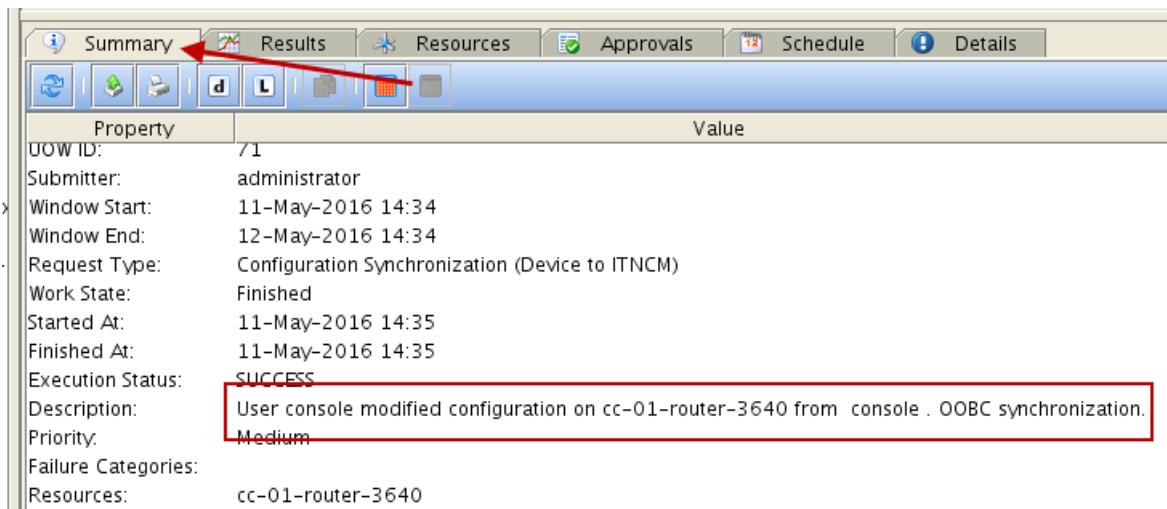
2. Look in the *queue manager* for the unit of work that was submitted for the change made to **cc-01-router-3640** through the console port. Find the configuration synchronization in the work log. The unit of work has the request type **Configuration Synchronization**.
- Click **Queue Manager**. Find the recent unit of work that synchronized the configuration from the **cc-01-router-3640** device to Netcool Configuration Manager.



The screenshot shows the ITNCM Queue Manager interface. On the left, there's a tree view with nodes like Queue Manager, Pending Approval Tickets, All Approval Tickets, Work Pending Approval, Work Waiting to Execute, Work Currently Executing, and Work That is Finished. The Work That is Finished node is selected and highlighted with a red box. On the right, a table lists various units of work (UOWs) with columns: UOW ID, Type, Submitter, Request Type, and Status. The last row, UOW ID 71, is highlighted with a red box. Its details are as follows:

UOW ID	Type	Submitter	Request Type	Status
64	UOW	engineer	Native Command Set	FAIL
65	UOW	engineer	Native Command Set	FAIL
66	UOW	engineer	Configuration Synchronization (Device to ITNCM)	SUC
67	UOW	engineer	Command Set (Report Only)	SUC
68	UOW	engineer	Command Set (Report Only)	SUC
69	UOW	engineer	Command Set	SUC
70	UOW	engineer	OS Upgrade (Report Only Mode)	FAIL
71	UOW	administrator	Configuration Synchronization (Device to ITNCM)	SUC

- Click the **Summary** tab in the *unit of work*. Notice that the description mentions **OOBC synchronization**.

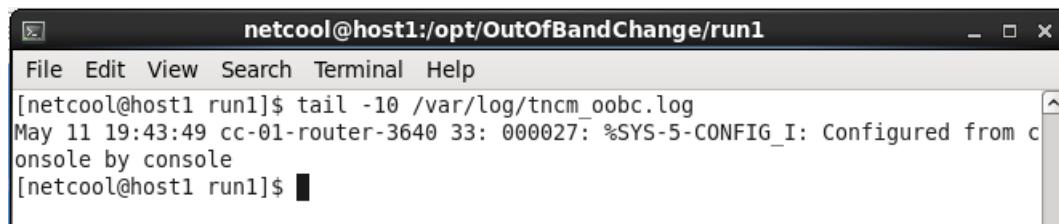


The screenshot shows the Unit of Work summary details. At the top, there's a toolbar with tabs: Summary (highlighted with a red arrow), Results, Resources, Approvals, Schedule, and Details. Below the toolbar is a table with properties and their values. The Description field contains the text "User console modified configuration on cc-01-router-3640 from console . OOBC synchronization.", which is highlighted with a red box.

Property	Value
UOW ID:	71
Submitter:	administrator
Window Start:	11-May-2016 14:34
Window End:	12-May-2016 14:34
Request Type:	Configuration Synchronization (Device to ITNCM)
Work State:	Finished
Started At:	11-May-2016 14:35
Finished At:	11-May-2016 14:35
Execution Status:	SUCCESS
Description:	User console modified configuration on cc-01-router-3640 from console . OOBC synchronization.
Priority:	Medium
Failure Categories:	
Resources:	cc-01-router-3640

3. Use the following command to read the last 10 lines of the **/var/log/tncm_oobc** file. You see events that relate to the configuration of the cc-01-router-3640 device through the console port.

```
tail -10 /var/log/tncm_oobc.log
```

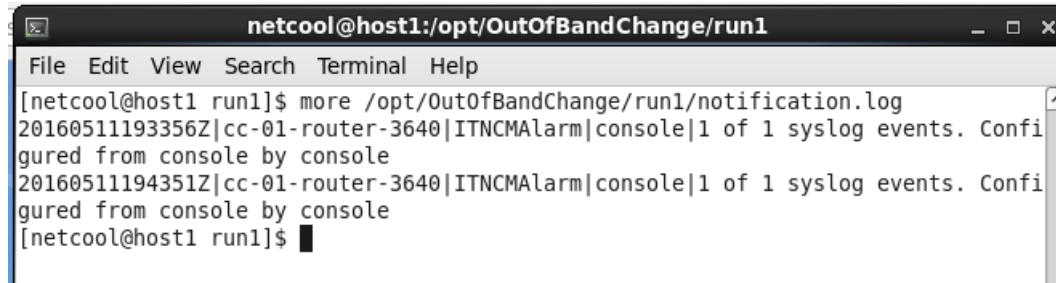


The screenshot shows a terminal window titled "netcool@host1:/opt/OutOfBandChange/run1". The window displays the output of the command "tail -10 /var/log/tncm_oobc.log". The output shows a log entry from May 11 at 19:43:49, indicating a configuration update from the console for the cc-01-router-3640 device.

```
[netcool@host1 run1]$ tail -10 /var/log/tncm_oobc.log
May 11 19:43:49 cc-01-router-3640 33: 000027: %SYS-5-CONFIG_I: Configured from c
onsole by console
[netcool@host1 run1]$
```

4. Use the following command to read the **/opt/OutOfBandChange/run1/notification.log** file.
You see events that relate to the synchronization of the device.

```
more /opt/OutOfBandChange/run1/notification.log
```

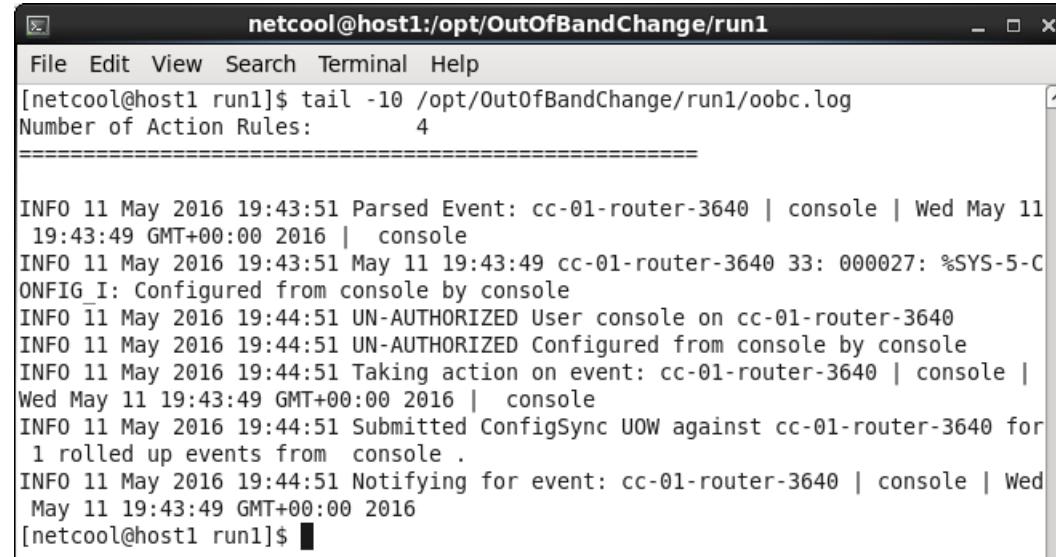


The terminal window title is "netcool@host1:/opt/OutOfBandChange/run1". The command entered is "more /opt/OutOfBandChange/run1/notification.log". The output shows two entries from May 11, 2016, at 19:43:56Z, both indicating ITNCMAalarm events on cc-01-router-3640, configured from console. The window has standard Linux terminal icons (minimize, maximize, close).

```
[netcool@host1 run1]$ more /opt/OutOfBandChange/run1/notification.log
20160511193356Z|cc-01-router-3640|ITNCMAalarm|console|1 of 1 syslog events. Configured from console by console
20160511194351Z|cc-01-router-3640|ITNCMAalarm|console|1 of 1 syslog events. Configured from console by console
[netcool@host1 run1]$
```

5. Use the following command to read the **/opt/OutOfBandChange/run1/oobc.log** file. You see events that relate to the operation of the out-of-band change daemon.

```
tail -10 /opt/OutOfBandChange/run1/oobc.log
```



The terminal window title is "netcool@host1:/opt/OutOfBandChange/run1". The command entered is "tail -10 /opt/OutOfBandChange/run1/oobc.log". The output shows several log entries related to configuration sync and user actions on cc-01-router-3640. The window has standard Linux terminal icons (minimize, maximize, close).

```
[netcool@host1 run1]$ tail -10 /opt/OutOfBandChange/run1/oobc.log
Number of Action Rules: 4
=====
INFO 11 May 2016 19:43:51 Parsed Event: cc-01-router-3640 | console | Wed May 11 19:43:49 GMT+00:00 2016 | console
INFO 11 May 2016 19:43:51 May 11 19:43:49 cc-01-router-3640 33: 000027: %SYS-5-C
ONFIG_I: Configured from console by console
INFO 11 May 2016 19:44:51 UN-AUTHORIZED User console on cc-01-router-3640
INFO 11 May 2016 19:44:51 UN-AUTHORIZED Configured from console by console
INFO 11 May 2016 19:44:51 Taking action on event: cc-01-router-3640 | console |
Wed May 11 19:43:49 GMT+00:00 2016 | console
INFO 11 May 2016 19:44:51 Submitted ConfigSync UOW against cc-01-router-3640 for 1 rolled up events from console .
INFO 11 May 2016 19:44:51 Notifying for event: cc-01-router-3640 | console | Wed May 11 19:43:49 GMT+00:00 2016
[netcool@host1 run1]$
```

Leave the configuration manager client as is. You return to it shortly.

Leave the browser session as is. You return to it shortly.





15 Compliance manager interface exercises

The exercise in this unit introduce you to the compliance manager user interface.

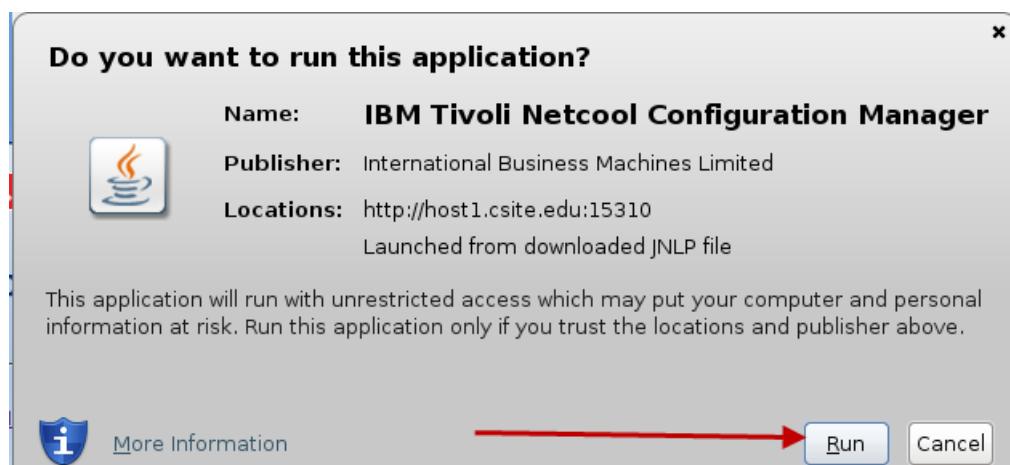
Exercise 1 Viewing devices, policies, and parameters

In this exercise, you verify that the devices you discovered are present in the compliance user interface and you view policies that are already present.

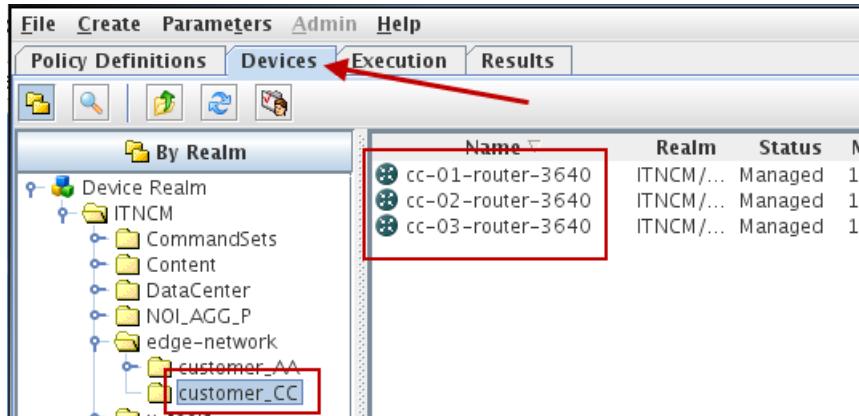
1. Start the *compliance manager* user interface as the **engineer** user.
 - a. Click **ITNCM Compliance**.



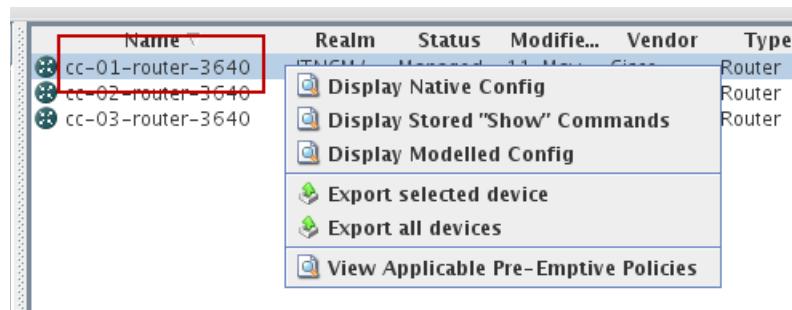
- b. Click **Run**.



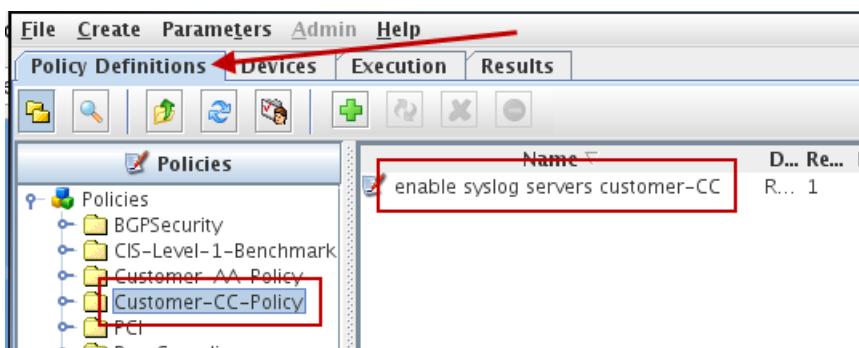
2. Use the **Devices** tab to verify that the three lab routers are present in the compliance user interface.
 - a. Click the **Devices** tab. Expand the **ITNCM > edge-network > customer_CC** subrealm. The three routers are present.



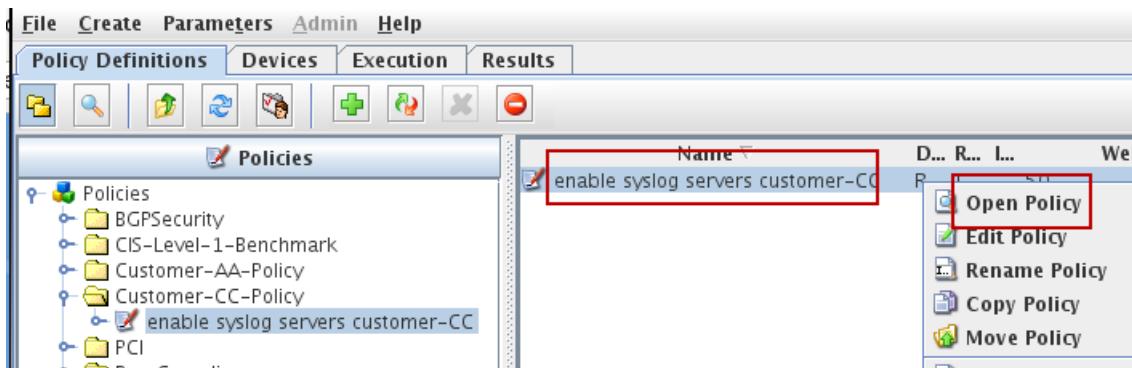
- b. Right-click one of the routers. You can view configuration data in the native configuration, in saved show commands, and in the modeled configuration.



3. Look in the **Customer-CC-Policy** realm in the **Policy Definitions** tab. One policy is listed in the realm.
 - a. Click the **Policy Definitions** tab. Click the **Policies** section. Expand the **Customer-CC-Policy** realm. The policy is named **enable syslog servers customer-CC**.



- b. Right-click the **enable syslog servers customer-CC** policy and click **Open Policy**.



The first window in the wizard shows that **Send Trap** is enabled and the associated rule is named **enable syslog servers customer-CC**.

- c. Click **Next**.

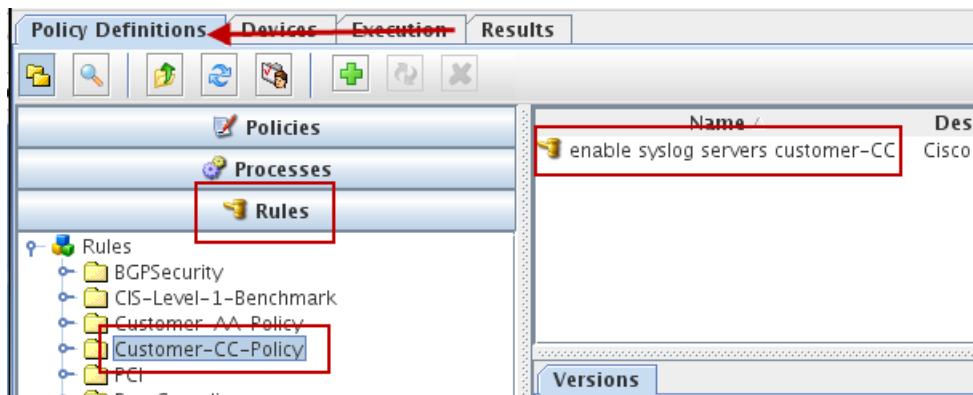
Vendor	Type	Model	OS
*	*	*	*

The next window in the wizard shows that it sends no email if this policy is violated.

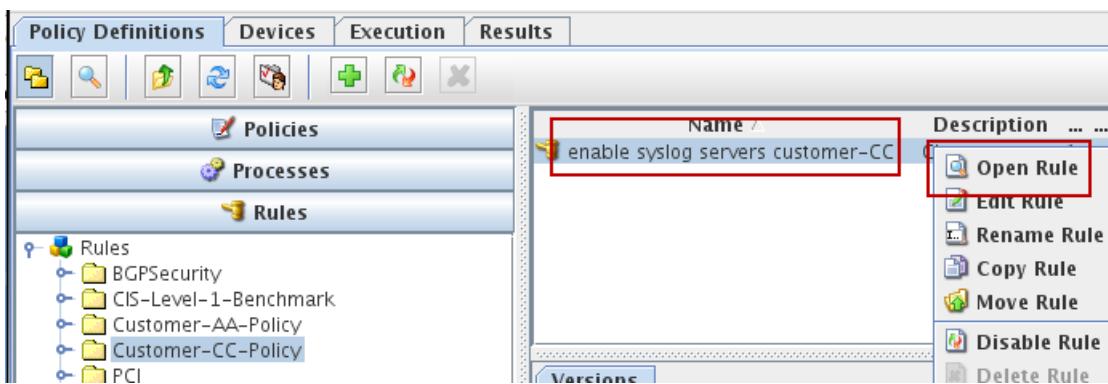
- d. Click **Cancel**.

4. Examine the rule.

- Click the **Policy Definitions** tab. Click the **Rules** section. Expand the **Customer-CC-Policy** realm. The rule is named **enable syslog servers customer-CC**.



- Right-click the **enable syslog servers customer-CC** rule and click **Open Rule**.



The first window in the wizard shows that the rule applies to all Cisco devices.

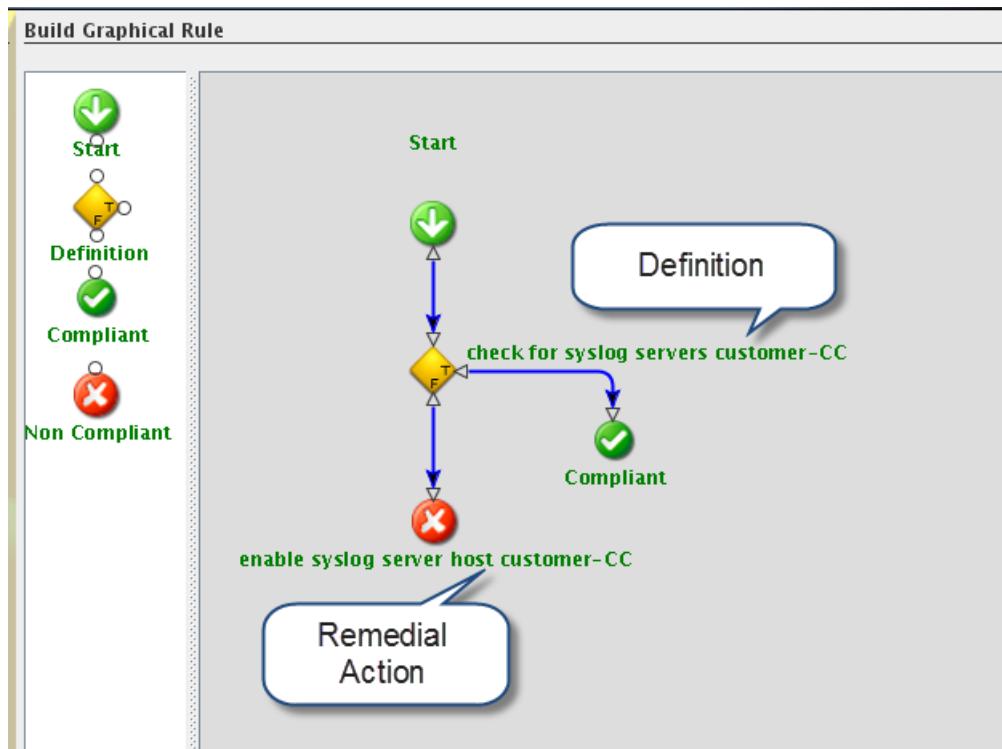
- Click **Next**.

This is a screenshot of a configuration wizard window titled 'Enter Rule Details...'. It has several sections:

- Rule Name & Description**: Contains fields for 'Name' (set to 'enable syslog servers customer-CC') and 'Revision' (set to '1').
- Description**: A text area containing the description: 'service simply accepts messages; and stores them in files or prints them according to a simple configuration file. This form of logging is the best available for Cisco routers; because it can provide'.
- Applicable Device Filter**: A table with columns 'Vendor', 'Type', 'Model', and 'OS'. A red box highlights the entire table. The data in the table is:

Vendor	Type	Model	OS
cisco	*	*	Advanced

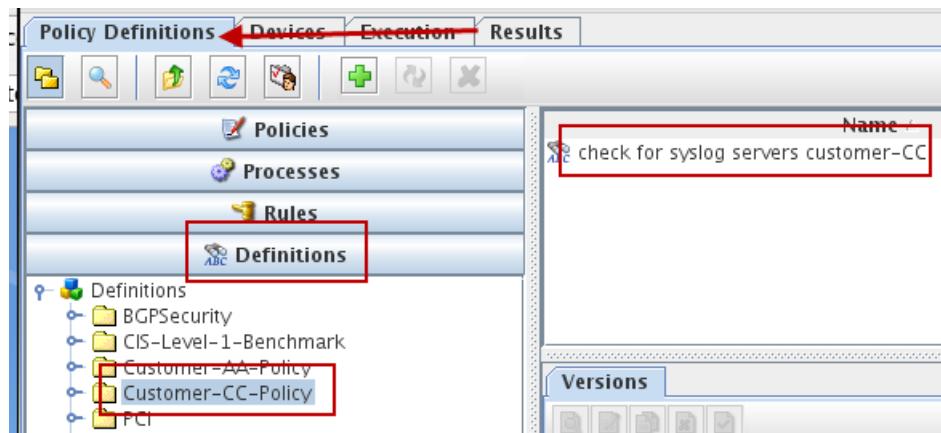
- d. Click **Cancel**.



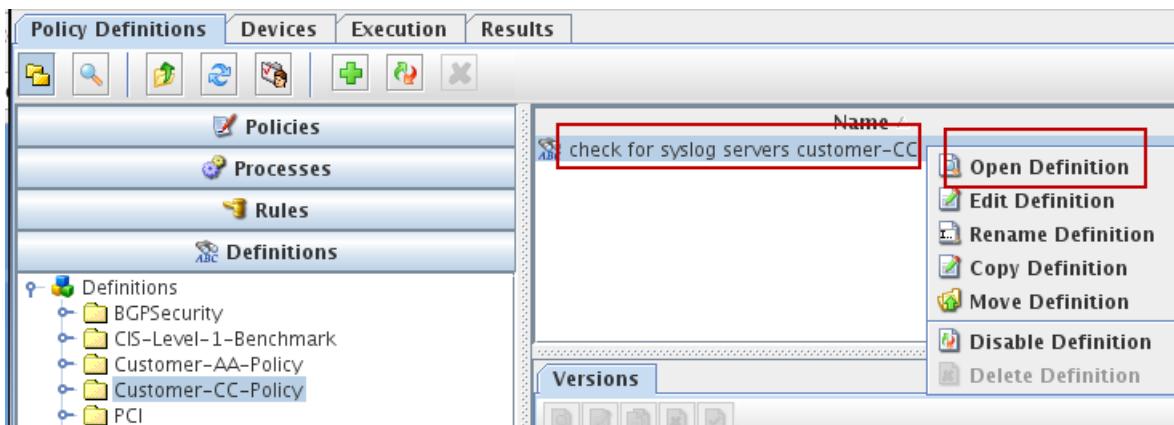
The definition is named **check for syslog servers customer-CC**, and the remedial action is called **enable syslog server host customer-CC**.

5. Examine the definition.

- a. Click the **Policy Definitions** tab. Click the **Definitions** section. Expand the **Customer-CC-Policy** realm. The definition is named **check for syslog servers customer-CC**.



- b. Right-click the **check for syslog servers customer-CC** definition and click **Open Definition**.



- c. Click **Next**.

Enter Definition Details

Definition Name & Description

Name: check for syslog servers customer-CC

Description: ^logging \$Global[SYSLOG_SERVER_HOST_GLOBAL_CC]
SYSLOG_HOST is a global parameter of the syslog IP address.
the IP must be found in the configuration for the definition to return "TRUE"

- d. Click **Cancel**.

Match Criteria: Match All Number: _____

Evaluation result if context not found: Fail

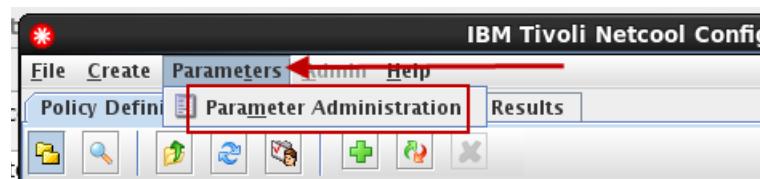
Evaluation List:

Evaluation
^logging \$Global[SYSLOG_SERVER_HOST_GLOBAL_CC]

The definition checks for the existence of the term **logging** followed by the value of the **SYSLOG_SERVER_HOST_GLOBAL_CC** global parameter.

6. Examine the parameter.

- a. Click **Parameters** and select **Parameter Administration**.



The list of available parameters opens.

- b. Scroll down and click **SYSLOG_SRVER_HOST_GLOBAL_CC**. Click **Edit**.

Parameter Administration		
Global Parameters	Parameter Groups	Script Parameters
Parameter	Description	Value
PCI_SYSLOGLevel	Level of detail logged	informational
PCI_TACACS_SERVER	TACACS+ server IP	172.25.0.99
SYSLOG_SERVER_HOST_GLOBAL_AA	the ip address of the syslog server that... <i>(This row is highlighted with a red box)</i>	10.191.101.52
SYSLOG_SERVER_HOST_GLOBAL_CC	the ip address of the syslog server that... <i>(This row is highlighted with a red box)</i>	192.168.12.101
Top10_LoginTimeout	Timeout for login to Console or VTY.	14000
Top10-SYSLOGInt	SYSLOG interface	Loopback0
Top10_SYSLOGLevel	Level of syslog detail	informational

The current value is 192.168.12.101. Modify this value.

- c. Change the value to **192.168.100.100**. Click **Apply**.

Edit Parameter Definition

Enter Parameter Definition

Parameter:	SYSLOG_SERVER_HOST_GLOBAL_CC
Description:	the ip address of the syslog server that is used by Customer CC
Value:	192.168.100.100
Realm:	Customer-CC-Policy

Cancel **Apply**

- d. Verify the updated value. Click **Cancel**.

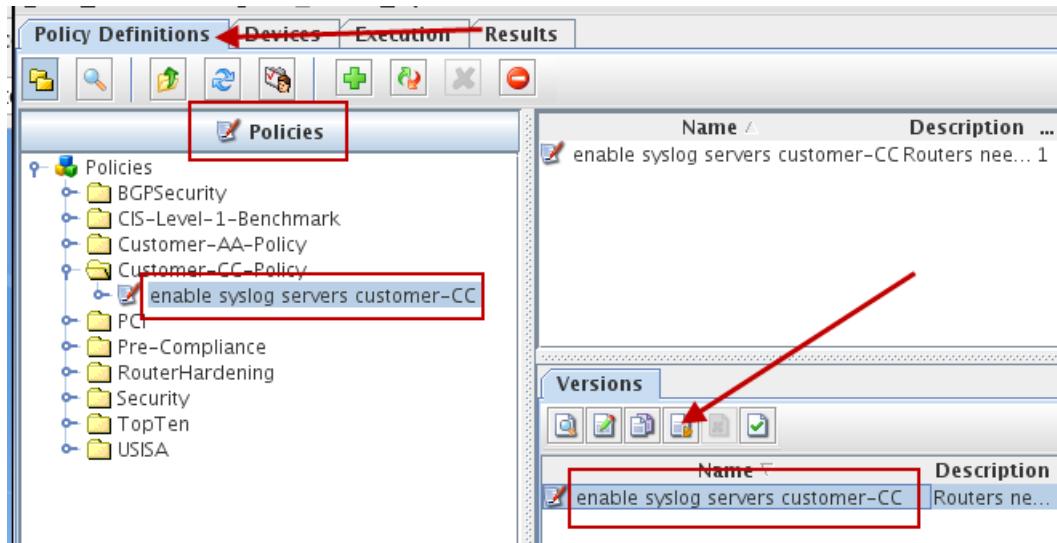
Parameter Administration		
Global Parameters	Parameter Groups	Script Parameters
Parameter	Description	Value
PCI_SYSLOGLevel	Level of detail logged	informational
PCI_TACACS_SERVER	TACACS+ server IP	172.25.0.99
SYSLOG_SERVER_HOST_GLOBAL_AA	the ip address of the syslog server that... <i>(This row is highlighted with a red box)</i>	10.191.101.52
SYSLOG_SERVER_HOST_GLOBAL_CC	the ip address of the syslog server that... <i>(This row is highlighted with a red box)</i>	192.168.100.100
Top10_LoginTimeout	Timeout for login to Console or VTY.	14000

7. Test the **enable syslog servers customer-CC** policy. Use the values in the following table to complete the test wizard. When you finish, view the details of the test results.

Field	Value
Description	Policy test

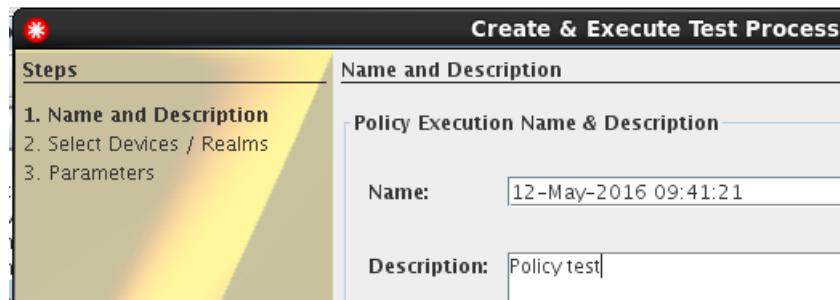
Field	Value
Realms	Use the ITNCM > edge-network > customer_CC subrealm
Parameter value	View the parameter and use the default value

- a. Click the **enable syslog servers customer-CC** policy. Click the **enable syslog servers customer-CC** policy in the **Versions** section. Click the **Test Policy** icon.

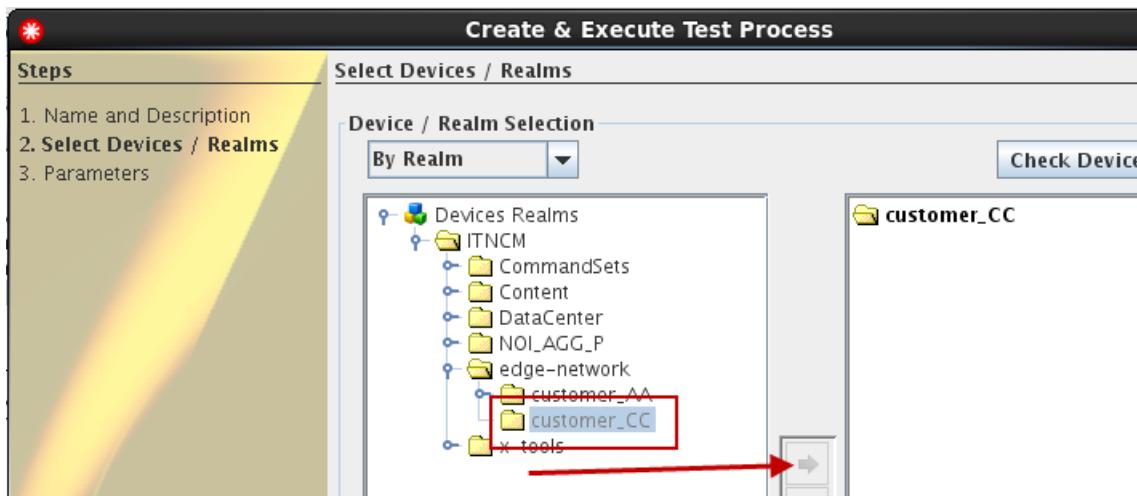


The test wizard starts.

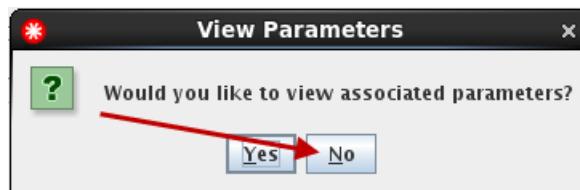
- b. Enter **Policy test** in the description field and click **Next**.



- c. Click the **ITNCM > edge-network > customer_CC** realm and click the right arrow icon to include it in the test. Click **Next**.



- d. Click **No** to view the associated parameters. You already examined the parameter.



- e. Click **Finish**.

- f. After you complete the test wizard, you see the **Results** tab.

Name	State	Executed By	Devices	Process Type
Test_12-May-...	Queued	engineer	?	Compliance

- g. Click the refresh icon until the state is **Finished**. After the test finishes, click the policy at the top of the window.

The screenshot shows the 'Results' tab selected in the navigation bar. In the 'Process Execution Summary' section, a row for 'Test_12-May...' is highlighted with a red box around its 'Name' column, which shows 'Finished'. In the 'Policy Validation Summary' section, a table shows one row with 'Passed' in the first column and 'Failed' in the second column, both highlighted with red boxes.

Policy Name	Severity	Revision	Date	Passed	Failed
enable syslog ... 3	1	12-May-2016 13...	1	1	2

The results show one device passes and two devices fail.

- h. Click the results at the bottom of the window and click **Details**. All of the devices in the test failed compliance for this policy.
- i. Click the results at the bottom of the window and click **Details**.

The screenshot shows a summary table with columns: Date, Passed, Failed, Not Assessed, and Exempt. The 'Passed' column is highlighted with a red box. Below the table is a large red arrow pointing from the table to a 'Details' button.

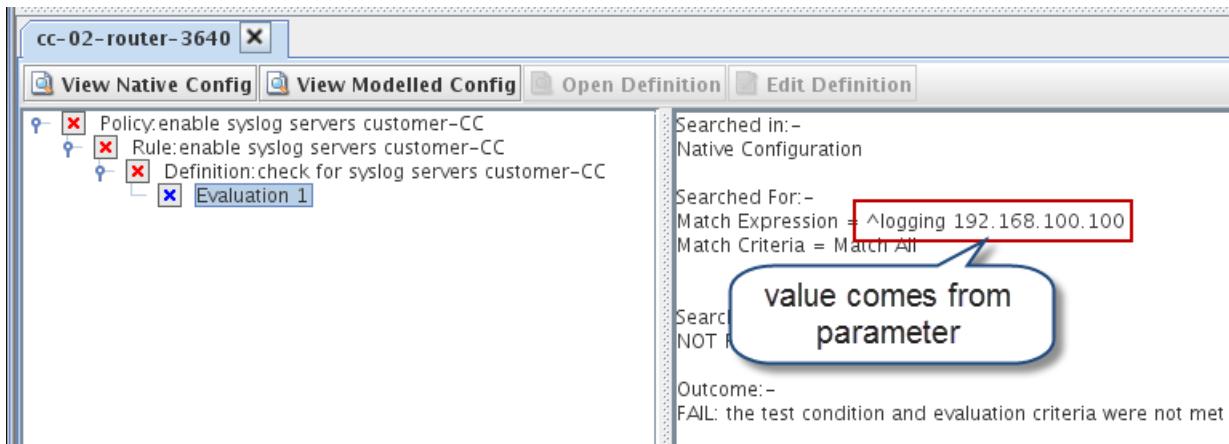
Date	Passed	Failed	Not Assessed	Exempt
12-May-2016 13... 1	2	0	0	0

- j. Double-click **cc-02-router-3640**.

The screenshot shows a table with columns: Device, Device Realm, Support Level, Date, and Comp. The second row, containing 'cc-02-router-3640', is highlighted with a red box. The status 'FAIL' is highlighted with a green box in the 'Comp' column of this row.

	Device	Device Realm	Support Level	Date	Comp
ervers c... cc-01-router-3640	ITNCM/edge-network/cus...	SmartModel	12-May-2016 13:30:45	PASS	
ervers c... cc-02-router-3640	ITNCM/edge-network/cus...	SmartModel	12-May-2016 13:30:45	FAIL	
ervers c... cc-03-router-3640	ITNCM/edge-network/cus...	SmartModel	12-May-2016 13:30:45	FAIL	

- k. View the detailed results.

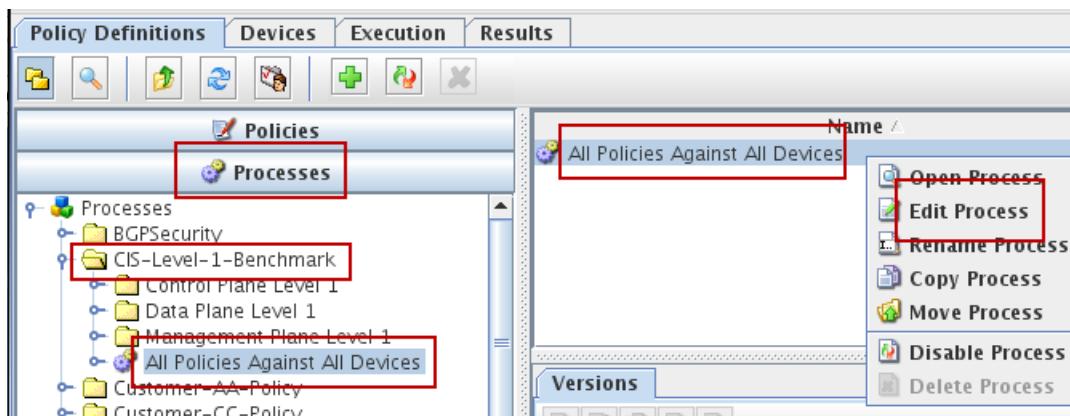


The evaluation uses the default value from the **SYSLOG_SRVER_HOST_GLOBAL_CC** parameter to test for the correct **logging** statement. The test fails on cc-02-router-3640.

Exercise 2 Working with processes

In this exercise, you view and run a process. You look at the results of the policies that the process runs and view the remedial queue that it creates. You use the **enable logging trap level** policy as an example of the relationship between policy results and remedial actions.

1. Look in the **CIS-Level-1-Benchmark** subrealm in the **Policy Definitions** tab. The subrealm contains one process. Add the customer CC devices to the process.
 - a. Click the **Processes** section. Expand the **CIS-Level-1-Benchmark** realm. The process is named **All Policies Against All Devices**. Right-click the process and click **Edit Process**.



- b. After the process wizard starts, you see all of the policies associated with this process. This process runs 12 policies. The **enable logging trap level** policy is included in this process. Click **Next**.

Process Name & Description

Name: All Policies Against All Devices * Revision: 1

Description:

Enable process for automatic validations

Policy Selection

Policies

- BGPSecurity
- CIS-Level-1-Benchmark
- Customer-AA-Policy
- Customer-CC-Policy
- PCI
- Pre-Compliance
- RouterHardening
- Security
- TopTen
- USISA

3.1.03 enable local authentication
3.1.04 enable only one local user
3.1.08 disable SNMP community read-write
3.1.09 and 10 disable SNMP community public an...
3.1.18 enable VTY exec timeout on lines
3.1.38 disable ip http server
3.1.39 enable service password-encryption
3.1.54 enable logging
3.1.55 enable syslog servers
3.1.59-2 disable logging console
3.1.60 enable logging trap level
3.1.73 and 74 disable directed broadcast

- c. Click **Next**.

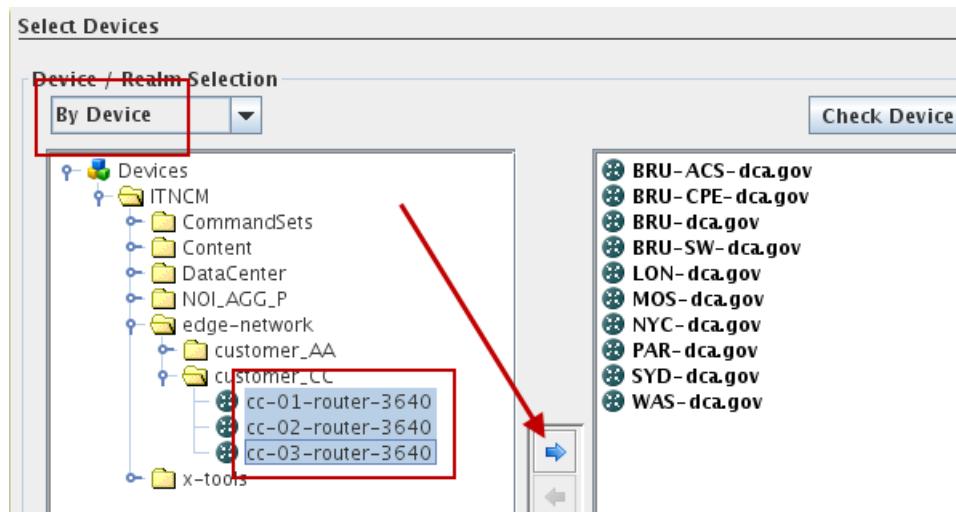
Pre-Emptive Options

Enable Pre-Emptive Compliance Options for this Process (SmartModel Policies Only)

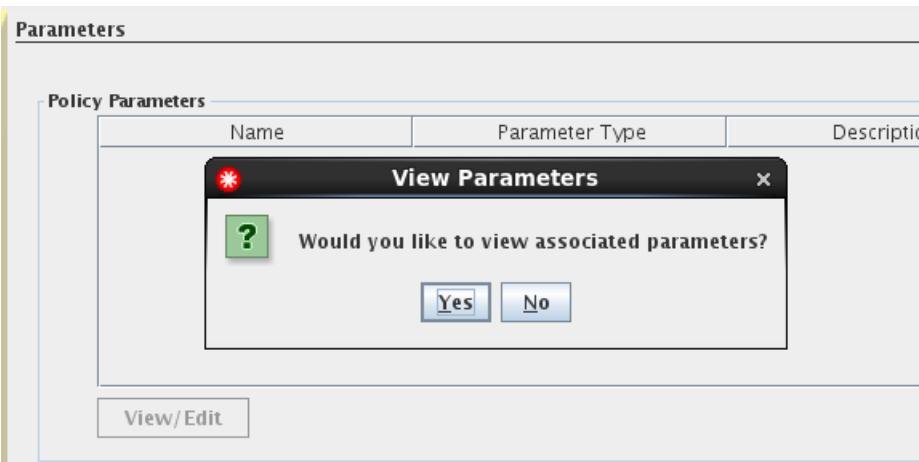
Select Pre-Emptive Policies

Policy Name	Enable
3.1.03 enable local authentication	<input type="checkbox"/>
3.1.04 enable only one local user	<input type="checkbox"/>
3.1.08 disable SNMP community read-write	<input type="checkbox"/>
3.1.09 and 10 disable SNMP community public an...	<input type="checkbox"/>
3.1.18 enable VTY exec timeout on lines	<input type="checkbox"/>
3.1.38 disable ip http server	<input type="checkbox"/>
3.1.39 enable service password-encryption	<input type="checkbox"/>
3.1.54 enable logging	<input type="checkbox"/>
3.1.55 enable syslog servers	<input type="checkbox"/>
3.1.59-2 disable logging console	<input type="checkbox"/>
3.1.60 enable logging trap level	<input type="checkbox"/>
3.1.73 and 74 disable directed broadcast	<input type="checkbox"/>

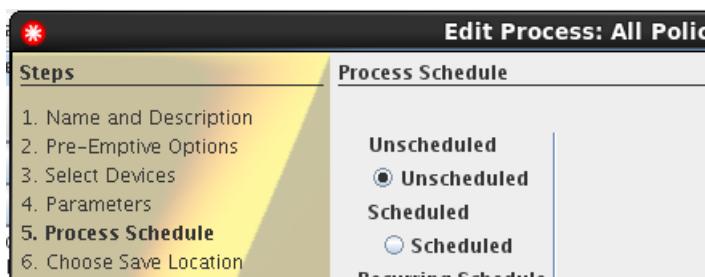
- d. Add all of the devices in the **customer_CC** realm to the process. Click **Next**.



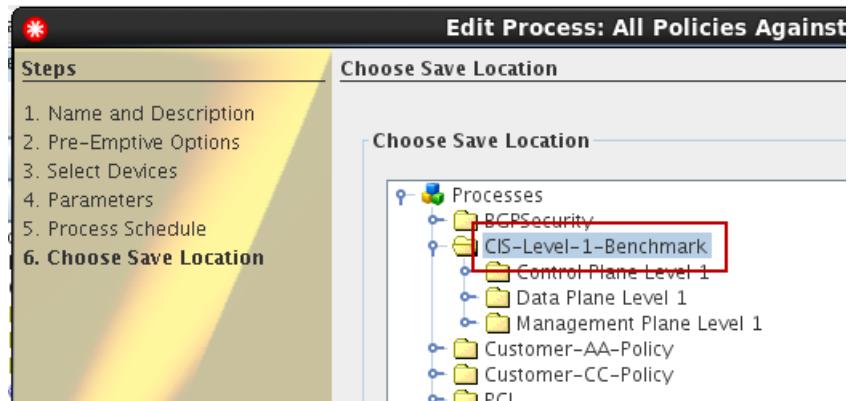
- e. Click **No** when you are prompted to view parameters. Click **Next**.



- f. Click **Next**.

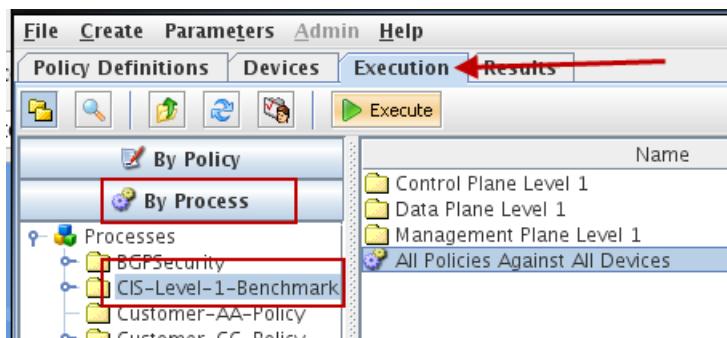


g. Click **Finish**.

