User Guide for Network Compliance Manager 1.2.1

CiscoWorks

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-10192-05

User Guide for Network Compliance Manager 1.2.1

Table of Contents

Chapter 7: Scheduling Tasks 275

Getting Started

Overview

As networks continue to expand, network topologies continue to increase in complexity. In addition, many networks must now comply with regulations and security best practices. This results in a complex infrastructure with multiple protocols, technologies, and vendors to support.

Centrally managing the network infrastructure in a secure, automated, and centralized fashion becomes vital for the effects of performance — from additional security vulnerabilities to a complete outage — all of which can cause increased liability, lost revenues, and lost productivity.

CiscoWorks Network Compliance Manager (NCM) 1.2.1 provides an enterprise class solution that tracks and regulates configuration and software changes across routers, switches, firewalls, load balancers, and wireless access points. NCM provides visibility into network changes, enabling an IT staff to identify and correct trends that could lead to problems, while mitigating compliance issues, security hazards, and disaster recovery risks. NCM also captures full audit trail information about each device change.

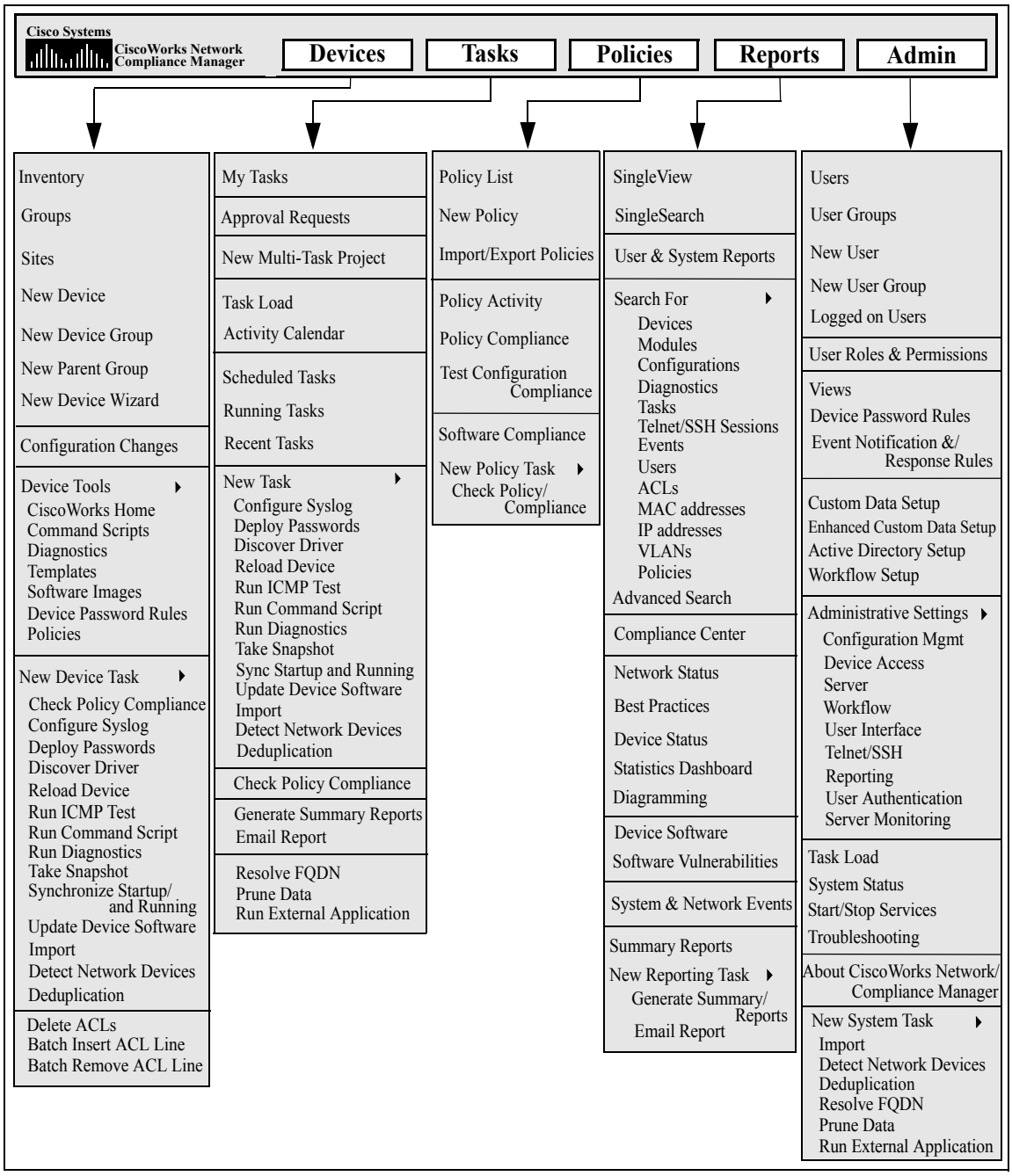
Network engineers can use NCM to pinpoint the following:

- Which device configuration changed
- What exactly was changed in the configuration
- Who made the change
- Why the change was made

In addition, NCM can enforce security and regulatory policies at the network level by making sure that configurations comply with pre-defined standards. The end result is a resilient and maintainable network that is compliant with standards and regulations.

NCM supports an array of devices from leading vendors, including Cisco, Nortel, F5 Networks, and Extreme, to provide insights into your network change process. NCM's scalable architecture enables you to incorporate the best devices from the best vendors, and support all your devices using one tool.

Main Menu Bar



Menu Bar Options

The following options are always available from the menu bar:

- Support — Opens the Cisco Customer Support page. This site provides Cisco customers with the most recent patch releases and documentation. In addition, you can upload files for issue resolution and troubleshooting.
- Docs — Opens the CiscoWorks Network Compliance Manager Documentation page. Refer to "Accessing NCM Documentation" on page 21 for information on the available NCM documentation.
- NCM Alert Center — Opens the Cisco Systems page, where you can download NCM Alert Center (CAC) data and other NCM Content Service material.
- Logout — Logs you out of NCM.

User Guide

The *User Guide for Network Compliance Manager 1.2.1* includes information on:

- Setting up and configuring the system
- Adding and configuring devices and device groups
- Adding users, groups, and roles
- Creating Workflows
- Using SecurID, TACACS+, and RADIUS to access network devices
- Importing users and user groups from Active Directory
- Managing Access Control Lists (ACLs)
- Using the Compliance Center
- Searching for information, creating custom reports, and running summary reports
- Deploying configurations
- Creating event rules and event notifications
- Viewing default diagnostics
- Creating and running diagnostics and command scripts
- Creating company-wide policy rules to prevent inconsistency
- Deploying device software from a central repository
- Connecting to devices using Telnet and SSH
- Running the command line interface (CLI)
- Exchanging data with other IT applications using Java and PERL APIs
- Using online Help, contacting Customer Support, and updating your software license

Note: The *User Guide for Network Compliance Manager 1.2.1* provides information on all options available to the NCM System Administrator. Depending on your permissions, some of the NCM menu options could be grayed-out.

Document Conventions

The following table explains the conventions used in the *User Guide for Network Compliance Manager 1.2.1*.

Convention	Description/Action
Italic	Used for system messages, paths, file names, and Web URLs. For example, *C:\cisco\client\docs.*
Link	Moves you from one location to another within a document, opens Web pages, or opens a new email message. Cross-references are contained within quotation marks and include a page number, while links to URLs and email addresses appear as underlined text.
Enter	Indicates that you should type the text or command that follows, then press the Enter key on the keyboard.
< >	Indicates variable information, such as a name or folder that you must supply. Do not include the angle brackets when replacing the placeholder.

Accessing NCM Documentation

To access user documentation:

- *User Guide for Network Compliance Manager 1.2.1* — To view the PDF version, after logging in, on the menu bar click Docs. The CiscoWorks Network Compliance Manager Documentation page opens.
- Online Help Files — To view Online Help files, after logging in, click the Help icon at the top of any NCM page.
- *Device Drive Reference for Network Compliance Manager 1.2.1* — To view the PDF version, after logging in, on the menu bar click Docs. The CiscoWorks Network Compliance Manager Documentation page opens.
- Integration API — To view the PDF version of *Java*, *PERL,* and *SOAP API Reference Guides for Network Compliance Manager 1.2.1*, after logging in, on the menu bar click Docs. The CiscoWorks Network Compliance Manager Documentation page opens.

- CLI Help — To view the command line Help on the server computer, click Start → Programs → CWNCM → CWNCM Client and login. There are two ways to view Help for CLI commands. Enter: `help` to see a list of all commands. Enter `help <command name>` to see detailed help on a specific command.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Send Troubleshooting Page Fields

To send troubleshooting information to Customer Support:

1. On the menu bar under Admin, click Troubleshooting. The Troubleshooting page opens.
2. Click the Send Troubleshooting Information link at the top of the page. The Send Troubleshooting Info page opens.