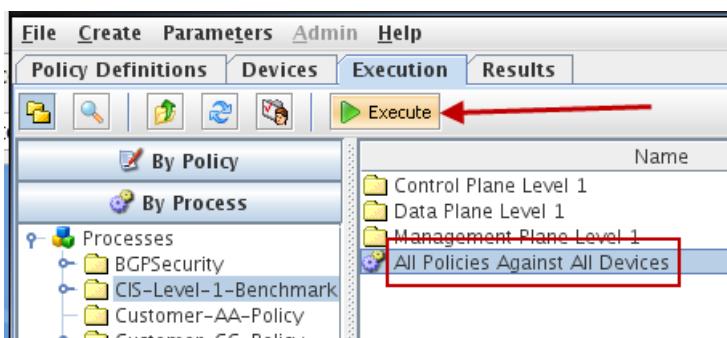


2. Run the **All Policies Against All Devices** process.

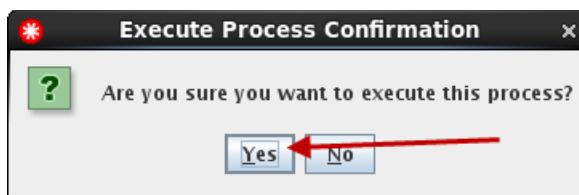
a. Click the **Execution** tab. Click the **By Process** section. Click the **CIS-Level-1-Benchmark** folder.



b. Select the **All Policies Against All Devices** process and click **Execute**.

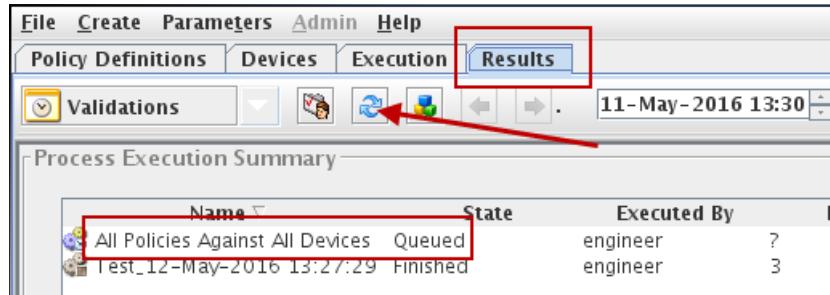


c. Click **Yes** to confirm.



The **Results** tab opens.

3. Click the refresh icon until the process is finished.



4. Click the **All Policies Against All Devices** process in the **Process Execution Summary** area.

Scroll through the results of the process in the **Process Validation Summary** area and view the policies that pass and fail.

The screenshot shows the 'Process Validation Summary' table. It highlights the first row, 'All Policies Against All Devices', which is marked as 'Finished'. This row is also highlighted in the 'Process Execution Summary' table above it. The table has columns for Name, State, Executed By, Devices, Process Type, and Execution. Below the table are navigation buttons for Show All, Page Size (50), and a search/filter button labeled 'Finished:'. The 'Policy Validation Summary' section below shows a detailed list of policies with their names, severity levels, revision numbers, dates, and counts of passed and failed tests. The 'Passed' and 'Failed' columns for the first row are also highlighted with a red box.

Policy Name	Severity	Revision	Date	Passed	Failed
3.1.03 enable local authentication	1	1	12-May-2016	0	13
3.1.04 enable only one local user	1	1	12-May-2016	11	2
3.1.08 disable SNMP community read-write	1	1	12-May-2016	7	6
3.1.09 and 10 disable SNMP community public and priv... 3.1.18 enable VTY exec timeout on lines	1	1	12-May-2016	2	11
3.1.38 disable ip http server	2	1	12-May-2016	0	13
3.1.39 enable service password-encryption	1	1	12-May-2016	9	4
3.1.54 enable logging	2	1	12-May-2016	1	12
3.1.55 enable syslog servers	3	1	12-May-2016	13	0
3.1.59-2 disable logging console	4	1	12-May-2016	0	13
3.1.60 enable logging trap level	4	1	12-May-2016	0	13
3.1.73 and 74 disable directed broadcast	2	1	12-May-2016	11	2

5. View the details of the policy named **3.1.60 enable logging trap level**. Check the compliance status of the three devices that you discovered previously in this exercise.
- Click the policy named **3.1.60 enable logging trap level**. Click **Details**.

Policy Validation Summary							
Policy Name	Severity	Revised	Date	Passed	Failed	Not Assessed	Exempt
3.1.03 enable local authentication	1	1	12-May-201...	0	13	0	0
3.1.04 enable only one local user	1	1	12-May-201...	11	2	0	0
3.1.08 disable SNMP community read-write	1	1	12-May-201...	7	6	0	0
3.1.09 and 10 disable SNMP community public and ...	1	1	12-May-201...	2	11	0	0
3.1.18 enable VTY exec timeout on lines	2	1	12-May-201...	0	13	0	0
3.1.38 disable ip http server	1	1	12-May-201...	9	4	0	0
3.1.39 enable service password-encryption	2	1	12-May-201...	1	12	0	0
3.1.54 enable logging	3	1	12-May-201...	13	0	0	0
3.1.55 enable syslog servers	3	1	12-May-201...	0	13	0	0
3.1.59 2 disable logging console	4	1	12-May-201...	13	0	0	0
3.1.60 enable logging trap level	4	1	12-May-201...	0	13	0	0
3.1.73 and 74 disable directed broadcast	2	1	12-May-201...	11	2	0	0

Export >> **Details**

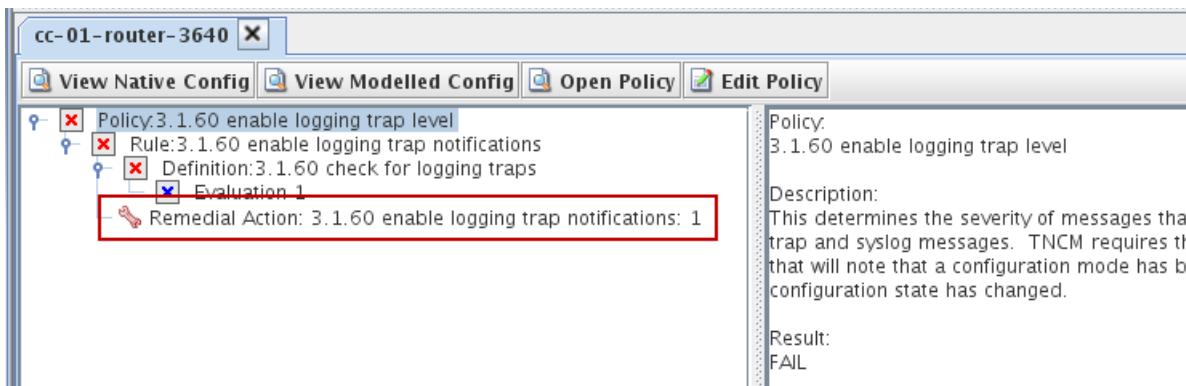
- Scroll through the devices that are in the results details. The **cc-01-router-3640**, **cc-02-router-3640**, and **CC-03-router-3640** devices all fail the **3.1.60 enable logging trap level** policy.

Filter By Device:		Compliance Status: ANY			
Policy	Device	Device Realm	Support Level	Date	Cor
3.1.60 enable log...	BRU-ACS-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	BRU-CPE-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	BRU-SW-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	BRU-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	LON-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	MOS-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	NYC-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	PAR-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	SYD-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	WAS-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	cc-01-router-3640	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	cc-02-router-3640	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	cc-03-router-3640	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL

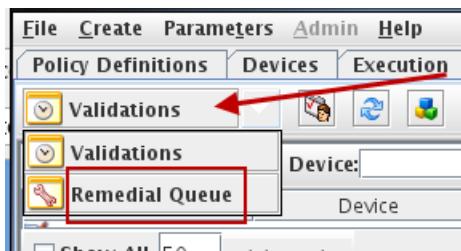
6. Double-click the row in the results that shows the compliance status of the **3.1.60 enable logging trap level** policy for the **cc-01-router-3640** device.

Policy	Device	Device Realm	Support Level	Date	Co
3.1.60 enable log...	BRU-ACS-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	BRU-CPE-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	BRU-SW-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	BRU-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	LON-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	MOS-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	NYC-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	PAR-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	SYD-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	WAS-dca.gov	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	cc-01-router-3640	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	cc-02-router-3640	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL
3.1.60 enable log...	cc-03-router-3640	ITNCM/edge-network/...	SmartModel	12-May-2016 15:12:...	FAIL

You can see the details of the compliance failure. The remedial action that is associated with this policy is named **3.1.60 enable logging trap notifications**.



- Click **Remedial Queue** in the **Results** tab.



The ITNCM >edge-network > customer-CC subrealm contains 18 remedial actions that are pending approval. The remedial action for the **3.1.60 enable logging trap level** policy is to run the **3.1.60 enable logging trap notifications** command set.

	CommandSet Name	Comm...	Policy	Dev
3.1.03 enable local authentication	na	3.1.03 enable local authentication	cc-01-n	
3.1.03 enable local authentication	na	3.1.03 enable local authentication	cc-02-n	
3.1.03 enable local authentication	na	3.1.03 enable local authentication	cc-03-n	
3.1.09 and 10 disable SNMP communit...	na	3.1.09 and 10 disable SNMP communit...	cc-03-n	
3.1.18 enable VTY exec-timeout	na	3.1.18 enable VTY exec timeout on li...	cc-01-n	
3.1.18 enable VTY exec-timeout	na	3.1.18 enable VTY exec timeout on li...	cc-02-n	
3.1.18 enable VTY exec-timeout	na	3.1.18 enable VTY exec timeout on li...	cc-03-n	
3.1.38 disable http server	na	3.1.38 disable ip http server	cc-01-n	
3.1.39 enable service password-encry...	na	3.1.39 enable service password-encry...	cc-01-n	
3.1.39 enable service password-encry...	na	3.1.39 enable service password-encry...	cc-03-n	
3.1.55 enable logging to syslog server	na	3.1.55 enable syslog servers	cc-01-n	
3.1.55 enable logging to syslog server	na	3.1.55 enable syslog servers	cc-02-n	
3.1.55 enable logging to syslog server	na	3.1.55 enable syslog servers	cc-03-n	
3.1.60 enable logging trap notifications	na	3.1.60 enable logging trap level	cc-01-n	
3.1.60 enable logging trap notifications	na	3.1.60 enable logging trap level	cc-02-n	
3.1.60 enable logging trap notifications	na	3.1.60 enable logging trap level	cc-03-n	
3.1.73 and 74 disable FE directed bro...	na	3.1.73 and 74 disable directed bro...	cc-02-n	
3.1.73 and 74 disable FE directed bro...	na	3.1.73 and 74 disable directed bro...	cc-03-n	

- Return to the *configuration manager* user interface.

9. Click ITNCM > edge-network > customer_CC. Click one of the devices in the customer_CC realm. Click the **Compliance** tab. The compliance status of each policy that you run is shown.

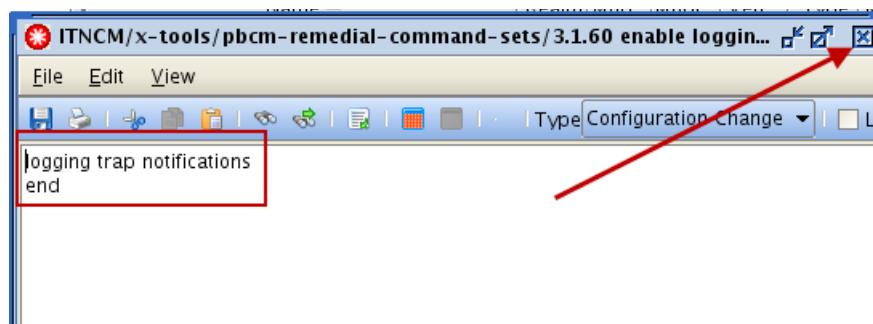
The screenshot shows the ITNCM interface. On the left, the Resource Browser tree includes 'edge-network' with 'customer_AA' and 'customer_CC' expanded. A red box highlights 'customer_CC'. In the center, a table lists four devices: 'cc-01-router-3640', 'cc-02-router-3640', 'cc-03-router-3640', and 'no_erase_squeeze'. A red arrow points from the 'customer_CC' node in the tree to the 'Compliance' tab in the top navigation bar. The 'Compliance' tab is selected, showing a table of policies and their validation dates. A red box highlights the 'Compliance Status' column, which contains icons indicating non-compliant (red flag) or compliant (green checkmark) status for each policy. The policies listed are: 3.1.03, 3.1.04, 3.1.08, 3.1.09, 3.1.18, 3.1.38, 3.1.39, 3.1.54, and 3.1.55.

10. In the *configuration manager* user interface, look at the command set named **3.1.60 enable logging trap notifications**. This command set is linked to a remedial action. Do not run this command set yet. When you finish, keep the configuration manager user interface open.

- a. Click ITNCM > x-tools > pBCM-remedial-command-sets in the resource browser.

The screenshot shows the Configuration Manager interface. The Resource Browser tree on the left has 'x-tools' expanded, with 'pBCM-remedial-command-sets' highlighted by a red box. In the center, a table lists several command sets. A red box highlights the row for '3.1.60 enable logging trap notifications'. Below the table, a message says 'No Compliance Data Found'.

- b. Double-click the command set named **3.1.60 enable logging trap notifications** to view the commands that are sent to the device.



- c. Close the command window.

11. Return to the Firefox browser. Click **Logoff**.



12. Close the browser.

Leave the *compliance manager* user interface as is.

Leave the *configuration manager* user interface as is.



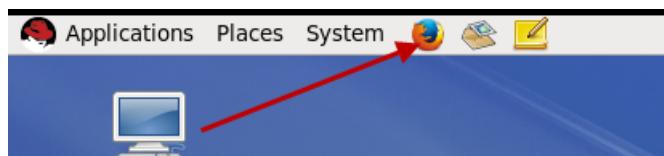
16 Compliance reports exercises

The exercises in this unit demonstrate some of the available reports for compliance analysis.

Exercise 1 Running compliance reports

In this exercise, you run Tivoli Common Reporting reports

1. Open the Firefox Internet browser. Log on to Dashboard Application Services Hub with the user name **engineer** and the password **object00**.
 - a. Click the icon and open a Firefox browser.



The browser home page default is:

<https://host1.csite.edu:16311/ibm/console/logon.jsp>

- b. Log in with the user name **engineer** and the password **object00**.

IBM Dashboard Application Services Hub

User ID
engineer

Password

Go

2. Open the Common Reporting menu. Access the **ITNCM Reports**.
 - a. Click the icon and select **Common Reporting**.



- b. Click **ITNCM Reports** in the Common Reporting tab.

	Name
<input type="checkbox"/>	Common Reporting
<input type="checkbox"/>	ITNCM Reports
<input type="checkbox"/>	Netcool_OMNIbus
<input type="checkbox"/>	Network Manager

3. Run the **Policy Compliance Summary (By Process)** report. Run the report from 12:00 AM today to 11:59 PM today. Drill down into the process that you ran in a preceding exercise. Continue to drill-down until you see the Policy Compliance Detail report for a single policy and a single device. When you finish, return to the list of reports. You might need to close some browser windows to return to the list of reports.

- a. Click **Policy Compliance Summary (By Process)** in the list of reports.

	Name
<input type="checkbox"/>	Configuration And OS Change Summary
<input type="checkbox"/>	Device Inventory List
<input type="checkbox"/>	Device Inventory VTMOS Summary
<input type="checkbox"/>	Policy Compliance Detail
<input type="checkbox"/>	Policy Compliance Detail (By Process)
<input type="checkbox"/>	Policy Compliance Grouped By Device
<input type="checkbox"/>	Policy Compliance Grouped By Device (By Process)
<input type="checkbox"/>	Policy Compliance Grouped By Policy
<input type="checkbox"/>	Policy Compliance Grouped By Policy (By Process)
<input type="checkbox"/>	Policy Compliance Score and Summary
<input type="checkbox"/>	Policy Compliance Score Trend
<input type="checkbox"/>	Policy Compliance Summary (By Process)
<input type="checkbox"/>	Security Groups

- b. Use 12:00 AM today to 11:59 PM today as the Date Range. Click **Next**.

Date Range:

From:

May 12, 2016

12 : 00 AM

To:

May 12, 2016

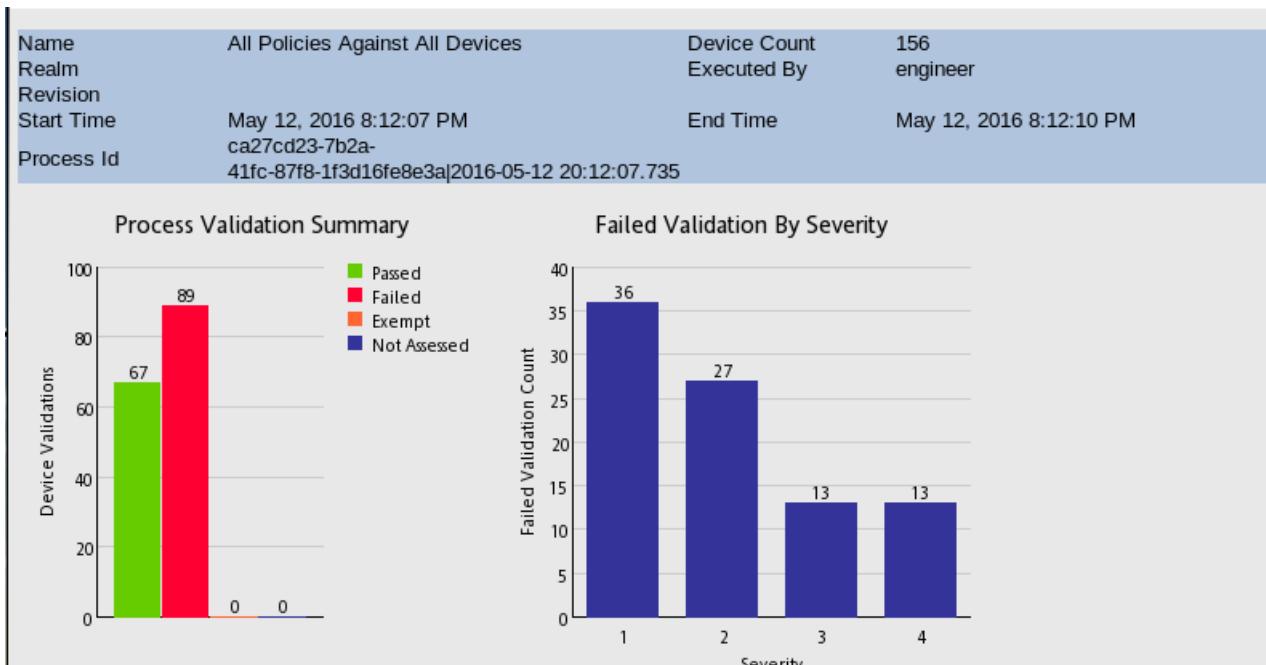
11 : 59 PM

- c. Click the process that you ran in the preceding exercise.

Policy Compliance Summary (By Process)				
Start Date	May 12, 2016 12:00:00 AM			End Date
Row Number	Process Name	Device Count	Executed By	
1	Test 12-May-2016 13:27:29	3	engineer	May
2	All Policies Against All Devices	13	engineer	May
Process Count	2			

Exercise 1 Running compliance reports

- d. Scroll down to view the report. Click the name of one of the policies to drill down in the report.



The following table summarizes the results for all policies that have been validated in this process

Policy Name	Severity	Passed	Failed	Exempt	Not Assess
3.1.03 enable local authentication	1	0	13	0	0
3.1.04 enable only one local user	1	11	2	0	0
3.1.08 disable SNMP community read-write	1	7	6	0	0
3.1.09 and 10 disable SNMP community public and private	1	2	11	0	0
3.1.18 enable VTY exec timeout on lines	2	0	13	0	0
3.1.38 disable ip http server	1	9	4	0	0
3.1.39 enable service password-encryption	2	1	12	0	0
3.1.54 enable logging	3	13	0	0	0
3.1.55 enable syslog servers	3	0	13	0	0
3.1.59-2 disable logging console	4	13	0	0	0
3.1.60 enable logging trap level	4	0	13	0	0
3.1.73 and 74 disable directed broadcast	2	11	2	0	0
Policy Count	12				

- e. Scroll down to view the report. Click the result for one of the devices to drill down in the report.

Policy Compliance Detail

Policy Information:		
Name	3.1.60 enable logging trap level This determines the severity of messages that will generate an SNMP trap and messages. TNCM requires the use of a logging level that will note that a configuration has been access or that the configuration state has changed.	
Description		
Severity	4	
Device Information:		
Device Name	Device Realm	Result
BRU-ACS-dca.gov	ITNCM/edge-network/customer_AA	FAIL
BRU-CPE-dca.gov	ITNCM/edge-network/customer_AA	FAIL
BRU-dca.gov	ITNCM/edge-network/customer_AA	FAIL
BRU-SW-dca.gov	ITNCM/edge-network/customer_AA	FAIL
cc-01-router-3640	ITNCM/edge-network/customer_CC	FAIL
cc-02-router-3640	ITNCM/edge-network/customer_CC	FAIL
cc-03-router-3640	ITNCM/edge-network/customer_CC	FAIL
LON-dca.gov	ITNCM/edge-network/customer_AA	FAIL
MOS-dca.gov	ITNCM/edge-network/customer_AA	FAIL
NYC-dca.gov	ITNCM/edge-network/customer_AA	FAIL
PAR-dca.gov	ITNCM/edge-network/customer_AA	FAIL
SYD-dca.gov	ITNCM/edge-network/customer_AA	FAIL
WAS-dca.gov	ITNCM/edge-network/customer_AA	FAIL
Device Count	13	

- f. View the details of the policy for the single device.

Policy Compliance Detail

Process Id	ca27cd23-7b2a-41fc-87f8-1f3d16fe8e3a 2016-05-12 20:12:07.735		
Device Name	cc-01-router-3640		
Device Realm	ITNCM/edge-network/customer_CC		
VTMOS	Cisco/Router/3640/C3640-I-M-12.3(5b)		
Policy	3.1.60 enable logging trap level	Policy Result	FAIL
Searched For	Match Expression = logging trap ((debugging) (informational) (notifications)) ([5-7]) Match Criteria = Match All		
Search Result	NOT FOUND		
Outcome	FAIL: the test condition and evaluation criteria were not met		

- g. Close the drill-down report windows.



- h. Click the *return* icon to go back to the list of reports.



4. Run the **Policy Compliance Grouped by Device** report. Use the following values to complete the prompts. When you finish, return to the list of reports. You might need to close some browser windows to return to the list of reports.
- Select the **ITNCM/edge-network/customer-CC** realm.
 - Click **Yes** to include subrealms.
 - Click **Select all** in the Policies prompt.
 - Use the default values for the Device Name & VTMOS Filter prompt.
 - Use the default values for the Policy Severity prompt.
 - Use the default values for the Policy Result prompt.
- a. Click **Policy Compliance Grouped by Device** in the list of reports.

	Name
<input type="checkbox"/>	Configuration And OS Change Summary
<input type="checkbox"/>	Device Inventory List
<input type="checkbox"/>	Device Inventory VTMOS Summary
<input type="checkbox"/>	Policy Compliance Detail
<input type="checkbox"/>	Policy Compliance Detail (By Process)
<input type="checkbox"/>	Policy Compliance Grouped By Device
<input type="checkbox"/>	Policy Compliance Grouped By Device (By Process)
<input type="checkbox"/>	Policy Compliance Grouped By Policy

b. Complete the prompts for the Policy Compliance Grouped by Device report. Click **Finish**.

Realms

- ITNCM/DataCenter
- ITNCM/DataCenter/ServiceCommandSets
- ITNCM/NOI_AGG_P
- ITNCM/edge-network
- ITNCM/edge-network/customer_AA
- ITNCM/edge-network/customer_CC**
- ITNCM/x-tools
- ITNCM/x-tools/command-set-examples
- ITNCM/x-tools/command-set-examples/Unit-0
- ITNCM/x-tools/os-upgrades
- ITNCM/x-tools/nbcm-remedial-command-sets

Select all Deselect all

Policies

- D1-EncryptPasswords
- D2-SecureAccess
- D3-DisableUnwantedServices
- D4-Logging
- D5-AccurateTime
- D6-ConsoleAccess
- D7-Banner
- D8-StrongEnablePassword
- D9-DisableDefaultSNMP
- D1.1 enable all interfaces have a description
- D1.2 enable VTY exec timeout on lines
- D1.3 enable only two SNMP community strings
- D10-LoginTimeout
- D3.1.03 enable local authentication
- D3.1.04 enable only one local user

Select all Deselect all

Device Name & VTMOS

Name	*
Vendor	VENDOR
Type	TYPE
Model	MODEL
OS	OS

Policy Severity

- 1
- 2
- 3
- 4
- 5

Select all Deselect all

Policy Result

- Pass
- Fail
- Exempt
- Not Assesed

Select all Deselect all

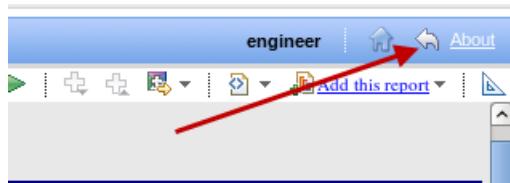
c. Scroll down to view the report.

Policy Compliance Grouped By Device

Device Name cc-01-router-3640
Device Realm ITNCM/edge-network/customer_CC
Device VTMOS Cisco/Router/3640/C3640-I-M-12.3(5b)

Policy Name	Policy Realm	Severity	Result
3.1.03 enable local authentication	CIS-Level-1-Benchmark/Management Plane Level 1/Local AAA Rules/	1	FAIL
3.1.04 enable only one local user	CIS-Level-1-Benchmark/Management Plane Level 1/Local AAA Rules/	1	FAIL
3.1.08 disable SNMP community read-write	CIS-Level-1-Benchmark/Management Plane Level 1/SNMP Rules/	1	FAIL
3.1.09 and 10 disable SNMP community public and private	CIS-Level-1-Benchmark/Management Plane Level 1/SNMP Rules/	1	PASS
3.1.18 enable VTY exec timeout on lines	CIS-Level-1-Benchmark/Management Plane Level 1/Access Rules/	2	FAIL
3.1.38 disable ip http server	CIS-Level-1-Benchmark/Management Plane Level 1/Management Service Rules/	1	FAIL
3.1.39 enable service password-encryption	CIS-Level-1-Benchmark/Management Plane Level 1/Management Service Rules/	2	FAIL
3.1.54 enable logging	CIS-Level-1-Benchmark/Control Plane Level 1/Logging Rules/	3	PASS
3.1.55 enable syslog servers	CIS-Level-1-Benchmark/Control Plane Level 1/Logging Rules/	3	FAIL
3.1.59-2 disable logging console	CIS-Level-1-Benchmark/Control Plane Level 1/Logging Rules/	4	PASS
3.1.60 enable logging tran level	CIS-Level-1-Benchmark/Control Plane Level 1/Logging Rules/	4	FAIL

- d. Click the *return* icon to go back to the list of reports.



5. Run the **Policy Compliance Grouped by Policy** report. Use the following values to complete the prompts. Drill down in the report until you see the Policy Compliance Detail report for a single policy and a single device. When you finish, return to the list of reports. You might need to close some browser windows to return to the list of reports.
- Select the **ITNCM/edge-network/customer-CC** realm.
 - Click **Yes** to include subrealms.
 - Click **Select all** in the Policies prompt.
 - Use the default values for the Device Name & VTMOS Filter prompt.
 - Use the default values for the Policy Severity prompt.
 - Use the default values for the Policy Result prompt.
- a. Click **Policy Compliance Grouped by Policy** in the list of reports.

	Name
<input type="checkbox"/>	Configuration And OS Change Summary
<input type="checkbox"/>	Device Inventory List
<input type="checkbox"/>	Device Inventory VTMOS Summary
<input type="checkbox"/>	Policy Compliance Detail
<input type="checkbox"/>	Policy Compliance Detail (By Process)
<input type="checkbox"/>	Policy Compliance Grouped By Device
<input type="checkbox"/>	Policy Compliance Grouped By Device (By Process)
<input type="checkbox"/>	Policy Compliance Grouped By Policy
<input type="checkbox"/>	Policy Compliance Grouped By Policy (By Process)

- b. Complete the prompts for the Policy Compliance Grouped by Policy report. Click **Finish**.

The screenshot shows the configuration interface for a Policy Compliance report. It includes four main sections:

- Realms:** A list of realms with one item selected: "ITNCM/edge-network/customer_CC".
- Policies:** A list of policies with several checked items, including "D1-EncryptPasswords" through "D9-DisableDefaultSNMP" and specific sub-items like "enable all interfaces have a description".
- Include SubRealms:** A radio button group where "Yes" is selected.
- Device Name & VTMO:** A panel for device filtering with fields for Name, Vendor, Type, Model, and OS.
- Policy Severity:** A list of severity levels (1-5) with all selected.
- Policy Result:** A list of result types (Pass, Fail, Exempt, Not Assesed) with all selected.

- c. Click the result for a device to drill down in the report.

Policy Compliance Grouped By Policy

Policy Information:

Name 3.1.03 enable local authentication
Description This policy ensures that there is a model for local authentication to the device. In most cases, auth by an authentication server (i.e. RADIUS or TACACS.) However, access to the device will be required if the authentication server is unavailable for authentication (e.g. server is down, network problems, the

Revision 1

Severity 1

Device Information:

Device Name	Device Realm	Vendor	Type	Model	OS	Result
cc-01-router-3640	ITNCM/edge-network/customer_CC	Cisco	Router	3640 (R4700)	C3640-I-M-12.3(5b)	FAIL
cc-02-router-3640	ITNCM/edge-network/customer_CC	Cisco	Router	3640 (R4700)	C3640-I-M-12.4(25c)	FAIL
cc-03-router-3640	ITNCM/edge-network/customer_CC	Cisco	Router	3640 (R4700)	C3640-IK9S-M-12.4(25c)	FAIL
Device Count	3					

- d. View the details of the policy for the single device.

Policy Compliance Detail

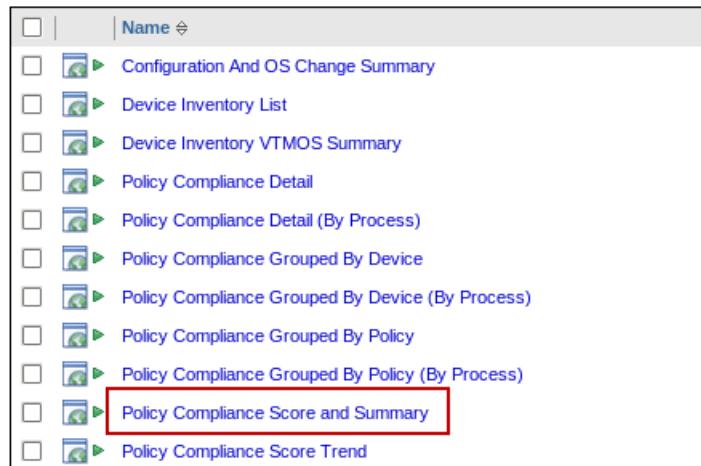
Process Id	ca27cd23-7b2a-41fc-87f8-1f3d16fe8e3a 2016-05-12 20:12:07.735		
Device Name	cc-01-router-3640		
Device Realm	ITNCM/edge-network/customer_CC		
VTMOS	Cisco/Router/3640/C3640-I-M-12.3(5b)		
Policy	3.1.03 enable local authentication	Policy Result	FAIL
Searched For	Match Expression = ^aaa authentication enable \S+ Match Criteria = Match All	Search Result	NOT FOUND
Outcome	FAIL: the test condition and evaluation criteria were not met		
Searched For	Match Expression = ^aaa authentication login default local Match Criteria = Match All	Search Result	NOT FOUND
Outcome	FAIL: the test condition and evaluation criteria were not met		
Searched For	Match Expression = ^aaa new-model Match Criteria = Match All	Search Result	1 match aaa new-model
Outcome	PASS: the test condition and evaluation criteria were met		

- e. Close the drill-down windows and click the **Return** icon to go back to the list of compliance reports.



6. Run the **Policy Compliance Score and Summary** report. Use the following values to complete the prompts. Drill down in the report until you see the Policy Compliance Detail report for a single policy and a single device. When you finish, return to the list of reports and keep the browser session open.
- Select the **ITNCM/edge-network/customer-CC** realm.
 - Click **Yes** to include subrealms.
 - Click **Select all** in the Policies prompt
 - Use the default values for the Device Name & VTMOS Filter prompt.

- a. Click **Policy Compliance Score and Summary** in the list of reports.



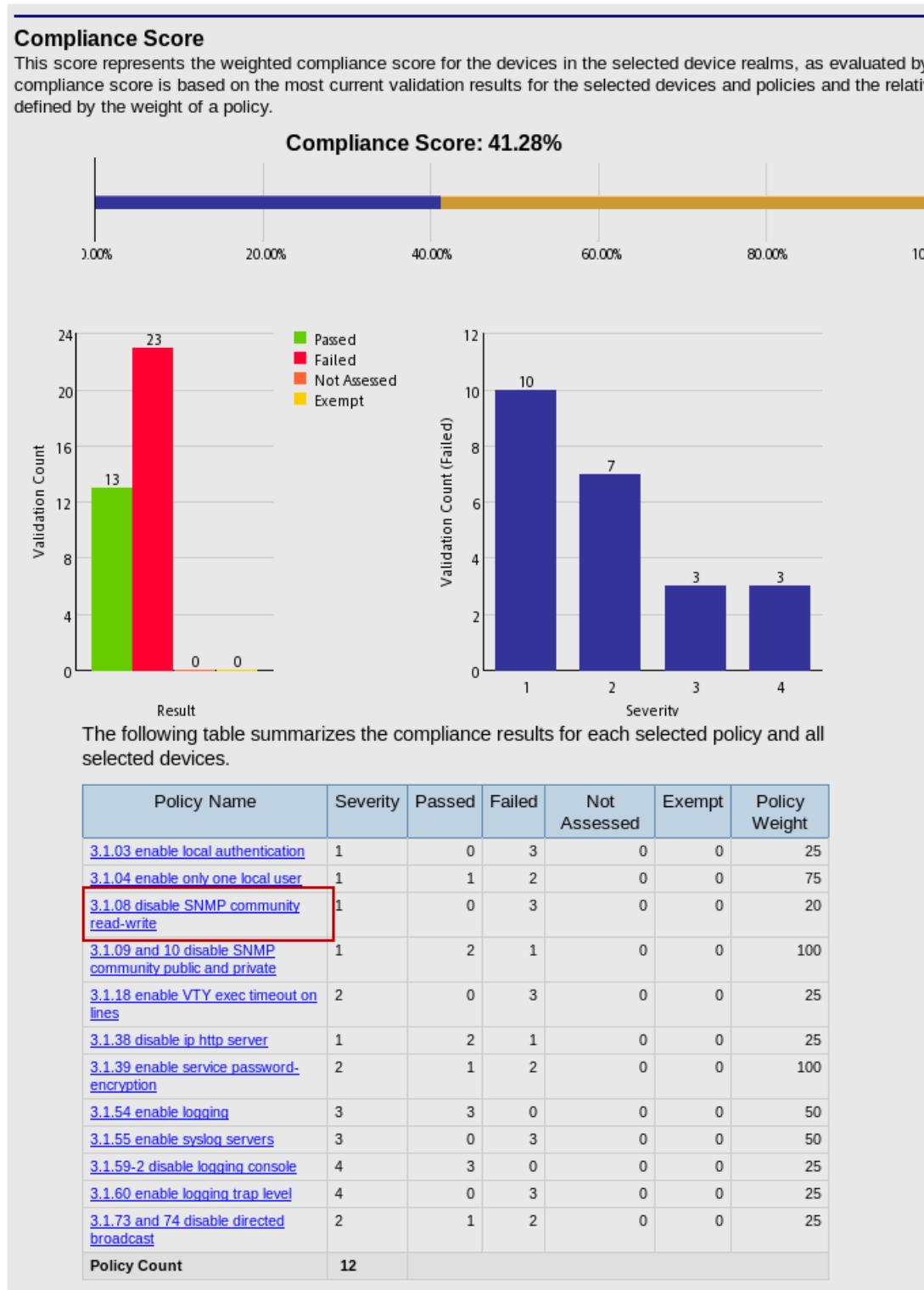
- b. Complete the prompts for the **Policy Compliance Score and Summary** report. Click **Finish**.

The screenshot shows the configuration interface for the 'Policy Compliance Score and Summary' report. It consists of three main panels:

- Realms:** A list of realms. The checkbox for 'ITNCM/edge-network/customer_CC' is checked and highlighted with a red box.
- Policies:** A list of policies. Many policies are checked, and a red arrow points to the 'Select all Deselect all' button at the bottom right of the list.
- Device Name:** A sidebar with fields for Name, Vendor, Type, Model, and OS, each with a placeholder value.

The compliance score is low.

- c. Click the name of a policy to drill down in the report.



- d. Click the result for a device to drill down in the report.

Policy Compliance Detail

Policy Information:		
Name	3.1.08 disable SNMP community read-write Enabling SNMP read-write enables remote (mis)management (i.e. via the community string.) It presents a possible avenue of attack. potential for such abuse.	
Description		
Severity	1	
Device Information:		
Device Name	Device Realm	
cc-01-router-3640	ITNCM/edge-network/customer_CC	FAIL
cc-02-router-3640	ITNCM/edge-network/customer_CC	FAIL
cc-03-router-3640	ITNCM/edge-network/customer_CC	FAIL
Device Count		3

- e. View the details of the policy for the single device.

Policy Compliance Detail

Process Id	ca27cd23-7b2a-41fc-87f8-1f3d16fe8e3a 2016-05-12 20:12:07.735
Device Name	cc-01-router-3640
Device Realm	ITNCM/edge-network/customer_CC
VTMOS	Cisco/Router/3640/C3640-I-M-12.3(5b)
Policy	3.1.08 disable SNMP community read-write
Policy Result	FAIL
Searched For	Match Expression = ^snmp-server community .* RW Match Criteria = Match All
Search Result	1 match snmp-server community wr1t3Str1ng RW
Outcome	PASS: the test condition and evaluation criteria were met



Note: The policy is designed to check for the existence of a read/write community string. The test passes because the read/write community string is found. However, the policy fails because you do not want a read/write community string defined.

- f. Close the drill-down windows.

The screenshot shows a browser window with three tabs open. The tabs are labeled "IBM Dashboard Appl...", "Policy Compliance Sum...", and "Policy Compliance Grou...". Red arrows point from the text above to the second and third tabs. Below the tabs, the address bar shows the URL "https://host1.csuite.edu:16311/tarf/servlet/dispatch". The main content area is titled "Viewer - Policy Compliance Grouped By Policy Device DrillDown".

- g. Click the *return* icon to go back to the list of reports.

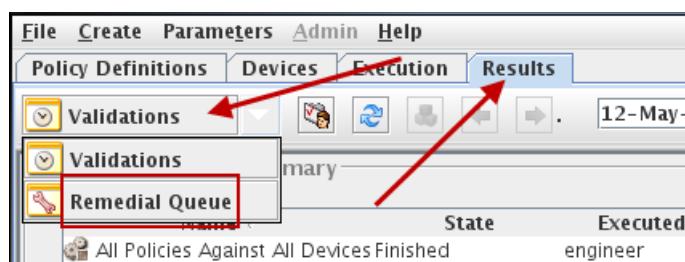
The screenshot shows a software interface with a toolbar at the top containing various icons. A red arrow points to the "About" icon in the toolbar. The menu bar has items like "engineer", "About", and "File".

Leave the browser session as is. You return to it shortly.

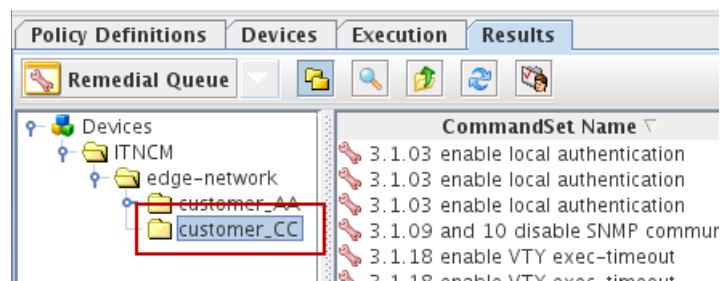
Exercise 2 Running remedial actions

In this exercise, you run the remedial actions that you queued in a preceding exercise. You queued these actions when you ran the All Policies Against All Devices process. After you run the remedial actions, you view the command sets that they run in *configuration manager*. The overall goal of this exercise is to increase the policy compliance score.

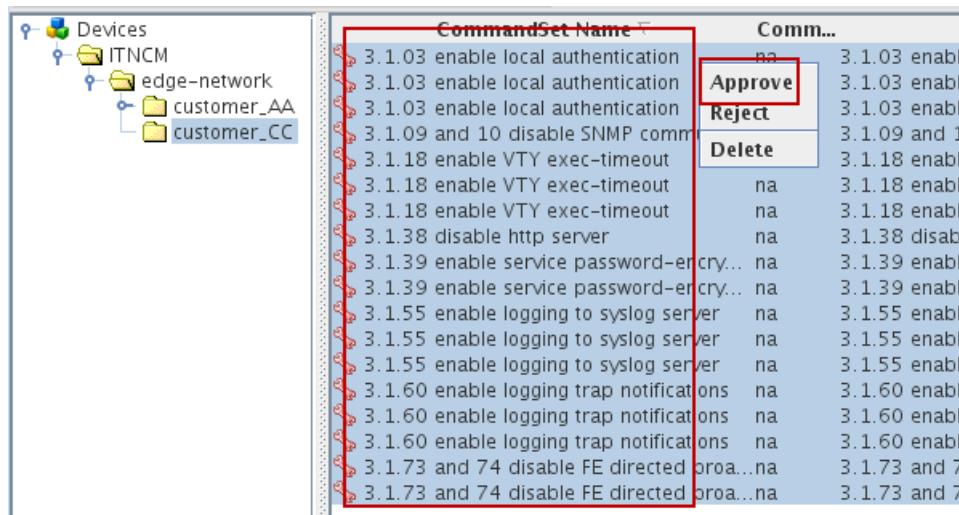
1. Return to the *compliance manager* user interface. View the remedial queue in the **Results** tab. Approve all of the actions in the remedial queue for the **ITNCM > edge-network > customer-CC** subrealm. Refresh the remedial queue until the status of the actions is **Sent to R-Series**. Ignore any actions that have the status of **ERROR**.
 - a. Click the **Results** tab in the *compliance manager* user interface. Click **Validations** and select **Remedial Queue**.



- b. Select the **customer_CC** realm.



- c. Select all of the actions. Right-click the selected actions and click **Approve**.



- d. Click **Yes** to confirm.



- e. Click the refresh icon until the status of the actions is **Sent to Work Queue**. Ignore any actions that have the status of **ERROR**. It might take up to 10 minutes for all the units of work to complete.

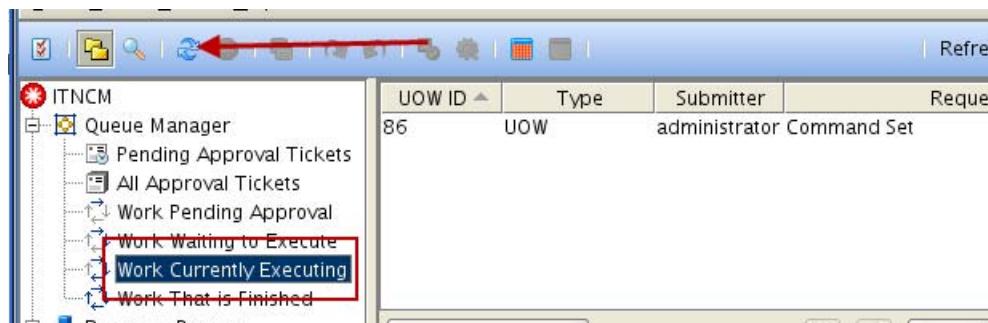
CommandSet Name	Comm...	Policy	Device	Realm	Status	O.....
3.1.03 enable local authentication	na	3.1.03 enable local au...	cc-01-router-...ITNC...	...	Sent to Work Queue	1.....
3.1.03 enable local authentication	na	3.1.03 enable local au...	cc-02-router-...ITNC...	...	Sent to Work Queue	1.....
3.1.03 enable local authentication	na	3.1.03 enable local au...	cc-03-router-...ITNC...	...	Sent to Work Queue	1.....
3.1.09 and 10 disable SNMP comm	na	3.1.09 and 10 disabl...	cc-03-router-...ITNC...	...	Sent to Work Queue	1.....
3.1.18 enable VTY exec-timeout	na	3.1.18 enable VTY ex...	cc-01-router-...ITNC...	...	Sent to Work Queue	1.....
3.1.18 enable VTY exec-timeout	na	3.1.18 enable VTY ex...	cc-02-router-...ITNC...	...	Sent to Work Queue	1.....
3.1.18 enable VTY exec-timeout	na	3.1.18 enable VTY ex...	cc-03-router-...ITNC...	...	Sent to Work Queue	1.....
3.1.38 disable http server	na	3.1.38 disable ip http	cc-01-router-...ITNC...	...	SENT TO WORK QUEUE	1.....
3.1.39 enable service password-encry...	na	3.1.39 enable service ...	cc-01-router-...ITNC...	...	SENT TO WORK QUEUE	0.....
3.1.39 enable service password-encry...	na	3.1.39 enable service ...	cc-03-router-...ITNC...	...	SENT TO WORK QUEUE	0.....
3.1.55 enable logging to syslog server	na	3.1.55 enable logging to sysl...	cc-01-router-...ITNC...	...	SENT TO WORK QUEUE	1.....
3.1.55 enable logging to syslog server	na	3.1.55 enable logging to sysl...	cc-02-router-...ITNC...	...	SENT TO WORK QUEUE	1.....
3.1.55 enable logging to syslog server	na	3.1.55 enable logging to sysl...	cc-03-router-...ITNC...	...	SENT TO WORK QUEUE	1.....
3.1.60 enable logging trap notifications	na	3.1.60 enable logging ...	cc-01-router-...ITNC...	...	SENT TO WORK QUEUE	1.....
3.1.60 enable logging trap notifications	na	3.1.60 enable logging ...	cc-02-router-...ITNC...	...	SENT TO WORK QUEUE	1.....
3.1.60 enable logging trap notifications	na	3.1.60 enable logging ...	cc-03-router-...ITNC...	...	SENT TO WORK QUEUE	1.....
3.1.73 and 74 disable FE directed proa...	na	3.1.73 and 74 disable...	cc-01-router-...ITNC...	...	SENT TO WORK QUEUE	1.....
3.1.73 and 74 disable FE directed proa...	na	3.1.73 and 74 disable...	cc-02-router-...ITNC...	...	SENT TO WORK QUEUE	1.....
3.1.73 and 74 disable FE directed proa...	na	3.1.73 and 74 disable...	cc-03-router-...ITNC...	...	SENT TO WORK QUEUE	1.....

2. Return to the **configuration manager** user interface. Look at **Work That is Finished** in the queue manager. You see several new units of work that ran successfully for native command sets. These command sets were automatically run in configuration manager when you

Exercise 2 Running remedial actions

approved the remedial actions in compliance manager. Verify that all of the command sets were successful. You might need to wait until all of the units of work finish.

- Return to the configuration manager user interface. Click **Work Currently Executing** in the queue manager. Click the *refresh* icon until the queue is empty.



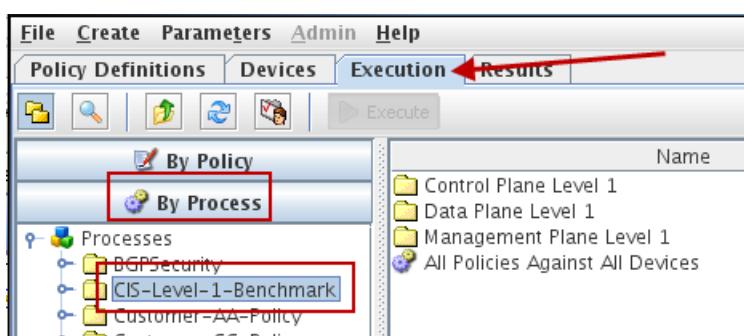
- Click **Work That is Finished** in the queue manager. View the successful command set units of work.

UOW ID	Type	Submitter	Request Type
78	UOW	administrator Native Command Set	SUCCESS
79	UOW	administrator Native Command Set	SUCCESS
80	UOW	administrator Command Set	SUCCESS
81	UOW	administrator Native Command Set	SUCCESS
82	UOW	administrator Native Command Set	SUCCESS
84	UOW	administrator Native Command Set	SUCCESS
85	UOW	administrator Command Set	SUCCESS
86	UOW	administrator Command Set	SUCCESS
87	UOW	administrator Native Command Set	SUCCESS
88	UOW	administrator Native Command Set	SUCCESS
89	UOW	administrator Command Set	SUCCESS

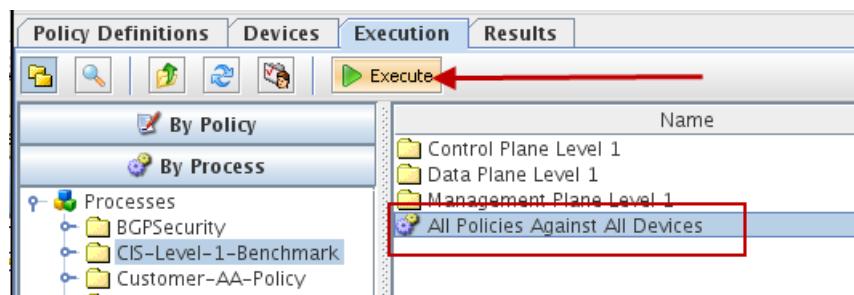
Exercise 3 Rerunning compliance reports

In this exercise, you run the All Policies Against All Devices process again. This process runs the policies again on the devices that you update with remedial actions. After you run the process again, you check the compliance score to see whether it improves after the remedial actions.

1. Run the **All Policies Against All Devices** process from the **Execution** tab in the *compliance manager* user interface.
 - a. Return to the *compliance manager* user interface. Click the **Execution** tab. Click the **By Process** section. Click the **CIS-Level-1-Benchmark** folder.



- b. Select the **All Policies Against All Devices** process and click **Execute**.



- c. Click **Yes** to confirm.



The **Results** tab opens.

- d. Click the *refresh* icon until the state changes to finished.

Name	State	Executed By
All Policies Against All Devices	Finished	engineer
All Policies Against All Devices	Finished	engineer
Test_12-May-2016 13:27:29	Finished	engineer

2. Run the **Policy Compliance Score and Summary** report again. Use the following values to complete the prompts. When you finish, return to the list of reports and keep the browser session open.
- Select the **ITNCM/edge-network/customer-CC** realm.
 - Click **Yes** to include subrealms.
 - Click **Select all** in the Policies prompt
 - Use the default values for the Device Name & VTMOS Filter prompt.
- a. Return to the Firefox browser.
 - b. Click **Policy Compliance Score and Summary** in the list of reports.

- Configuration And OS Change Summary
- Device Inventory List
- Device Inventory VTMOS Summary
- Policy Compliance Detail
- Policy Compliance Detail (By Process)
- Policy Compliance Grouped By Device
- Policy Compliance Grouped By Device (By Process)
- Policy Compliance Grouped By Policy
- Policy Compliance Grouped By Policy (By Process)
- Policy Compliance Score and Summary
- Policy Compliance Score Trend

- c. Complete the prompts for the **Policy Compliance Score and Summary** report. Click **Finish**.

The first screenshot shows the 'Realms' selection screen with several realms listed. One realm, 'ITNCM/edge-network/customer_CC', is selected and highlighted with a red box. The second screenshot shows the 'Policies' selection screen with a long list of policies checked. A red arrow points from the 'Select all Deselect all' button at the bottom right of this screen to the 'Select all Deselect all' button at the bottom right of the 'Realms' screen. The third screenshot shows a 'Device Name' configuration panel with fields for Name, Vendor, Type, Model, and OS.

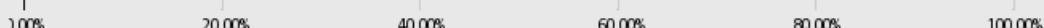
The compliance score improves.

Policy Compliance Score & Summary

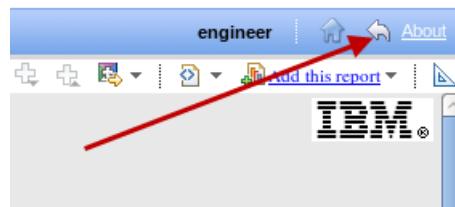
Compliance Score

This score represents the weighted compliance score for the devices in the selected device realms, as evaluated by the system. The compliance score is based on the most current validation results for the selected devices and policies and the relative importance defined by the weight of a policy.

Compliance Score: 79.51%



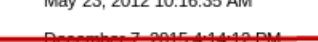
- d. Click the *return* icon to go back to the list of reports.



Exercise 4 Running alternative report formats and scheduling a report

In this exercise, you run a report in PDF format and schedule a report for recurring email delivery.

1. Run the **Policy Compliance Grouped by Device** report in PDF format. Use the following values to complete the prompts. Use Evince as the PDF viewer. When you finish, return to the list of reports. You might need to close some browser windows to return to the list of reports.
 - Select the **ITNCM/edge-network/customer-CC** realm.
 - Click **Yes** to include subrealms.
 - Click **Select all** in the Policies prompt.
 - Use the default values for the Device Name & VTMOS Filter prompt.
 - Use the default values for the Policy Severity prompt.
 - Use the default values for the Policy Result prompt.
- a. Click the **Run with options** icon for the **Policy Compliance Grouped by Device** report in the list of reports.



	Name	Modified	Actions
<input type="checkbox"/>	Configuration And OS Change Summary	December 7, 2015 11:53:06 AM	
<input type="checkbox"/>	Device Inventory List	November 24, 2015 10:38:39 AM	
<input type="checkbox"/>	Device Inventory VTMOS Summary	November 24, 2015 10:50:47 AM	
<input type="checkbox"/>	Policy Compliance Detail	November 25, 2015 10:51:39 AM	
<input type="checkbox"/>	Policy Compliance Detail (By Process)	May 23, 2012 10:16:35 AM	
<input type="checkbox"/>	Policy Compliance Grouped By Device	December 7, 2015 4:14:12 PM	
<input type="checkbox"/>	Policy Compliance Grouped By Device (By Process)	May 23, 2012 10:21:50 AM	
<input type="checkbox"/>	Policy Compliance Grouped By Policy	November 25, 2015 10:59:08 AM	
<input type="checkbox"/>	Policy Compliance Grouped By Policy (By Process)	May 23, 2012 10:24:03 AM	
<input type="checkbox"/>	Policy Compliance Score and Summary	December 7, 2015 4:24:26 PM	
<input type="checkbox"/>	Policy Compliance Score Trend	November 25, 2015 11:29:15 AM	

- b. Select **PDF** as the format. Make sure that **Delivery** is set to **View the report now** and that **Prompt for values** is selected. Click **Run**.

Run with options - Policy Compliance Grouped By Device

Select how you want to run and receive your report.

Format: To save or delete

Accessibility: Enable accessibility support

Language: English

Delivery:

- View the report now
- Save the report
- Print the report:
Printer location:
- Send me the report by email

Prompt values:
No values saved

Prompt for values

- c. Complete the prompts for the Policy Compliance Grouped by Device report. Click **Finish**.

Realms

- ITNCM/DataCenter
- ITNCM/DataCenter/ServiceCommandSets
- ITNCM/NOI_AGG_P
- ITNCM/edge-network
- ITNCM/edge-network/customer_AA
- ITNCM/edge-network/customer_CC
- ITNCM/x-tools
- ITNCM/x-tools/command-set-examples
- ITNCM/x-tools/command-set-examples/Unit-0
- ITNCM/x-tools/os-upgrades
- ITNCM/x-tools/pbcm-remedial-command-sets

Include SubRealms

Yes No

Policies

- 01-EncryptPasswords
- 02-SecureAccess
- 03-DisableUnwantedServices
- 04-Logging
- 05-AccurateTime
- 06-ConsoleAccess
- 07-Banner
- 08-StrongEnablePassword
- 09-DisableDefaultSNMP
- 1.1 enable all interfaces have a description
- 1.2 enable VTY exec timeout on lines
- 1.3 enable only two SNMP community strings
- 10-LoginTimeout
- 3.1.03 enable local authentication
- 3.1.04 enable one local user

Policy Severity

- 1
- 2
- 3
- 4
- 5

Policy Result

- Pass
- Fail
- Exempt
- Not Assesed

The report opens in PDF format.

IBM® Tivoli®

Policy Compliance Grouped By Device

Device Name: cc-01-router-3640
 Device Realm: ITNCM/edge-network/customer_CC
 Device VTMOS: Cisco/Router/3640/C3640-I-M-12.3(5b)

Policy Name	Policy Realm	Severity	Result
3.1.03 enable local authentication	CIS-Level-1-Benchmark/Management Plane Level 1/Local AAA Rules/	1	PASS
3.1.04 enable only one local user	CIS-Level-1-Benchmark/Management Plane Level 1/Local AAA Rules/	1	FAIL
3.1.08 disable SNMP community read-write	CIS-Level-1-Benchmark/Management Plane Level 1/SNMP Rules/	1	FAIL
3.1.09 and 10 disable SNMP community public and private	CIS-Level-1-Benchmark/Management Plane Level 1/SNMP Rules/	1	PASS
3.1.18 enable VTY exec timeout on lines	CIS-Level-1-Benchmark/Management Plane Level 1/Access Rules/	2	PASS
3.1.38 disable ip http server	CIS-Level-1-Benchmark/Management Plane Level 1/Management Service Rules/	1	FAIL

From this view, you can save the report as a PDF file.

- Click the *return* icon to go back to the list of reports.



2. Schedule the **Policy Compliance Score and Summary** report. Use the following settings for the scheduled report.
- Start the report today and set it to **No end date**.
 - Schedule the report to run every Monday and Friday.
 - Run the report in PDF format.
 - Send an email with the report as an attachment to **customercontact@customer-cc.com**.
 - Select the **ITNCM/edge-network/customer-CC** realm.
 - Click **Yes** to include subrealms.
 - Click **Select all** in the Policies prompt.
 - Use the default values for the Device Name & VTMOS Filter prompt.
- a. Click the **Schedule** icon for the **Policy Compliance Score and Summary** report in the list of reports.

Name	Modified	Actions
Configuration And OS Change Summary	December 7, 2015 11:53:06 AM	
Device Inventory List	November 24, 2015 10:38:39 AM	
Device Inventory VTMOS Summary	November 24, 2015 10:50:47 AM	
Policy Compliance Detail	November 25, 2015 10:51:39 AM	
Policy Compliance Detail (By Process)	May 23, 2012 10:16:35 AM	
Policy Compliance Grouped By Device	December 7, 2015 4:14:12 PM	
Policy Compliance Grouped By Device (By Process)	May 23, 2012 10:21:50 AM	
Policy Compliance Grouped By Policy	November 25, 2015 10:59:08 AM	
Policy Compliance Grouped By Policy (By Process)	May 23, 2012 10:24:03 AM	
Policy Compliance Score and Summary	December 7, 2015 4:24:26 PM	
Policy Compliance Score Trend	November 25, 2015 11:29:15 AM	

- b. At the top of the Schedule window, make sure that **No end date** is selected. Select **Monday** and **Friday** as the Frequency.

Schedule - Policy Compliance Score and Summary Help 

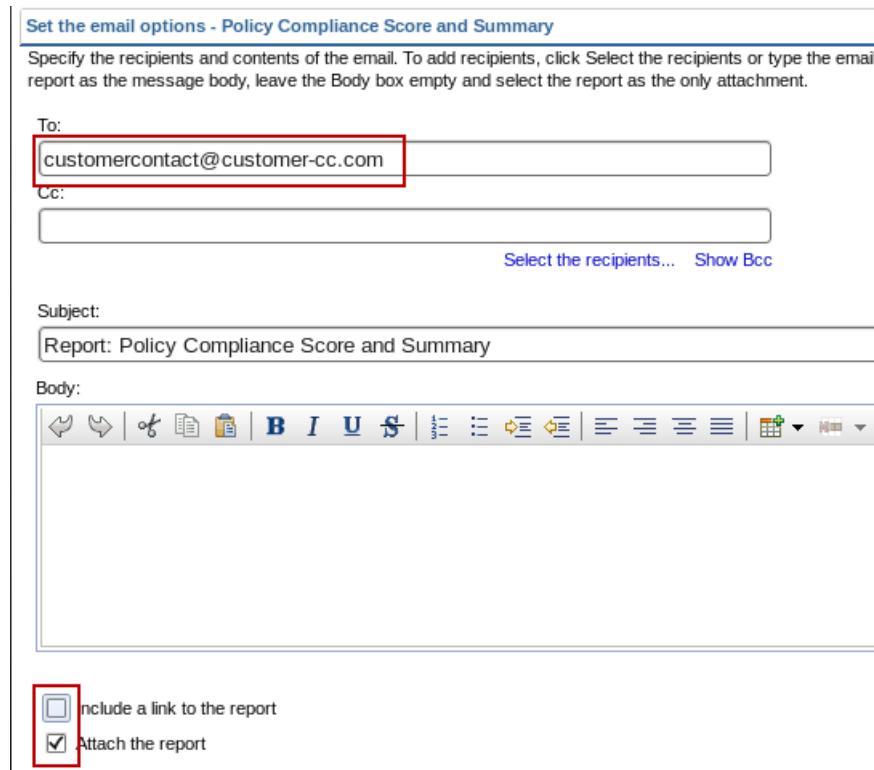
Schedule this entry to run at a recurring date and time. You can run using the default values or specify the options. You can disable the schedule without losing any its details.

<input type="checkbox"/> Disable the schedule	Priority: 3	Start: May 13, 201
Frequency:		End: <input checked="" type="radio"/> No end date <input type="radio"/> End by: May 13, 3 : 50 PM
<input type="button" value="By Day"/> <input type="button" value="By Week"/> <input type="button" value="By Month"/> <input type="button" value="By Year"/> <input type="button" value="By Trigger"/>		
Every 1 week(s) on: <input checked="" type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday		
Daily Frequency: <input type="checkbox"/> Every 1 Minute(s) between 9 : 00 AM and 5 : 00 PM		

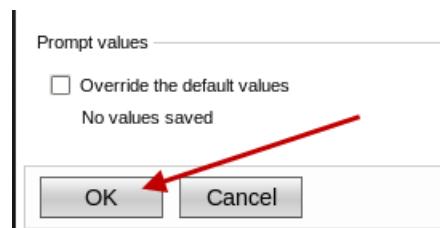
- c. Scroll down in the window, and select **Override the default values**. Select **PDF** as the format. Select **Send a link to the report by email** as the Delivery method. Click the **Edit the options** link next to the **Send a link to the report by email** option. The email options window opens.

<p><input checked="" type="checkbox"/> Override the default values</p> <p>Formats:</p> <p><input checked="" type="checkbox"/> HTML</p> <p>Number of rows per Web page: 20</p> <p><input checked="" type="checkbox"/> Enable selection-based interactivity</p> <p><input checked="" type="checkbox"/> PDF</p> <p>No options saved Set...</p> <ul style="list-style-type: none"> <input type="checkbox"/> Excel 2007 <input type="checkbox"/> Excel 2007 Data <input type="checkbox"/> Excel 2002 <input type="checkbox"/> Delimited text (CSV) <input type="checkbox"/> XML 	<p>Delivery:</p> <p>Select at least one delivery method. For burst reports, the email recipients are determined by the burst specification.</p> <p><input type="checkbox"/> Save: Select</p> <p><input checked="" type="radio"/> Save the report</p> <p><input type="radio"/> Save the report as a report view Edit the options...</p> <p> Report View of Policy Compliance Score and Summary</p> <p><input type="checkbox"/> Print the report</p> <p>Printer location: Select</p> <p><input checked="" type="checkbox"/> Send a link to the report by email Edit the options...</p> <p>engineer (engineer)</p>
---	--

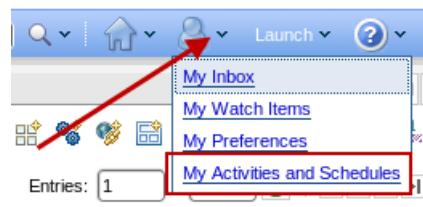
- d. In the email options window, enter **customercontact@customer-cc.com** in the **To** field. Select **Attach the report**. Click **OK** to return to the Schedule window.



- e. At the bottom of the Schedule window, click **OK**.



3. Use the My Activities and Schedules feature to verify that the report is scheduled.
a. Click **My Area > My Activities and Schedules**.



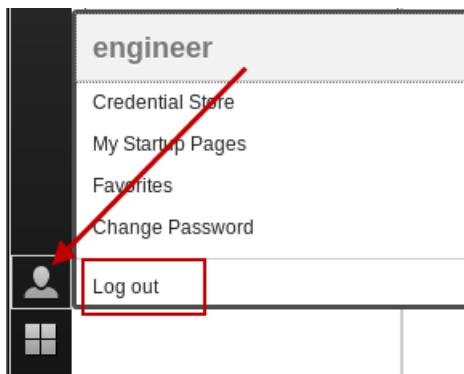
- b. Click **Schedules** in the My Activities and Schedules window.



- c. Verify that the report that you scheduled is present and enabled.



4. Log out of Dashboard Application Services Hub.



5. Close the Firefox browser.
6. Close the configuration manager client.
7. Close the compliance manager client.



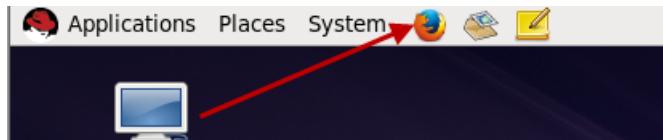
17 Build and run a policy exercises

The exercises in this unit demonstrate how to create compliance policies.

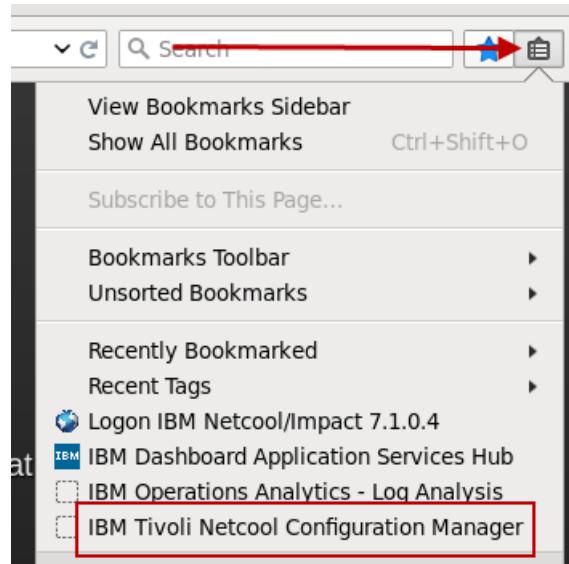
Exercise 1 Creating a policy realm

In this exercise, you create a policy realm. Later in this unit, you create policy objects and save them in this new realm.

1. Open a Firefox browser.



2. Open the list of bookmarks, and select IBM Tivoli Netcool Configuration Manager.



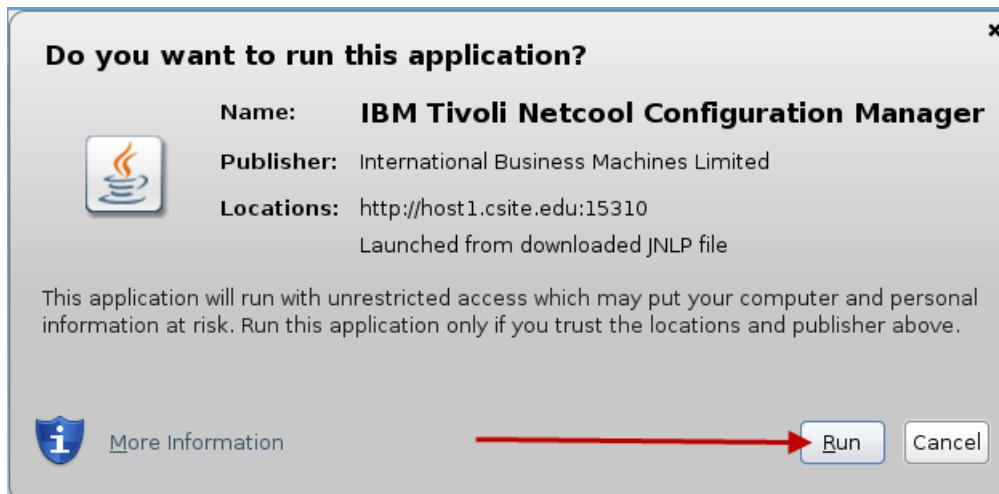
3. Open the list of bookmarks, and select **IBM Tivoli Netcool Configuration Manager**.



4. Select **ITNCM Compliance**.



5. Click **Run**.

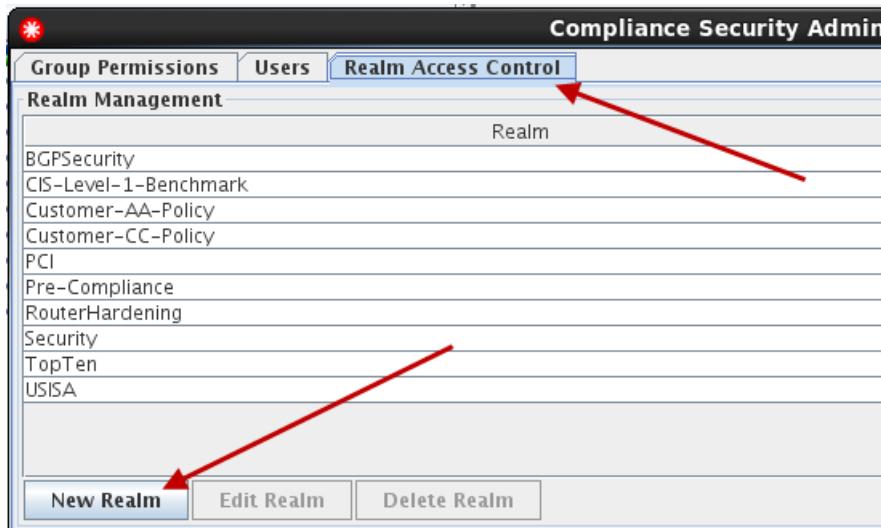


6. Create a new top-level realm named **Training_Realm**. Allow the **administrator**, **operations**, and **engineering** groups to access the new realm.

- a. Click **Admin > User Security Options**.



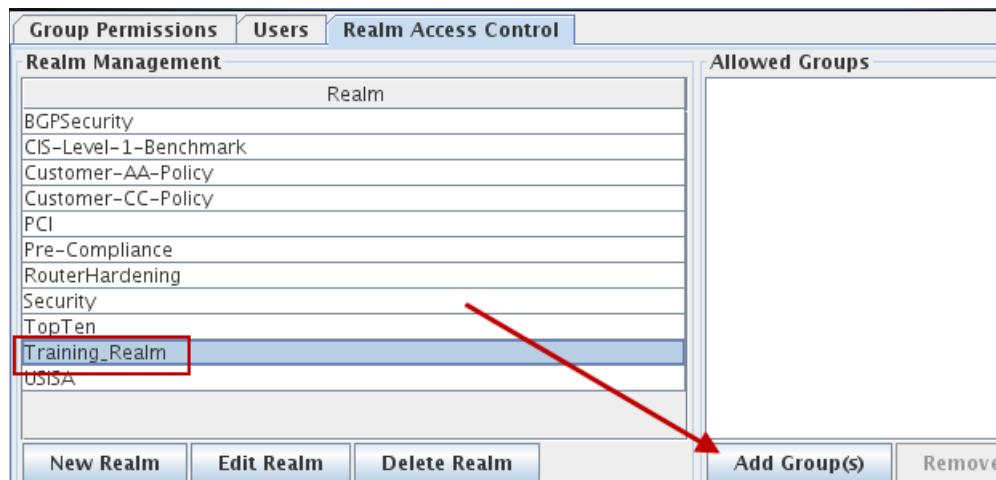
- b. Click the **Realm Access Control** tab. Click **New Realm**.



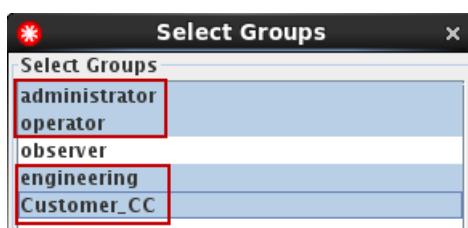
- c. Enter **Training_Realm** as the name of the new realm. Click **OK**.



- d. Select the **Training_Realm** and click **Add Group(s)**.



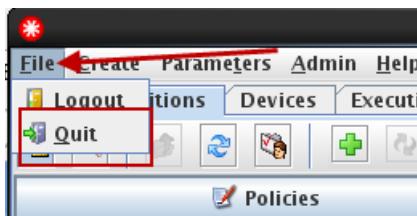
- e. Use Ctrl + click to select the **administrator**, **operator**, **engineering**, and **Customer_CC** groups. Click **Add**.



f. Click **Close**.

7. Close the *compliance manager* user interface. Log back in with the user name **engineer** and the password **object00**.

a. Click **File > Quit**.



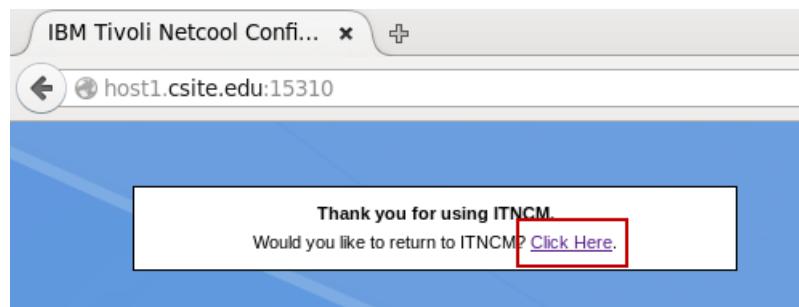
b. Click **Yes** to confirm.



c. Return to the Firefox browser. Click **Logoff**.



d. Select **Click Here**.



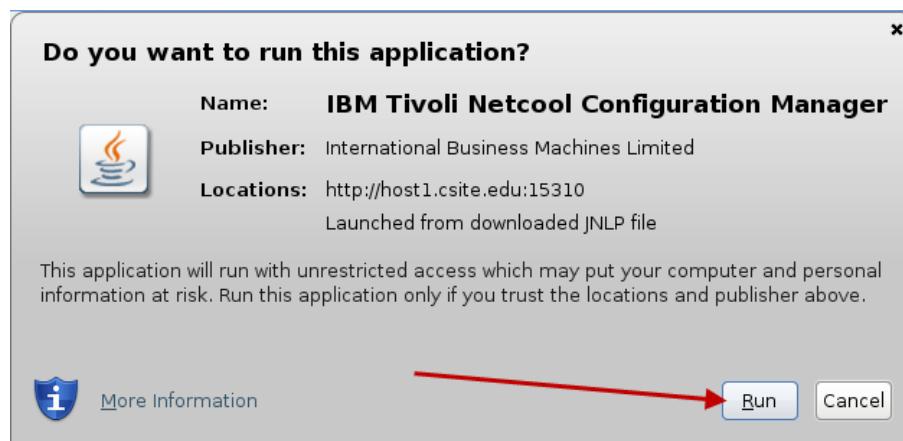
e. Enter the user name **engineer** and the password **object00**. Click **Login**.



f. Click **ITNCM Compliance**.



g. Click **Run**.



Exercise 2 Creating definitions

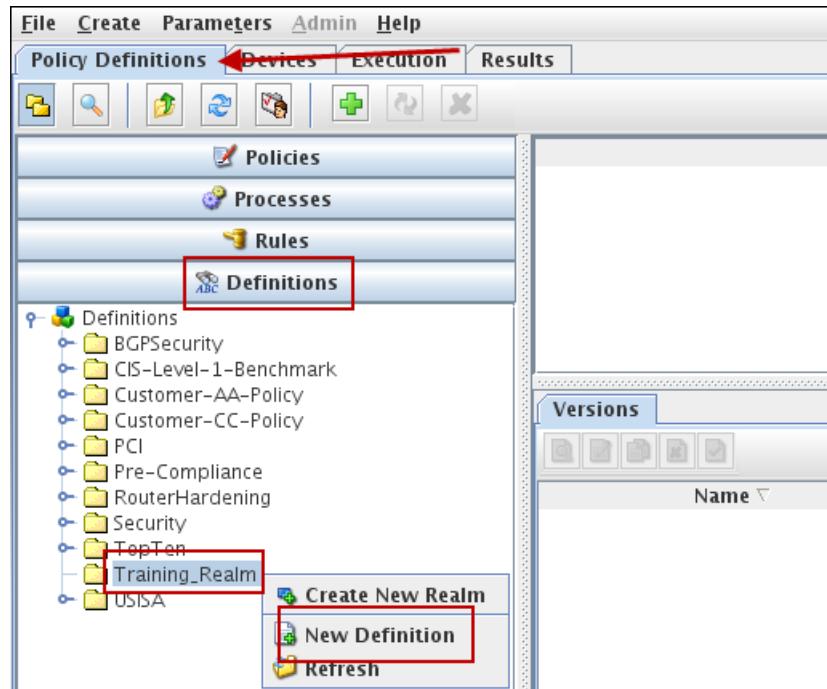
In this exercise, you create three definitions.

1. Create a definition in the Training_Realm named **check for service nagle**. This definition searches for the configuration command **service nagle**. If the command is not found, the definition returns the result *fail*. Use the following values to complete the wizard.

Field	Value
Name	Check for service nagle
Description	This definition looks for the following command: ^service nagle
	The service nagle command is found in the global configuration of Cisco routers that run IOS version 10.0 and higher.
Select Definition Type	Create Compliance Definition using CLI configuration lines
Enter lines that you want to match	^service nagle
Match Criteria	Match All
Evaluation result if context not found	Fail
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Definition** section. Right-click **Training_Realm** and click **New Definition**.

The **Create a Definition** wizard starts.



- b. Enter **check for service nagle** in the **Name** field. Enter the description from the preceding table. Select **Create Compliance Definition using CLI configuration lines**. Click **Next**.

Enter Definition Details

Definition Name & Description

Name: **Revision:**

Description: This definition looks for the following command:
^service nagle

The service nagle command is found in the global configuration of Cisco routers running IOS version 10.0 and higher

Select Definition Type

Create Compliance Definition using CLI configuration lines

Create Compliance Definition using Native Commands

- c. Type **^service nagle** in the **Enter lines you want to match** field. Select **Match All** in the **Match Criteria** field. Select **Fail** in the **Evaluation result if context not found** field. Click **Add**.

Evaluations

Enter line(s) to you want to match:

Parameters(Optional): Local Parameter

Match Criteria: Number:

Evaluation result if context not found:

Regex Tool

Evaluation List: Evaluation List Criteria: Match All

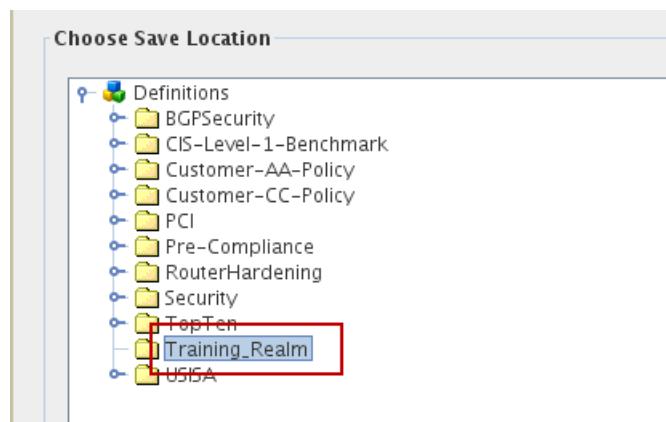
Evaluation	Match Crit...	Match Cri...	Default R...
^service nagle	Match All		Fail

The evaluation is added to the evaluation list at the bottom of the window.

- d. Click **Next**.

Evaluation List:		Evaluation List Criteria: Match All		
Evaluation	Match Crit...	Match Cri...	Default R...	
^service nagle	Match All			Fail

- e. Click **Training_Realm**. Click **Finish**.

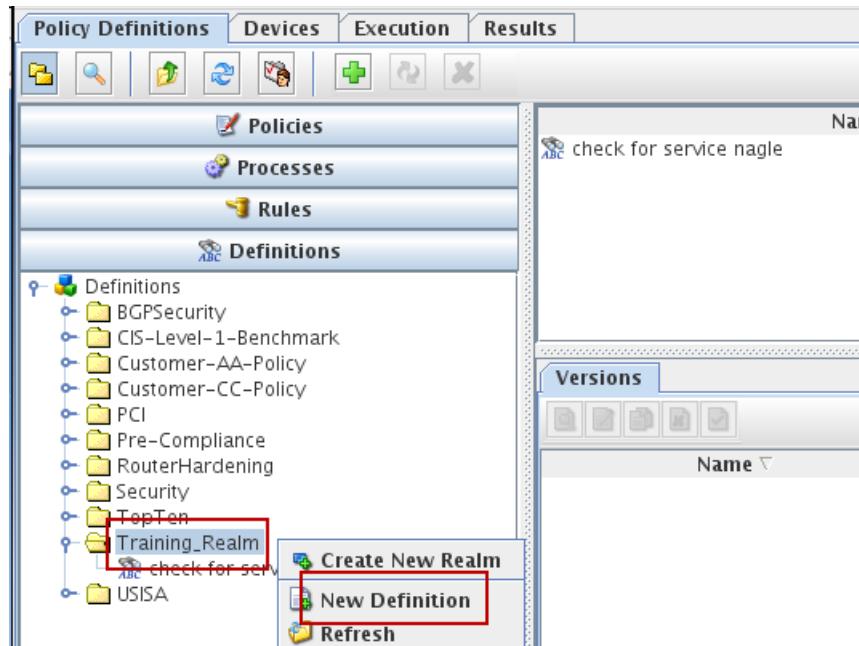


2. Create a definition in the **Training_Realm** named **check for service compress-config**. This definition searches for the configuration command **service compress-config**. If the command is not found, the definition returns the result **fail**. Use the following values to complete the wizard.

Field	Value
Name	Check for service compress-config
Description	This definition looks for the following command: ^service compress-config
	The service compress-config command is found in the global configuration of Cisco routers that run IOS version 10.0 and higher.
Select Definition Type	Create Compliance Definition using CLI configuration lines
Enter lines you want to match	^service compress-config
Match Criteria	Match All
Evaluation result if context not found	Fail
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Definition** section. Right-click **Training_Realm** and click **New Definition**.

The Create a Definition wizard starts.



- b. Enter **check for service compress-config** in the **Name** field. Enter the description from the preceding table. Select **Create Compliance Definition using CLI configuration lines**. Click **Next**.

Enter Definition Details

Definition Name & Description

Name:	check for service compress-config	Revision:	1
Description:	This definition looks for the following command: <code>^service compress-config</code> The service compress-config command is found in the global configuration of Cisco routers running IOS version 10.0 and higher.		

Select Definition Type

<input checked="" type="radio"/> Create Compliance Definition using CLI configuration lines
<input type="radio"/> Create Compliance Definition using Native Commands

- c. Type **^service compress-config** in the **Enter lines you want to match** field. Select **Match All** in the **Match Criteria** field. Select **Fail** in the **Evaluation result if context not found** field. Click **Add**.

Evaluations

Enter line(s) to you want to match: Parameters(Optional): Local Parameter ▼ Insert Par
^service compress-config

Match Criteria: Match All ▼ Number: Regex Tool Add Update

Evaluation result if context not found: Fail

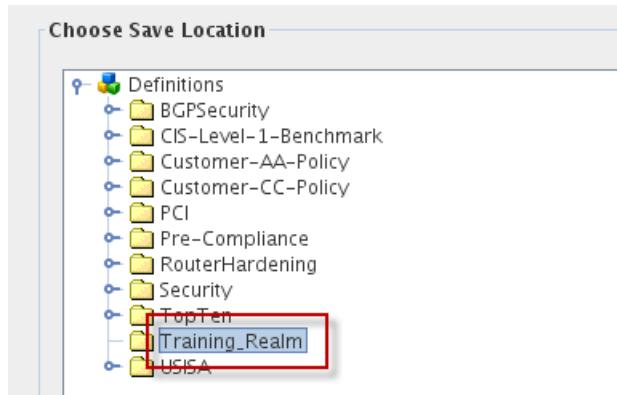
Evaluation List: Evaluation List Criteria: Match All ▼ Number:
Evaluation Match Crit... Match Cri... Default R...

- d. The evaluation is added to the evaluation list at the bottom of the window. Click **Next**.

Evaluation result if context not found: Fail

Evaluation List: Evaluation List Criteria: Match All ▼ Number:
Evaluation Match Crit... Match Cri... Default R...
^service compress-config Match All Fail

- e. Click **Training_Realm**. Click **Finish**.



3. Create a definition in the Training_Realm named **check for process-max-time**. Use a local parameter for the time in milliseconds with the default value of **100**. Name the parameter **PROCESS-MAX-TIME-MILLISECONDS**.

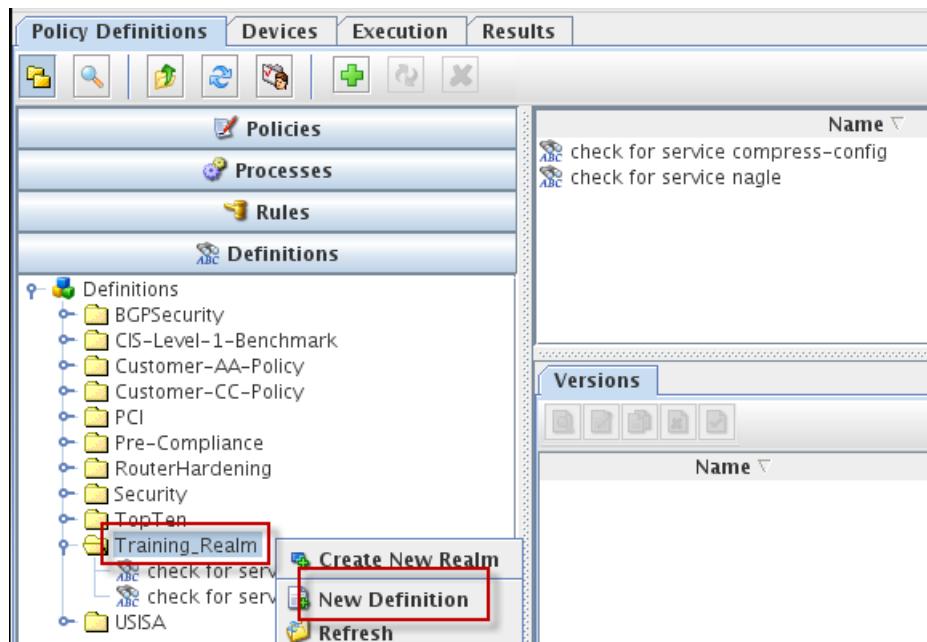
The goal of this definition is to search for the command **process-max-time 100**. If the command is not found, the definition returns the result *fail*. Use the following values to complete the wizard.

Field	Value
Name	check for process-max-time
Description	This definition looks for the following command: <code>^process-max-time \${PROCESS-MAX-TIME-MILLISECONDS=100}</code>
	The process-max-time command is found in the global configuration of Cisco routers that run IOS version 12.1 and higher. PROCESS-MAX-TIME-MILLISECONDS is a local parameter of the maximum process time.
Select Definition Type	Create Compliance Definition using CLI configuration lines
Enter lines you want to match	<code>^process-max-time \${PROCESS-MAX-TIME-MILLISECONDS=100}</code>
Match Criteria	Match All
Evaluation result if context not found	Fail
Choose Save Location	Training_Realm

Exercise 2 Creating definitions

- Click the **Policy Definitions** tab. Click the **Definition** section. Right-click **Training_Realm** and click **New Definition**.

The Create a Definition wizard starts.



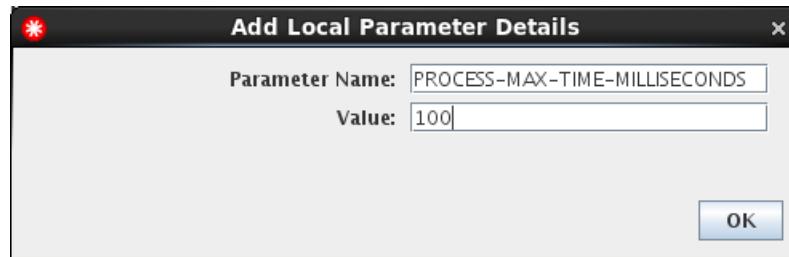
- Enter **check for process-max-time** in the **Name** field. Enter the description from the preceding table. Click **Create Compliance Definition using CLI configuration lines**. Click **Next**.

Definition Name & Description	
Name:	<input type="text" value="check for process-max-time"/>
Description:	<input type="text" value="^process-max-time \${PROCESS-MAX-TIME-MILLISECONDS=100}"/> <p>The process-max-time command is found in the global configuration of Cisco routers running IOS version 12.1 and higher. PROCESS-MAX-TIME-MILLISECONDS is a local parameter of the maximum process time.</p>
Select Definition Type	
<input checked="" type="radio"/> Create Compliance Definition using CLI configuration lines	

- Type **^process-max-time** in the **Enter lines you want to match** field. Add a space after the command. Select **Local Parameter** and click **Insert Parameter**.

Evaluations	
Enter line(s) to you want to match: Parameters(Optional): <input type="text" value="^process-max-time"/> Local Parameter <input type="button" value="▼"/>	
space on end	

- d. Enter **PROCESS-MAX-TIME-MILLISECONDS** in the **Parameter Name** field. Enter **100** in the **Value** field. Click **OK**.



- e. Select **Match All** in the **Match Criteria** field. Select **Fail** in the **Evaluation result if context not found** field. Click **Add**.

The screenshot shows the "Evaluations" configuration window. At the top, there's a search bar with the regex pattern "^process-max-time \${PROCESS-MAX-TIME-MILLISECONDS=100}". Below it are two dropdowns: "Match Criteria" set to "Match All" and "Evaluation result if context not found" set to "Fail". A red arrow points to the "Add" button. Below these are sections for "Evaluation List" and "Evaluation List Criteria". The evaluation list table has one row: "Evaluation" with "Match Crit..." and "Match Cri..." columns both showing "Match All" and the "Default R..." column showing "Fail".

The evaluation is added to the evaluation list at the bottom of the window.

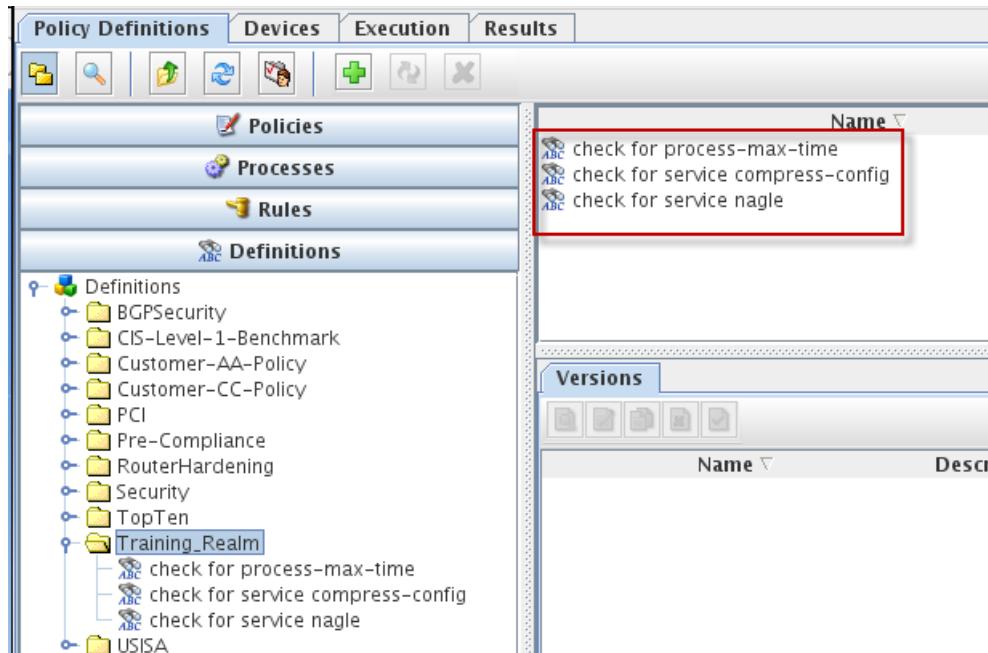
- f. Click **Next**.

The screenshot shows the "Evaluation List" table from the previous window. A single row is selected and highlighted with a red box. The row contains the regex pattern "^process-max-time \${PROCESS-MAX-TIME-MILLISECONDS=100}" and evaluation criteria "Match All" and "Fail".

- g. Click **Training_Realm**. Click **Finish**.

The screenshot shows the "Choose Save Location" dialog box. It displays a tree view of policy definitions under a root node "Definitions". The nodes include "BGPSecurity", "CIS-Level-1-Benchmark", "Customer-AA-Policy", "Customer-CC-Policy", "PCI", "Pre-Compliance", "RouterHardening", "Security", "TopTen", and "USISA". A folder named "Training_Realm" is selected and highlighted with a red box.

The Training_Realm contains three definitions.



Exercise 3 Creating rules

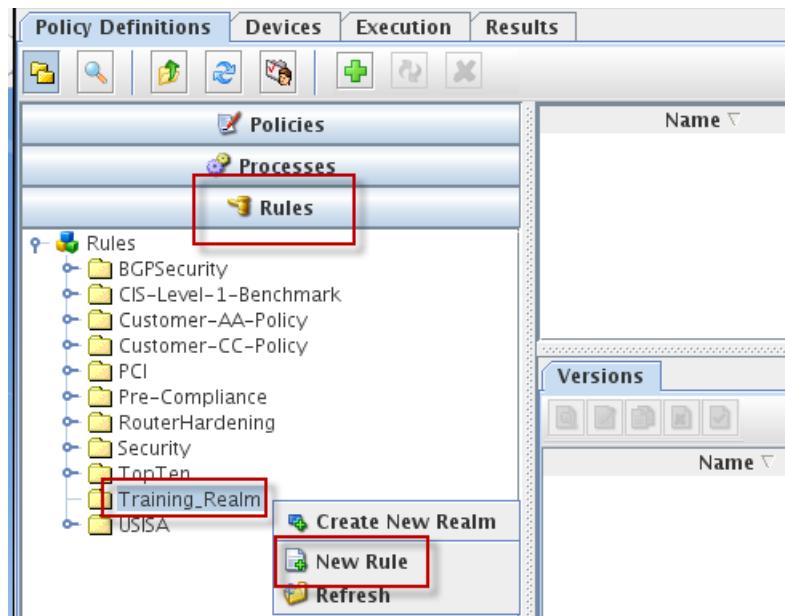
In this exercise, you create three rules. These rules use the definitions that you created in the preceding exercise.

1. Create a rule in the Training_Realm named **enable service nagle**. Configure this rule to determine that the device is compliant if the command service nagle is present. If the command is not present in the device configuration, configure the rule to determine that the device is not compliant. Use the following values to complete the wizard.

Field	Value
Name	enable service nagle
Description	This rule determines that a device configuration is compliant if the command service nagle is present.
Application Device Filter	Use these values. <ul style="list-style-type: none"> • Vendor: Cisco • Type: Router • Model: * • OS: Choose the advanced OS options. Configure the rule to use operating systems >=10.0

Field	Value
Build Graphical Rule	<p>Use the following objects in this graphical rule.</p> <ul style="list-style-type: none">• Add one Start icon.• Add one Definition icon. Use the check for service nagle definition. Link the Start icon to the Definition icon.• Add one Compliant icon to use if the definition is true. Link the T side of the Definition to the Compliant icon.• Add one Non Compliant icon to use if the definition is false. Configure no action if the device is not compliant. Link the F side of the Definition to the Non Compliant icon.
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Rules** section. Right-click **Training_Realm** and click **New Rule**. The Create a Rule wizard starts.



- b. Enter **enable service nagle** in the **Name** field. Enter the description from the preceding table. Select **Cisco** as the vendor. Select **Router** as the type. Select ***** as the model. Click the **OS** field and select **Advanced**. The advanced selection window opens.

Rule Name & Description

Name:	enable service nagle	Revision:	1
Description:	This rule determines that a device configuration is compliant if the command se nagle is present.		

Applicable Device Filter

Vendor	Type	Model	OS
Cisco	Router	*	*

Advanced

- c. Click the **>=** option. Enter **10.0** in the **>=** field. Click **OK**.

OS Advanced

Choose OS Filter

>= 10.0

<=

Range Fr... To

- d. Click **Next**.

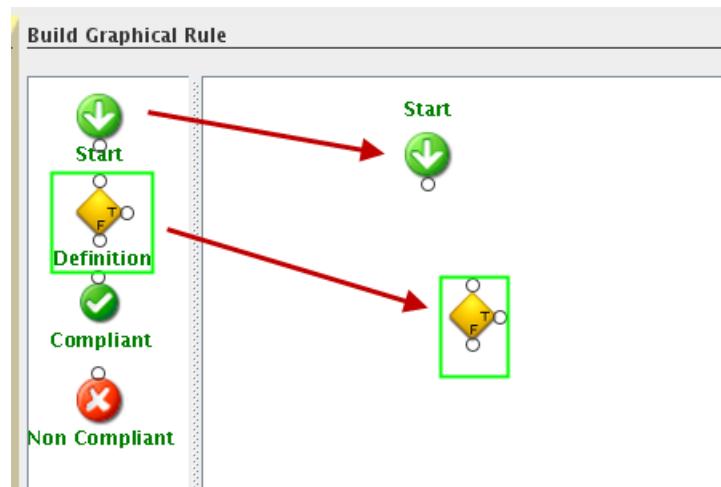
Rule Name & Description

Name:	enable service nagle	Revision:	1
Description:	This rule determines that a device configuration is compliant if the command se nagle is present.		

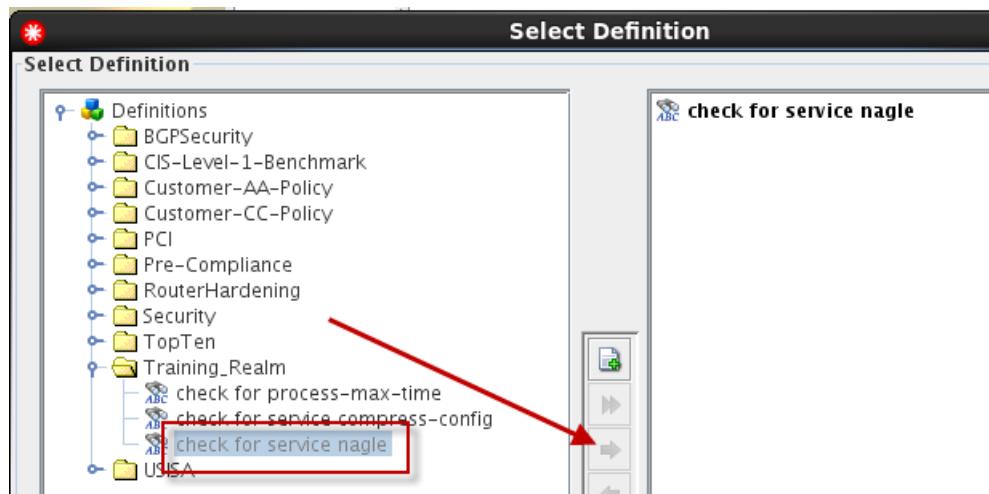
Applicable Device Filter

Vendor	Type	Model	OS
Cisco	Router	*	Advanced

- e. Drag the **Start** icon into the rule. Drag the **Definition** icon into the rule. When you drop the **Definition** icon, the Select Definition window opens.