Fields	Description/Action
To	The Customer Support email address should appear by default.
Subject	The subject line should appear by default as "Cisco System Info."
Problem Number	Enter the problem number related to an open ticket, if applicable.
Comments	Enter comments regarding the issue. Be sure to include your return email address and direct phone (or cell number). The contact information on file is not always accurate or specific to the person with the issue.
Include	Select one or more of the following options: • Server logs for the last < > hours — Enter the number of hours worth of stored logs you want to send. The default is 4. • Administrative settings — Include everything on the Administrative Settings pages. • Wrapper Log — If requested, this sends the Jboss_Wrapper log file. • System Status File — If requested, the System Status page displays the results of the most recent monitor runs.

Be sure to click Send when finished.

Viewing the Latest Software Version

You can view detailed information about the current NCM software version. In addition, this page includes links to other important pages, including:

- Downloading Driver Update Packages — Opens the Cisco download page.
- Viewing the latest Release Notes — Opens the Cisco Knowledge Base page.
- Viewing License Information — Opens the License Information page. Refer to "Viewing License Information" on page 28 for information.
- Viewing System Configuration — Opens the View System Configuration page. Refer to "View System Configuration" on page 29 for information.
- Creating a Customer Support ticket — Opens the *support@cisco.com* email page.
- Emailing Customer Support — Opens the *support@cisco.com* email page.
- Requesting new driver support — Opens the *support@cisco.com* email page.
- List of device drivers installed on your system — Displays all of the installed drivers in use by the system. Refer to the *Device Driver Reference for Network Compliance Manager 1.2.1* for detailed information on supported devices.

To view the About CiscoWorks Network Compliance Manager page, on the menu bar under Admin click About CiscoWorks Network Compliance Manager. The About CiscoWorks Network Compliance Manager page opens.

Product Licenses

CiscoWorks Network Compliance Manager (NCM) licenses are obtained from Cisco. Refer to the *Quick Start Guide for CiscoWorks Network Compliance Manager 1.2.1* for information on how to obtain product licenses.

Licenses are issued for specific NCM products, including NCM Cores, High Availability Distributed Systems, and the Cisco Satellite (or Gateway). Evaluation licenses expire 90 days after installation. The date in the evaluation license file is not used. If a NCM server has both an evaluation and permanent license for the same product, the evaluation license is ignored.

Note: To obtain product licenses, you must be running NCM 1.2.1.

Host IDs

Host IDs are required to generate permanent NCM licenses. To obtain a Host ID, run the lmutil program found in the *\CWNCM_INSTALL_DIR\server\ext\wrapper\bin* directory. Enter: lmutil lmhostid

Note: The lmutil lmhostid command returns multiple ‘hostids’ if there are multiple network interface cards installed. Only one ‘hostid’ should be used to generate a license.

Installing the NCM License File (Windows)

To install a NCM license file, you can either:

1. Copy the license file to the \CWNCM_INSTALL_DIR root directory (the license text must be contained in a file with the *.lic* extension).
2. Login to NCM.
3. On the main menu bar, click Admin and then click Start/Stop Services. The Start/Stop Services page opens.
4. Under Management Engine, click the Restart button.

— OR —

1. Login to NCM.
2. On the main menu bar, click Admin and then click About CiscoWorks Network Compliance Manager. The About CiscoWorks Network Compliance Manage page opens.
3. Click the View License Information link. The License Information page opens.
4. Paste the text from the license file into the text area.
5. Click the Update License button. (**Note**: When you click the Update License button, a new license file is created with a unique name. If you choose to copy the license file, be sure enter a filename that does not already exist, otherwise you will overwrite the existing license file. Keep in mind that all license files must end with the *.lic* extension.)
6. On the main menu bar, click Admin and then click Start/Stop Services. The Start/Stop Services page opens.
7. Under Management Engine, click the Restart button.

Note: When NCM starts, a license server parses the license files and caches the information. As a result, when new license files are added, either through the License Information page or by copying a license file to the license directory, you must restart NCM.

High Availability Distributed System Licenses

When installing a High Availability Distributed System configuration, both a High Availability Distributed System and NCM Core licenses are required — with a license count equal to or greater than your total device inventory in the NCM Mesh. (Inactive devices do not count toward this number.)