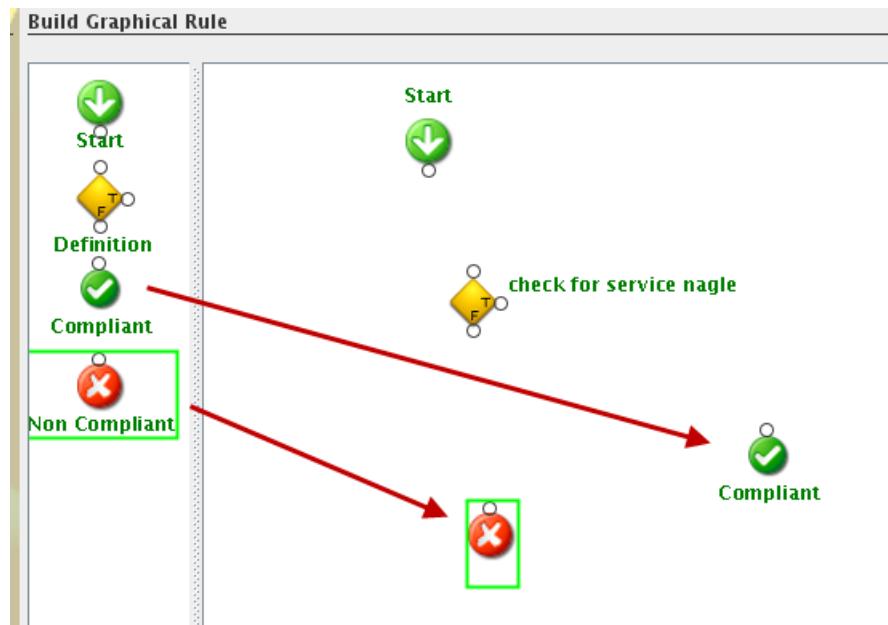


- f. Expand **Training_Realm**. Click the **Training_Realm > check for service nagle** definition. Click the right arrow icon to move the definition to the right of the window. Click **OK**.

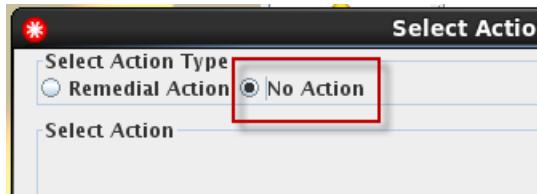


- g. Drag the **Compliant** icon into the rule. Drag the **Non Compliant** icon into the rule.

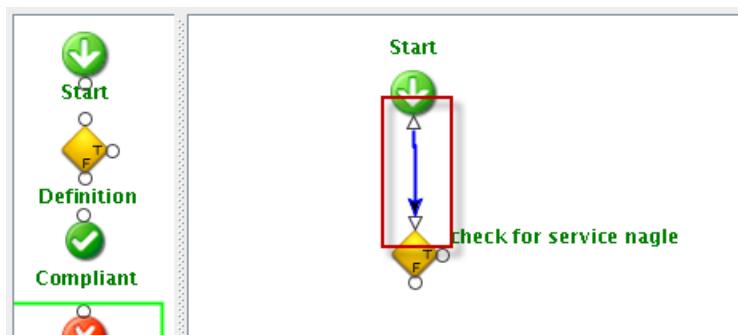
When you drop the **Non Compliant** icon, the Select Action Type window opens.



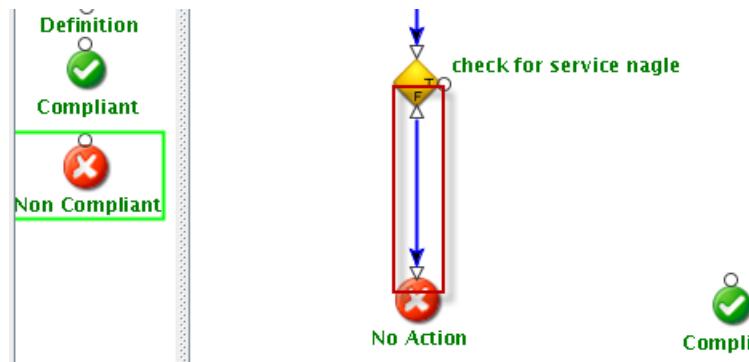
- h. Select **No Action**. Click **OK**.



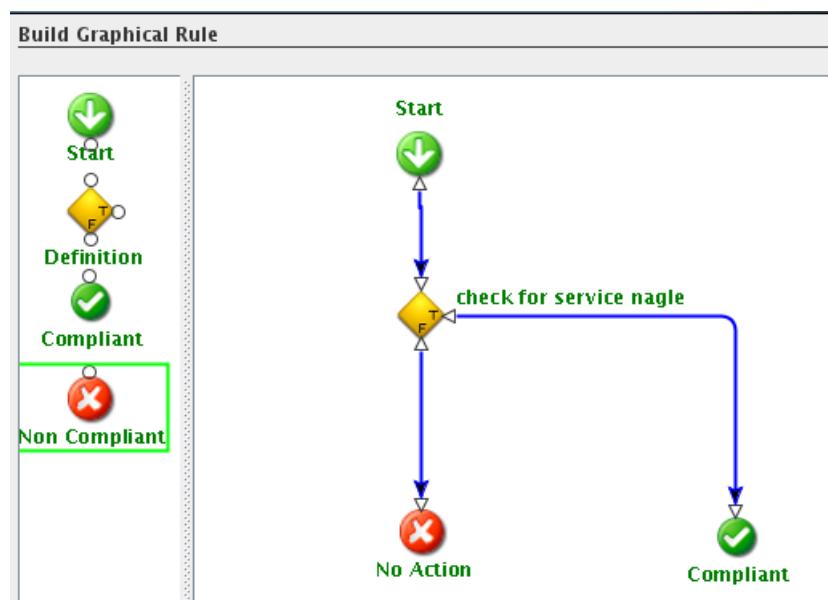
- i. Add a line from the **Start** icon to the **Definition** icon by dragging your cursor from one icon to the other.



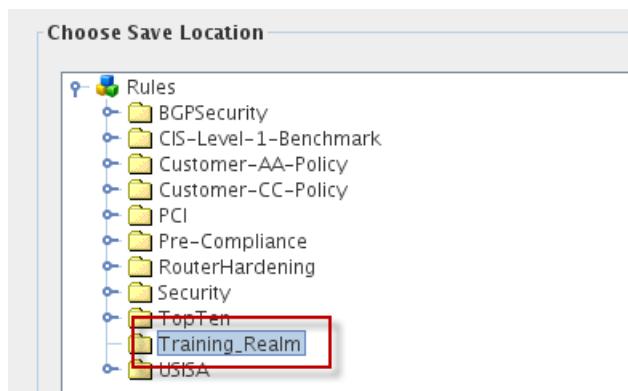
- j. Add a line from the **F** in the **Definition** icon to the **Non Compliant** icon.



- k. Add a line from the **T** in the **Definition** icon to the **Compliant** icon. Click **Next**.



- l. Click **Training_Realm**. Click **Finish**.

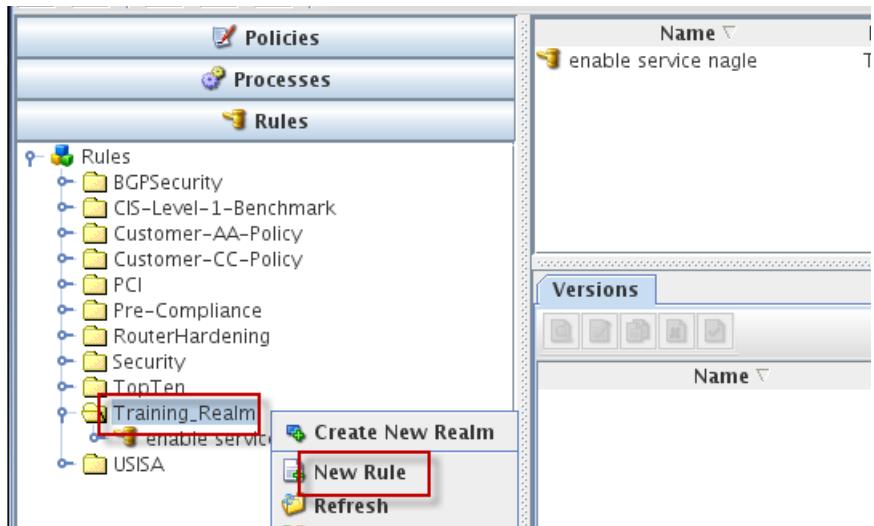


2. Create a rule in the **Training_Realm** named **disable service compress-config**. Configure this rule to determine that the device is not compliant if the command `service compress-config` is present. If the command is not present in the device configuration, the rule should determine that the device is compliant. This behavior is the opposite of the previous rule. Use the following values to complete the wizard.

Field	Value
Name	disable service compress-config
Description	This rule determines that a device configuration is not compliant if the command service compress-config is present.
Application Device Filter	<p>Use these values.</p> <ul style="list-style-type: none"> • Vendor: Cisco • Type: Router • Model: * • OS: Choose the advanced OS options. Configure the rule to use operating systems >=10.0
Build Graphical Rule	<p>Use the following objects in this graphical rule.</p> <ul style="list-style-type: none"> • Add one Start icon. • Add one Definition icon. Use the check for service compress-config definition. Link the Start icon to the Definition icon. • Add one Compliant icon to use if the definition is false. Link the F side of the Definition to the Compliant icon. • Add one Non Compliant icon to use if the definition is true. Configure no action if the device is not compliant. Link the T side of the Definition to the Non Compliant icon.
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Rules** section. Right-click **Training_Realm** and click **New Rule**.

The Create a Rule wizard starts.



- b. Enter **disable service compress-config** in the **Name** field. Enter the description from the preceding table. Select **Cisco** as the vendor. Select **Router** as the type. Select the asterisk (*) as the model. Click the **OS** field and select **Advanced**.

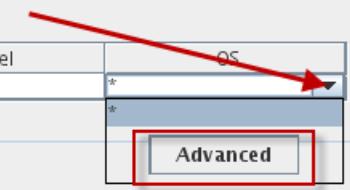
The advanced selection window opens.

Rule Name & Description

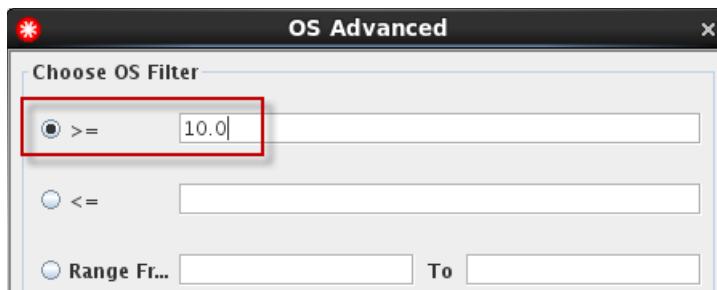
Name:	disable service compress-config	Revision:	1
Description:	This rule determines that a device configuration is not compliant if the command service compress-config is present.		

Applicable Device Filter

Vendor	Type	Model	OS
Cisco	Router	*	Advanced



- c. Click the **>=** option. Enter **10.0** in the **>=** field. Click **OK**.



- d. Click **Next**.

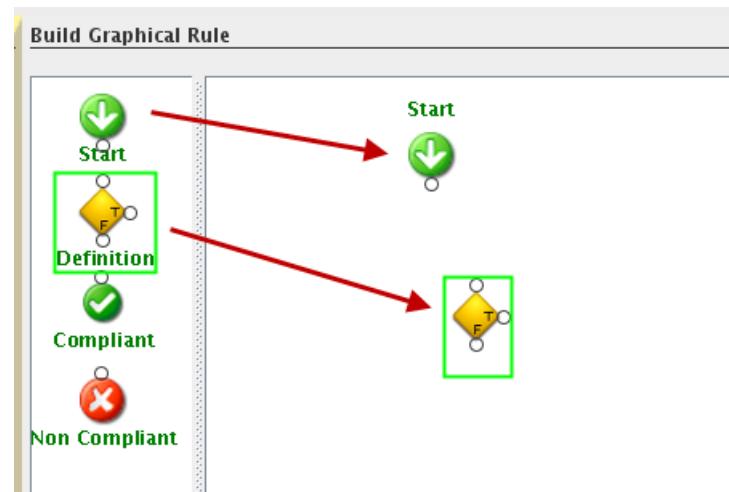
Rule Name & Description

Name:	disable service compress-config	Revision:	1
Description:	This rule determines that a device configuration is not compliant if the command service compress-config is present.		

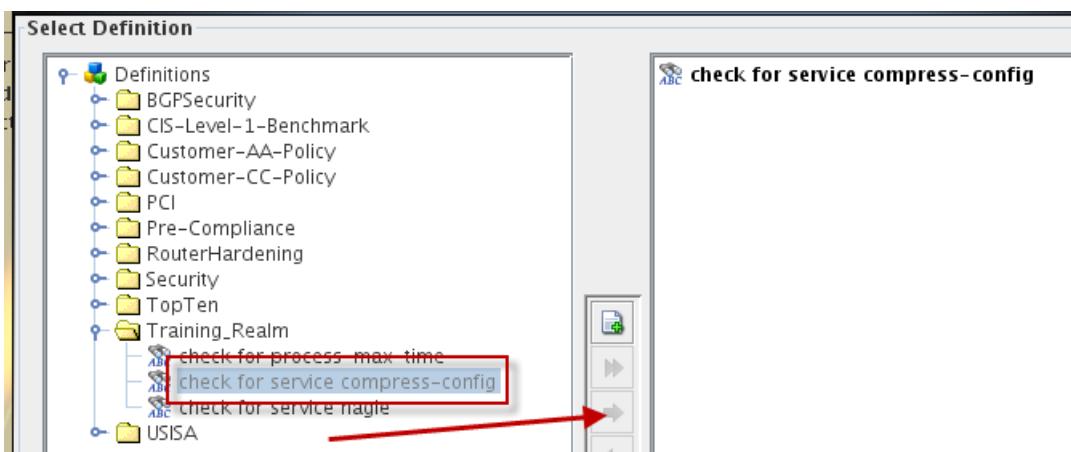
Applicable Device Filter

Vendor	Type	Model	OS
Cisco	Router	*	Advanced

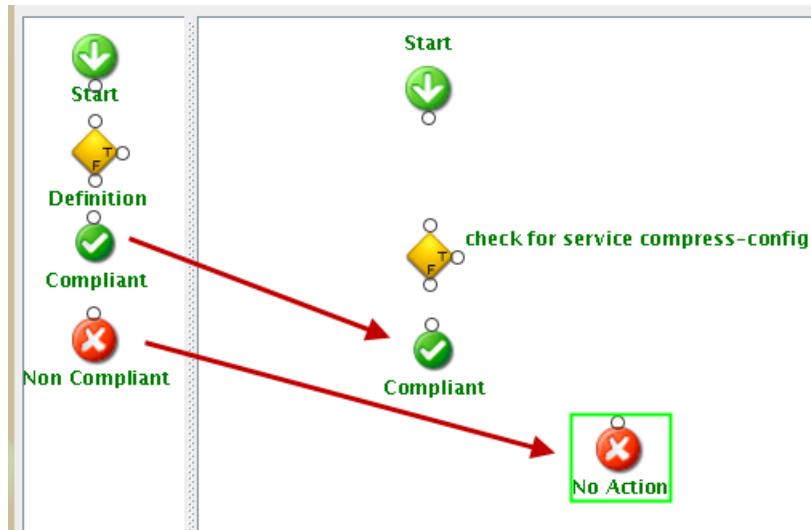
- e. Drag the **Start** icon into the rule. Drag the **Definition** icon into the rule. When you drop the **Definition** icon, the Select Definition window opens.



- f. Expand **Training_ Realm**. Click the **Training_ Realm > check for service compress-config** definition. Click the right arrow icon to move the definition to the right of the window. Click **OK**.

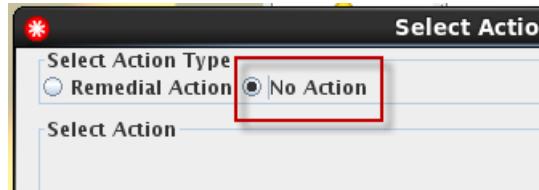


- g. Drag the **Compliant** icon into the rule. Drag the **Non Compliant** icon into the rule. When you drop the **Non Compliant** icon, the Select Action Type window opens.



Important: Pay attention to the location of these icons.

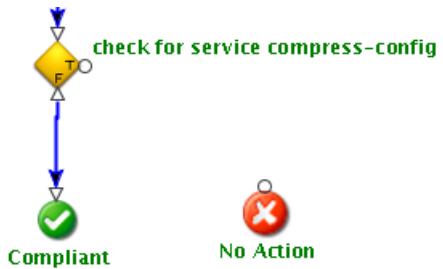
- h. Select **No Action**. Click **OK**.



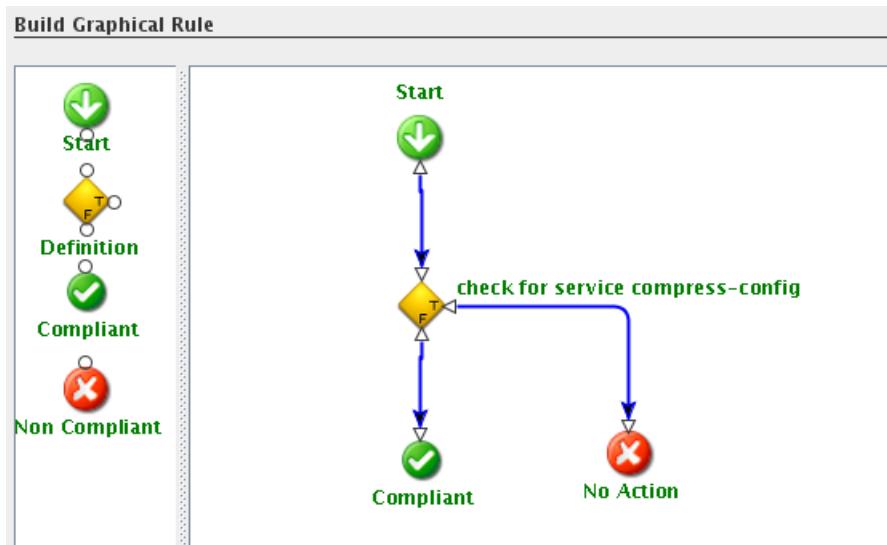
- i. Add a line from the **Start** icon to the **Definition** icon by dragging your cursor from one icon to the other.



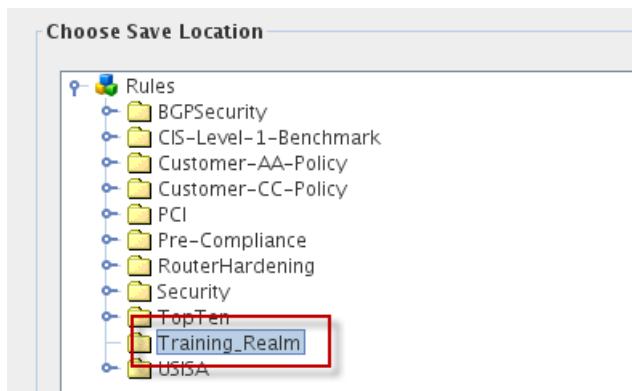
- j. Add a line from the **F** in the **Definition** icon to the **Compliant** icon.



- k. Add a line from the **T** in the **Definition** icon to the **Non Compliant** icon. Click **Next**.



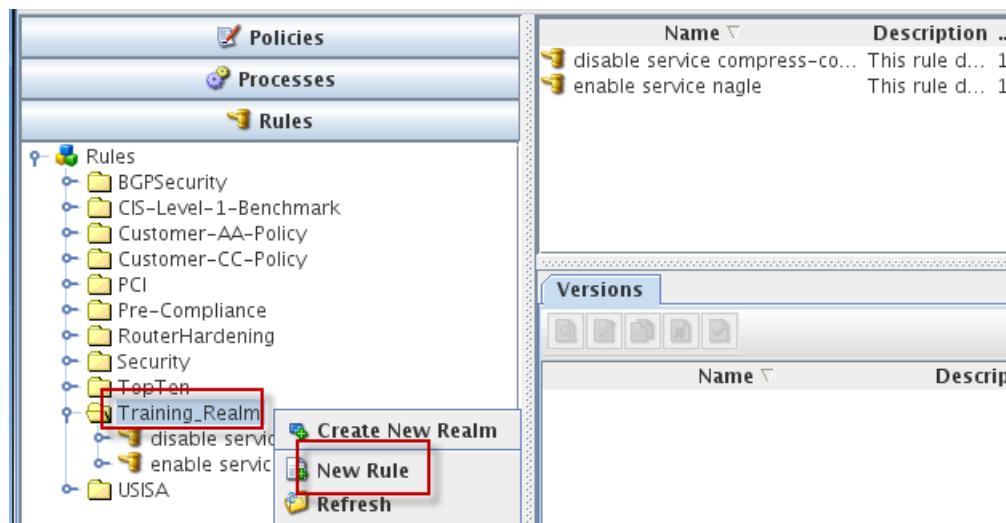
- l. Click **Training_Realm**. Click **Finish**.



3. Create a rule in the **Training_Realm** named **enable process-max-time**. Configure this rule to determine that the device is compliant if the command **process-max-time 100** is present. If the command is not present in the device configuration, the rule should determine that the device is not compliant. Use the following values to complete the wizard.

Field	Value
Name	enable process-max-time
Description	This rule determines that a device configuration is compliant if the command process-max-time is present and set to a defined number of milliseconds.
Application Device Filter	<p>Use these values.</p> <ul style="list-style-type: none"> • Vendor: Cisco • Type: Router • Model: * • OS: Choose the advanced OS options. Configure the rule to use operating systems >=12.1
Build Graphical Rule	<p>Use the following objects in this graphical rule.</p> <ul style="list-style-type: none"> • Add one Start icon. • Add one Definition icon. Use the check for process-max-time definition. Link the Start icon to the Definition icon. • Add one Compliant icon to use if the definition is true. Link the T side of the Definition to the Compliant icon. • Add one Non Compliant icon to use if the definition is false. There should be no action if the device is not compliant. Link the F side of the Definition to the Non Compliant icon.
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Rules** section. Right-click **Training_Realm** and click **New Rule**. The Create a Rule wizard starts.



- b. Enter **enable process-max-time** in the **Name** field. Enter the description from the preceding table. Select **Cisco** as the vendor. Select **Router** as the type. Select the asterisk

(*) as the Model. Click the **OS** field and select **Advanced**. The advanced selection window opens.

Enter Rule Details...

Rule Name & Description

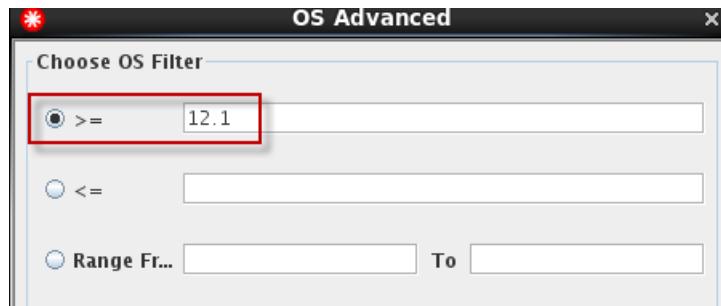
Name: enable process-max-time Revision: 1

Description: This rule determines that a device configuration is compliant if the command process-max-time is present and set to a defined number of milliseconds.

Applicable Device Filter

Vendor	Type	Model	OS
Cisco	Router	*	<input type="button" value="Advanced"/>

c. Click the **>=** option. Enter **12.1** in the **>=** field. Click **OK**.



d. Click **Next**.

Rule Name & Description

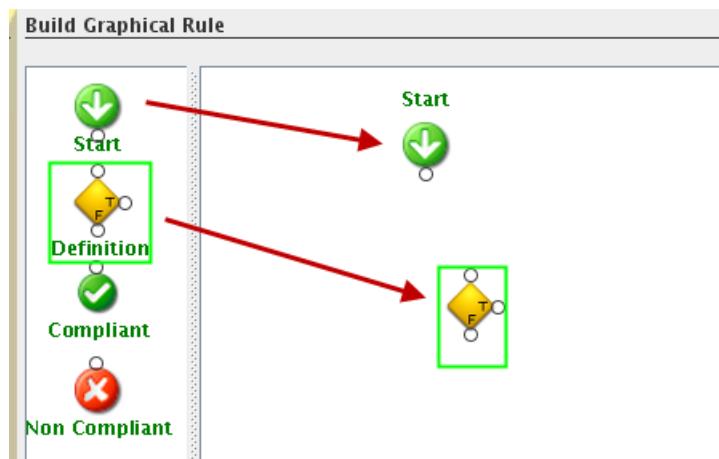
Name: enable process-max-time Revision: 1

Description: This rule determines that a device configuration is compliant if the command process-max-time is present and set to a defined number of milliseconds.

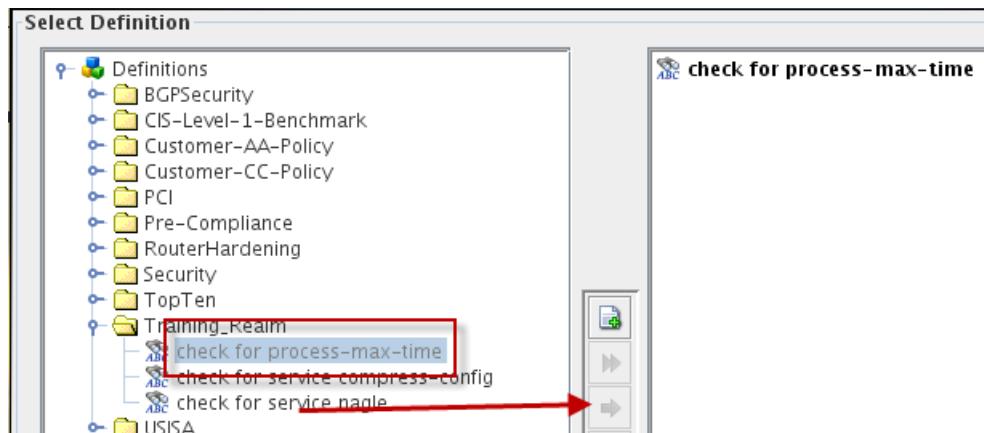
Applicable Device Filter

Vendor	Type	Model	OS
Cisco	Router	*	Advanced

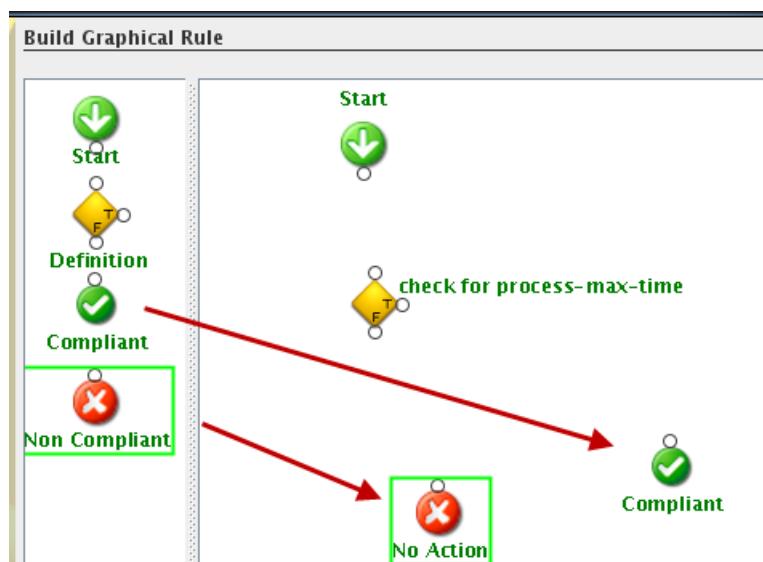
- e. Drag the **Start** icon into the rule. Drag the **Definition** icon into the rule. When you drop the **Definition** icon, the Select Definition window opens.



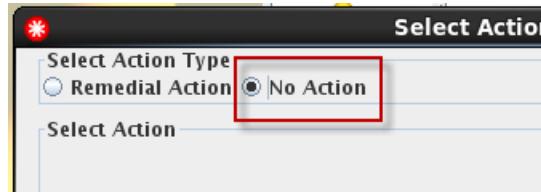
- f. Expand **Training_Realm**. Click the **Training_Realm > check for process-max-time** definition. Click the right arrow icon to move the definition to the right of the window. Click **OK**.



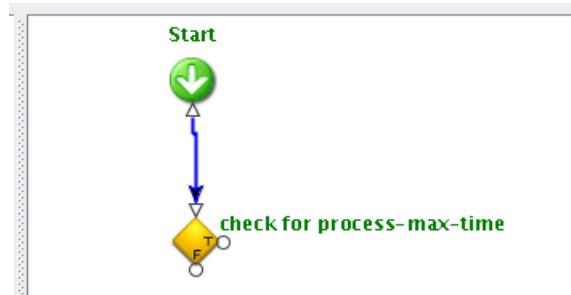
- g. Drag the **Compliant** icon into the rule. Drag the **Non Compliant** icon into the rule. When you drop the **Non Compliant** icon, the Select Action Type window opens.



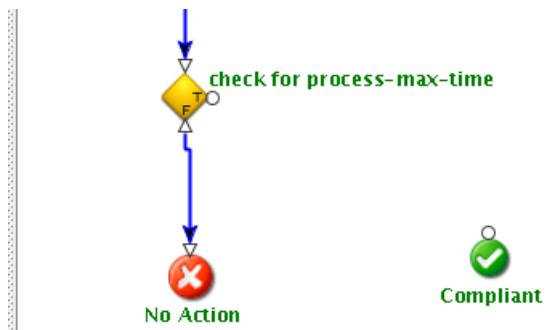
- h. Select **No Action**. Click **OK**.



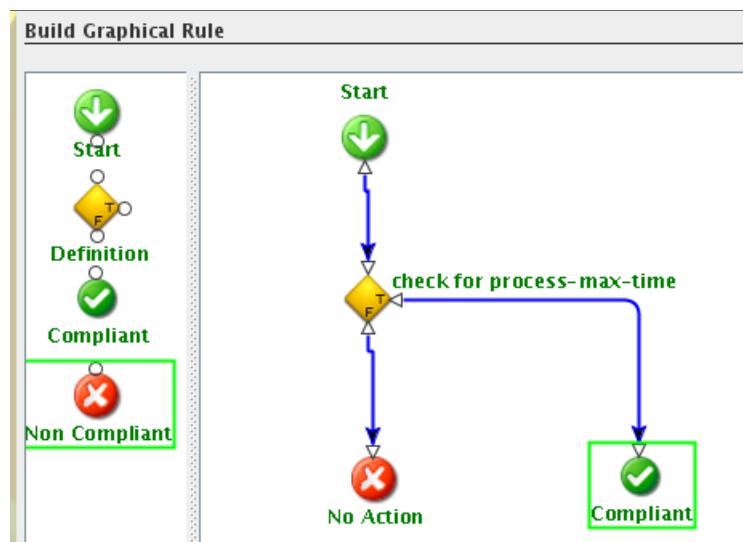
- i. Add a line from the **Start** icon to the **Definition** icon by dragging your cursor from one icon to the other.



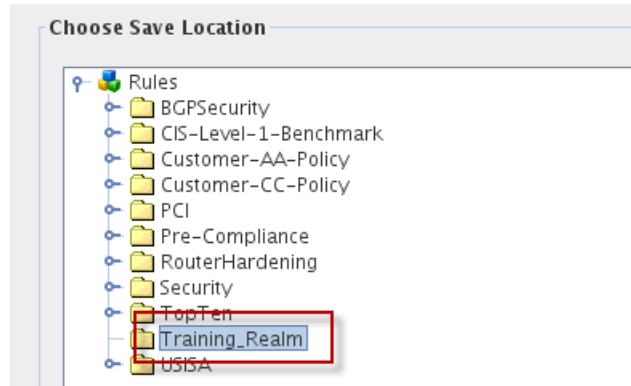
- j. Add a line from the **F** in the **Definition** icon to the **Non Compliant** icon.



- k. Add a line from the **T** in the **Definition** icon to the **Compliant** icon. Click **Next**.



I. Click **Training_Realm**. Click **Finish**.



The Training_Realm contains three rules.

Exercise 4 Creating an email action

In this exercise, you create an email action. You use this email action in the next exercise.

- Create an email action in Training_Realm named **email to training NOC**. Use the following values to complete the wizard.

Field	Value
Name	email to training NOC
Description	This action sends an email notification to the network operations center if a managed device is not compliant.
Action Type	E-mail Template
E-mail Header	Use the following settings in this email action. <ul style="list-style-type: none"> To: noc@training.ibm.com Subject: Alert: Managed Device Non Compliant
E-mail Body	One or more managed devices are not compliant. Log on to Netcool Configuration Manager or Compliance Manager to resolve this problem.
Choose Save Location	Training_Realm

- Click the **Policy Definitions** tab. Click the **Email Actions** section. Right-click **Training_Realm** and click **New Action**. The Create an Action wizard starts.



- b. Enter **email to training NOC** in the **Name** field. Enter the description from the preceding table. Select **email Template** as the **Action Type**. Click **Next**.

Choose An Action

Action Name & Description

Name: * **Revision:**

Description: This action sends an email notification to the network operations center if a managed device is not compliant.

Action Type

E-Mail Template

- c. Enter **noc@training.ibm.com** in the **To** field. Enter **Alert: Managed Device Non Compliant** in the **Subject** field. Enter the body text from the preceding table. Click **Next**.

E-mail Header

To:

Cc:

Bcc:

Subject:

E-mail Body

One or more managed devices are not compliant. Log on to Netcool Configuration Manager or Complia

- d. Click **Training_Realm**. Click **Finish**.

Choose Save Location

Email Actions

- ↳ Email Actions
- ↳ BGPSecurity
- ↳ CIS-Level-1-Benchmark
- ↳ Customer-AA-Policy
- ↳ Customer-CC-Policy
- ↳ PCI
- ↳ Pre-Compliance
- ↳ RouterHardening
- ↳ Security
- ↳ TopTen
- ↳ Training_Realm
- ↳ USISA

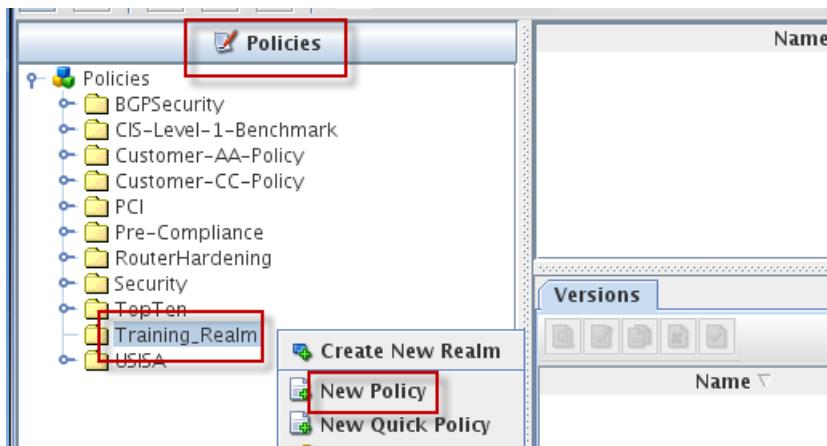
Exercise 5 Creating policies

In this exercise, you create three policies. These policies use the rules that you created in a previous exercise.

1. Create a policy in the Training_Realm named **enable service nagle**. Configure this policy to use the rule **enable service nagle**. Use the following values to complete the wizard.

Field	Value
Name	enable service nagle
Description	Service nagle should be enabled on all remotely managed devices. This policy enables the service if it is not present.
Severity	4
Weight	30
Send Trap	Configure this policy to send a trap.
Applicable Device Filter	Use the following settings in this policy <ul style="list-style-type: none"> • Vendor: * • Type: * • Model: * • OS: *
Rules Included	enable service nagle
Action Type	EMail
Action	email to training NOC
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Policies** section. Right-click **Training_Realm** and click **New Policy**. The Create a Policy wizard starts.



- b. Enter **enable service nagle** in the **Name** field. Enter the description from the preceding table. Select **Severity 4**. Enter **30** in the **Weight** field.

Policy Name, Description & Severity

Name:	enable service nagle	Revision ...
Description:	Service nagle should be enabled on all remotely managed devices. This policy enables the service if it is not present.	
Impact:		
Severity:	4	Weight: 30
		<input checked="" type="checkbox"/> Send Trap <input checked="" type="checkbox"/> Preemptive

- c. Leave the asterisk (*) in the **Vendor**, **Type**, **Model**, and **OS** fields. Click the **Training_Realm** > **enable service nagle** rule. Click the right arrow icon to move the rule to the right of the window. Click **Next**.

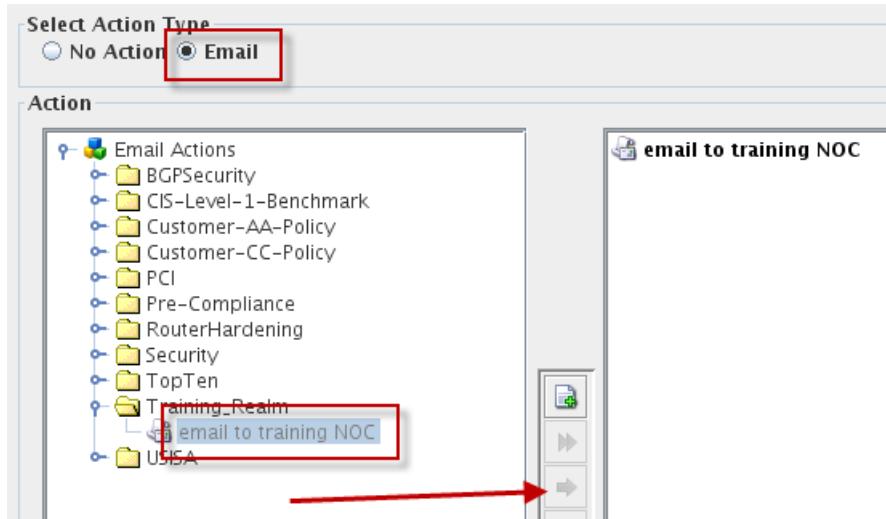
Applicable Device Filter

Vendor	Type	Model	OS
*	*	*	*

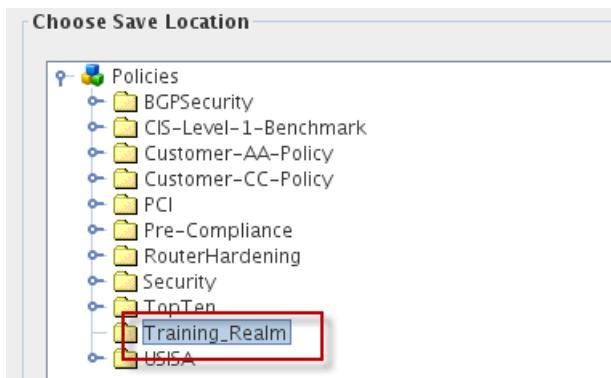
Rules Included

The screenshot shows the 'Rules Included' section of a policy configuration tool. On the left, there's a tree view of policy categories like Customer-CC-Policy, PCI, Pre-Compliance, RouterHardening, Security, TopTen, Training_Realm, and USBA. Under 'Training_Realm', three rules are listed: 'disable service compress-config', 'enable process max-time', and 'enable service nagle'. A red arrow points from the 'enable service nagle' rule in the tree to a right-hand pane where it is currently listed. The right-hand pane also contains icons for creating new rules and moving them between panes.

- d. Select **email** as the **Action Type**. Click the **Training_Realm > email to training NOC** email action. Click the right arrow icon to move the email action to the right of the window. Click **Next**.



- e. Click **Training_Realm**. Click **Finish**.

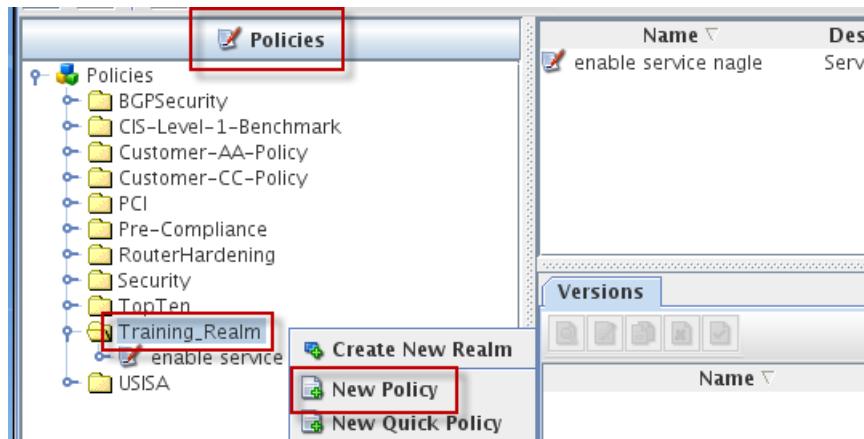


2. Create a policy in the **Training_Realm** named **disable service compress-config**. Configure this policy to use the rule **disable service compress-config**. Use the following values to complete the wizard.

Field	Value
Name	disable service compress-config
Description	Service compress-config should be disabled on all devices. This policy disables the service if it is present.
Severity	3
Weight	45
Send Trap	Configure this policy to send a trap.

Field	Value
Applicable Device Filter	Use the following settings in this policy <ul style="list-style-type: none"> • Vendor: * • Type: * • Model: * • OS: *
Rules Included	disable service compress-config
Action Type	EMail
Action	email to training NOC
Choose Save Location	Training_Realm

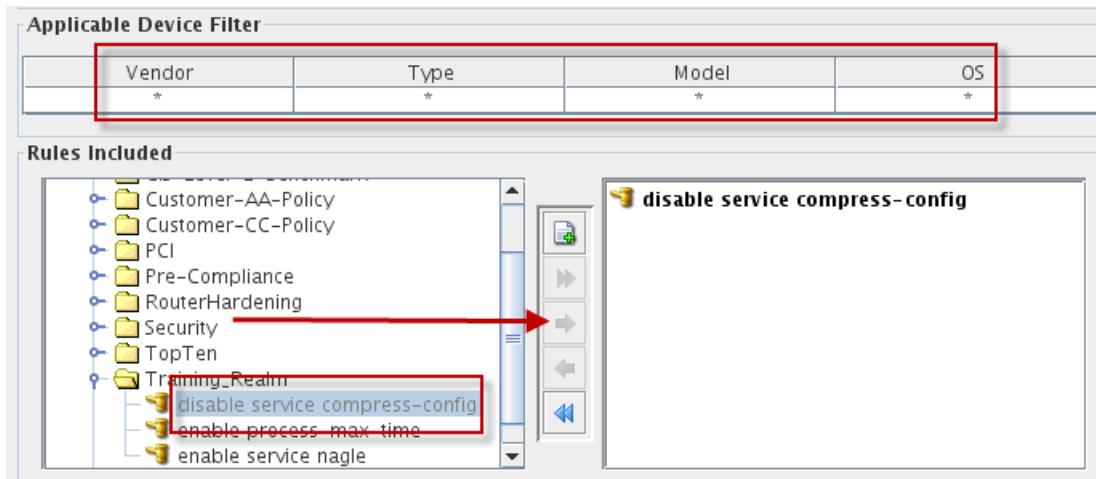
- a. Click the **Policy Definitions** tab. Click the **Policies** section. Right-click **Training_Realm** and click **New Policy**. The Create a Policy wizard starts.



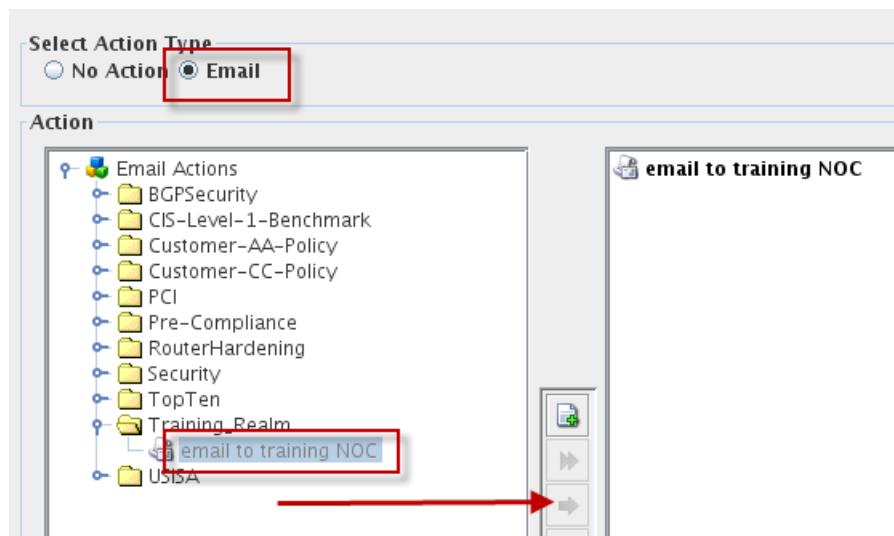
- b. Enter **disable service compress-config** in the **Name** field. Enter the description from the preceding table. Select **Severity 3**. Enter **45** in the **Weight** field. Select **Send Trap**.

Policy Name, Description & Severity	
Name:	disable service compress-config
Description:	Service compress-config should be disabled on all devices. This policy disables the service if it is present.
Impact:	
Severity:	3
Weight:	45
<input checked="" type="checkbox"/> Send Trap <input type="checkbox"/> Preemptive	

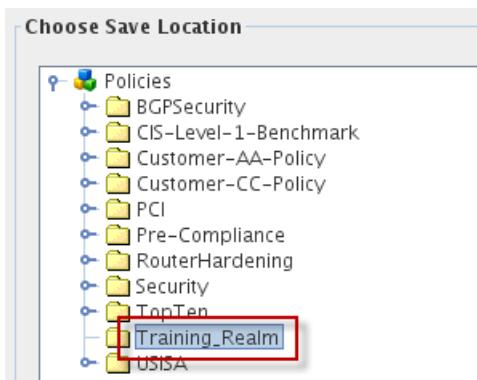
- c. Leave the value of * in the **Vendor**, **Type**, **Model**, and **OS** fields. Click the **Training_Realm > disable service compress-config** rule. Click the right arrow icon to move the rule to the right of the window. Click **Next**.



- d. Select **Email** as the **Action Type**. Click the **Training_Realm > email to training NOC** email action. Click the right arrow icon to move the email action to the right of the window. Click **Next**.



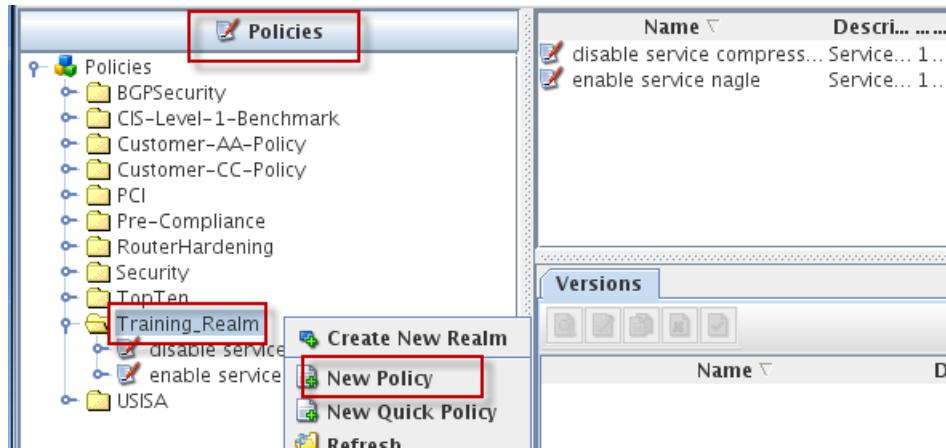
- e. Click **Training_Realm**. Click **Finish**.



3. Create a policy in the **Training_Realm** named **enable process-max-time**. Configure this policy to use the rule **enable process-max-time**. Use the following values to complete the wizard.

Field	Value
Name	enable process-max-time
Description	Process-max-time should be enabled and set on all routers. This policy enables and sets process-max-time to a user-defined parameter if it is not present.
Severity	5
Weight	20
Send Trap	Configure this policy to send a trap.
Applicable Device Filter	Use the following settings in this policy <ul style="list-style-type: none"> • Vendor: * • Type: * • Model: * • OS: *
Rules Included	enable process-max-time
Action Type	EMail
Action	email to training NOC
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Policies** section. Right-click **Training_Realm** and click **New Policy**. The Create a Policy wizard starts.



- b. Enter **enable process-max-time** in the **Name** field. Enter the description from the preceding table. Select **Severity 5**. Enter **20** in the **Weight** field. Select **Send Trap**.

Policy Name, Description & Severity

Name: enable process-max-time

Description: Process-max-time should be enabled and set on all routers. This policy enables and sets process-max-time to a user defined parameter if it is not present.

Impact: [empty]

Severity: 5

Weight: 20

Send Trap

Preemptive

- c. Enter **enable process-max-time** in the **Name** field. Enter the description from the preceding table. Select **Severity 5**. Enter **20** in the **Weight** field. Select **Send Trap**. Leave the value of * in the **Vendor**, **Type**, **Model**, and **OS** fields. Click the **Training_Realm** > **enable process-max-time** rule. Click the right arrow icon to move the rule to the right of the window. Click **Next**.

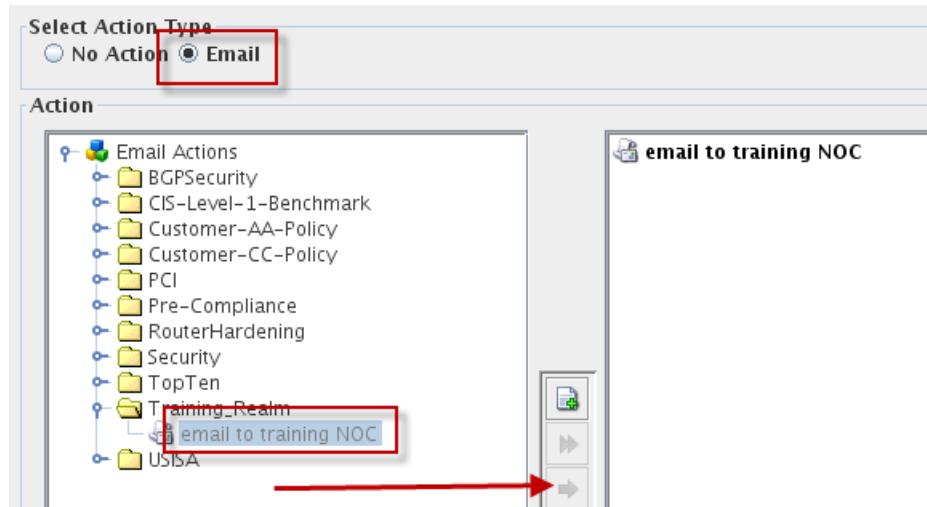
Applicable Device Filter

Vendor	Type	Model	OS
*	*	*	*

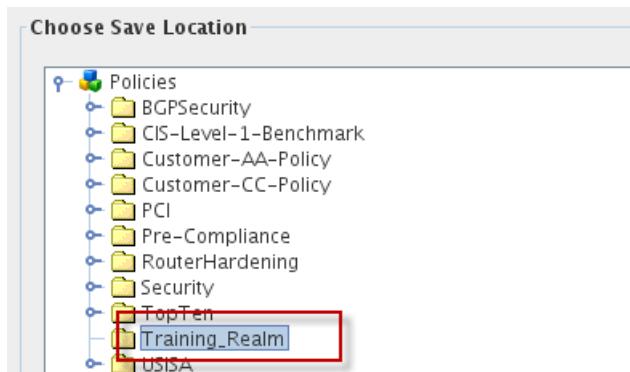
Rules Included

- Customer-CC-Policy
- PCI
- Pre-Compliance
- RouterHardening
- Security
- TopTen
- Training_Realm
 - enable process-max-time
 - enable service compress-config
 - enable service nagle
- USISA

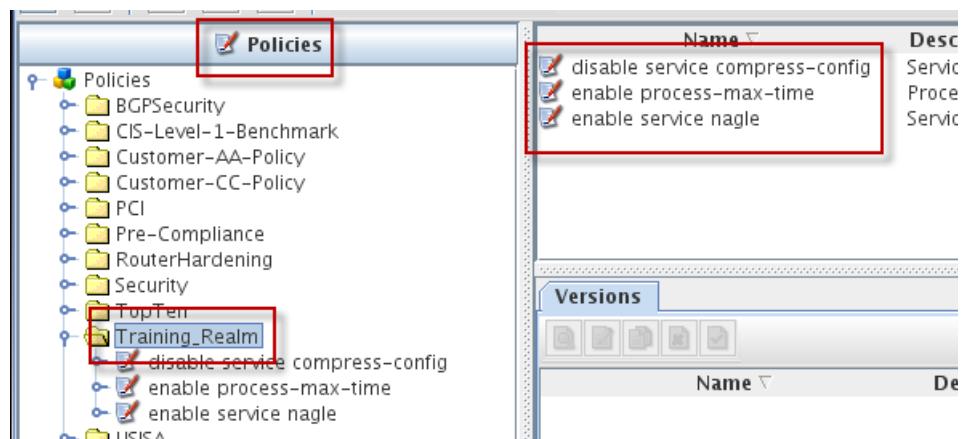
- d. Select **Email** as the **Action Type**. Click the **Training_Realm > email to training NOC** email action. Click the right arrow icon to move the email action to the right of the window. Click **Next**.



- e. Click **Training_Realm**. Click **Finish**.



The **Training_Realm** contains three policies.



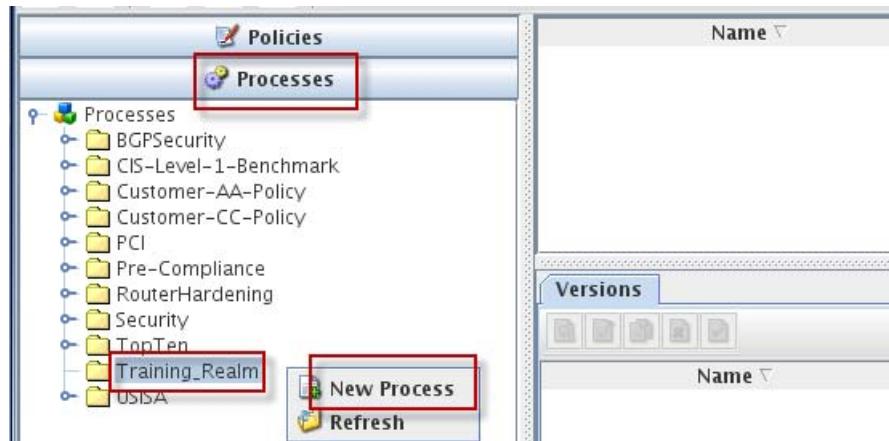
Exercise 6 Working with processes

In this exercise, you create a process. This process runs the three policies you created in the preceding exercise. You also schedule the process and run it.

1. Create a process in the Training_Realm named **training process for customer-CC**. Configure the process to run the three policies you created in the preceding exercise every Thursday. Use the following values to complete the wizard.

Field	Value
Name	training process for customer-CC
Description	This process runs policies on the devices that belong to customer-CC
Enable process for automatic validations	Configure this process to run automatic validations
Policy Selection	Use these policies in the Training_realm folder. <ul style="list-style-type: none">• enable service nagle• disable service compress-config• enable process max-time
Pre-Emptive Options	Do not enable any pre-emptive compliance options
Realm selection	Apply this process to the customer_CC realm. Check the device coverage in the customer_CC realm.
Include Subrealms	Configure this process to include subrealms
Policy parameters	View the associated parameters. View the PROCESS-MAX-TIME-MILLISECONDS parameter and confirm that the value is 100.
Process schedule	Recurring Schedule > Weekly. Every 1 week on a Thursday.
Choose Save Location	Training_Realm

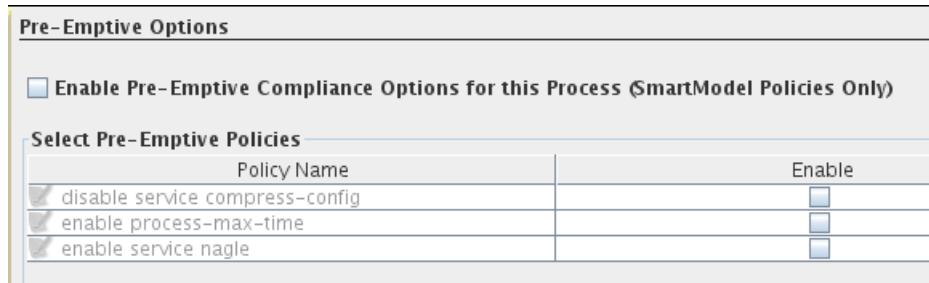
- Click the **Policy Definitions** tab. Click the **Processes** section. Right-click **Training_Realm** and click **New Process**. The Create a Process wizard starts.



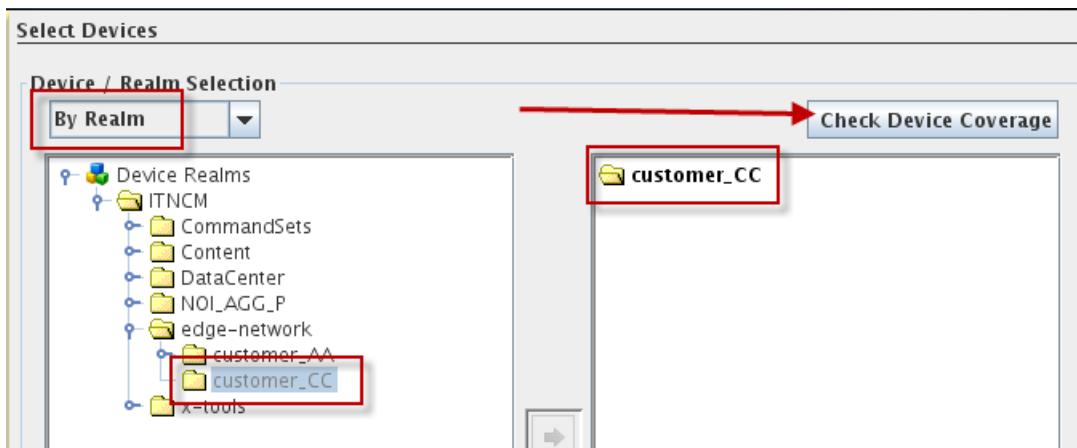
- Enter **training process for customer-CC** in the **Name** field. Enter the description from the preceding table. Select the **Enable process for automatic validations** option. Expand **Training_Realm**. Use the right arrow icon to move the three policies in the Training_Realm to the right of the window. Click **Next**.

The screenshot shows the 'Process Name & Description' step of the 'Create a Process' wizard. It includes fields for 'Name' (containing 'training process for customer-CC'), 'Description' (containing 'This process runs policies on the devices that belong to customer-CC'), and 'Enable process for automatic validations' (unchecked). The 'Policy Selection' section shows a tree view of policies under 'Training_Realm', with three specific policies checked: 'disable service compress-config', 'enable process-max-time', and 'enable service nagle'.

- c. Click **Next** in the Pre-Emptive Options window.



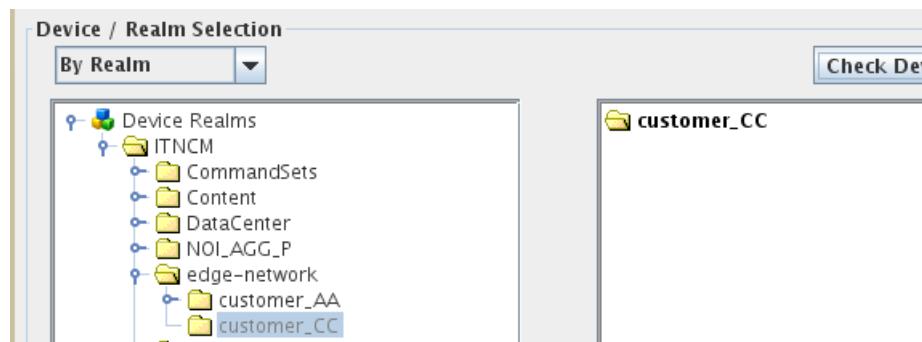
- d. Expand **ITNCM > edge-network > customer_CC**. Use the right arrow icon to move the **customer_CC** realm to the right of the window. Select the option to **Include Subrealms**. Click the **Check Device Coverage** icon.



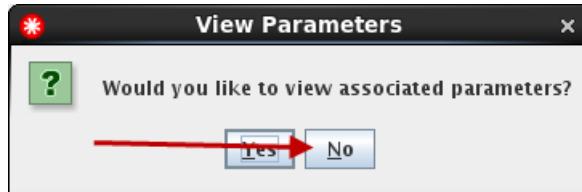
- e. Click **OK**.



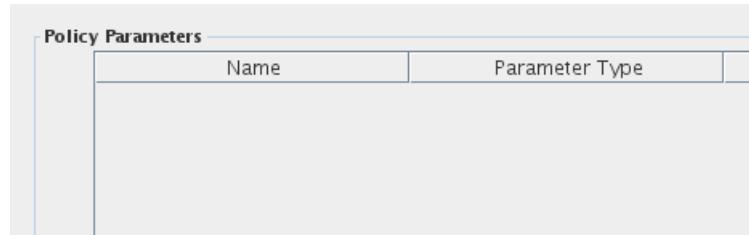
- f. Click **Next** in the Select Devices window.



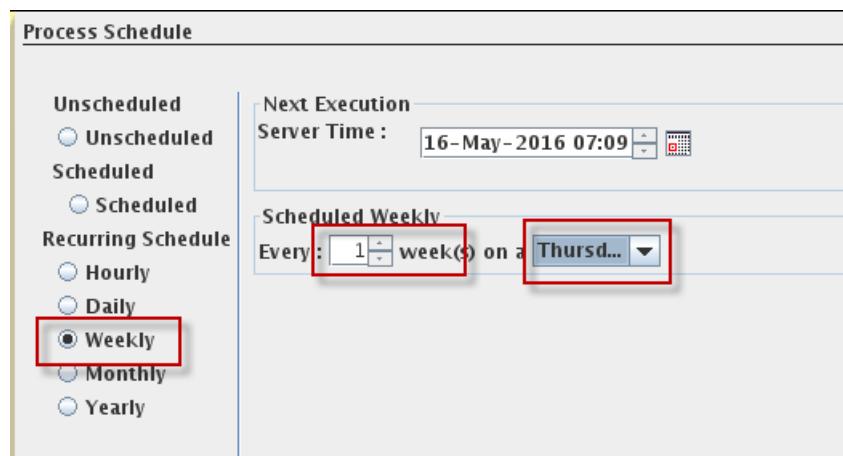
g. Click **No** to view parameters.



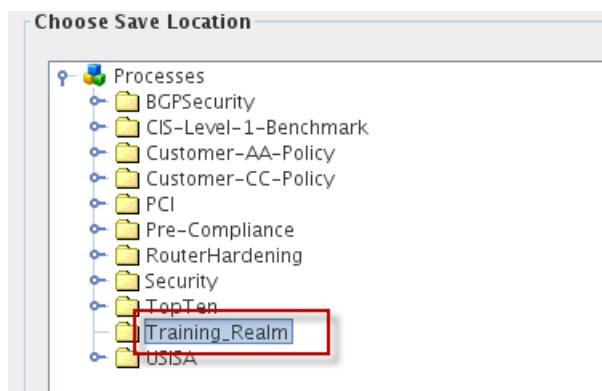
h. Click **Next** in the Parameters window.



i. Click **Recurring Schedule > Weekly**. Enter **1** in the **Every** field. Select **Thursday** in the **week(s)** field. Click **Next**.



j. Click **Training_Realm**. Click **Finish**.



2. After you create the process, it runs automatically. Wait until the process finishes, and then look at the **Policy Validation Summary** for the process you just ran. Notice that the devices fail some of the policies and pass others.
- Click the **Results** tab.

Name	State	Executed By	Devices	Process Type
training process for customer-CC	Scheduled	engineer	?	Compliance
training process for customer-CC	Finished	engineer	3	Compliance

You see two results with the same name. One result is scheduled and the other is finished. The scheduled process represents the recurring schedule that you created in this exercise.

- Click the **training process for customer-CC** process with the state of finished.

Name	State	Executed By	Devices	Process Type	Execution
training process for customer-CC	Scheduled	engineer	?	Compliance	Recurring Sc
training process for customer-CC	Finished	engineer	3	Compliance	Recurring Sc

Policy Name	Severity	Revision	Date	Passed	Failed	Not Applicable
disable service compress-config	3	1	16-May-2016 ..	0	3	0
enable process-max-time	5	1	16-May-2016 ..	0	3	0
enable service nagle	4	1	16-May-2016 ..	1	2	0

Leave the compliance manager client as is. You return to it shortly.



18 Remediation exercises

The exercises in this unit build on the previous unit by expanding compliance policies to include remediation actions.

Exercise 1 Creating command sets

In this exercise, you create three native command sets in the *configuration manager*.

1. Log in to the Netcool Configuration Manager user interface with the user name **engineer** and the password **object00**.
 - a. Return to the browser session and click **ITNCM Webstart GUI**.

The screenshot shows the 'Netcool Configuration Manager' login page. At the top right, it says 'User: engineer, Logoff'. Below the title, there are two links: 'ITNCM Webstart GUI (Web Start Client)' and 'ITNCM Compliance (Web Start Client)'. The 'ITNCM Webstart GUI' link is highlighted with a red rectangular box.

- b. Click **Run**.

The screenshot shows a Java security dialog box titled 'Do you want to run this application?'. It displays the following information:
Name: IBM Tivoli Netcool Configuration Manager
Publisher: International Business Machines Limited
Locations: http://host1.csite.edu:15310
Launched from downloaded JNLP file

A warning message at the bottom states: 'This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the locations and publisher above.'

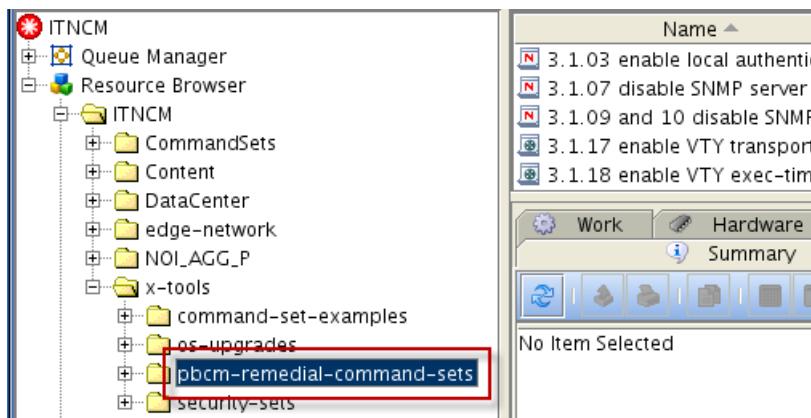
At the bottom left is a blue shield icon with a white 'i'. To its right are 'More Information', 'Run', and 'Cancel' buttons.

Exercise 1 Creating command sets

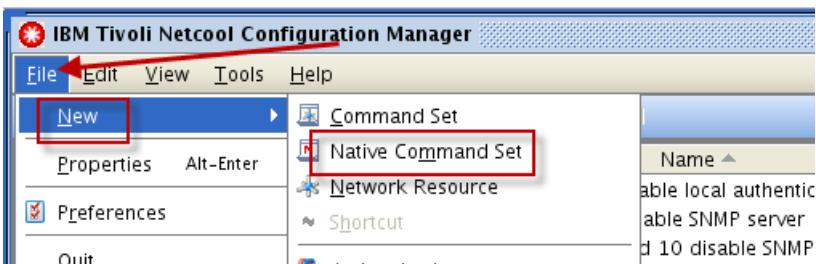
2. Create a native command set that is named **enable service nagle** in the **ITNCM > x-tools > pbcm-remedial-command-sets** realm. Use the following VTMOS settings for the command set.

- Vendor: Cisco
- Type: Router
- Model: *
- OS: *

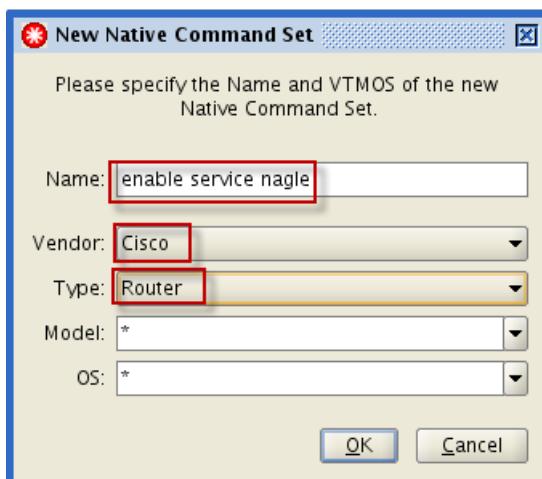
- a. Click the **ITNCM > x-tools > pbcm-remedial-command-sets** realm in the *resource browser*.



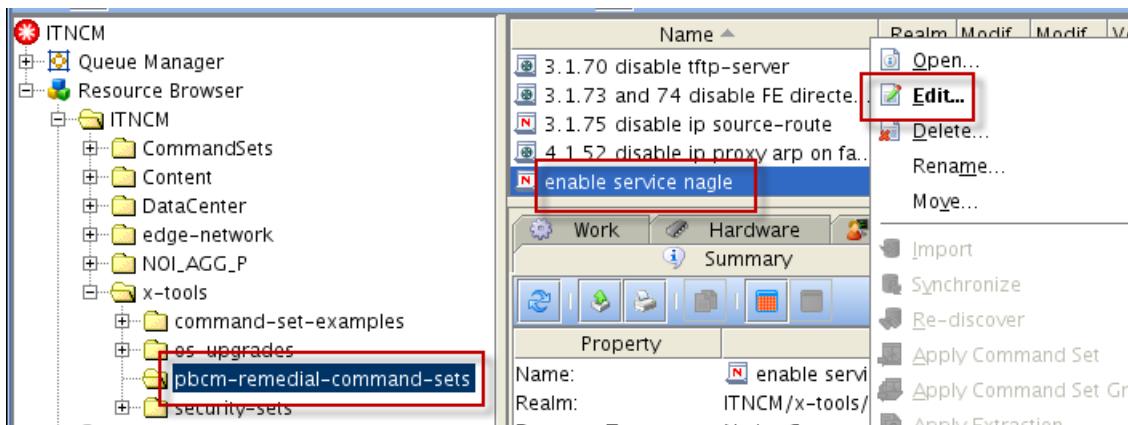
- b. Click **File > New > Native Command Set**.



- c. Enter **enable service nagle** into the **Name** field. Choose the VTMOS settings and click **OK**.

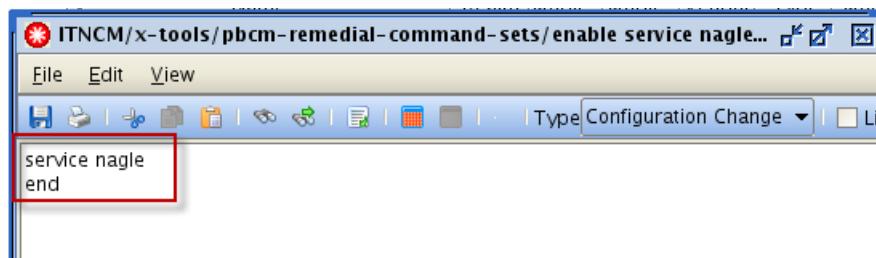


3. Configure the **enable service nagle** native command set to run the command **service nagle**. Enter the word **end** on a line after the command. Save and close the command set when you finish.
 - a. Right-click the new **enable service nagle** command set in the **ITNCM > x-tools > pbcm-remedial-command-sets** realm and click **Edit**.

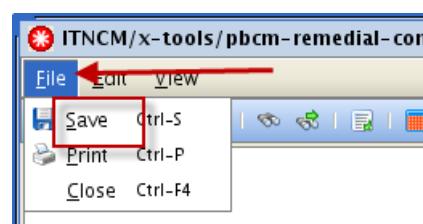


- b. Enter the following lines into the command set:

```
service nagle  
end
```

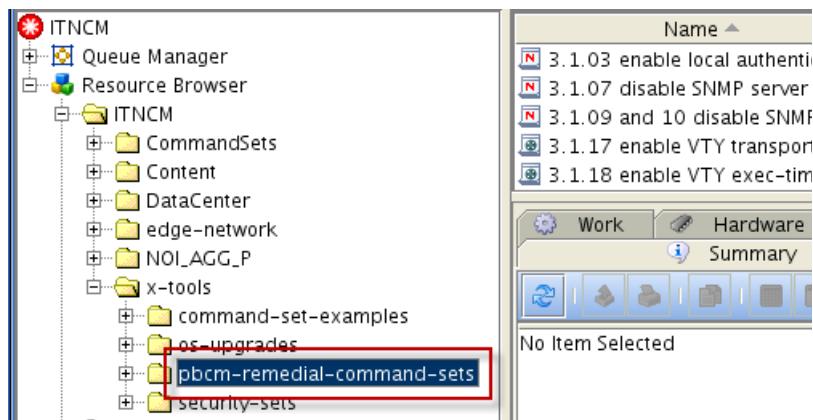


- c. Click **File > Save**. Close the command set.

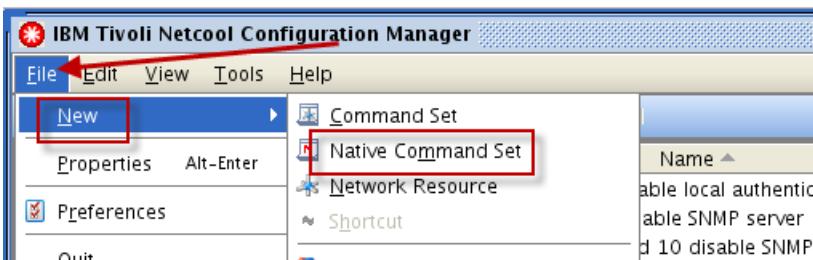


Exercise 1 Creating command sets

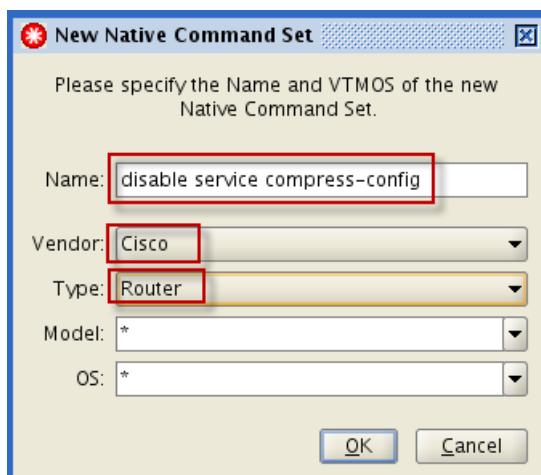
4. Create a native command set that is named **disable service compress-config** in the **ITNCM > x-tools > pbcm-remedial-command-sets** realm. Use the following VTMOS settings for the command set.
- Vendor: Cisco
 - Type: Router
 - Model: *
 - OS: *
- a. Click the **ITNCM > x-tools > pbcm-remedial-command-sets** realm in the *resource browser*.



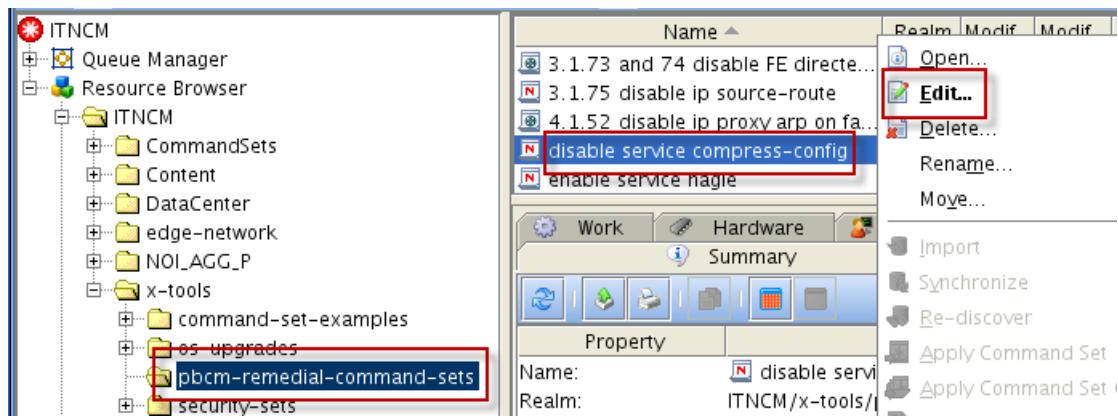
- b. Click **File > New > Native Command Set**.



- c. Enter **disable service compress-config** into the **Name** field. Choose the VTMOS settings and click **OK**.

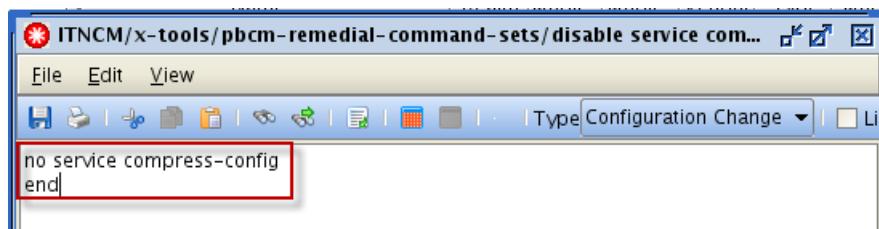


5. Configure the **disable service compress-config** command set to run the command **no service compress-config**. Enter the word **end** on a line after the command. Save and close the command set when you finish.
 - a. Right-click the new **disable service compress-config** command set in the **ITNCM > x-tools > pbcm-remedial-command-sets** realm and click **Edit**.

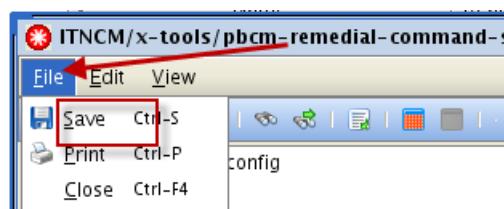


- b. Enter the following lines into the command set:

```
no service compress-config  
end
```



- c. Click **File > Save**. Close the command set.

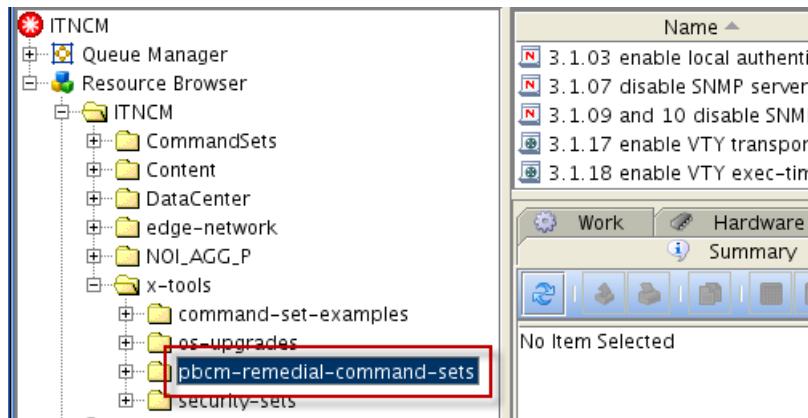


Exercise 1 Creating command sets

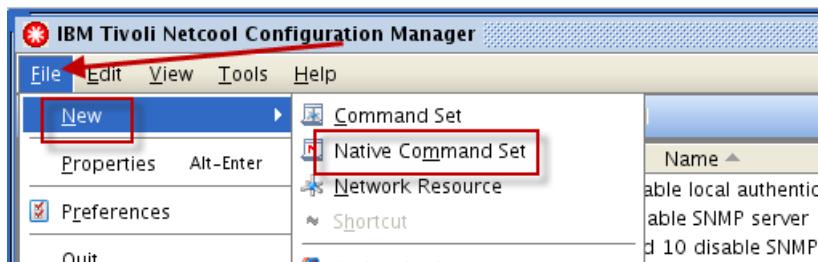
6. Create a native command set named **enable process-max-time** in the **ITNCM > x-tools > pbcm-remedial-command-sets** realm. Use the following VTMOS settings for the command set.

- Vendor: Cisco
- Type: Router
- Model: *
- OS: *

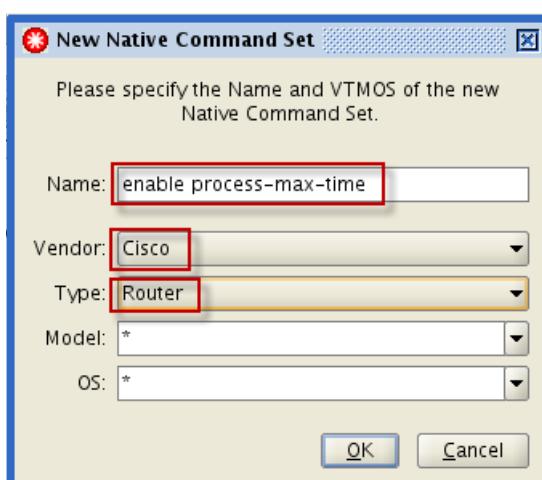
- a. Click the **ITNCM > x-tools > pbcm-remedial-command-sets** realm in the *resource browser*.



- b. Click **File > New > Native Command Set**.

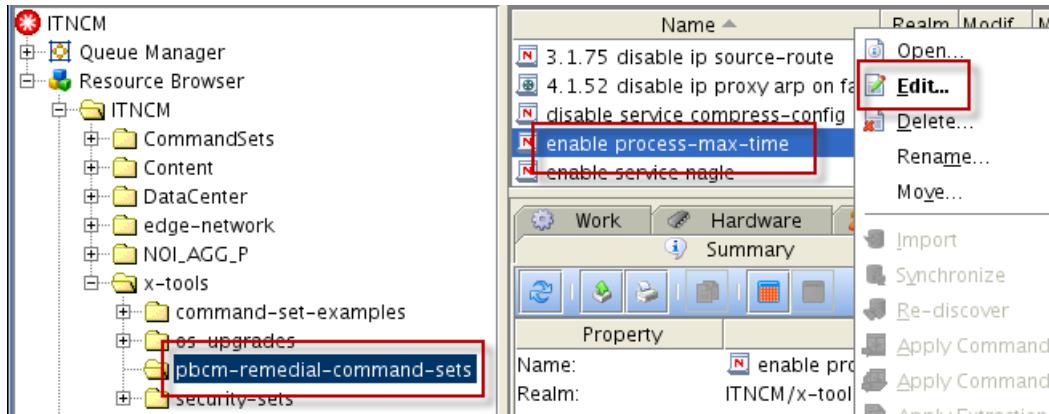


- c. Enter **enable process-max-time** into the **Name** field. Choose the VTMOS settings and click **OK**.



7. Configure the new **enable process-max-time** command set to run the command **process-max-time \$PROCESS-MAX-TIME-MILLISECONDS\$**. The string **\$PROCESS-MAX-TIME-MILLISECONDS\$** is a parameter that you created in a definition in a previous exercise. Enter the word **end** on a line after the command. Save and close the command set when you finish.

- a. Right-click the **enable process-max-time** command set in the **ITNCM > x-tools > pbcm-remedial-command-sets** realm and click **Edit**.

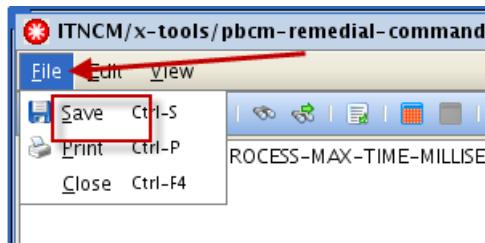


- b. Enter the following lines into the command set:

```
process-max-time $PROCESS-MAX-TIME-MILLISECONDS$  
end
```



- c. Click **File > Save**. Close the command set.



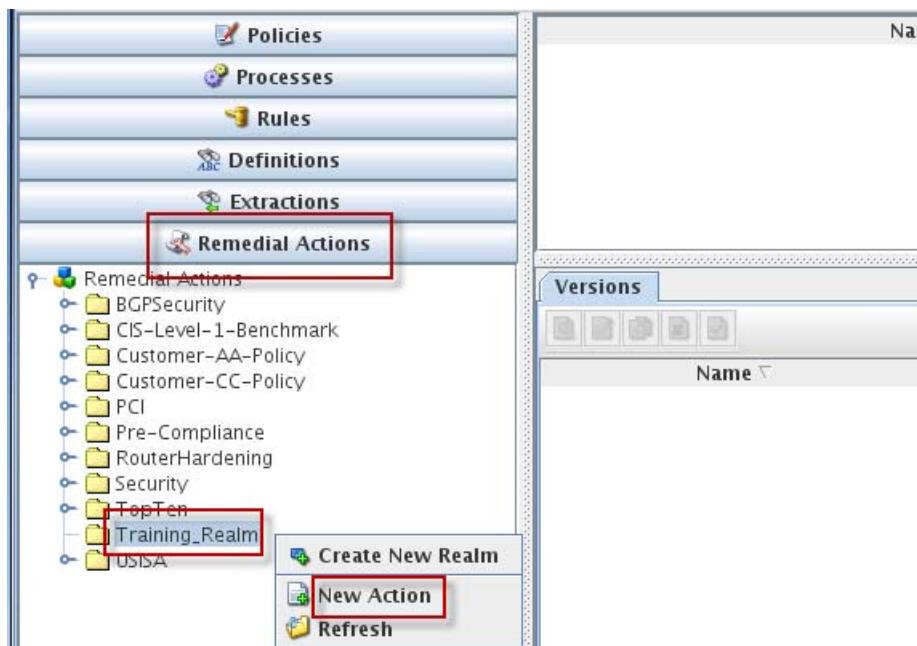
Exercise 2 Creating remedial actions

In this exercise, you create three remedial actions that run the command sets you configured in the preceding exercise.

1. Return to the *compliance manager* user interface. Create a remedial action in the **Training_Realm** named **enable service nagle**. Configure this remedial action to use the command set **enable service nagle**. Use the following values to complete the wizard.

Field	Value
Name	enable service nagle
Description	This remedial action runs a command set to enable service nagle on a Cisco router.
Action Type	Remedial Action
Remedial Action	ITNCM > x-tools > pbcm-remedial-command-sets > enable service nagle
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Remedial Actions** section. Right-click **Training_Realm** and click **New Action**. The Create an Action wizard starts.



- b. Enter **enable service nagle** in the **Name** field. Enter the description from the preceding table. Select **Remedial Action**. Click **Next**.

Action Name & Description

Name: **enable service nagle** * Revision: 1

Description: This remedial action runs a command set to enable service nagle or...

Action Type

E-Mail Template

Remedial Action

- c. Expand the **ITNCM > x-tools > pbcm-remedial-command-sets** realm at the left of the window. Click **enable service nagle**. Click **Next**.



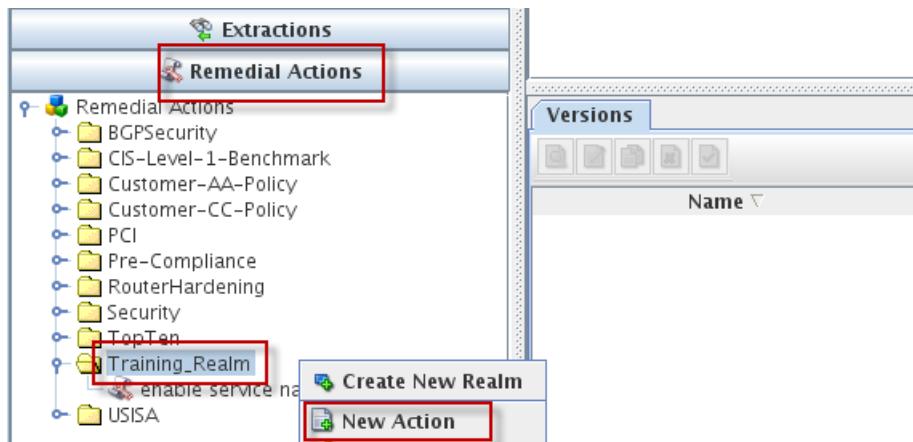
- d. Click **Training_Realm**. Click **Finish**.



2. Create a remedial action in the **Training_Realm** that is named **disable service compress-config**. Configure this remedial action to use the command set **disable service compress-config**. Use the following values to complete the wizard.

Field	Value
Name	disable service compress-config
Description	This remedial action runs a command set to disable service compress-config on a Cisco router.
Action Type	Remedial Action
Remedial Action	ITNCM > x-tools > pbcm-remedial-command-sets > disable service compress-config
Choose Save Location	Training_Realm

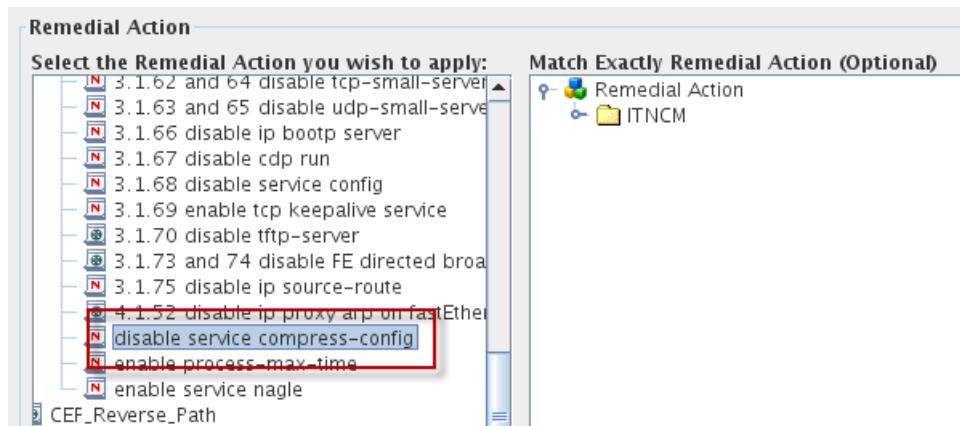
- a. Click the **Policy Definitions** tab. Click the **Remedial Actions** section. Right-click **Training_Realm** and click **New Action**. The Create an Action wizard starts.



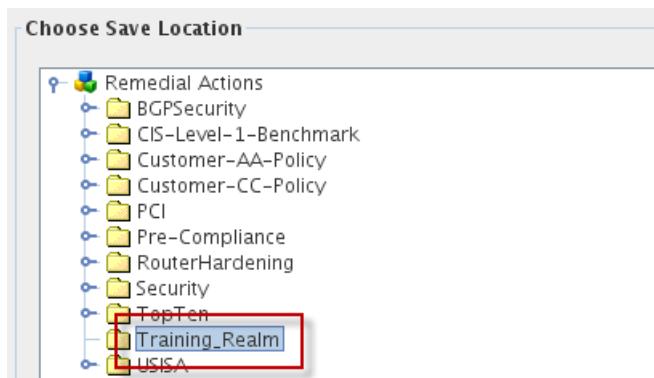
- b. Enter **disable service compress-config** in the **Name** field. Enter the description from the preceding table. Select **Remedial Action**. Click **Next**.

Name:	disable service compress-config	Revision:	1
Description: This remedial action runs a command set to disable service compress-config on a Cisco router.			
Action Type <input type="radio"/> E-Mail Template <input checked="" type="radio"/> Remedial Action			

- c. Expand the **ITNCM > x-tools > pbcm-remedial-command-sets** realm at the left of the window. Click **disable service compress-config**. Click **Next**.



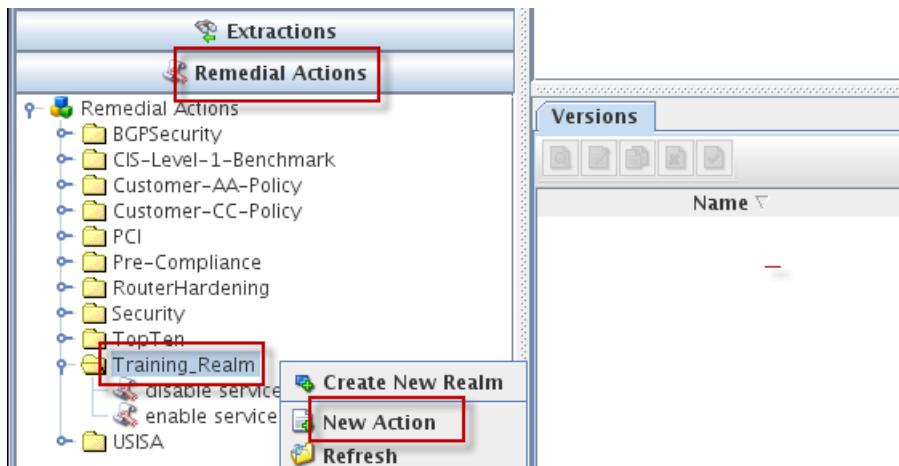
- d. Click **Training_Realm**. Click **Finish**.



3. Create a remedial action in the **Training_Realm** named **enable process-max-time**. Configure this remedial action to use the command set **enable process-max-time**. Use the following values to complete the wizard.

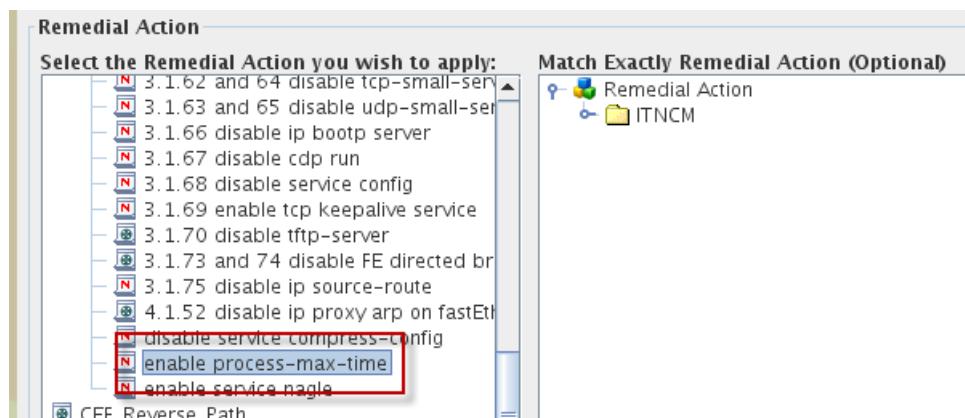
Field	Value
Name	enable process-max-time
Description	This remedial action runs a command set to enable process-max-time on a Cisco router.
Action Type	Remedial Action
Remedial Action	ITNCM > x-tools > pbcm-remedial-command-sets > enable process-max-time
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Remedial Actions** section. Right-click **Training_Realm** and click **New Action**. The Create an Action wizard starts.

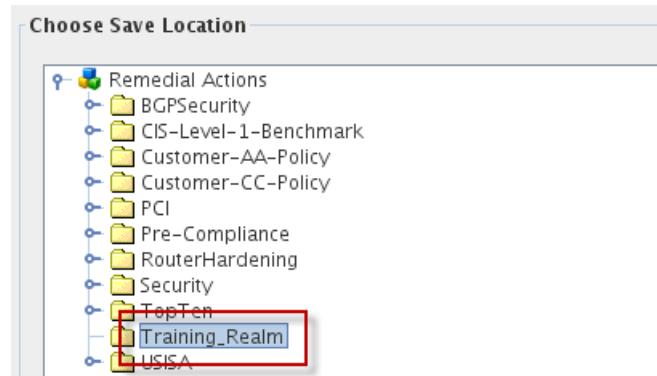


- b. Enter **enable process-max-time** in the **Name** field. Enter the description from the preceding table. Select **Remedial Action**. Click **Next**.

- c. Expand the **ITNCM > x-tools > pbcn-remedial-command-sets** realm at the left of the window. Click **enable process-max-time**. Click **Next**.



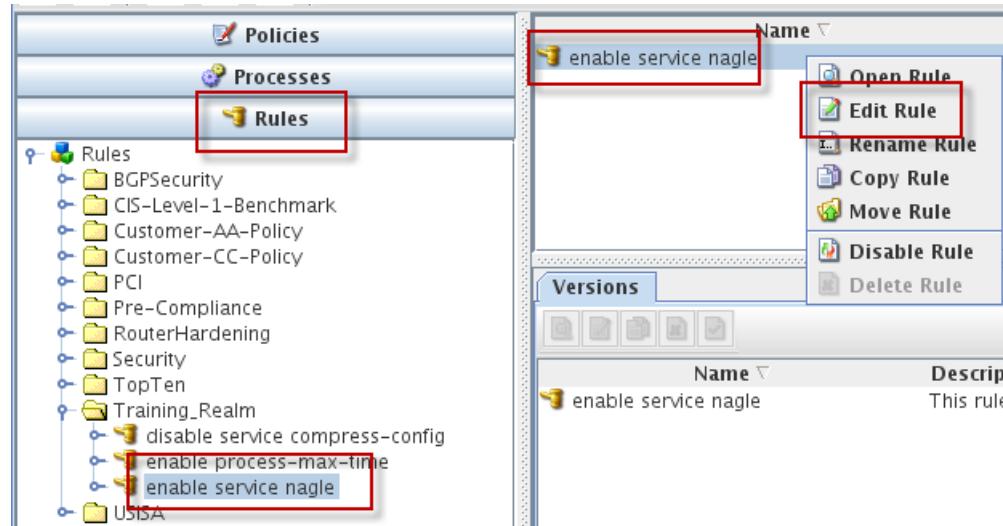
- d. Click **Training_Realm**. Click **Finish**.



Exercise 3 Adding remedial actions to rules

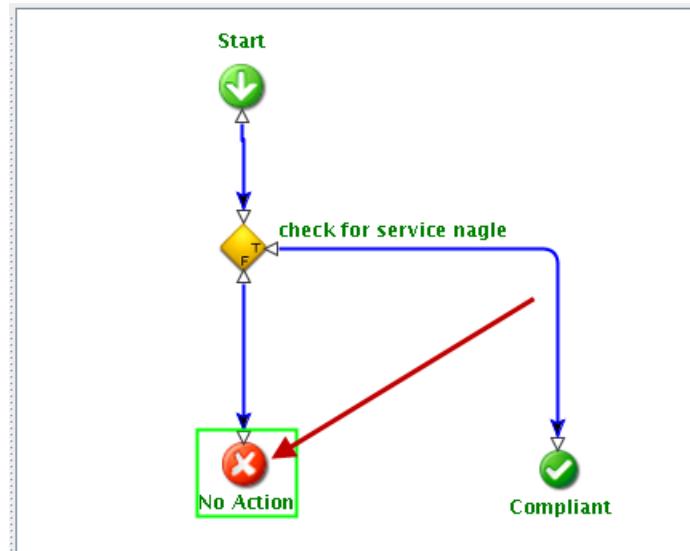
In this exercise, you edit existing rules to include the three new remedial actions.

1. Edit the **enable service nagle** rule to include the **enable service nagle** remedial action.
Associate the remedial action with the noncompliant icon in the graphical rule.
 - a. Click the **Policy Definitions** tab. Click the **Rules** section. Expand **Training_Realm**. Right-click the **enable service nagle** rule and click **Edit Rule**. The Edit Rule wizard starts.