Each NCM Core server must be able to manage the entire device inventory in the event that one or more NCM Core servers within the NCM Mesh go off-line and devices need to be assigned to different managed NCM Cores. As a result, any on-line NCM Core server should have license capacity to manage the device inventory.

License Error Message

If a NCM server has multiple licenses installed, the device count allowed is the sum of all valid licenses. If the device count exceeds the number of valid licenses, you will not be able to login to NCM. The login screen displays a "License Error" message. Keep in mind that NCM records when the license server starts and how many license files are found. If you encounter license errors, the NCM log files can provide helpful troubleshooting information.

The licensing information log key is named *xyz*. If you want to set license logging:

1. Login to NCM.
2. On the main menu bar, click Admin and then click Troubleshooting. The Troubleshooting page opens.
3. In the “Enabling logging for” field, scroll down and click xyz [Error].
4. In the “at level” field, click Debug from the drop-down menu.
5. Enter the number of days you want to keep the data.
6. Click the Submit button.

Note: Before changing your logging level, it is recommended that you contact Technical Support. The software components are obscure at best and some generate a significant amount of data.

For information on NCM license configuration settings and License Monitor messages, refer to “Server Monitoring Page Fields” on page 117.

Viewing License Information

The License Information page enables you to determine:

- Whom your product is licensed to
- How many nodes does the license include
- How many nodes are actually in use
- When your license expires

You can also update your license from this page.

To view the License Information page:

1. On the menu bar under Admin, click About CiscoWorks Network Compliance Manager. The About CiscoWorks Network Compliance Manager page opens.
2. Click the View License Information link. The License Information page opens.

Fields	Description/Action
Product	Displays the software version you are licensed to use.
Licensed to	Displays the name of your company or division.
Number of nodes licensed	Displays the number of nodes the software is allowed to recognize. Keep in mind that some devices, such as the Cisco 6500, contain cards that operate as separate nodes.
Number of nodes in use	Displays the number of nodes activated in NCM.
License expiration	Displays when your software license expires.
Update License button	When it is time to update your software license, Cisco sends you new license text. Paste the text into the box, then click Update License to install the new license.

View System Configuration

If the High Availability Distributed System configuration is enabled and you have configured NCM Cores, the View System Configuration page enables you to determine:

- How many NCM Cores are configured
- How many Device Views are configured
- How many Sites are configured

Refer to "Segmenting Devices and Users" on page 163 for information on Overlapping IP Networks and Restricted Device Views. Refer to the *High Availability Distributed System Configuration Guide on Oracle for Network Compliance Manager* for information on installing and configuring a High Availability Distributed System.

Chapter 1: Installation

Use the following table to quickly locate information.

Pre-Install Checklist

Customer Support should have provided you with a pre-installation checklist to fill out and discuss before you install NCM. The checklist includes:

- The vendors, models, operating systems, and firmware versions of the devices on your network.
- Your device authentication parameters.
- Whether you will import devices from another application or comma-separated value (CSV) file.
- Whether you will regularly update the devices from another application or list.
- What protocols are available to NCM for communicating with devices on your network.
- Whether you use AAA (TACACS+ or RADIUS). NCM supports popular AAA servers such as CiscoSecure ACS. Be sure to discuss which AAA server you use with Support.
- The change detection mechanisms you will use (AAA or Syslog).
- For email, what SMTP server is available for email notifications.
- The type of events that should trigger notifications and how you want to receive notifications.
- How often you want devices to be polled for changes.
- Your network topology and how devices are organized.
- Your server specifications, including a static IP address. Note: NCM does not support a DHCP IP address. If you have questions, contact Customer Support (see "Obtaining Documentation, Obtaining Support, and Security Guidelines" on page 22).
- Your network security policies.
- Your administrative account (Windows) or root account (Unix).

Note: If you are using Oracle, you will need to create an Oracle database. Please refer to your Oracle documentation for information on configuring an Oracle database.

Protocols & Ports

NCM communicates with devices using a combination of the following protocols and ports. If you use a given protocol, NCM requires access to the corresponding port. Specifically, if NCM communicates with devices protected by firewalls, these ports need to be opened.