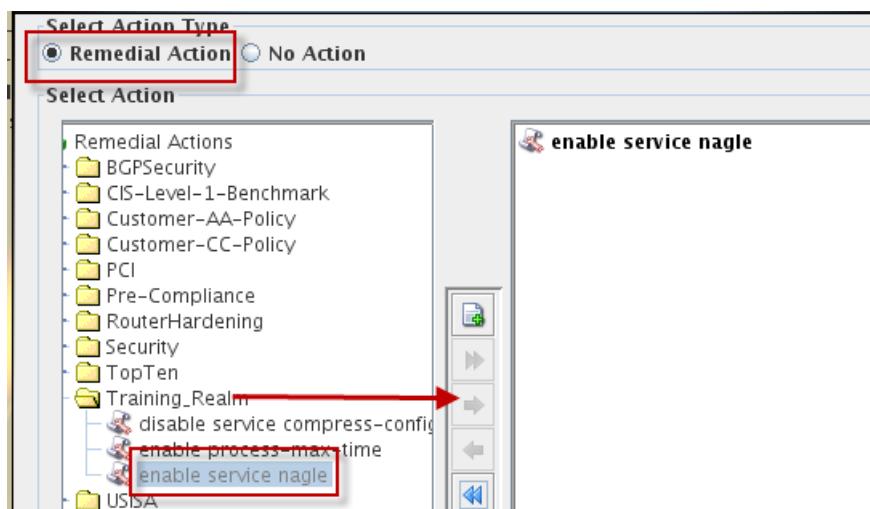


- b. Click **Next** in the Enter Rule Details window.

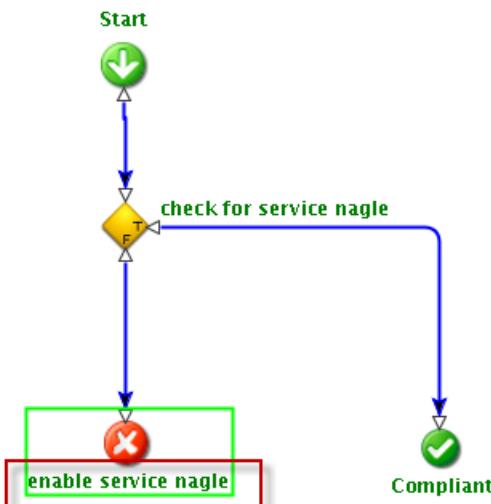
- c. Double-click the **Non Compliant** icon.



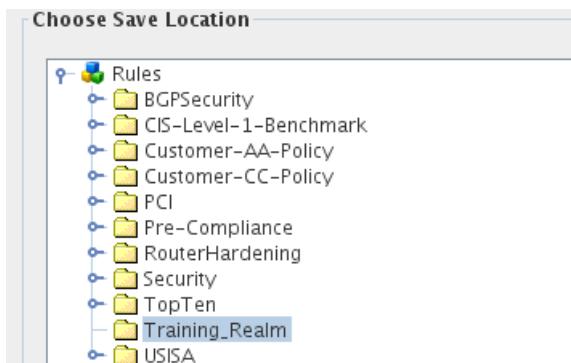
- d. Select **Remedial Action**. Click the **Training_Realm > enable service nagle** remedial action. Click the right arrow icon to move the action to the right of the window. Click **OK**.



e. Click **Next**.



f. Click **Finish**.



2. Edit the **disable service compress-config** rule to include the **disable service compress-config** remedial action. Associate the remedial action with the non-compliant icon in the graphical rule.

- a. Click the **Policy Definitions** tab. Click the **Rules** section. Expand **Training_Realm**. Right-click the **disable service compress-config** rule and click **Edit Rule**. The Edit Rule wizard starts.

The screenshot shows the 'Edit Rule' wizard in progress. The left pane lists policies like BGPSecurity, CIS-Level-1-Benchmark, etc., and the 'Rules' section is selected. Under 'Training_Realm', three rules are listed: 'disable service compress-config', 'enable process max time', and 'enable service nagle'. The 'disable service compress-config' rule is selected and highlighted with a red box. On the right, the rule details are shown: Name: 'disable service compress-config', Description: 'This rule d...', and a 'Versions' section. A context menu is open over the rule, with 'Edit Rule' highlighted with a red box. Other options in the menu include Open Rule, Rename Rule, Copy Rule, Move Rule, Disable Rule, and Delete Rule.

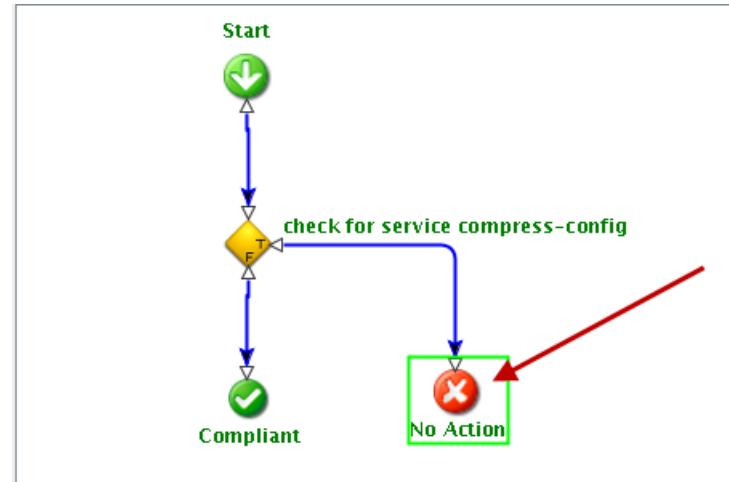
- b. Click **Next** in the Enter Rule Details window.

Rule Name & Description

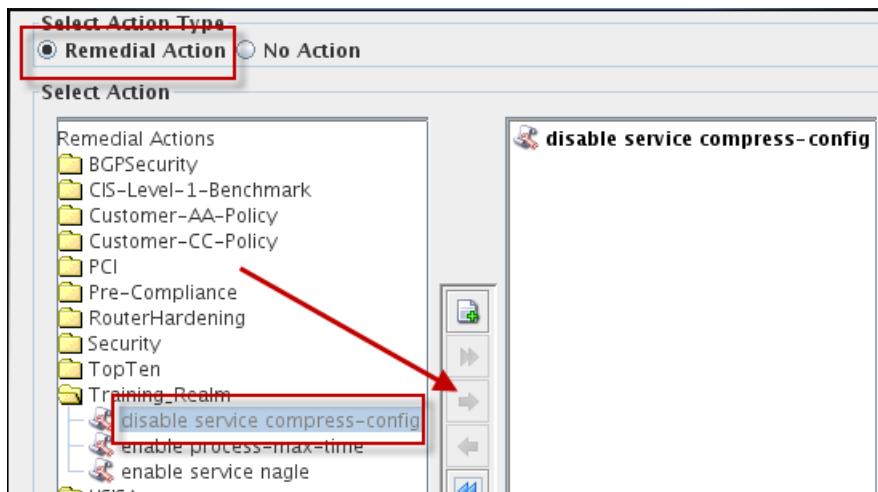
Name: disable service compress-config Revision: 1

Description: This rule determines that a device configuration is not compressed. compress-config is present.

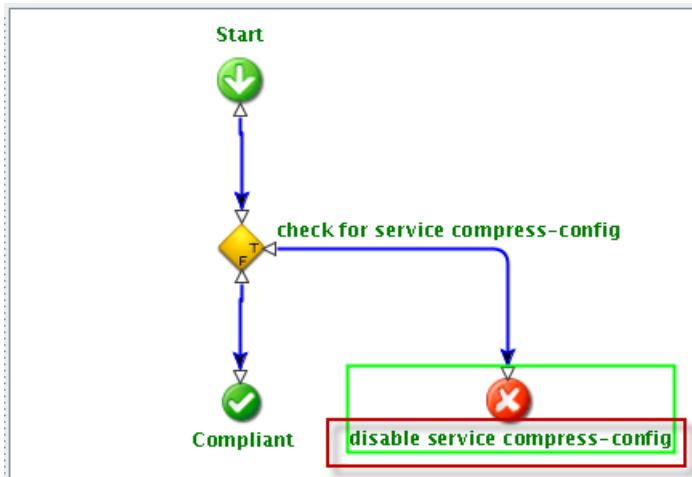
- c. Double-click the Non Compliant icon.



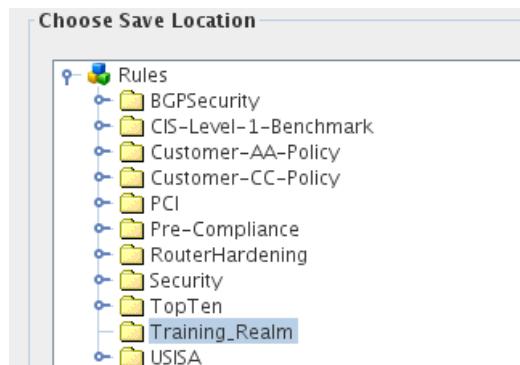
- d. Select **Remedial Action**. Click the **Training_Realm > disable service compress-config** remedial action. Click the right arrow icon to move the action to the right of the window. Click **OK**.



e. Click **Next**.



f. Click **Finish**.



3. Edit the **enable process-max-time** rule to include the **enable process-max-time** remedial action. Associate the remedial action with the non-compliant icon in the graphical rule.
- a. Click the **Policy Definitions** tab. Expand **Training_Realm**. Click the **Rules** section. Right-click the **enable process-max-time** rule and click **Edit Rule**. The Edit Rule wizard starts.

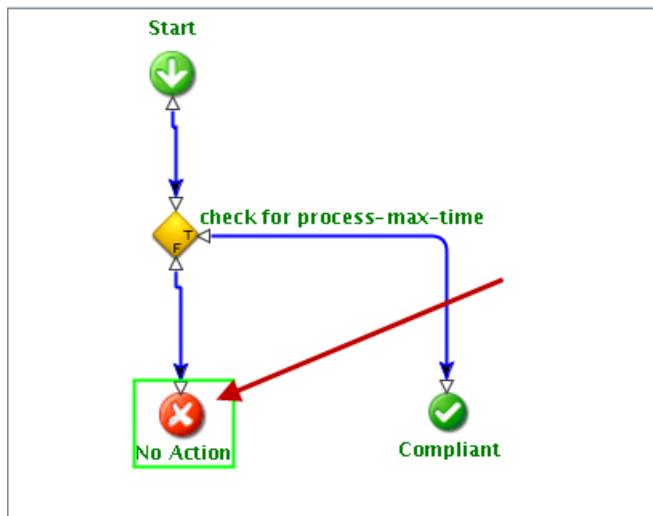
Name	Description
enable process-max-time	This rule d...

- b. Click **Next** in the Enter Rule Details window.

Rule Name & Description	
Name:	enable process-max-time
Revision:	1

Description:	This rule determines that a device configuration is compliant if process-max-time is present and set to a defined number of seconds.
--------------	--

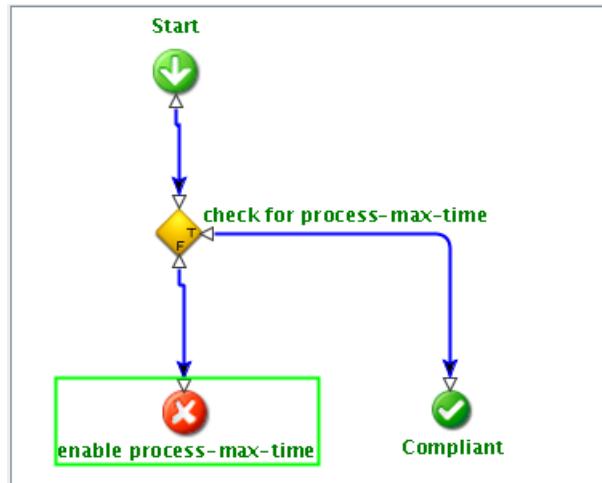
- c. Double-click the Non Compliant icon.



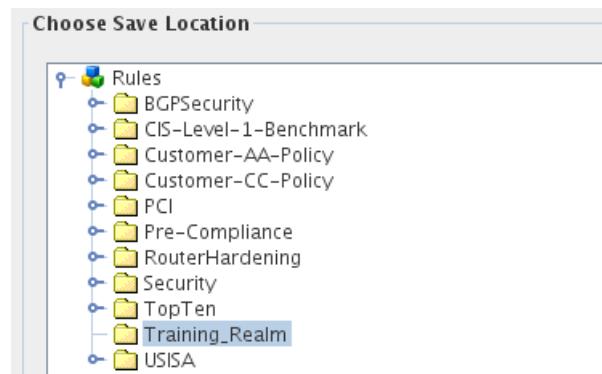
- d. Select **Remedial Action**. Click the **Training_Realm > enable process-max-time** remedial action. Click the right arrow icon to move the action to the right of the window. Click **OK**.

The screenshot shows a software interface for managing network security configurations. On the left, a tree view titled 'Select Action Type' displays various remedial actions under categories like BGP Security, CIS-Level-1-Benchmark, Customer-AA-Policy, Customer-CC-Policy, PCI, Pre-Compliance, RouterHardening, Security, TopTen, and Training_Realm. Under 'Training_Realm', three specific actions are listed: 'enable service compress-config', 'enable process-max-time' (which is highlighted with a red box), and 'enable service nagle'. On the right, a details panel for the selected action 'enable process-max-time' is shown, featuring a thumbnail icon of a person, the action name, and a set of control buttons (add, move up, move down, remove).

e. Click **Next**.



f. Click **Finish**.



Exercise 4 Running remedial actions

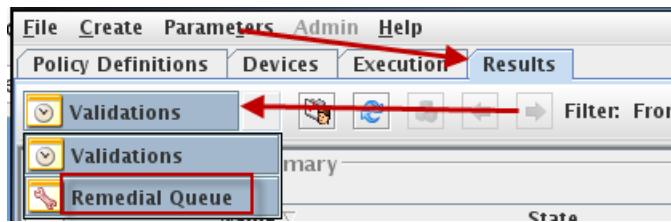
In this exercise, you run the process that you created in a previous exercise and approve the remedial actions.



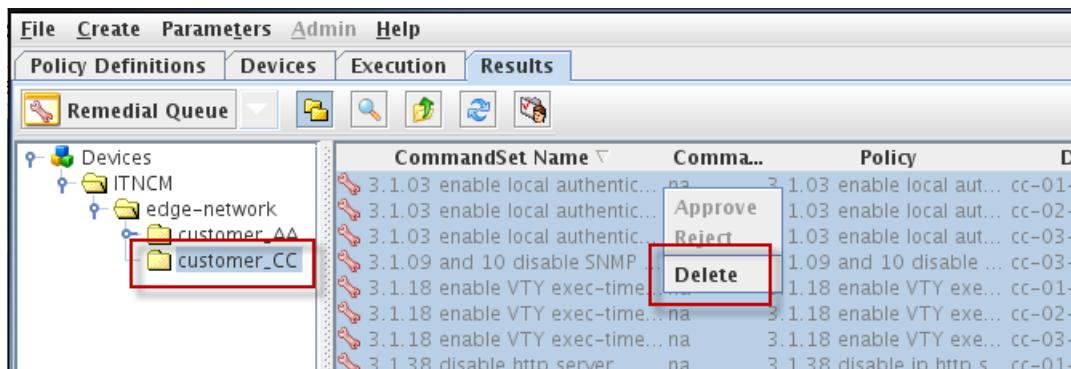
Note: You ran a process in a previous unit that generated remedial actions. You approved the actions. The completed actions remain in the remedial queue. Remove those actions now to eliminate any possible confusion in the next exercise.

1. Remove the old remedial actions.

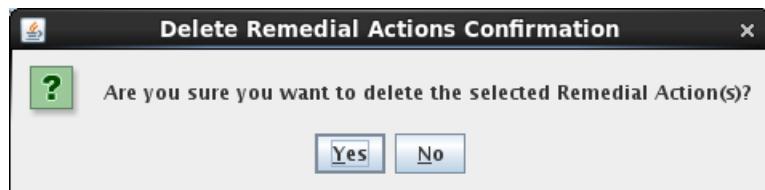
- a. Click the **Results** tab.



- b. Expand **ITNCM > edge-network > customer_CC**. Select all of the remedial actions. Right-click the selected actions and click **Delete**.

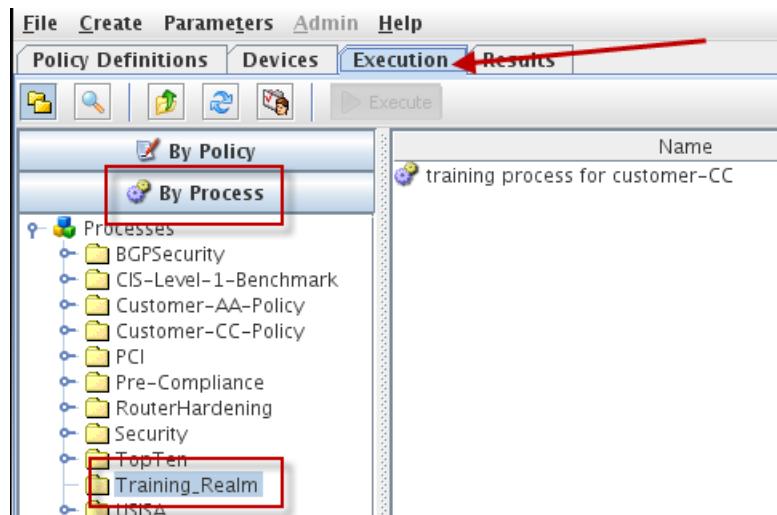


- c. Click **Yes** to confirm.

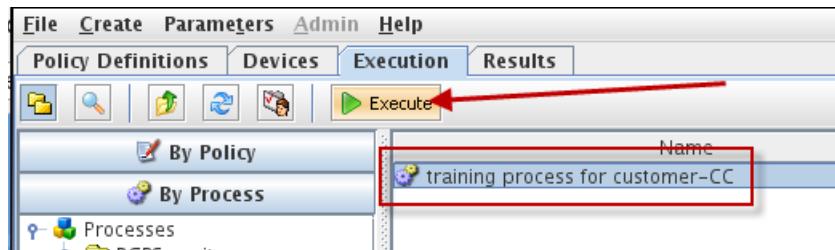


2. Run the training process for customer-CC process from the **Execution** tab.

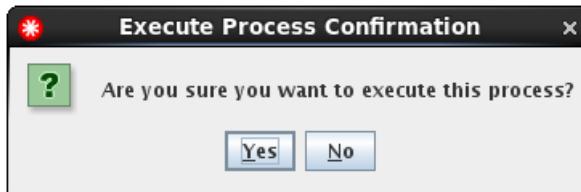
- a. Click the **Execution** tab. Click the **By Process** section. Click the **Training_Realm** realm.



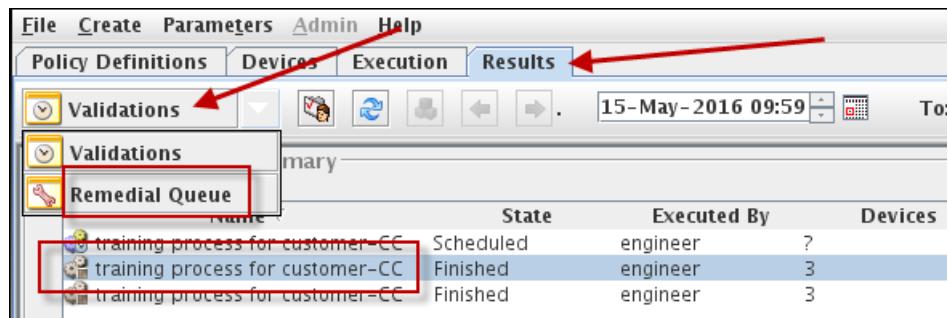
- b. Select the training process for customer-CC process and click the **Execute** icon.



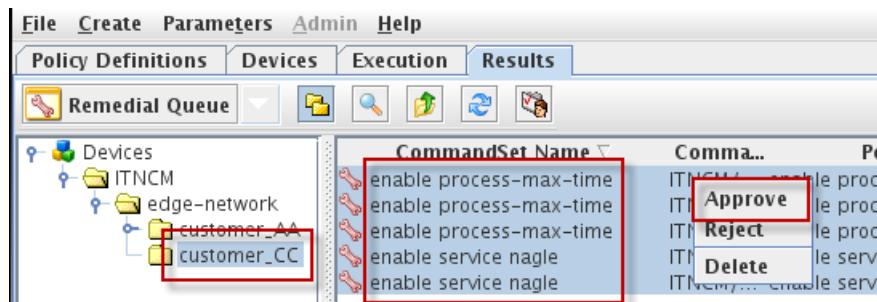
- c. Click **Yes** to confirm.



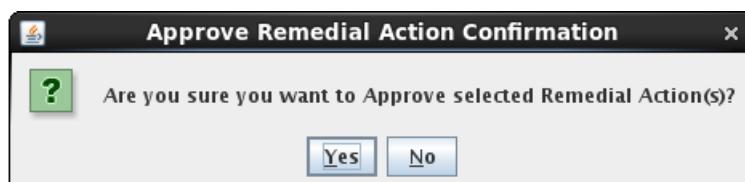
3. After you run the process, the **Results** tab is shown. View the Remedial Queue. Approve the **enable service nagle** and **enable process-max-time** remedial actions.
- a. Select the process that you ran. Click **Validations** and select **Remedial Queue**.



- b. Expand **ITNCM > edge-network > customer_CC**. Select all of the **enable service nagle** and **enable process-max-time** remedial actions. Right-click the selected actions and click **Approve**.



- c. Click **Yes** to confirm.



4. Click the Refresh icon until the status of the actions is **Sent to Work Queue** or **FINISHED**.

CommandSet Name	Comma...	Policy	Device	Realm	Status	Op...
enable process-max-time	ITNCM/...	enable process...	cc-01-router-...	ITNCM...	Sent to Work Queue	16-Ma
enable process-max-time	ITNCM/...	enable process...	cc-02-router-...	ITNCM...	Sent to Work Queue	16-Ma
enable process-max-time	ITNCM/...	enable process...	cc-03-router-...	ITNCM...	Sent to Work Queue	16-Ma
enable service nagle	ITNCM/...	enable service ...	cc-02-router-...	ITNCM...	Sent to Work Queue	16-Ma
enable service nagle	ITNCM/...	enable service ...	cc-03-router-...	ITNCM...	Sent to Work Queue	16-Ma

5. Return to the *configuration manager* user interface. Look at **Work That is Finished** in the *queue manager*. You see several new units of work that ran successfully for native command sets. These command sets were automatically run in configuration manager when you approved the remedial actions in compliance manager. Verify that all of the command sets are successful. You might need to wait until all of the units of work finish.
- Return to the configuration manager user interface. Click **Work That is Finished** in the queue manager. View the successful command set units of work.

UOW ID	Type	Submitter	Request Type	Result
84	UOW	administrator	Native Command Set	SUCCESS
85	UOW	administrator	Command Set	SUCCESS
86	UOW	administrator	Command Set	SUCCESS
87	UOW	administrator	Native Command Set	SUCCESS
88	UOW	administrator	Native Command Set	SUCCESS
89	UOW	administrator	Command Set	SUCCESS
90	UOW	administrator	Native Command Set	SUCCESS
91	UOW	administrator	Native Command Set	SUCCESS
92	UOW	administrator	Native Command Set	SUCCESS
93	UOW	administrator	Native Command Set	SUCCESS
94	UOW	administrator	Native Command Set	SUCCESS

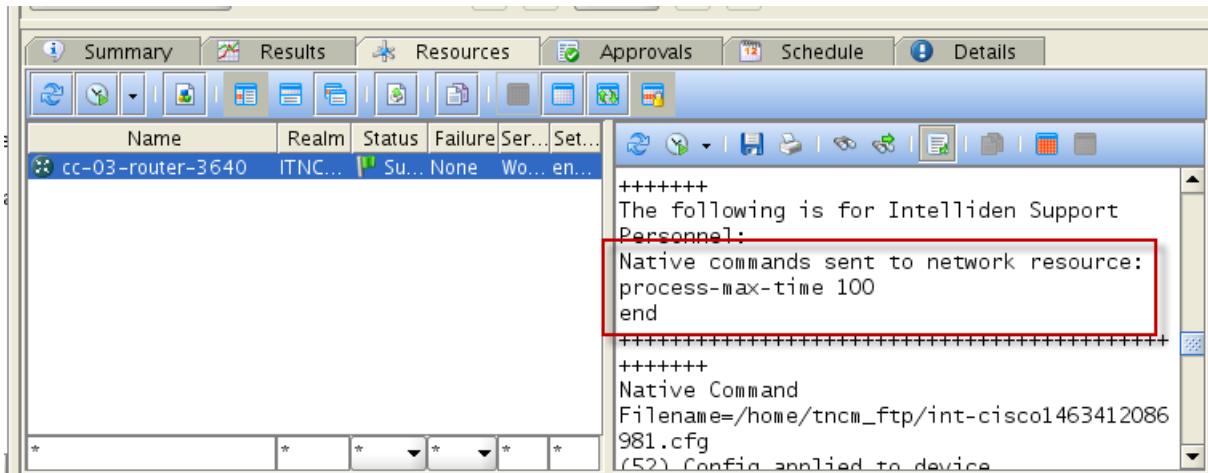
6. View the work log of one of the units of work. Find the command that the command set ran.
- Click one of the units of work. Click the **Resources** tab. Click the device in the **Resources** tab.

UOW ID	Type	Submitter	Request Type	Result
84	UOW	administrator	Native Command Set	SUCCESS
85	UOW	administrator	Command Set	SUCCESS
86	UOW	administrator	Command Set	SUCCESS
87	UOW	administrator	Native Command Set	SUCCESS
88	UOW	administrator	Native Command Set	SUCCESS
89	UOW	administrator	Command Set	SUCCESS
90	UOW	administrator	Native Command Set	SUCCESS
91	UOW	administrator	Native Command Set	SUCCESS
92	UOW	administrator	Native Command Set	SUCCESS
93	UOW	administrator	Native Command Set	SUCCESS
94	UOW	administrator	Native Command Set	SUCCESS

The 'Resources' tab is selected. Below it is a table of devices:

Name	Realm	Status	Fail...	Se...	Se...
cc-03-router-	TN...	P...	S...	None	W...

- b. Scroll down in the work log and find the command that the command set ran.



The screenshot shows a software interface with a toolbar at the top and a main window divided into two panes. The left pane is a table with columns: Name, Realm, Status, Failure, Ser..., Set... and contains one row for 'cc-03-router-3640' with status 'Su...' and 'None'. The right pane is a log window with the following text:

```
+++++++
The following is for Intelliden Support Personnel:
Native commands sent to network resource:
process-max-time 100
end
+++++++
Native Command
Filename=/home/tncm_ftp/int-cisco1463412086
981.cfg
(52) Config applied to device
```

Feel free to examine the other units of work.

Leave the compliance manager client as is.

Leave the configuration manager client as is.



19 Advanced definitions exercises

In this unit, you learn how to use various advanced features in policies, including XPath to search for text, and the extract function to retrieve text from a device.

Exercise 1 Creating a policy that uses XPath definitions

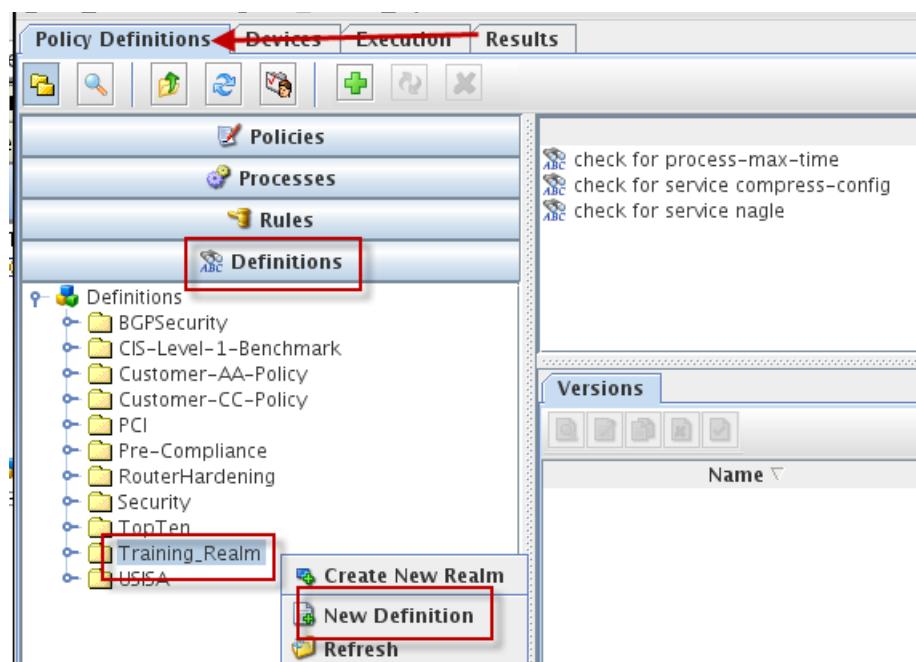
In this exercise, you create two definitions, one rule, and one policy. The goal of this policy is to mark a Cisco router as noncompliant if any interface is configured to automatically negotiate either duplex mode or speed.

1. Return to the compliance manager client.
2. Create a definition in the Training_Realm named **check for duplex auto**. This definition searches to check whether any interface on a Cisco router is set to auto-negotiate the duplex mode setting. If the command is not found on any interface, the definition returns the result *fail*. Use the following values to complete the wizard.

Field	Value
Name	check for duplex auto
Description	This definition is looking for the command auto in the interface duplex subcommand.
	The auto command is found in the interface configuration of Cisco routers that run IOS version 11.2(10)P and higher. There are also full-duplex and half-duplex interface commands, but only the command duplex auto configures auto-negotiation.
Select Definition Type	Create Compliance Definition using SmartModel
Choose Model based on VTMOS	Vendor: Cisco Type: Router Model: 36* OS: *12.3*

Field	Value
Modelled Definition	Create Contextual XPath
Model	configuration > interface > FastEthernet > duplex
In context	auto
Match criteria	Match any
Evaluation result if context not found	Fail
Manual Override: Context Xpath	configuration/interface/*/duplex
Manual Override: Defined Xpath	auto
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Definition** section. Right-click **Training_Realm** and click **New Definition**. The **Create a Definition** wizard starts.



Exercise 1 Creating a policy that uses XPath definitions

- b. Enter **check for duplex auto** in the **Name** field. Enter the description from the preceding table. Select **Create Compliance Definition using SmartModel**. Click **Next**.

Definition Name & Description

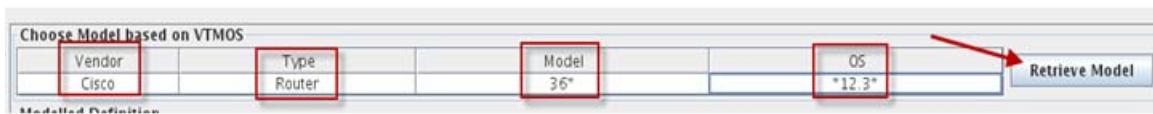
Name: check for duplex auto

Description: This definition is looking for the command auto in the interface duplex subcommand.

Select Definition Type

- Create Compliance Definition using CLI configuration lines
- Create Compliance Definition using Native Commands
- Create Compliance Definition using SmartModel

- c. Select **cisco** as the Vendor at the top of the window. Select **router** as the Type. Select **36*** as the Model. Select ***12.3*** as the OS. Click the **Retrieve Model** icon.



- d. Click **Create Contextual XPath**. Click **configuration > interface > FastEthernet > duplex** in the Model field. Click **auto** in the **In context** field. Click the **Add Evaluation** icon.

Modelled Definition

Create Direct XPath Create Contextual XPath

Model:

- diffserv
- dlsw
- dsru
- duplex**
- encapsulation
- fair-queue*
- fras
- full-duplex

In context:

- duplex
- auto**
- full
- half

XPath: auto

Add Evaluation

e. Click **Next**.

Enter variable details

Argument List		
Node	Node Description	XPath Fu...
configuration/interface/FastEthernet/ARG...	FastEthernet IEEE 802.3 – FastEthernet in...	=

f. Select **Match any** in the **Match criteria** field. Verify that **Fail** is selected in the **Evaluation result if context not found** field. Click **Finish**.

Enter test condition

Test conditions	
Test Condition:	Present in config
Match Criteria:	Match Any
Evaluation result if context not found:	Fail

g. Select the only evaluation in the evaluation list. Click the **Manual Override** icon.

Evaluation List							Evaluation List Criteria: Match All	Number:
Context Xpath	Defined Xpath	Test Condition	Match Criteria	Match Criteria Argument	Default Result	ContextOverride		
configuration/interface/FastEthernet/d...	auto	Present in con...	Match Any		Fail	configuration/interface/FastEthernet/		

Edit **Delete** **Test** **Manual Override**

h. Replace the text in the **Context Xpath** field with the following text:

configuration/interface/*/duplex

i. Verify that the following text is in the **Defined Xpath** field:

auto

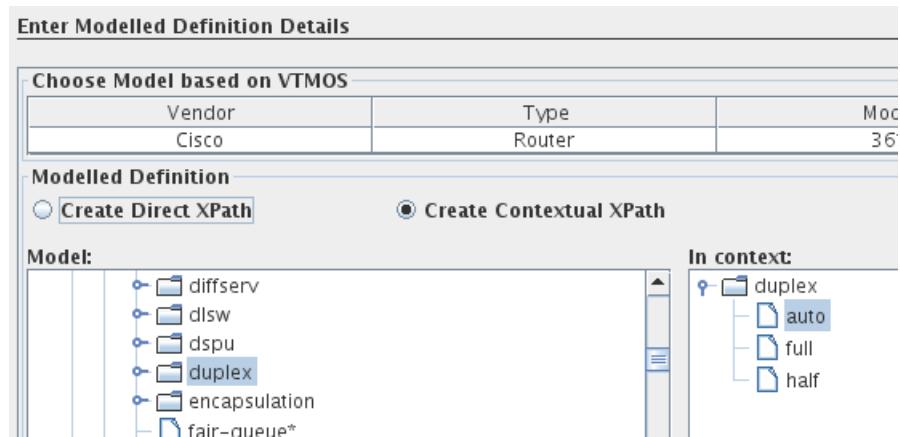
j. Click **OK**.

Manual Override

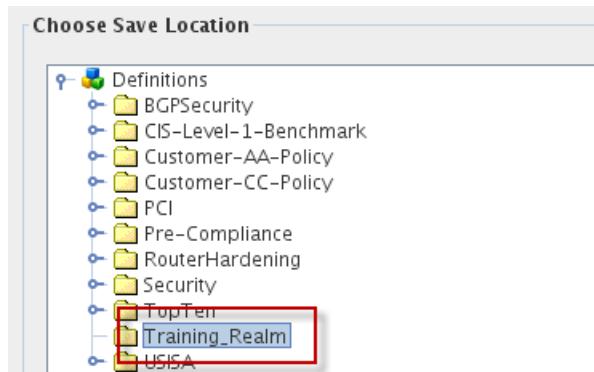
This option allows the Context Xpath and Defined XPath to be edited manually

Context Xpath:	configuration/interface/*/duplex
Context Nodes:	auto
Defined Xpath:	

- k. Click **Next** at the **Enter Modelled Definition Details** window.



- l. Click **Training_Realm**. Click **Finish**.

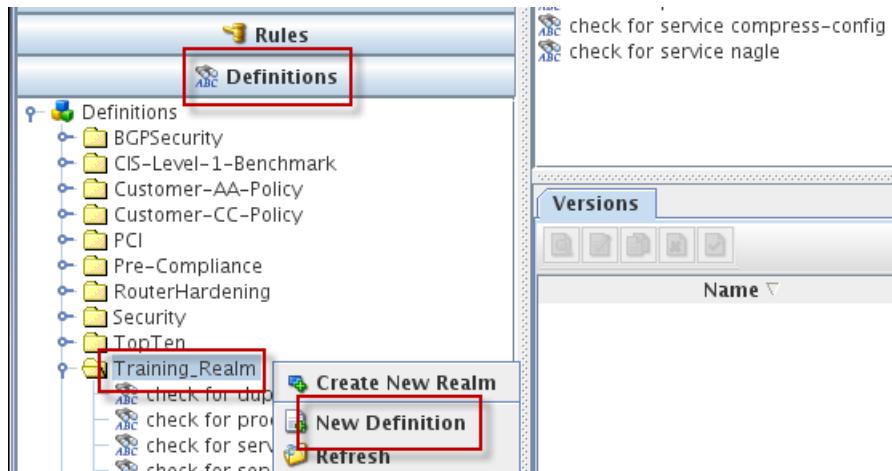


3. Create a definition in the Training_Realm named **check for speed auto**. This definition checks whether any interface on a Cisco router is set to auto-negotiate the speed setting. If the command is not found on any interface, the definition returns the result *fail*. Use the following values to complete the wizard.

Field	Value
Name	check for speed auto
Description	This definition is looking for the command auto in the interface speed subcommand.
	The speed auto command is found in the interface configuration of Cisco routers that run IOS version 11.2(10)P and higher.
Select Definition Type	Create Compliance Definition using SmartModel
Choose Model based on VTMOS	Vendor: Cisco Type: Router Model: 36* OS: *12.3*

Field	Value
Modelled Definition	Create Contextual XPath
Model	configuration > interface > FastEthernet > speed
In context	auto
Match criteria	Match any
Evaluation result if context not found	Fail
Manual Override: Context Xpath	configuration/interface/*/speed
Manual Override: Defined Xpath	auto
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Definition** section. Right-click **Training_Realm** and click **New Definition**. The **Create a Definition** wizard starts.



Exercise 1 Creating a policy that uses XPath definitions

- b. Enter **check for speed auto** in the **Name** field. Enter the description from the preceding table. Select **Create Compliance Definition using SmartModel**. Click **Next**.

Definition Name & Description

Name: check for speed auto

Description: This definition is looking for the command auto in the interface speed sub-command.

Select Definition Type

- Create Compliance Definition using CLI configuration lines
- Create Compliance Definition using Native Commands
- Create Compliance Definition using SmartModel

- c. Select **cisco** as the Vendor. Select **router** as the Type. Select **36*** as the Model. Select ***12.3*** as the OS. Click the **Retrieve Model** icon.

Choose Model based on VTMOS				
Vendor	Type	Model	OS	Retrieve Model
Cisco	Router	36*	*12.3*	

- d. Click **Create Contextual XPath**. Click **configuration > interface > FastEthernet > speed** in the Model field. Click **auto** in the In context field. Click the **Add Evaluation** icon.

Modelled Definition

Create Direct XPath Create Contextual XPath

Model:

- sna
- snapshot
- snmp
- spanning-tree
- speed**
- standby
- switchport
- tarp

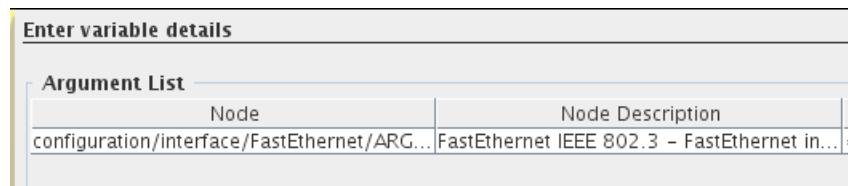
In context:

- speed
- _310
- 3100
- auto**

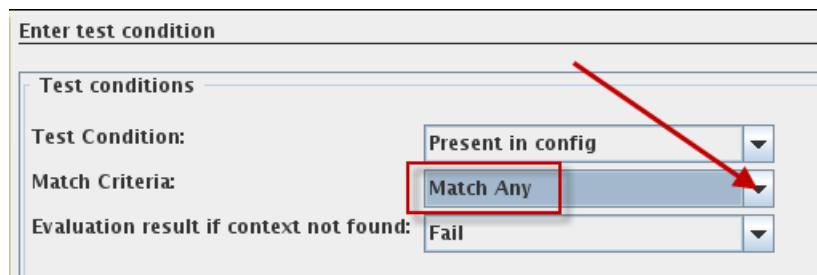
XPath: auto

Add Evaluation

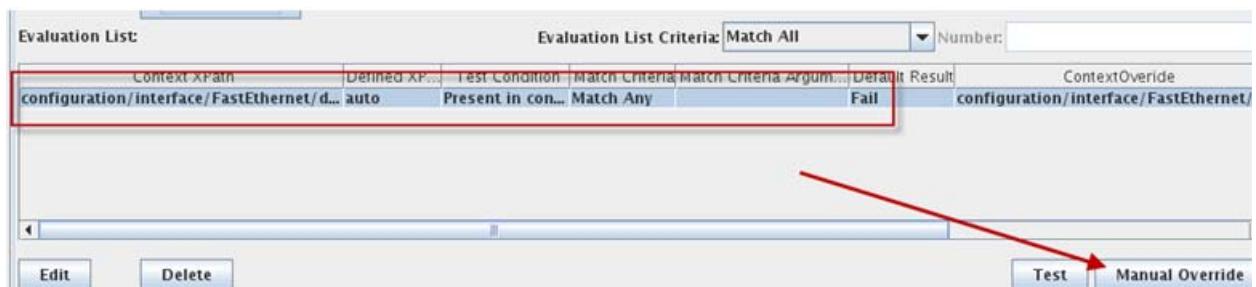
e. Click **Next**.



f. Select **Match any** in the **Match criteria** field. Verify that **Fail** is selected in the **Evaluation result if context not found** field. Click **Finish**.



g. Select the only evaluation in the evaluation list. Click the **Manual Override** icon.



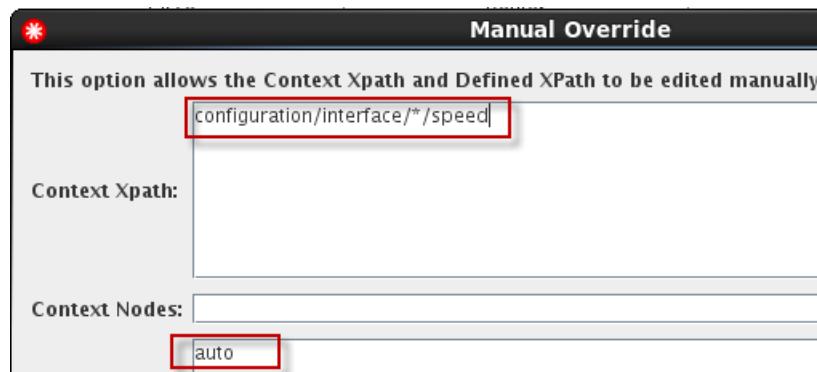
h. Replace the text in the **Context Xpath** field with the following text:

configuration/interface/*/speed

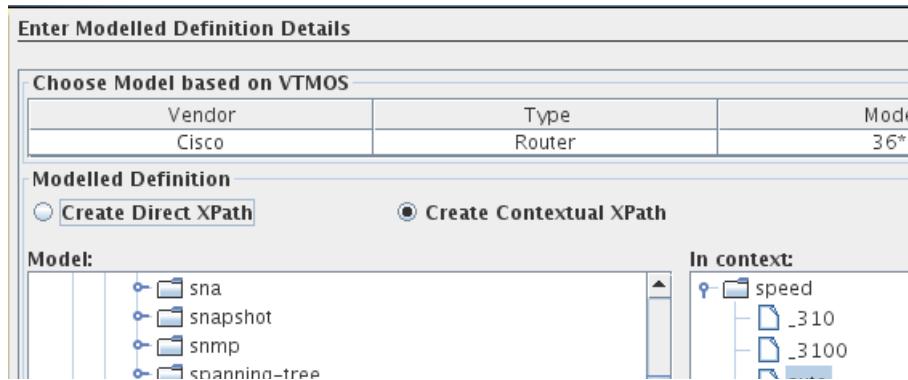
i. Verify that the following text is in the **Defined Xpath** field:

auto

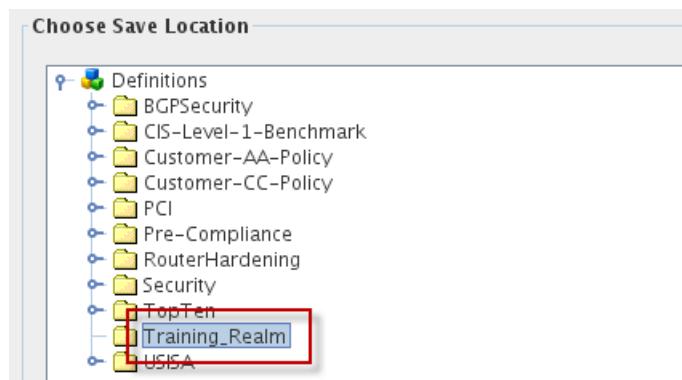
j. Click **OK**.



- k. Click **Next** at the **Enter Modelled Definition Details** window.



- l. Click **Training_Realm**. Click **Finish**.



4. Create a rule in the Training_Realm named **disable interface auto-negotiate**. Configure this rule to determine that the device is not compliant if either of the following interface sub commands is present.

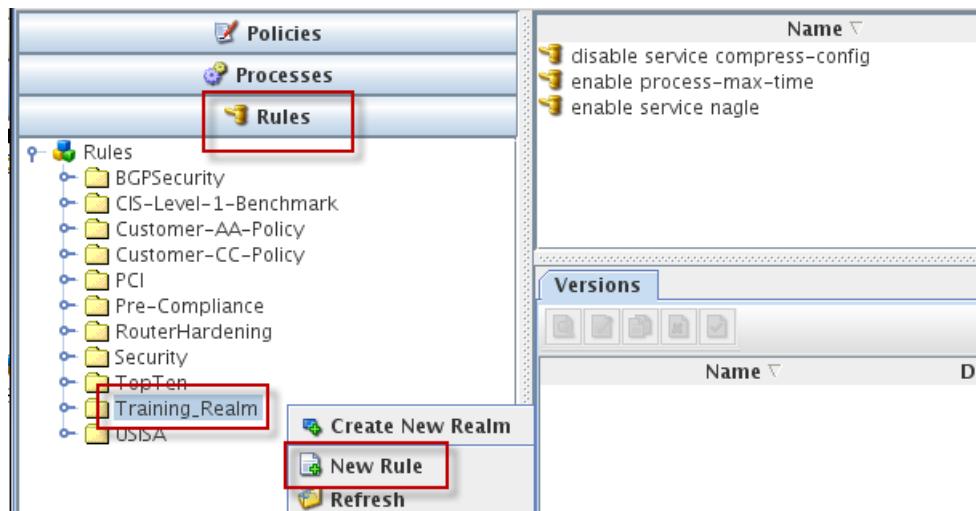
- duplex auto
- speed auto

If the commands are not present in the device configuration, the rule should determine that the device is compliant. Use the following values to complete the wizard.

Field	Value
Name	disable interface auto-negotiate
Description	This rule determines that a device configuration is not compliant if the duplex and speed settings on an interface are configured for auto-negotiation.
Application Device Filter	Use these values. <ul style="list-style-type: none"> • Vendor: Cisco • Type: Router • Model: * • OS: Choose the advanced OS options. Configure the rule to use operating systems >=11.2

Field	Value
Build Graphical Rule	<p>Use the following objects in this graphical rule.</p> <ul style="list-style-type: none"> • Add one start icon. • Add the first definition icon. Use the check for duplex auto definition. Link the start icon to this definition icon. • Add the second definition icon. Use the check for speed auto definition. Link the F side of the check for duplex auto definition icon to the check for speed auto definition icon. • Add one compliant icon to use if both definitions are false. Link the F side of the check for speed auto definition to the compliant icon. • Add one non-compliant icon to use if either of the definitions is true. There should be no action if the device is noncompliant. Link the T side of both definition icons to the noncompliant icon.
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Rules** section. Right-click **Training_Realm** and click **New Rule**. The Create a Rule wizard starts.



Exercise 1 Creating a policy that uses XPath definitions

- b. Enter **disable interface auto-negotiate** in the **Name** field. Enter the description from the preceding table. Select **Cisco** as the vendor. Select **Router** as the type. Select * as the model. Click the OS field and select **Advanced**. The advanced selection window opens.

Rule Name & Description

Name: disable interface auto-negotiate **Revision:** 1

Description: This rule determines that a device configuration is not compliant if the duplex and speed settings on an interface are configured for auto-negotiation.

Applicable Device Filter

Vendor	Type	Model	OS
Cisco	Router	*	<input type="button" value="Advanced"/>

- c. Select the **>=** option. Enter **11.2** in the **>=** field. Click **OK**.

*** OS Advanced**

Choose OS Filter

>= 11.2
 <= _____
 Range Fr... _____ To _____

- d. Click **Next**.

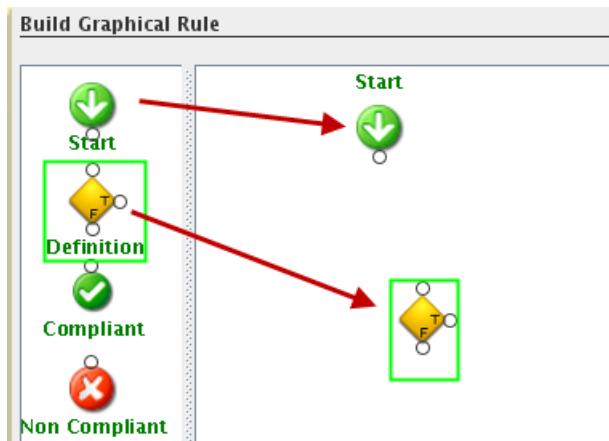
Enter Rule Details...

Rule Name & Description

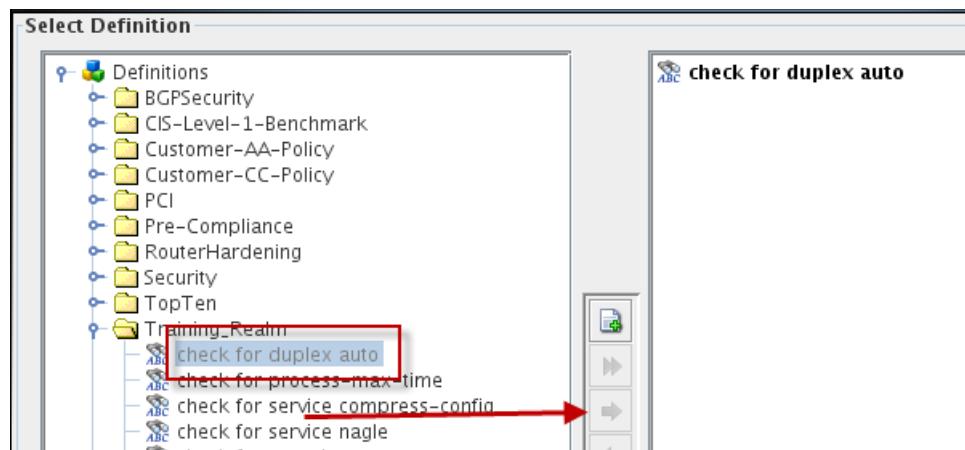
Name: disable interface auto-negotiate **Revision:** []

Description: This rule determines that a device configuration is not compliant if the duplex and speed settings on an interface are configured for auto-negotiation.

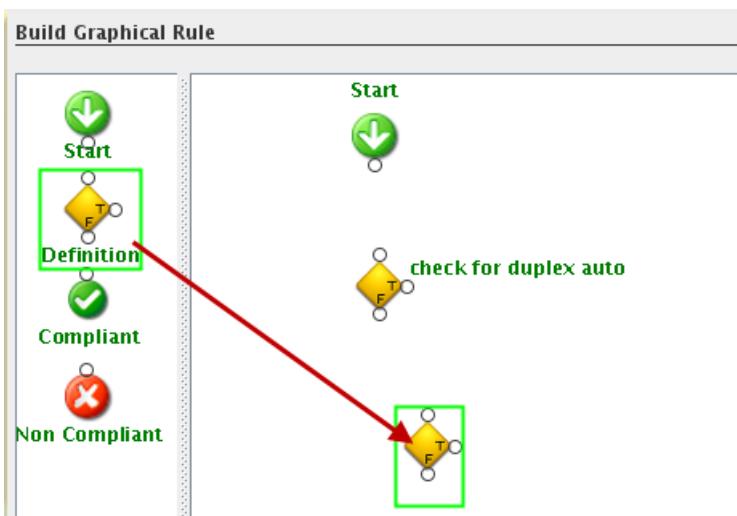
- e. Drag the **Start** icon into the rule. Drag the first **Definition** icon into the rule. When you drop the Definition icon, the Select Definition window opens.



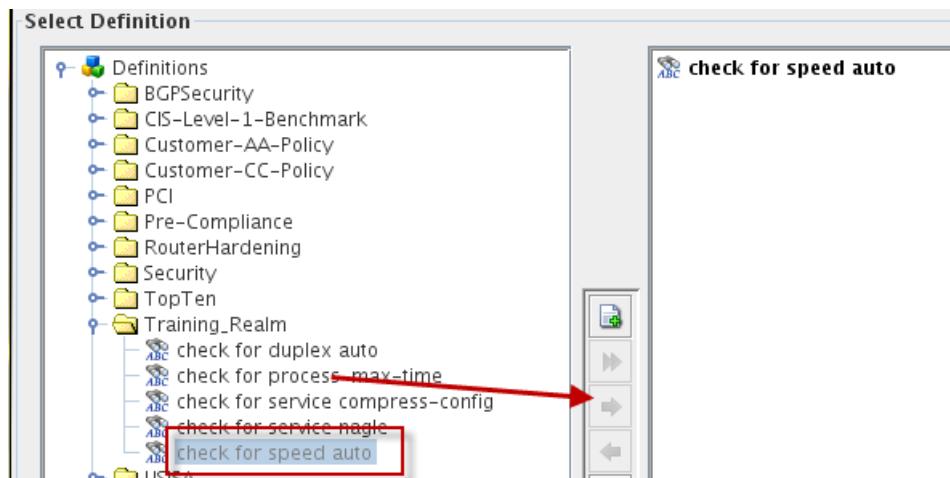
- f. Expand **Training_Realm**. Click the **Training_Realm > check for duplex auto** definition. Click the right arrow icon to move the definition to the right of the window. Click **OK**.



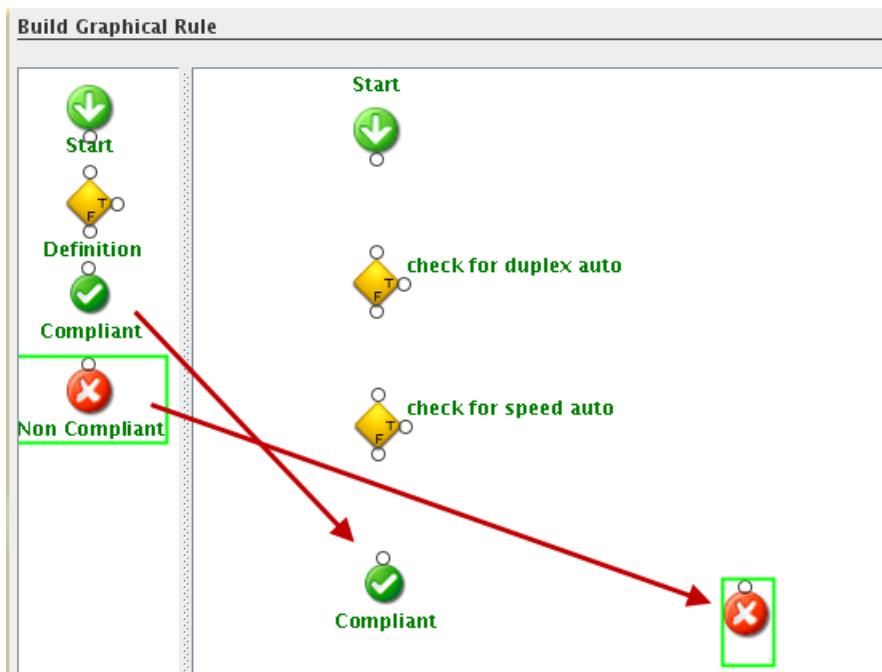
- g. Drag the second **Definition** icon into the rule. When you drop the second Definition icon, the Select Definition window opens.



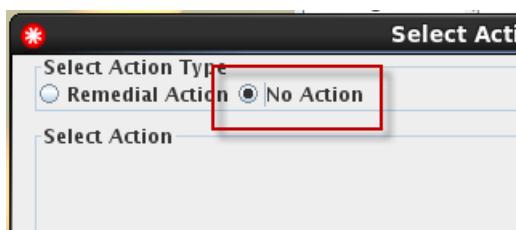
- h. Expand **Training_Realm**. Click the **Training_Realm > check for speed auto** definition. Click the right arrow icon to move the definition to the right of the window. Click **OK**.



- i. Drag the **Compliant** icon into the rule. Drag the **Non Compliant** icon into the rule. When you drop the Non Compliant icon, the Select Action Type window opens.

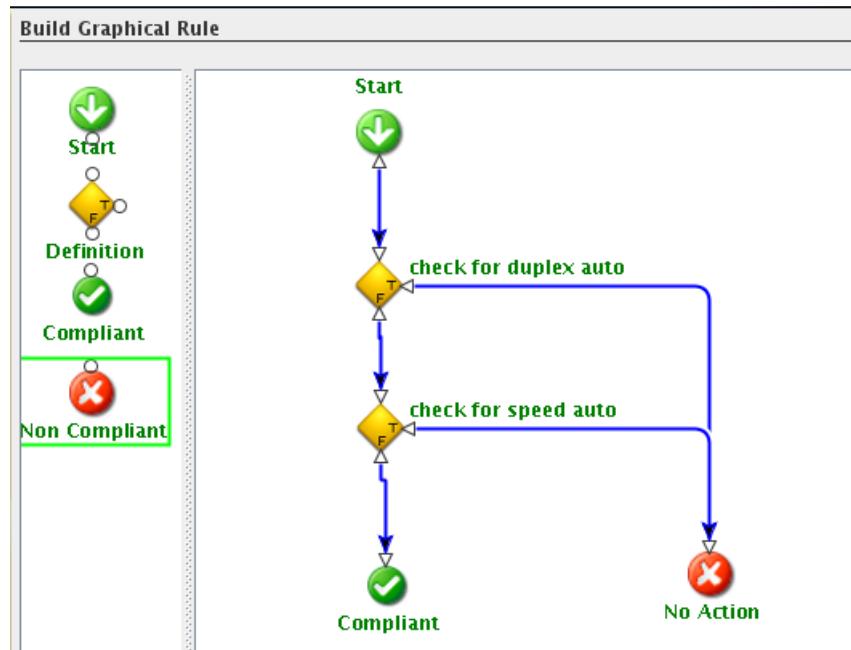


- j. Click **No Action**. Click **OK**.

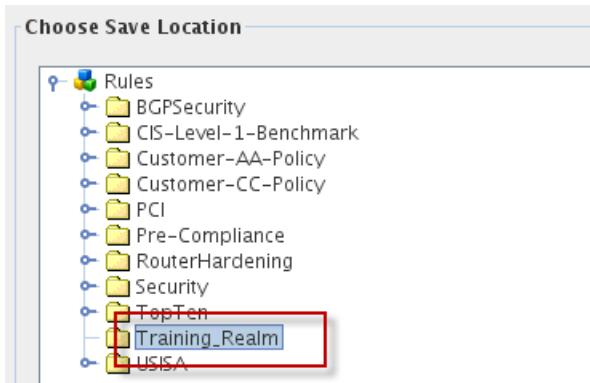


- k. Add a line from the **Start** icon to the **check for duplex auto** definition icon by dragging your cursor from one icon to the other. Add a line from the **F** in the **check for duplex auto** definition icon to the **check for speed auto** definition icon. Add a line from the **F** in the

check for speed auto definition icon to the **Compliant** icon. Add a line from the **T** in both of the definition icons to the **Non Compliant** icon. Click **Next**.



- I. Click **Training_Realm**. Click **Finish**.

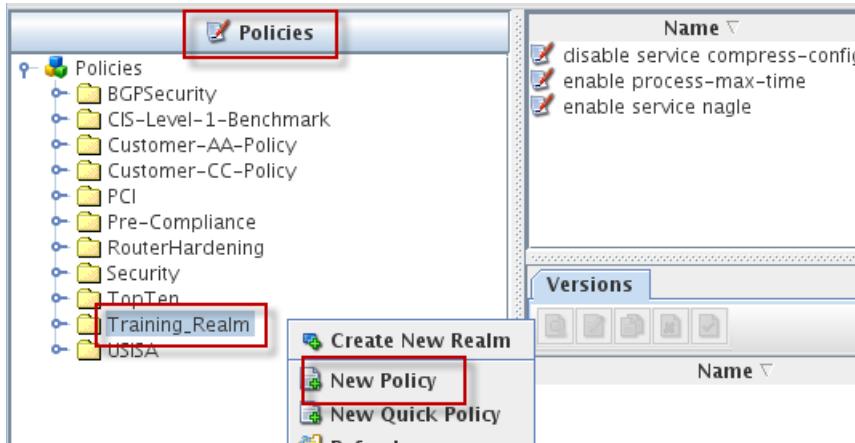


5. Create a policy in the **Training_Realm** named **disable interface auto-negotiate**. Configure this policy to use the rule **disable interface auto-negotiate**. Use the following values to complete the wizard.

Field	Value
Name	disable interface auto-negotiate
Description	Auto-negotiation should be disabled on all interfaces. This policy marks a device as non-compliant if any interface is set to auto-negotiate duplex mode or speed.
Severity	2
Weight	65
Send Trap	Configure this policy to send a trap.

Field	Value
Applicable Device Filter	Use the following settings in this policy <ul style="list-style-type: none"> • Vendor: * • Type: * • Model: * • OS: *
Rules Included	disable interface auto-negotiate
Action Type	EMail
Action	email to training NOC
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Policies** section. Right-click **Training_Realm** and click **New Policy**. The Create a Policy wizard starts.

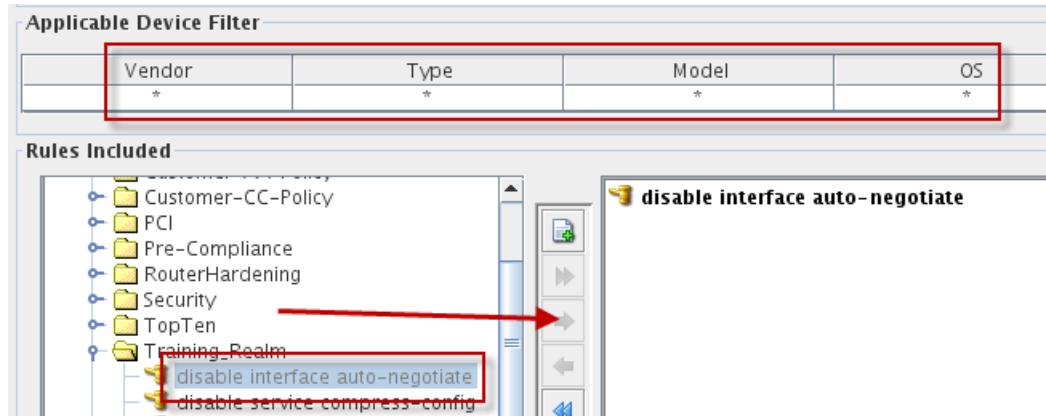


- b. Enter **disable interface auto-negotiate** in the **Name** field. Enter the description from the preceding table. Select **Severity 2**. Enter **65** in the **Weight** field. Select **Send Trap**.

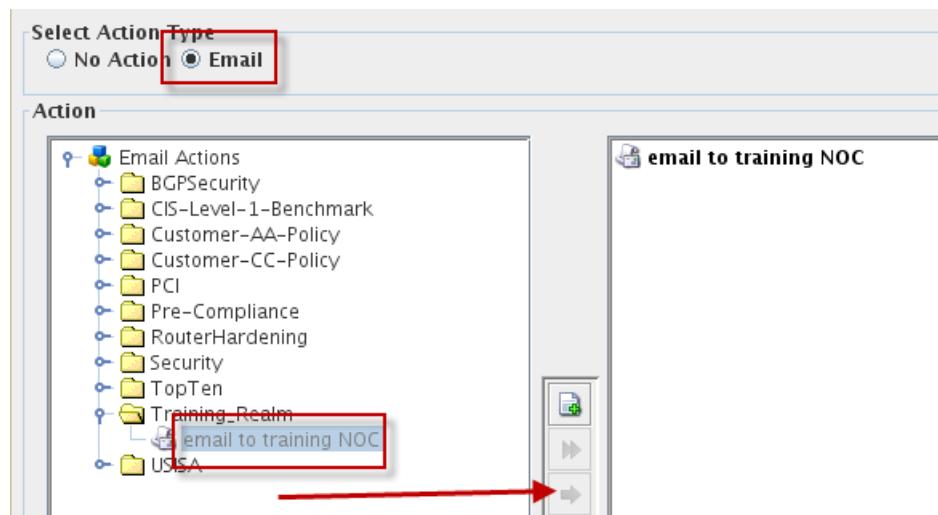
This is a configuration dialog for a new policy. The fields are as follows:

- Name:** disable interface auto-negotiate (highlighted by a red box)
- Description:** Auto-negotiation should be disabled on all interfaces. This policy marks a device as non-compliant if any interface is set to auto-negotiate duplex mode or speed.
- Impact:** (empty field)
- Severity:** 2 (highlighted by a red box)
- Weight:** 65 (highlighted by a red box)
- Send Trap:** (highlighted by a red box)
- Preemptive:**

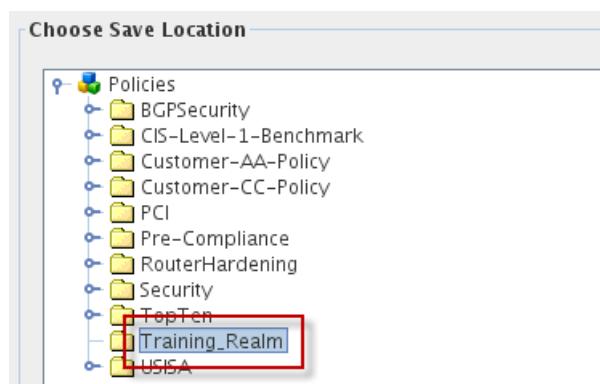
- c. Leave the value of * in the **Vendor**, **Type**, **Model**, and **OS** fields. Click the **Training_Realm > disable interface auto-negotiate** rule. Click the right arrow icon to move the rule to the right of the window. Click **Next**.



- d. Select **email** as the **Action Type**. Click the **Training_Realm > email to training NOC** email action. Click the right arrow icon to move the email action to the right of the window. Click **Next**.



- e. Click **Training_Realm**. Click **Finish**.



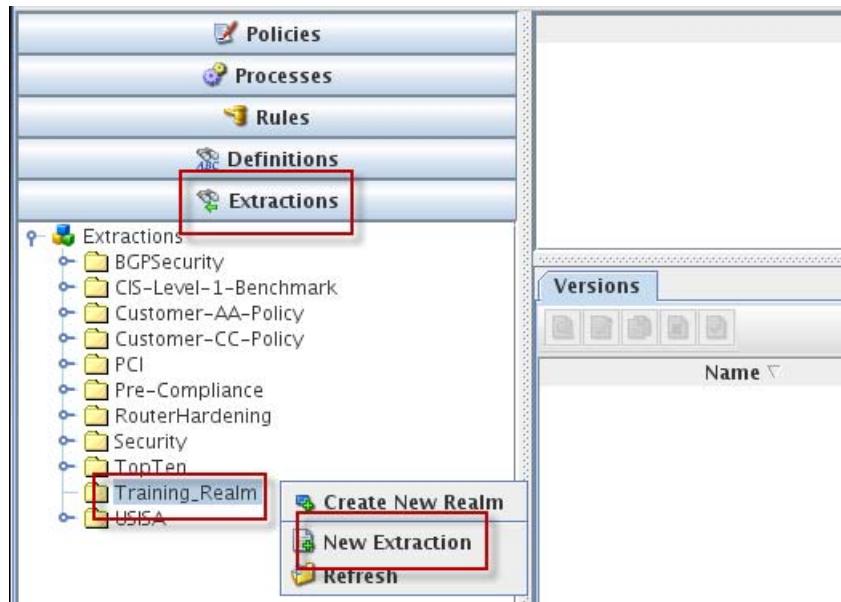
Exercise 2 Creating a policy that uses an extraction

In this exercise, you create one extraction, one definition, one rule, and one policy. The goal of this policy is to mark a Cisco router as compliant if the TACACS server IP addresses in the configuration are also included in an access list.

1. Create an extraction in the Training_Realm named **extract TACACS server IP addresses**. Configure this extraction to obtain the IP addresses of all instances of the tacacs-server host command in a Cisco router configuration. Use the following values to complete the wizard.

Field	Value
Name	extract TACACS server IP addresses
Description	This extraction obtains all TACACS server IP addresses from a Cisco device configuration.
Select Extraction Type	Create extraction using CLI configuration lines
Enter lines to you want to match	tacacs-server host.*
Extract what	3
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Extractions** section. Right-click **Training_Realm** and click **New Extraction**. The Create an Extraction wizard starts.



- b. Enter **extract TACACS server IP addresses** in the **Name** field. Enter the description from the preceding table. Select **Create extraction using CLI configuration lines**. Click **Next**.

Extraction Name & Description

Name: Extract TACACS server IP addresses

Description: This extraction obtains all TACACS server IP addresses from a Cisco device configuration.

Select Extraction Type

Create extraction using CLI configuration lines

- c. Enter the following text in the **Enter lines to you want to match** field:

```
tacacs-server host .*
```

- d. Enter **3** in the **Extract what** field. Click **Next**.

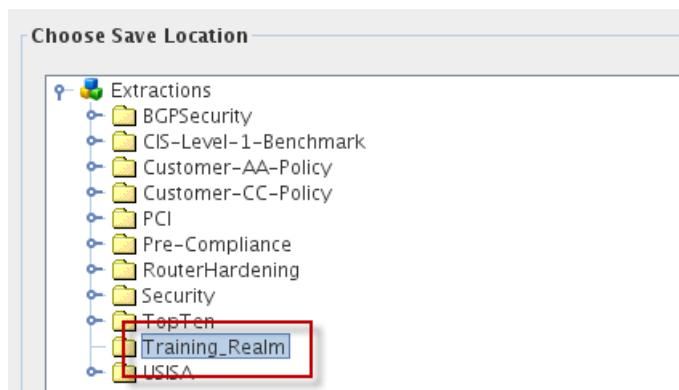
Enter Native Extraction Details

Extraction Details

Enter line(s) to you want to match: tacacs-server host .*

Extract what? (e.g. To extract second word of matching line enter '1') 3

- e. Click **Training_Realm**. Click **Finish**.

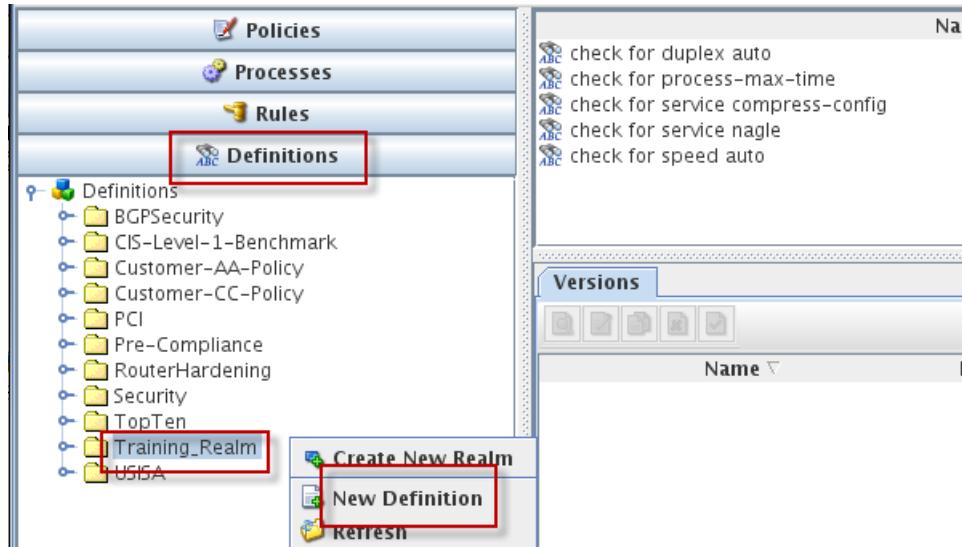


2. Create a definition in the **Training_Realm** named **check for TACACS servers**. Use the extraction that is named **extract TACACS server IP addresses**. The goal of this definition is to search for the list of IP addresses obtained by the extraction in the command **permit tcp host**.

If the IP addresses are not found, the definition returns the result *fail*. Use the following values to complete the wizard.

Field	Value
Name	check for TACACS servers
Description	This definition looks for the following command: permit tcp host \$Extraction{extract TACACS server IP addresses}
	The permit tcp host command is used to configure access lists. This definition compares the IP addresses obtained by the extraction to the access list entries on the device to verify that traffic to and from all TACACS servers is permitted.
Select Definition Type	Create Compliance Definition using CLI configuration lines
Enter lines you want to match	permit tcp host \$Extraction{extract TACACS server IP addresses}
Match Criteria	Match All
Evaluation result if context not found	Fail
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Definition** section. Right-click **Training_Realm** and click **New Definition**. The Create a Definition wizard starts.



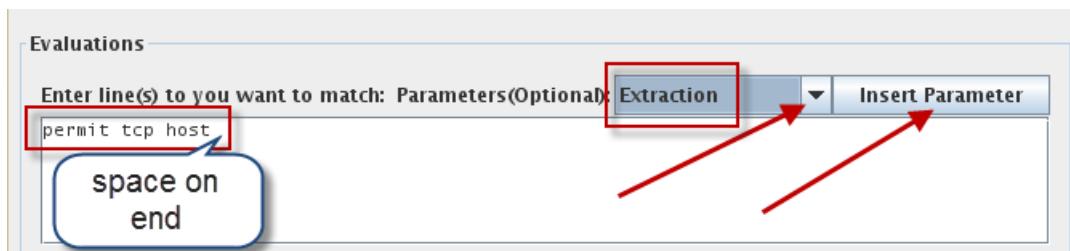
- b. Enter **check for TACACS servers** in the **Name** field. Enter the description from the preceding table. Select **Create Compliance Definition using CLI configuration lines**. Click **Next**.

Definition Name & Description

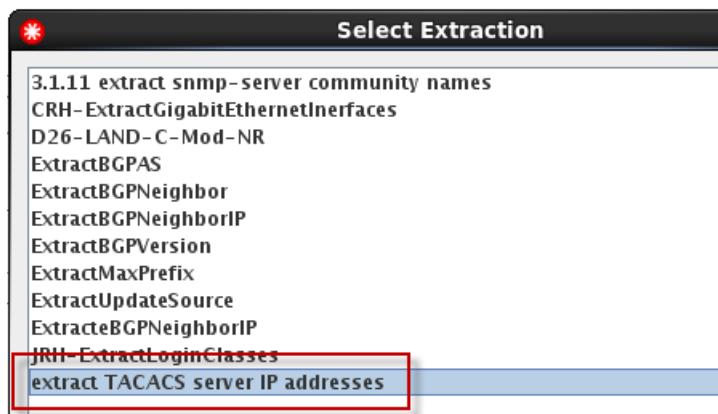
Name: check for TACACS servers

Description: This definition looks for the following command:
permit tcp host \$Extraction{extract TACACS server IP addresses}

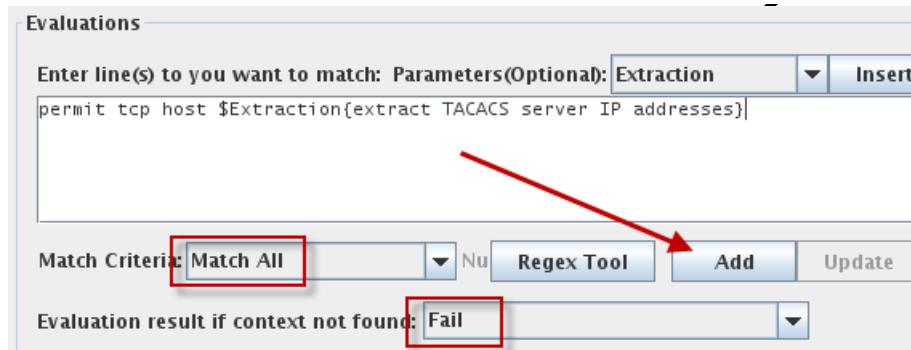
- c. Type the following text in the **Enter lines you want to match** field:
permit tcp host
- d. Add a space after the command. Select **Extraction** and click the **Insert Parameter** icon.



- e. Select **extract TACACS server IP addresses**. Click **OK**.



- f. Select **Match All** in the **Match Criteria** field. Select **Fail** in the **Evaluation result if context not found** field. Click **Add**.

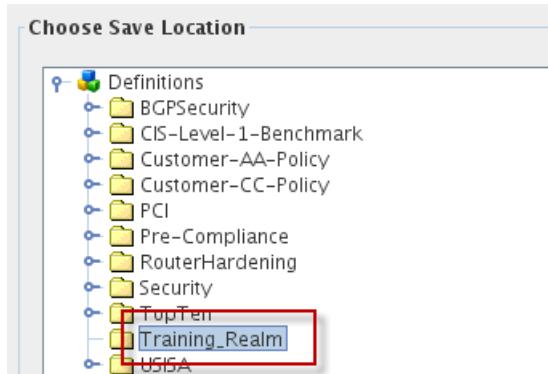


The evaluation is added to the evaluation list at the bottom of the window.

- g. Click **Next**.

Evaluation List:	Evaluation List Criteria:	Match All	Number:
permit tcp host \$Extraction{extract TACACS server IP addresses}		Match All	Fail

- h. Click **Training_Realm**. Click **Finish**.



3. Create a rule in the **Training_Realm** named **enable TACACS tcp traffic**. Configure this rule to determine that the device is compliant if all TACACS servers that the extraction finds are present in a tcp permit access list. If the TACACS server IP addresses are not present in the device configuration, the rule should determine that the device is not compliant. Use the following values to complete the wizard.

Field	Value
Name	enable TACACS tcp traffic
Description	This rule determines that a device configuration is compliant if all TACACS servers that are listed in the configuration have an entry in a tcp permit access list.

Field	Value
Application Device Filter	Use these values. <ul style="list-style-type: none"> Vendor: Cisco Type: Router Model: * OS: *
Build Graphical Rule	Use the following objects in this graphical rule. <ul style="list-style-type: none"> Add one Start icon. Add one Definition icon. Use the check for TACACS servers definition. Link the Start icon to the Definition icon. Add one Compliant icon to use if the definition is true. Link the T side of the Definition to the Compliant icon. Add one Non Compliant icon to use if the definition is false. There should be no action if the device is noncompliant. Link the F side of the Definition to the Non Compliant icon.
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Rules** section. Right-click **Training_Realm** and click **New Rule**. The Create a Rule wizard starts.

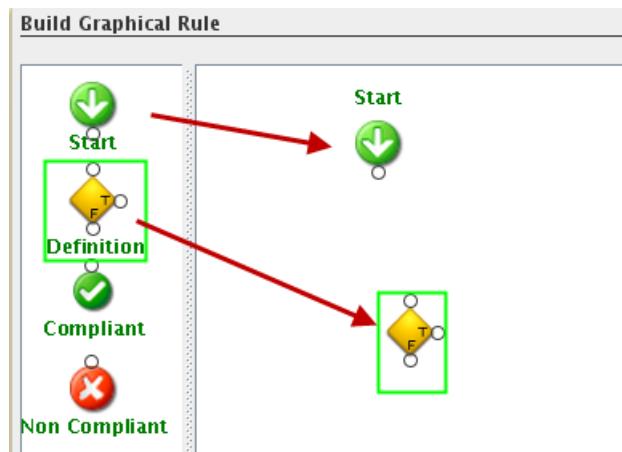


Exercise 2 Creating a policy that uses an extraction

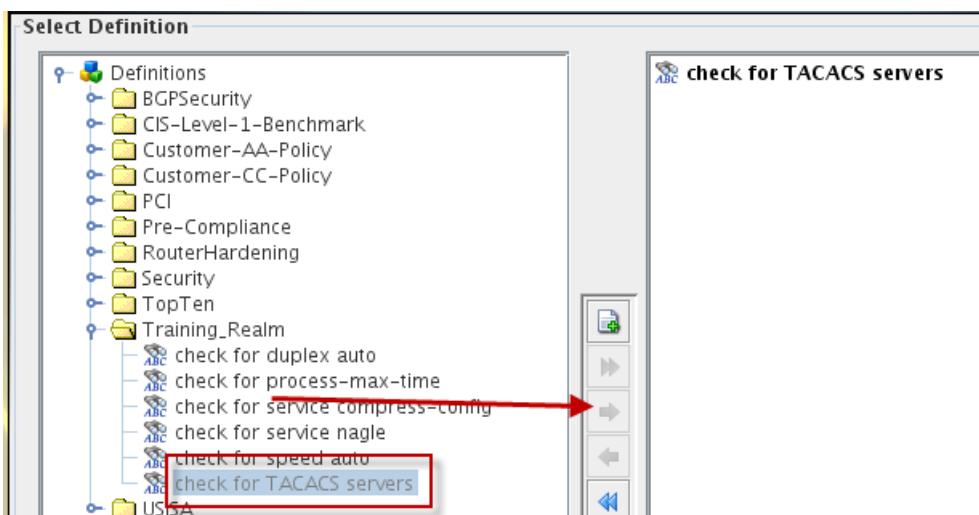
- b. Enter **enable TACACS tcp traffic** in the **Name** field. Enter the description from the preceding table. Select **Cisco** as the vendor. Select **Router** as the type. Select * as the model. Select * as the OS. Click **Next**.

Vendor	Type	Model	OS
Cisco	Router	*	*

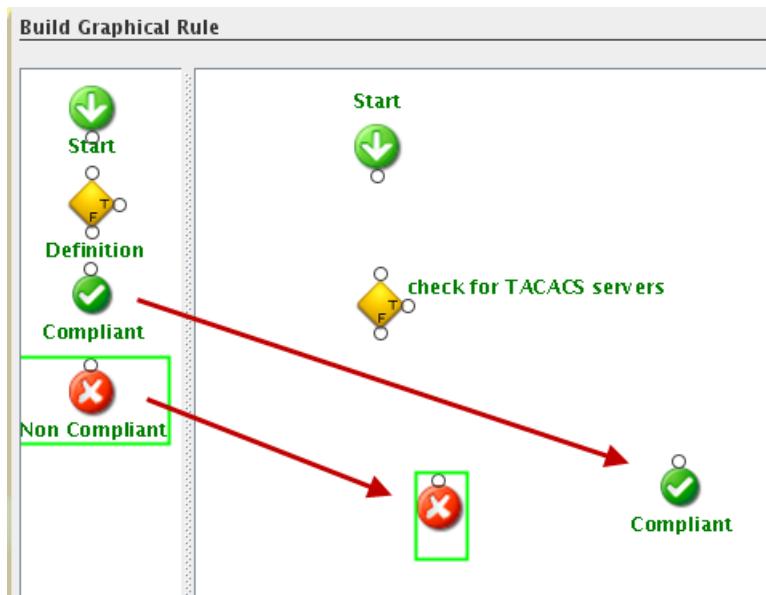
- c. Drag the **Start** icon into the rule. Drag the **Definition** icon into the rule. When you drop the **Definition** icon, the Select Definition window opens.



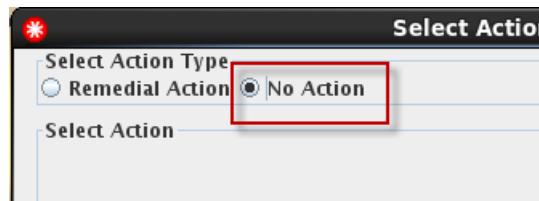
- d. Expand **Training_Realm**. Click the **Training_Realm > check for TACACS servers** definition. Click the right arrow icon to move the definition to the right of the window. Click **OK**.



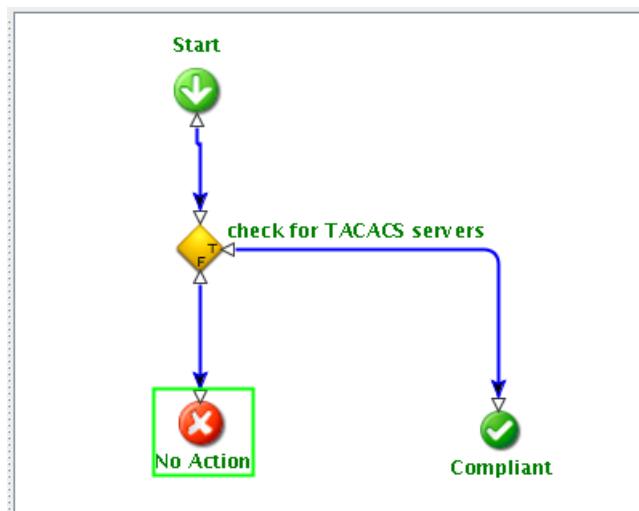
- e. Drag the **Compliant** icon into the rule. Drag the **Non Compliant** icon into the rule. When you drop the **Non Compliant** icon, the Select Action Type window opens.



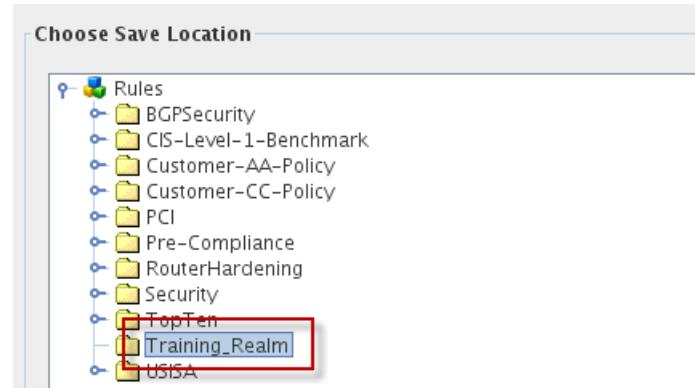
- f. Click **No Action**. Click **OK**.



- g. Add a line from the **Start** icon to the **Definition** icon by dragging your cursor from one icon to the other. Add a line from the **F** in the **Definition** icon to the **Non Compliant** icon. Add a line from the **T** in the **Definition** icon to the **Compliant** icon. Click **Next**.



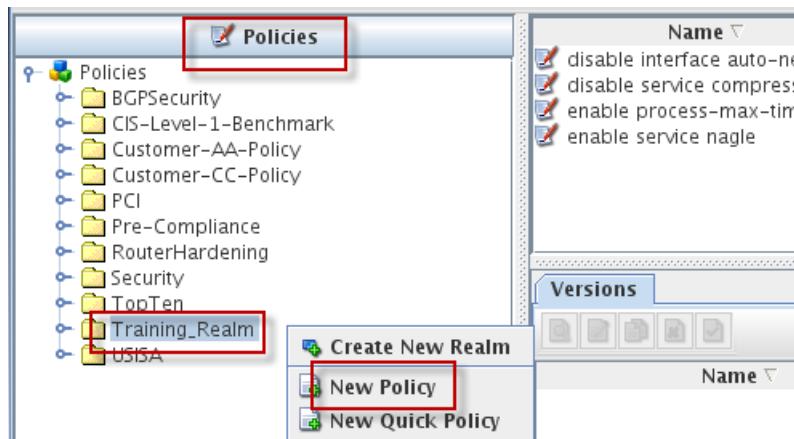
h. Click **Training_Realm**. Click **Finish**.



4. Create a policy in the **Training_Realm** named **enable TACACS tcp traffic**. Configure this policy to use the rule **enable TACACS tcp traffic**. Use the following values to complete the wizard.

Field	Value
Name	enable TACACS tcp traffic
Description	TCP traffic should be permitted to and from all TACACS servers. This policy marks a device as non-compliant if any TACACS server that is listed in the configuration is not permitted in an access list.
Severity	2
Weight	70
Send Trap	Configure this policy to send a trap.
Applicable Device Filter	Use the following settings in this policy <ul style="list-style-type: none"> • Vendor: * • Type: * • Model: * • OS: *
Rules Included	enable TACACS tcp traffic
Action Type	EMail
Action	email to training NOC
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Policies** section. Right-click **Training_Realm** and click **New Policy**. The Create a Policy wizard starts.



- b. Enter **enable TACACS tcp traffic** in the **Name** field. Enter the description from the preceding table. Select **Severity 2**. Enter **70** in the **Weight** field. Select **Send Trap**.

Policy Name, Description & Severity	
Name:	<input type="text" value="enable TACACS tcp traffic"/>
Description:	TCP traffic should be permitted to and from all TACACS servers. This policy marks a device as non-compliant if any TACACS server listed in the configuration is not permitted in an access list.
Impact:	
Severity:	<input type="text" value="2"/> <input type="button" value="▼"/>
Weight:	<input type="text" value="70"/> <input type="button" value="▼"/>
<input checked="" type="checkbox"/> Send Trap <input type="checkbox"/> Preemptive	

- c. Enter **enable TACACS tcp traffic** in the **Name** field. Enter the description from the preceding table. Select **Severity 2**. Enter **70** in the **Weight** field. Select **Send Trap**. Leave the value of * in the **Vendor**, **Type**, **Model**, and **OS** fields. Click the **Training_Realm > enable TACACS tcp traffic** rule. Click the right arrow icon to move the rule to the right of the window. Click **Next**.

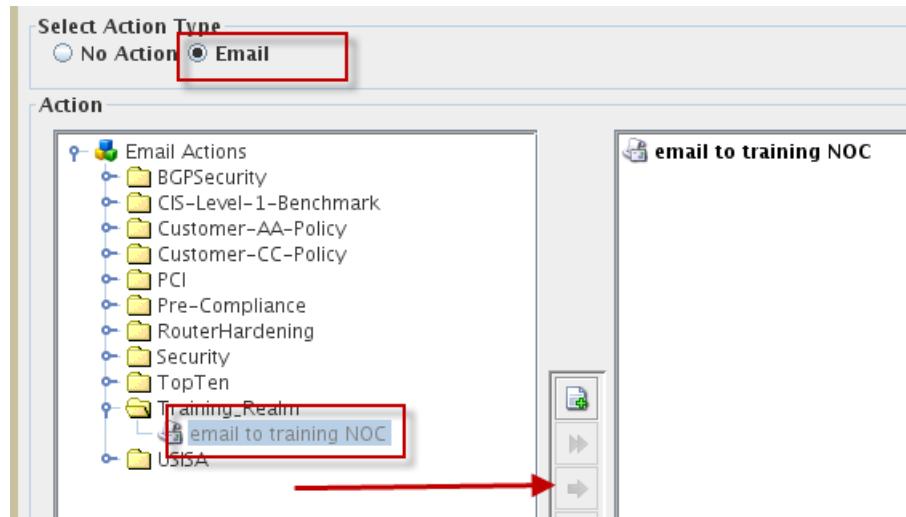
Applicable Device Filter			
Vendor	Type	Model	OS
*	*	*	*

Rules Included

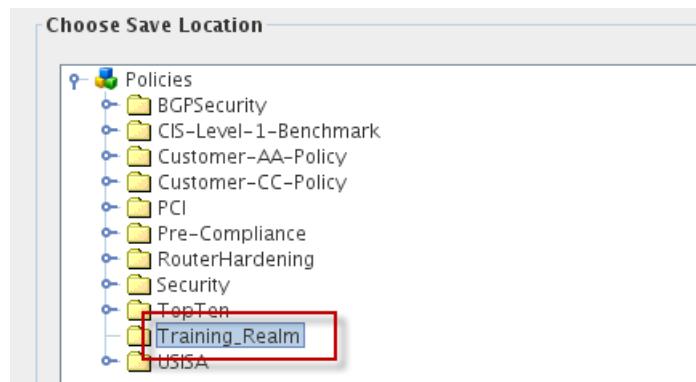
- Pre-Compliance
- RouterHardening
- Security
- TopTen
- Training_Realm
 - disable interface auto-negotiate
 - disable service compress-config
 - enable process-max-time
 - enable service nagle
 - enable TACACS tcp traffic**
- USISA

A red arrow points from the 'enable TACACS tcp traffic' rule in the 'Rules Included' list to the right arrow icon in the center of the window, indicating the action to move it to the right pane.

- d. Select **email** as the **Action Type**. Click the **Training_Realm > email to training NOC** email action. Click the right arrow icon to move the email action to the right of the window. Click **Next**.



- e. Click **Training_Realm**. Click **Finish**.



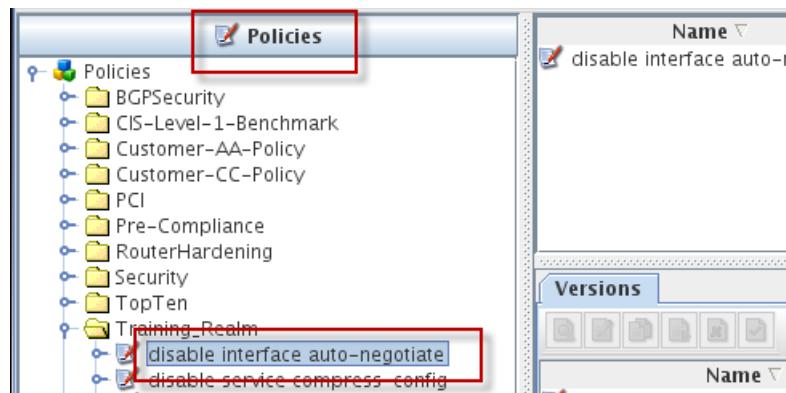
Exercise 3 Testing the new policies

In this exercise, you test the two policies that include XPath and extraction definitions.

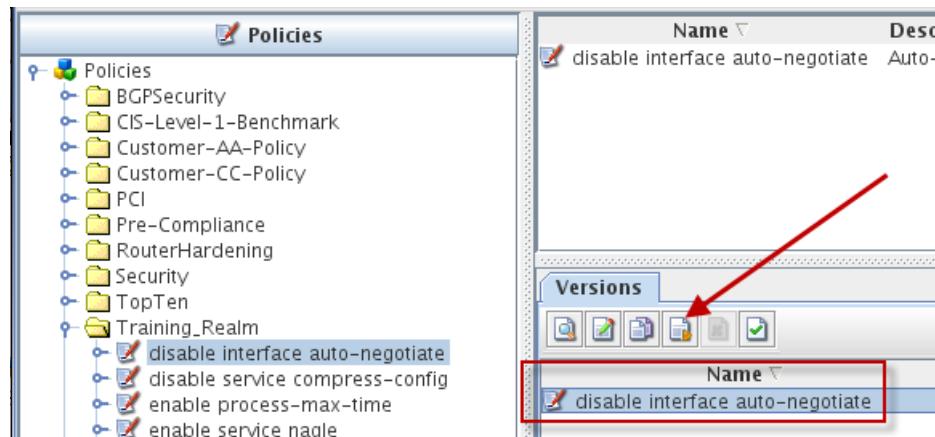
1. Test the **disable interface auto-negotiate** policy. Use the values in the following table to complete the test wizard. When you finish, view the details of the test results. Inspect the results of the evaluations to verify that they work as you intend. Notice that a device is not compliant if auto duplex or auto speed is enabled on any interface. If either evaluation returns the result PASS (green check), the rule determines that the device is not compliant.

Field	Value
Description	Policy test
Realms	Use the ITNCM > edge-network > customer_CC subrealm
Parameter value	Do not view parameters

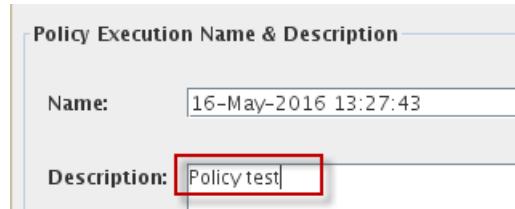
- a. Click the **Policy Definitions** tab. Click the **Policies** section. Expand **Training_Realm**. Click the **disable interface auto-negotiate** policy.



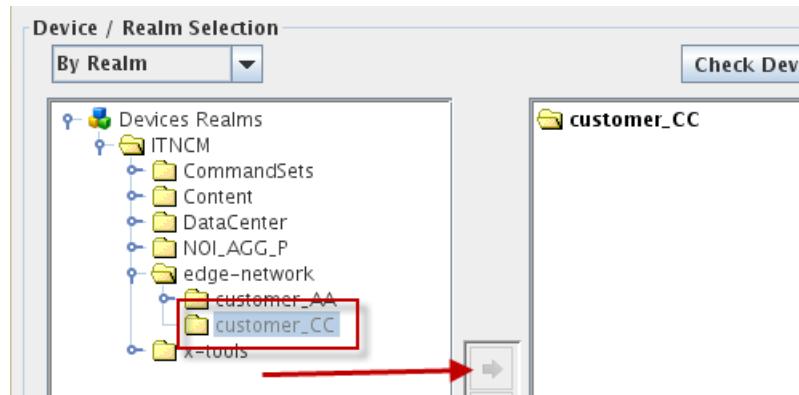
- b. Click the **Policy Definitions** tab. Click the **Policies** section. Expand **Training_Realm**. Click the **disable interface auto-negotiate** policy. Click the **disable interface auto-negotiate** policy in the **Versions** section. Click the **Test Policy** icon. The test wizard starts.



- c. Enter **Policy test** in the description field and click **Next**.



- d. Click the **ITNCM > edge-network > customer_CC** subrealm and click the right arrow icon to include it in the test. Click **Next**.



- e. When you are prompted to view associated parameters, click **No**.

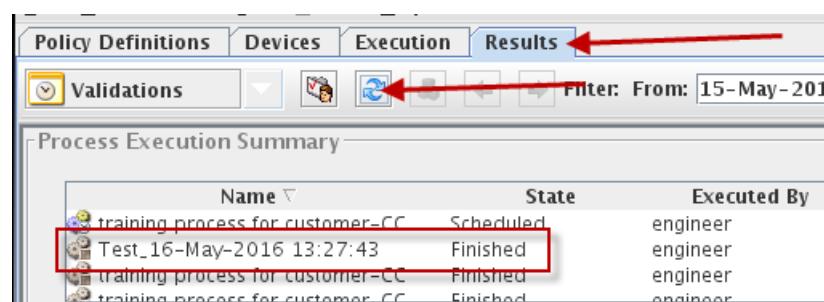


- f. Click **Finish**.



After you complete the test wizard, you see the **Results** tab.

- g. Click the refresh icon until the state of the test is finished.



- h. After you complete the test wizard, you see the **Results** tab. Click the refresh icon until the state of the test is Finished. After the test finishes, click the policy at the bottom of the window and click **Details**.

Policy Name	Severity	Revised	Date	Passes	Failed	Not Assessed	Exceptions
disable interface auto-negotiate	2	1	16-May-2016 13:32...0	3	0	0	

- i. Double-click one of the devices in the test results.

Policy	Device	Device Realm	Support Level
disable interface a...	cc-01-router-3640	ITNCM/edge-network...	SmartModel
disable interface a...	cc-02-router-3640	ITNCM/edge-network...	SmartModel
disable interface a...	cc-03-router-3640	ITNCM/edge-network...	SmartModel

- j. View the detailed results of each evaluation. Notice that if either evaluation returns the result PASS (green check), the rule determines that the device is not compliant.

cc-01-router-3640

[View Native Config](#) [View Modelled Config](#) [Open Policy](#) [Edit Policy](#)

- Policy:disable interface auto-negotiate
- Rule:disable interface auto-negotiate
- Definition:check for duplex auto
- Evaluation 1
- Definition:check for speed auto
- Evaluation 1

Searched in:-
XML Modelled Configuration

Searched For:-
Context XPath = configuration/interface/*/speed
Defined XPath = auto
Context Nodes =
Test Condition = Present in config
Evaluation Criteria = Match Any

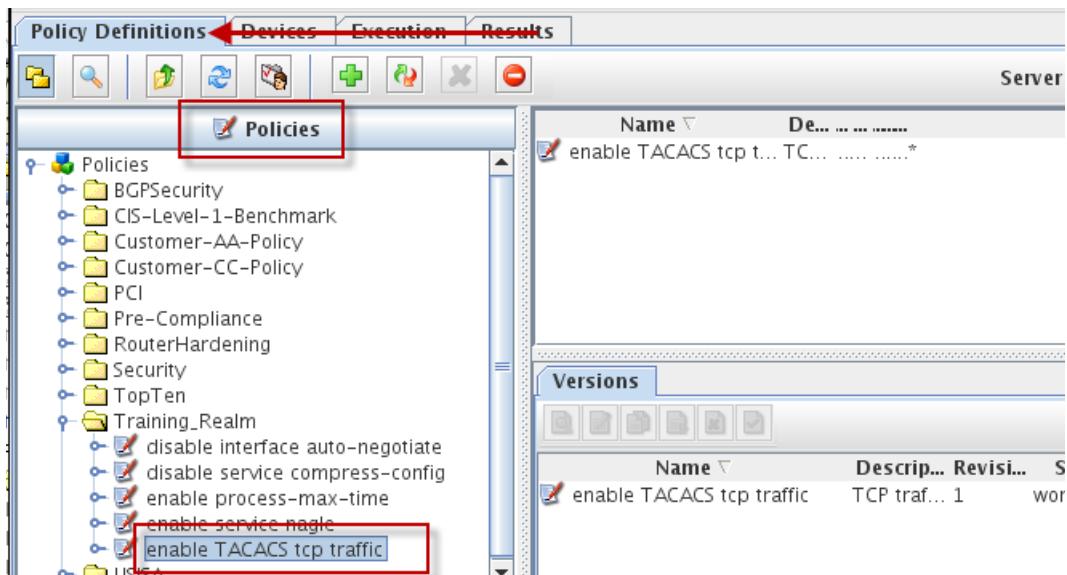
Search Result:-
speed auto - NOT FOUND
auto - FOUND

2. Test the **enable TACACS tcp traffic** policy. Use the values in the following table to complete the test wizard. When you finish, view the details of the test results. Inspect the results of the

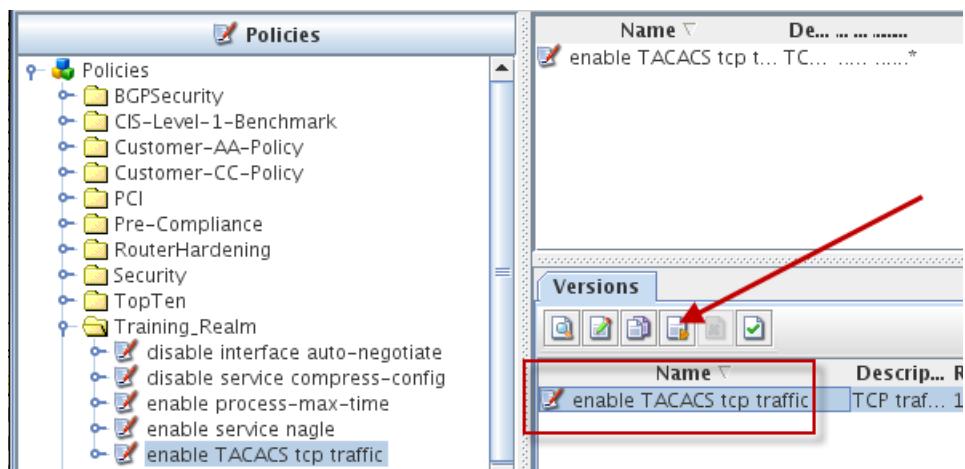
evaluations to verify that they work as you intend. Notice that a device is not compliant if any of the TACACS server IP address in the configuration is not permitted in an access list. If the evaluation returns the result FAIL (blue X), the rule determines that the device is not compliant.

Field	Value
Description	Policy test
Realms	Use the ITNCM > edge-network > customer_CC subrealm
Parameter value	Do not view parameters

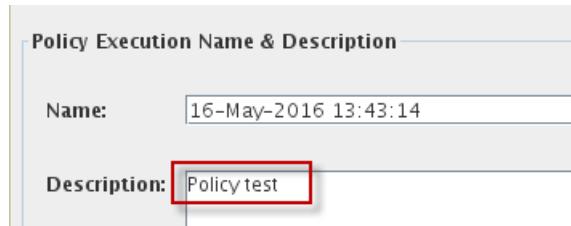
- Click the **Policy Definitions** tab. Click the **Policies** section. Expand **Training_Realm**. Click the **enable TACACS tcp traffic** policy.



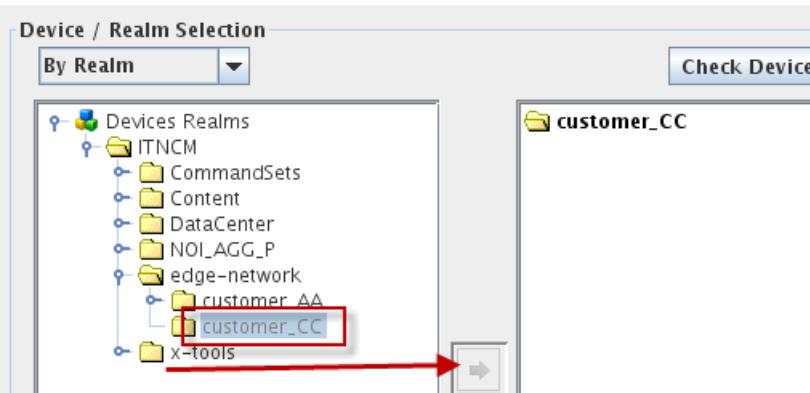
- Click the **enable TACACS tcp traffic** policy in the **Versions** section. Click the **Test Policy** icon. The test wizard starts.



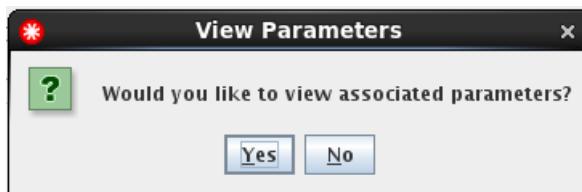
- c. Enter **Policy test** in the description field and click **Next**.



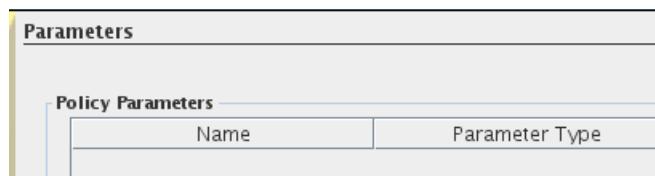
- d. Click the **ITNCM > edge-network > customer_CC** subrealm and click the right arrow icon to include it in the test. Click **Next**.



- e. When you are prompted to view associated parameters, click **No**.

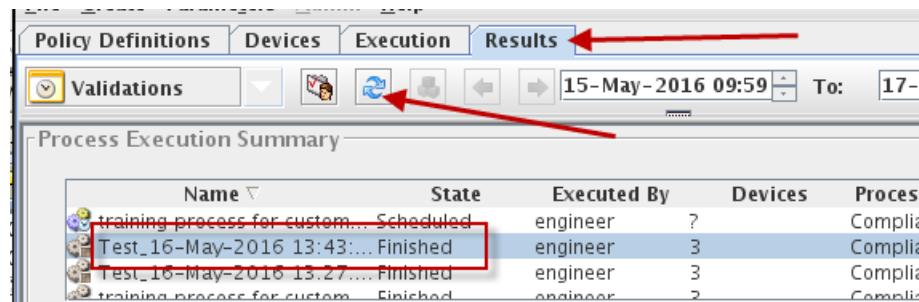


- f. Click **Finish**.



After you complete the test wizard, you see the **Results** tab.

- g. Click the refresh icon until the state of the test is Finished.



- h. After the test finishes, click the policy at the bottom of the window and click **Details**.

The screenshot shows two windows side-by-side. The top window is titled 'Process Execution Summary' and displays a table of execution results. The bottom window is titled 'Policy Validation Summary' and shows a table of policies with their details. A red arrow points from the 'enable TACACS tcp traffic' row in the validation summary table to the 'Details' button at the bottom right of the same window.

Name	State	Executed By	Devices	Process Ty...	Execution Ty...	Start Ti...	End Time
training process for custo...	Scheduled	engineer	?	Compliance	Recurring Sch...	26-May...	
Test_16-May-2016 13:4...	Finished	engineer	3	Compliance	Test	16-May...	16-May...
Test_16-May-2016 13:2...	Finished	engineer	3	Compliance	Test	16-May...	16-May...
training process for custo...	finished	engineer	2	Compliance	Recurring Sch...	16 May	16 May

Policy Name	Sever...	Revis...	Date	Pass...	Failed	Not Ass...	Exempt
enable TACACS tcp traffic	2	1	16-May-2016 13:4...	1	2	0	0

- i. Double-click one of the devices in the test results.

The screenshot shows the 'Results' tab of the configuration manager interface. It displays a table of device evaluations for the 'enable TACACS tcp traffic' policy. The 'Device' column is highlighted with a red box. A red arrow points from the 'Device' column to the 'Details' button at the bottom right of the window.

Policy	Device	Device Realm	Support Level	Date	Complia...
enable TACACS tc...	cc-01-router-3640	ITNCM/edge-networ...	SmartModel	16-May-2016 13:4...	FAIL
enable TACACS tc...	cc-02-router-3640	ITNCM/edge-networ...	SmartModel	16-May-2016 13:4...	FAIL
enable TACACS tc...	cc-03-router-3640	ITNCM/edge-networ...	SmartModel	16-May-2016 13:4...	PASS

- j. View the detailed results of each evaluation. Notice that if either evaluation returns the result FAIL (blue X), the rule determines that the device is not compliant.

The screenshot shows the detailed results for the device 'cc-01-router-3640'. On the left, there is a tree view of policy, rule, and definition evaluations. On the right, there are several text boxes displaying search results, match expressions, extracted values, and the final outcome.

- Searched in:-** Native Configuration
- Searched For:-**

```
Match Expression = permit tcp host $Extraction{extract TACACS server IP addresses}
Match Criteria = Match All
```
- Search Result:-**

```
Extracted Value(s):
192.20.5.55
192.20.7.22
1 match
permit tcp host 192.20.5.55 - FOUND
permit tcp host 192.20.7.22 - NOT FOUND
```
- Outcome:-** FAIL: the test condition and evaluation criteria were not n

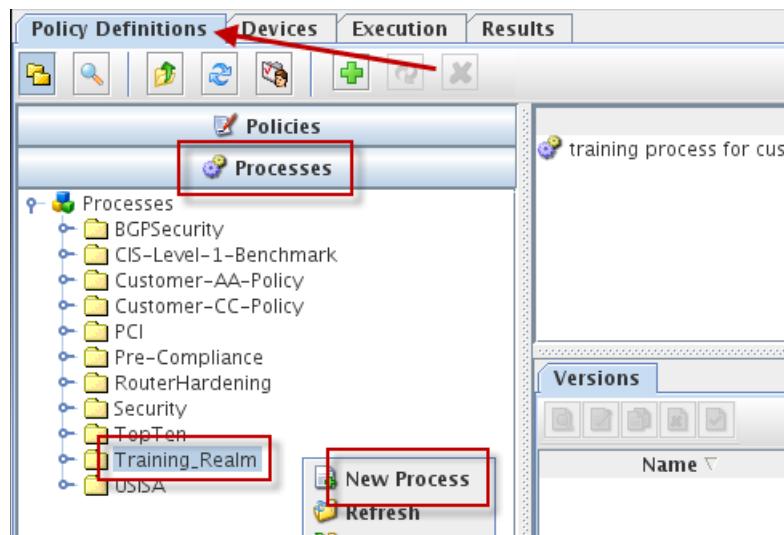
Exercise 4 Creating a process

In this exercise, you create a process. This process runs the two policies you created in a preceding exercise. You also schedule the process and run it.

1. Create a process in the Training_Realm named **process for advanced definitions**. Configure the process to run the two policies you created in the preceding exercise every Monday. Use the following values to complete the wizard.

Field	Value
Name	process for advanced definitions
Description	This process runs policies that contain advanced definition examples.
Enable process for automatic validations	Configure this process to run automatic validations
Policy Selection	Use these policies in the Training_realm folder. <ul style="list-style-type: none">• disable interface auto-negotiate• enable TACACS tcp traffic
Pre-Emptive Options	Do not enable any pre-emptive compliance options
Realm selection	Apply this process to the customer_CC realm. Check the device coverage in the customer_CC realm.
Include Subrealms	Configure this process to include subrealms.
Policy parameters	Do not view the associated parameters.
Process schedule	Recurring Schedule > Weekly. Every 1 week on a Monday.
Choose Save Location	Training_Realm

- a. Click the **Policy Definitions** tab. Click the **Processes** section. Right-click **Training_Realm** and click **New Process**. The Create a Process wizard starts.



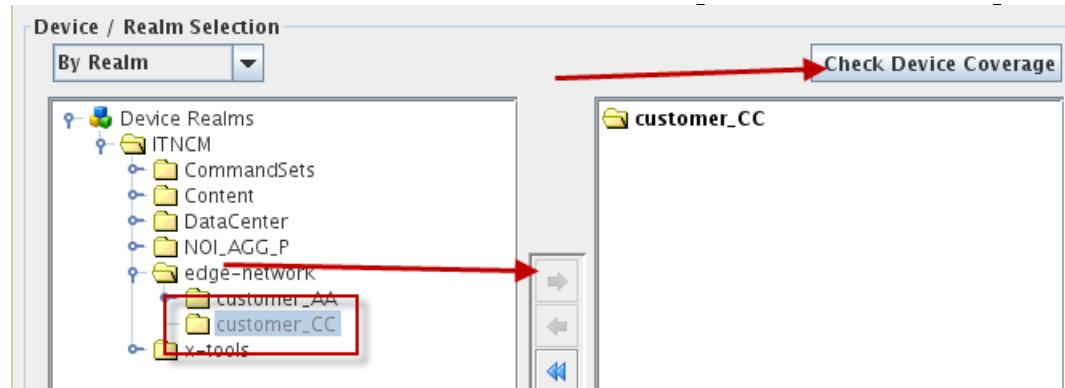
- b. Enter **process for advanced definitions** in the **Name** field. Enter the description from the preceding table. Select the **Enable process for automatic validations** option. Expand **Training_Realm**. Use the right arrow icon to move the **disable interface auto-negotiate** and **enable TACACS tcp traffic** policies in the Training_Realm to the right of the window. Click **Next**.

Process Name & Description	
Name:	<input type="text" value="process for advanced definitions"/> *
Description:	This process runs policies that contain advanced definition examples.
<input type="checkbox"/> Enable process for automatic validations	
Policy Selection	
<div style="border: 1px solid #ccc; padding: 5px;"> TopTen Training_Realm </div>	<input checked="" type="checkbox"/> disable interface auto-negotiate <input checked="" type="checkbox"/> enable TACACS tcp traffic

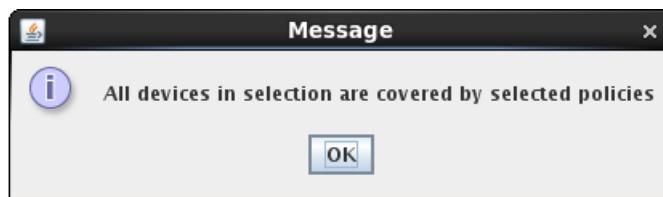
- c. Click **Next** in the Pre-Emptive Options window.

Pre-Emptive Options	
<input type="checkbox"/> Enable Pre-Emptive Compliance Options for this Process (SmartM	
Select Pre-Emptive Policies	
Policy Name	
<input checked="" type="checkbox"/> disable interface auto-negotiate	
<input checked="" type="checkbox"/> enable TACACS tcp traffic	

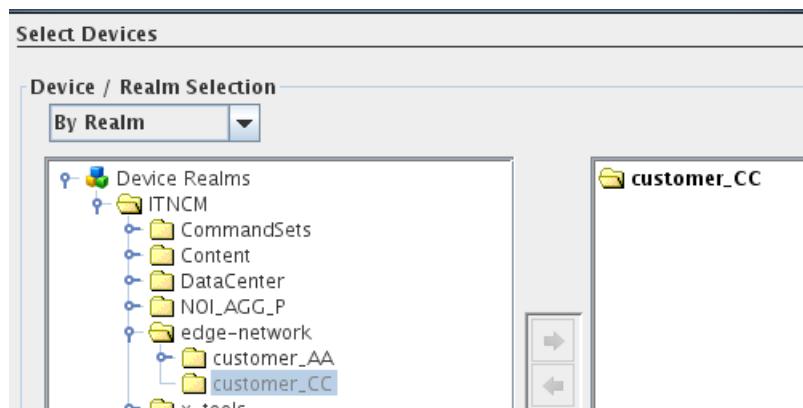
- d. Expand **ITNCM > edge-network > customer_CC**. Use the right arrow icon to move the **customer_CC** realm to the right of the window. Select the option to **Include Subrealms**. Click the **Check Device Coverage** icon.



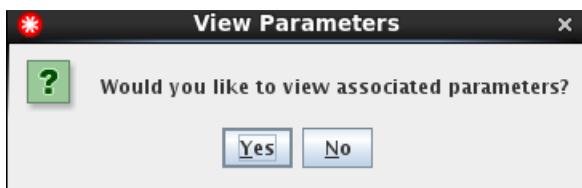
- e. Click **OK**.



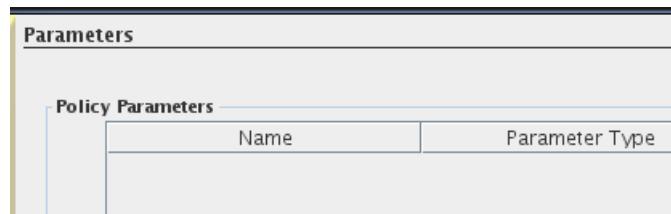
- f. Click **Next** in the Select Devices window.



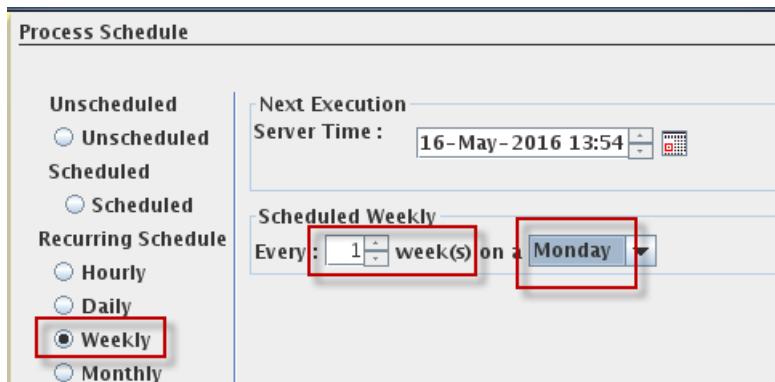
- g. Click **No** when you are prompted to view parameters.



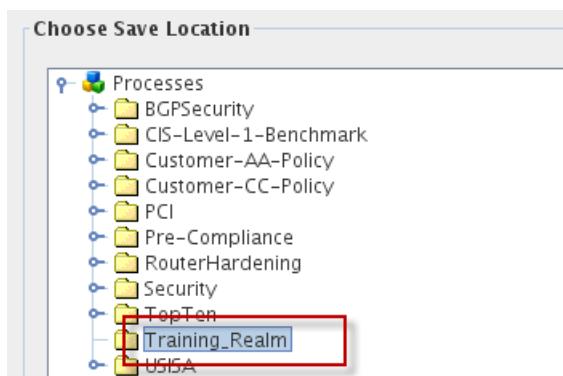
- h. Click **Next** in the Parameters window.



- i. Click **Recurring Schedule > Weekly**. Enter **1** in the **Every** field. Select **Monday** in the **week(s)** field. Click **Next**.



- j. Click **Training_Realm**. Click **Finish**.



2. After you create the process, the process runs automatically. Click the **Results** tab. Wait until the process finishes, and then look at the **Policy Validation Summary** for the process you just ran.

- a. Click the **Results** tab. Select **Validations**. Click the refresh icon until the process shows finished.

Policy Definitions **Devices** **Execution** **Results** **Validations** **Refresh** 15-May-2016 14:05 To:

Process Execution Summary

Name	State	Executed By	Devices
process for advanced definitions	Scheduled	engineer	?
training process for customer-CC	Scheduled	engineer	?
process for advanced definitions	Finished	engineer	3
Test_16-May-2016 13:43:14	Finished	engineer	3
Test_16-May-2016 13:27:43	Finished	engineer	3

- b. Click the **process for advanced definitions** process in the **Process Execution Summary** area. Scroll through the results of the process in the **Process Validation Summary** area and view the passing and failing policies.

The screenshot shows two tables from the Configuration Manager client:

Process Execution Summary

Name	State	Executed By	Devices	Process Type	Execution Ty
process for advanced definitions	Scheduled	engineer	?	Compliance	Recurring Sched
training process for customer-CC	Scheduled	engineer	?	Compliance	Recurring Sched
process for advanced definitions	Finished	engineer	3	Compliance	Recurring Sched
Test_16-May-2016 13:43:14	Finished	engineer	3	Compliance	Test
Test_16-May-2016 13:27:43	Finished	engineer	3	Compliance	Test

Policy Validation Summary

Policy Name	Severity	Revision	Date	Passed	Failed
disable interface auto-negotiate	2	1	16-May-2016 14:03:51	0	3
enable TACACS tcp traffic	2	1	16-May-2016 14:03:51	1	2

Leave the configuration manager client as is.

Leave the compliance manager client as is.



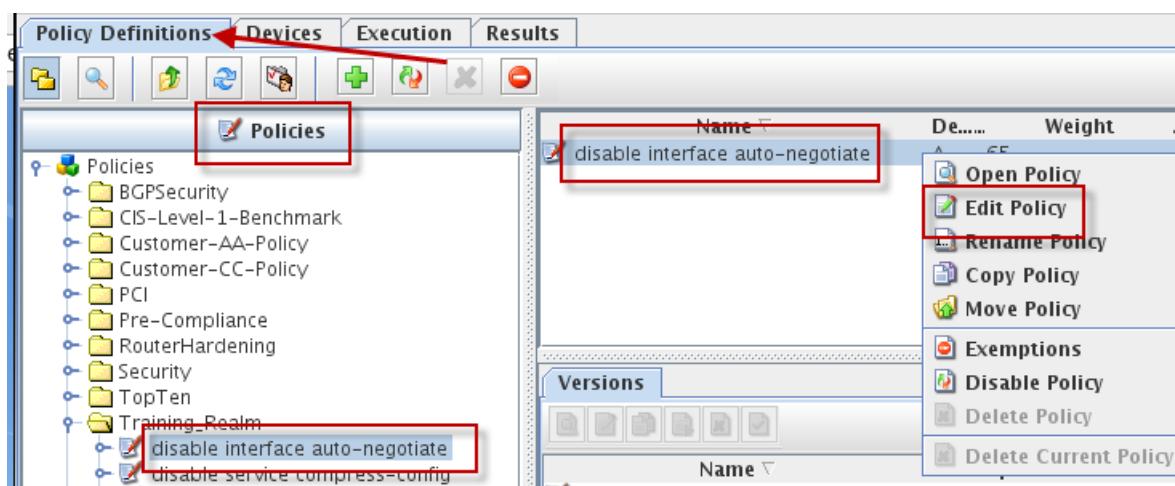
20 Preemptive compliance exercises

The exercise in this unit demonstrate how to implement preemptive compliance to prevent a change from making a compliant device no longer compliant.

Exercise 1 Enabling preemptive compliance

In this exercise, you enable the preemptive compliance feature on a policy and a process.

1. Enable preemptive compliance on the **disable interface auto-negotiate** policy.
 - a. Click the **Policy Definitions** tab. Click the **Policies** section. Expand **Training_Realm**. Right-click the **disable interface auto-negotiate** policy and click **Edit Policy**.



- b. Select the **Preemptive** option. Click **Next**.

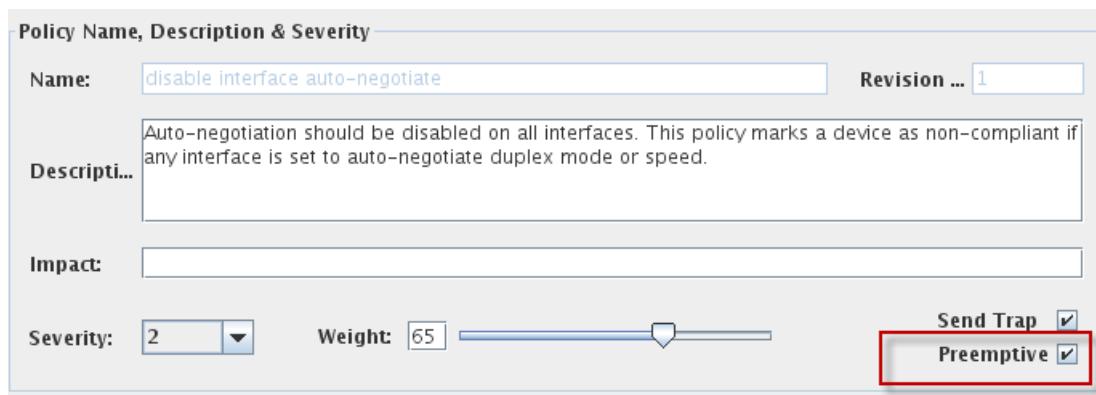
Policy Name, Description & Severity

Name: disable interface auto-negotiate Revision ... 1

Descript... Auto-negotiation should be disabled on all interfaces. This policy marks a device as non-compliant if any interface is set to auto-negotiate duplex mode or speed.

Impact:

Severity: 2 Weight: 65 Send Trap Preemptive



- c. Click **Next**.

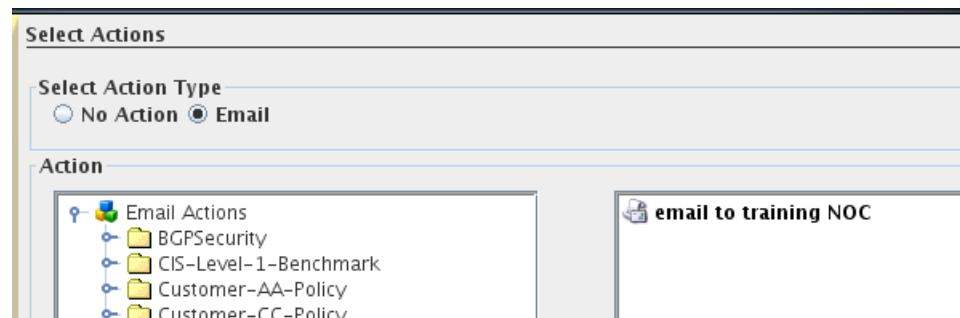
Select Actions

Select Action Type
 No Action Email

Action

Email Actions
BGPSecurity
CIS-Level-1-Benchmark
Customer-AA-Policy
Customer-CC-Policy

email to training NOC

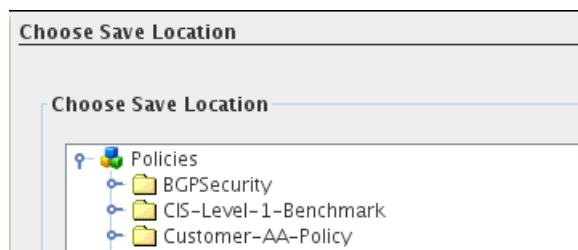


- d. Click **Finish**.

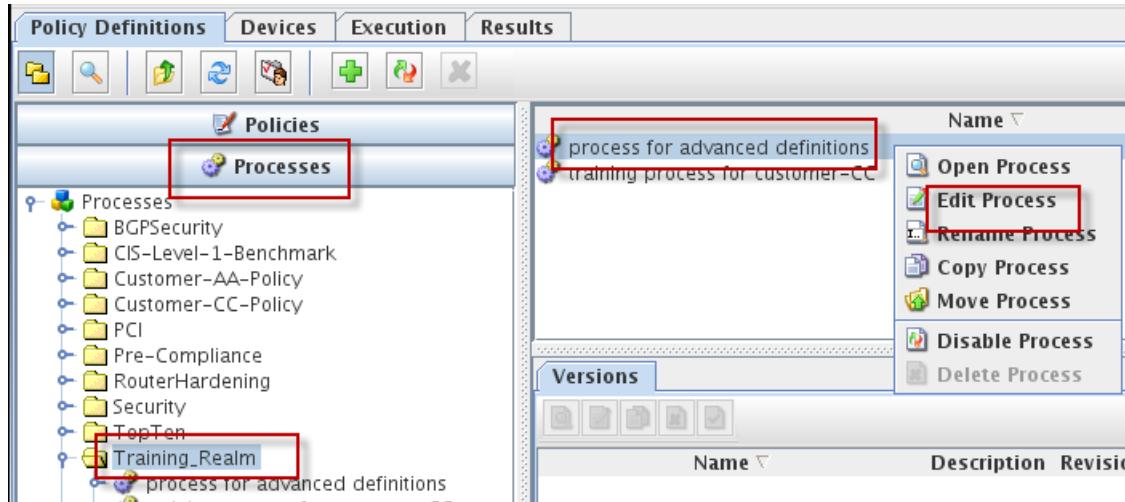
Choose Save Location

Choose Save Location

Policies
BGPSecurity
CIS-Level-1-Benchmark
Customer-AA-Policy



2. Edit the process for advanced definitions process. Enable the **disable interface auto-negotiate** policy for pre-emptive compliance.
 - a. Click the **Processes** section. Expand **Training_Realm**. Right-click the **process for advanced definitions** process and click **Edit Process**.



- b. Click **Next**.

Name and Description	
Process Name & Description	
Name:	<input type="text" value="process for advanced definitions"/> *
Revision:	<input type="text" value="1"/>
Description:	This process runs policies that contain advanced definition examp

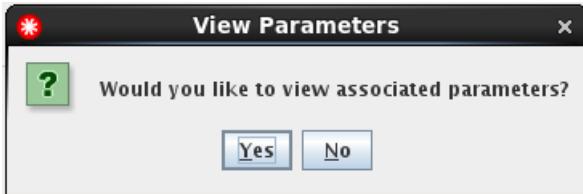
- c. Select **Enable Pre-Emptive Compliance Options**. Select **Enable** for the **disable interface auto-negotiate** policy. Click **Next**.

Pre-Emptive Options	
<input checked="" type="checkbox"/> Enable Pre-Emptive Compliance Options for this Process (SmartModel Policies Only)	
Select Pre-Emptive Policies	
Policy Name	Enable
<input checked="" type="checkbox"/> disable interface auto-negotiate	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> enable TACACS tcp traffic	<input checked="" type="checkbox"/>

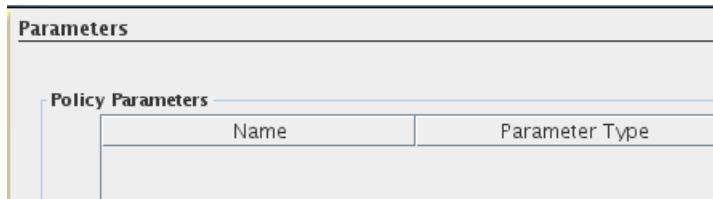
- d. Click **Next**.

Select Devices	
Device / Realm Selection	
By Realm	
Devices Realms	<input checked="" type="checkbox"/> customer_CC
ITNCM	

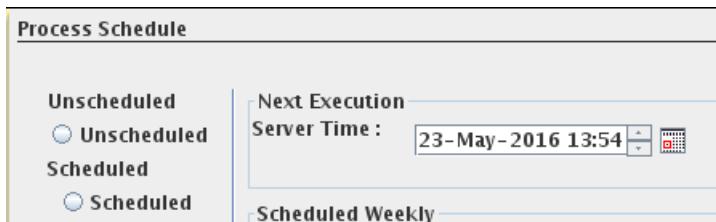
e. Click **No**.



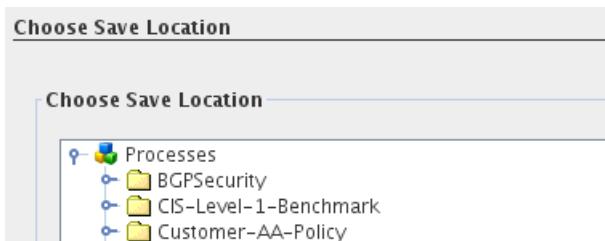
f. Click **Next**.



g. Click **Next**.



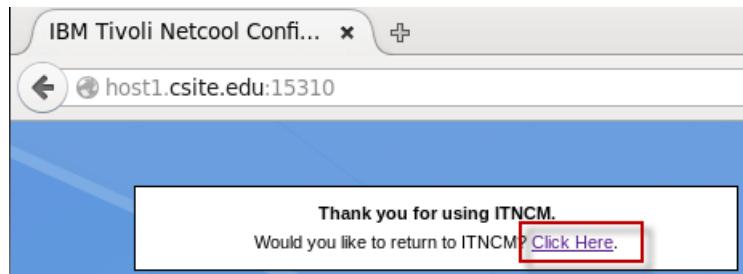
h. Click **Finish**.



3. Close the configuration manager client.
4. Close the compliance manager client.
5. Return to the browser session and click **Logoff**.



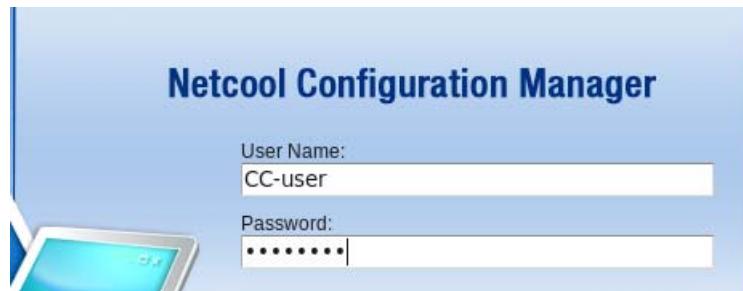
6. Select **Click Here**.



Exercise 2 Testing preemptive compliance

In this exercise, you use configuration manager to change a device configuration. You then view the unit of work log to verify that it uses the preemptive policy.

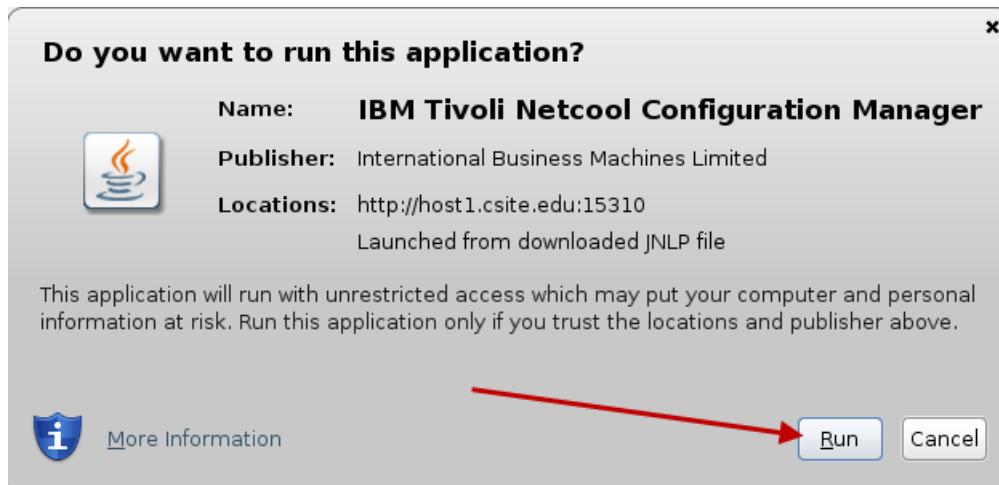
1. Log on to the Netcool Configuration Manager user interface with the user name **CC-user** and the password **object00**.



2. Click **ITNCM Webstart GUI**.



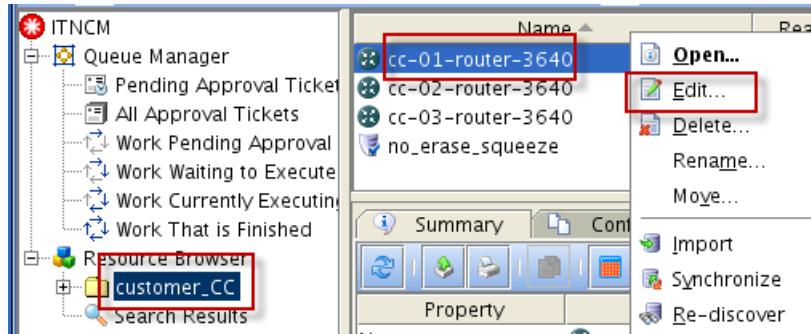
3. Click Run.



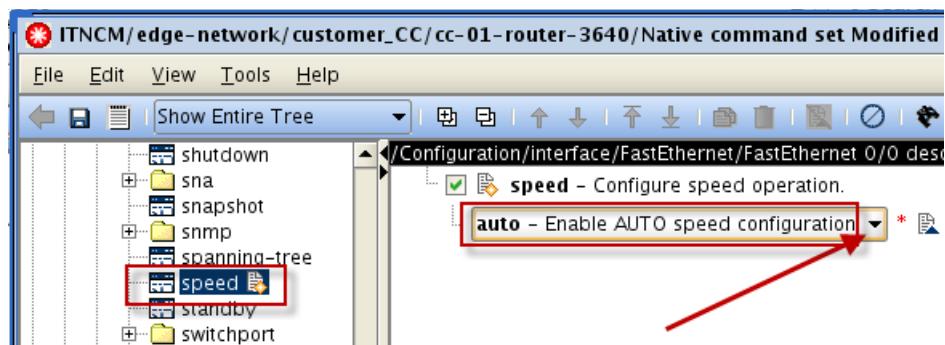
4. Edit the configuration of the **cc-01-router-3640** device. Set the **interface speed** for **FastEthernet 0/0** to **auto**. Submit the configuration change. Use the following table to complete the unit of work wizard.

Field	Value
Execution Mode	Execute Mode
Password Override	Do not override
Config Change	Merge
Execution Priority	Medium
Rollback Options	No Rollback
Schedule Work	Single Schedule > Immediate
Describe Work	Preemptive compliance test

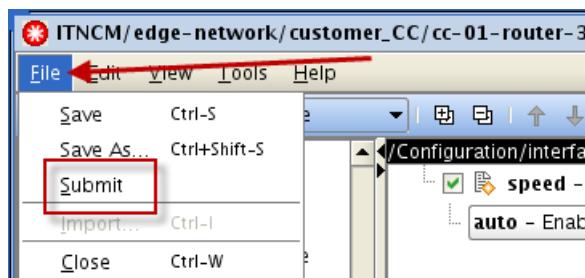
- a. Expand the **ITNCM > edge-network > customer_CC** realm in the resource browser. Right-click the **cc-01-router-3640** device and click **Edit**.



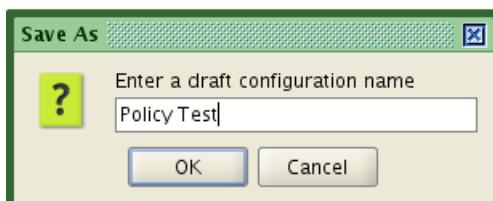
- b. Expand **interface > FastEthernet > FastEthernet 0/0 > speed**. Select **auto - Enable AUTO speed configuration**.



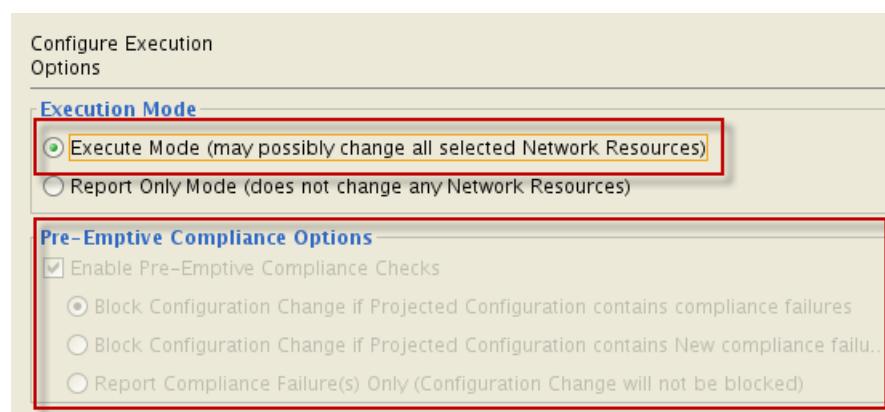
- c. Click **File > Submit**.



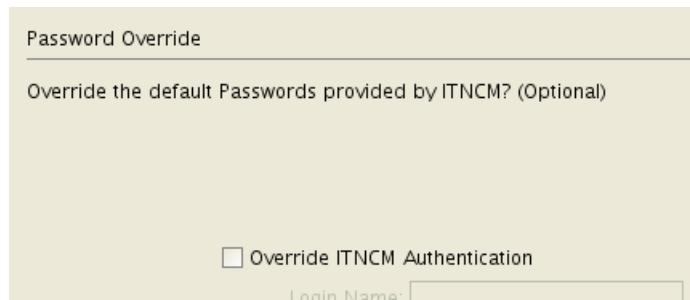
- d. Enter **Policy Test** as the configuration name. Click **OK**.



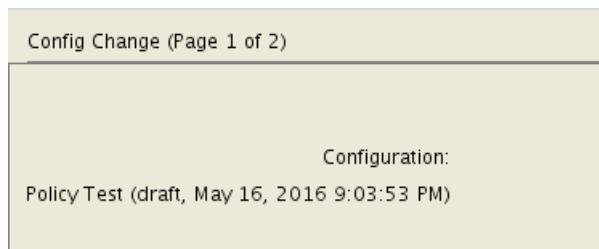
- e. Select **Execute Mode**. Notice the Pre-Emptive Compliance options. Click **Next**.



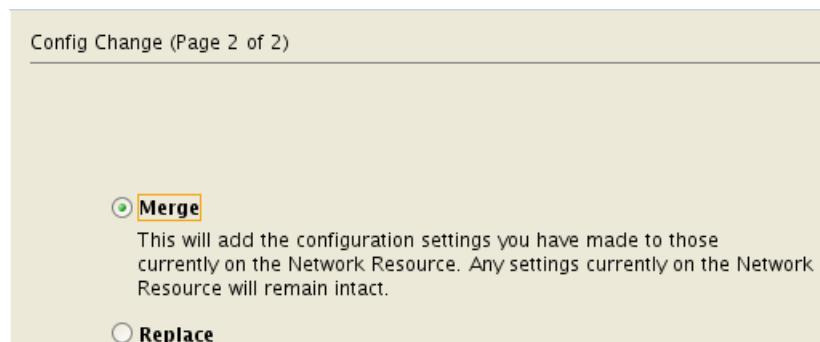
f. Click **Next**.



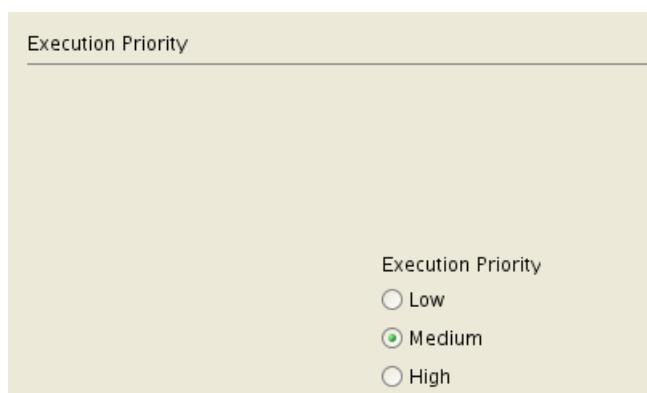
g. Click **Next**.



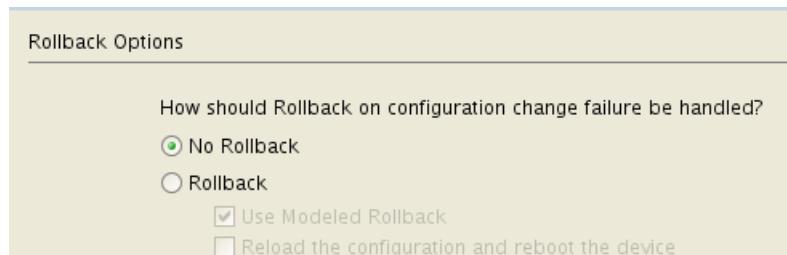
h. Select **Merge**. Click **Next**.



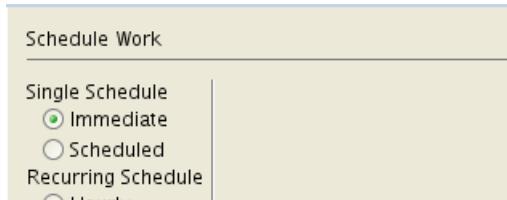
i. Click **Next**.



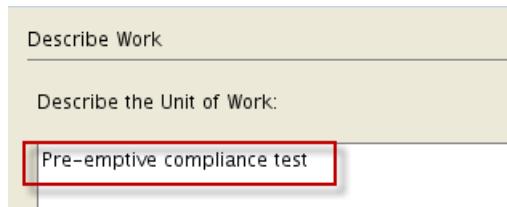
j. Click Next.



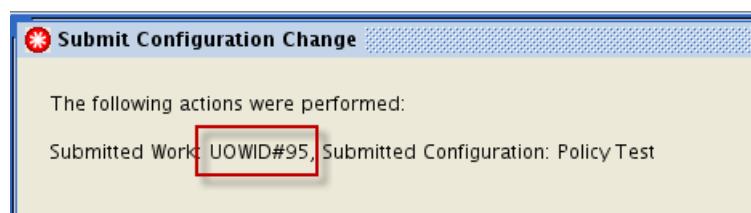
k. Click Next.



l. Enter **Pre-emptive compliance test** as the description. Click **Finish**.



m. Note the unit of work number and click **Close**.



5. Find the failed unit of work. Look at the unit of work log and the **Pre-Emptive Compliance** tab.

a. Click **Processed Work** in the queue manager. Click the unit of work you created. Click the **Resources** tab. Click the **cc-01-router-3640** device.

- b. Scroll down in the work log. Find the log entry that shows that the **disable interface auto-negotiate** policy fails if this configuration change is completed.

The screenshot shows a 'Work Log' window with a green checkmark icon and the title 'Pre-Emptive Compliance'. The log entries are as follows:

- (6) Options: On Compliance Failure :Stop
- (7) Getting the new config
- (8) Running compliance checks against current and projected configs
- (9) Got applicable policies
- (10) Finished running policies
- (11) Policy Name Current Config
- Projected Config
-
- disable interface auto-negotiate FAIL
- FAIL
- (12) Task End Time: 2016/05/16 21:09:46.716 GMT+00:00
- *****

A red box highlights the log entry 'disable interface auto-negotiate FAIL FAIL'.

- c. Click the **Pre-Emptive Compliance** tab. Double-click the **disable interface auto-negotiate** policy.



- d. Click the **check for speed auto** evaluation. Look at the results.

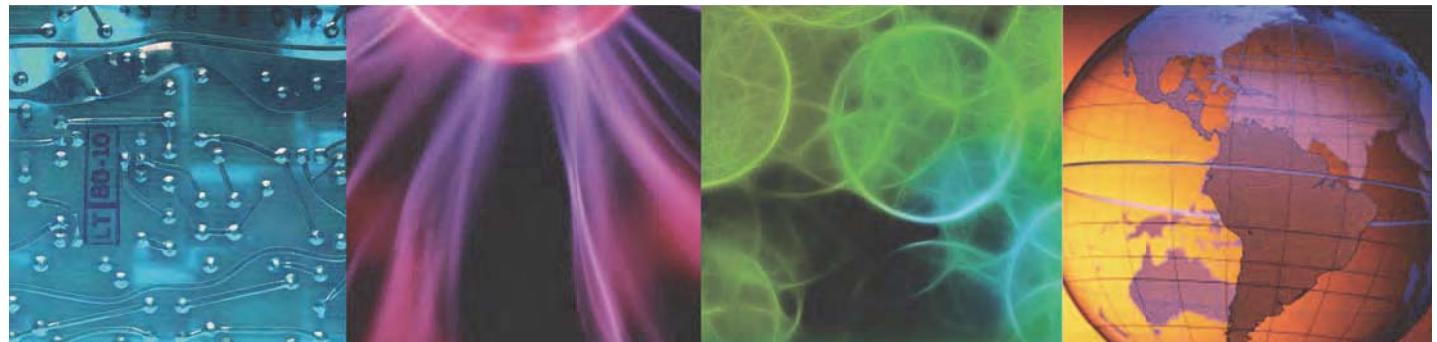
The screenshot shows the 'Pre Compliance Details: disable interface auto-negotiate' window. On the left, a tree view shows the policy structure:

- Policy: disable interface auto-negotiate
- Rule: disable interface auto-negotiate
- Definition: check for duplex auto
 - Evaluation: 1
- Definition: check for speed auto
 - Evaluation: 1

The 'Evaluation: 1' under the 'check for speed auto' definition is highlighted with a red border. On the right, detailed information is displayed:

- Searched in:- Projected XML Configuration
- Searched For:- Context XPath = configuration/interface/*/speed
Defined XPath = auto
Context Nodes =
Test Condition = Present in config
Evaluation Criteria = Match Any
- Search Result:-
auto - FOUND
auto - FOUND
- Outcome:-
PASS: the test condition and evaluation criteria were met

TOD44 1.0



ibm.com/training

Authorized
IBM | Training