Protocol/Port	From/To
NCM server (running the Mgmt Engine, Syslog, TFTP) and network devices	
Telnet (port 23)	From the NCM server to network devices.
SSH (port 22)	From the NCM server to network devices.
TFTP (port 69/udp)	From network devices to the NCM server.
Syslog (port 514/udp)	From network devices to the NCM server.
SNMP (port 161/udp)	From the NCM server to network devices.
NCM server and the NMS	
SNMP-trap (port 162/udp)	From the NCM server to the NMS.
NCM server and the AAA server	
JNDI (port 1099)	From the AAA server to the NCM server. You can change this by editing the NCM configuration files. Please contact Customer Support for assistance.
RMI (port 4444)	From the AAA server to the NCM server. You can change this by editing the NCM configuration files. Please contact Customer Support for assistance.
NCM server and the NCM client	
HTTPS (port 443)	From the NCM client to the NCM server. You can change this by editing the NCM configuration files. Please contact Customer Support for assistance.
Telnet (port 23 - Windows or 8023 - Solaris)	From the NCM client to the NCM server. This can be changed from the Administrative Settings option.
SSH (port 22 - Windows or 8022 - Solaris)	From the NCM client to the NCM server. This can be changed from the Administrative Settings option.

Windows System Requirements

The following tables provide the recommended requirements when installing NCM on a Windows platform. Keep in mind that the application server and the database server can be configured together or separately.

Application Server	
OS	Windows Server 2003 Enterprise Edition
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Disk	10 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Database Server	
Supported Databases	Oracle 9.2, Oracle 10.2.0.2 Enterprise (32 bit), Microsoft SQL Server 2000 (SP2) and 2005, and MySQL Max 3.23 (included)
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Disk	18 GB, Single Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Application and Database Server	
OS	Windows Server 2003 Enterprise Edition
Database	MySQL Max 3.23 (included)
CPU	Dual Processor Intel Xeon, 3.0+ GHz
Memory	4 GB RAM
Disk	28 GB, Dual Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Note: When installing NCM on a Windows platform, Nmap 3.81 and WinPcap (Windows Packet Capture Library) Version 3.1 is required for Nmap scanning when running the Detect Network Devices task.

You will also need the following applications:

- Microsoft Internet Explorer version 5.5 or higher or Mozilla Firefox version 1.0 or higher (refer to "Installing Web Browsers" on page 39)
- Microsoft Excel 2000 or higher (for viewing Summary Reports)
- Adobe® Acrobat® Reader™ version 4.0 or higher (for viewing documentation)

Note: You must stop other network management applications, Web servers, databases, and syslog/TFTP servers running on the same system before installing NCM. Applications include anti-virus (during Setup only) and WWW Publishing Server applications.

Linux System Requirements

The following tables provide the recommended requirements when installing NCM on a Linux platform. Keep in mind that the application server and the database server can be configured together or separately.

Note: When installing NCM on Linux, the version of Nmap distributed with NCM (Nmap 3.81) is required for Nmap scanning when running the Detect Network Devices task.

Application Server	
OS	RedHat Linux AS 3.0 Update 2, RHAS 3 and RHAS 4 Update 2, and SUSE Enterprise Server 9 (32 bit)
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Swap Space	4 GB
Disk	14 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Database Server	
Supported Databases	Oracle 9.2, Oracle 10.2.0.2 Enterprise (32 bit), and MySQL Max 3.23 (included)
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	22 GB, Single Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Application and Database Server	
OS	RedHat Linux AS 3.0 Update 2, RHAS 3 and RHAS 4 Update 2, and SUSE Enterprise Server 9 (32 bit)
Database	MySQL Max 3.23 (included)
CPU	Dual Processor Intel Xeon, 3.0+ GHz
Memory	4 GB RAM
Swap Space	8 GB Swap
Disk	36 GB, Dual Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

You will also need the following applications:

- KDE Desktop Manager (K Desktop Environment is a desktop environment that runs on Linux. Installing KDE automatically installs all of the X11 libraries. X Window System (commonly X11) provides the standard toolkit and protocol to build graphical user interfaces on Linux.)
- Mozilla Firefox 1.0+ (refer to "Installing Web Browsers" on page 39)
- Adobe® Acrobat® Reader™ version 4.0 or higher (for viewing documentation)

Note: You must stop other network management applications, Web servers, databases, and syslog/TFTP servers running on the same system before installing NCM. Applications include Anti-virus (during Setup only) and WWW Publishing Server applications.

Summary Reports (Linux)

The Summary reports are generated in the Microsoft Excel XLS format. Excel does not run on Linux. You can either run the Summary reports from a Windows client computer connected to your NCM server or you can use one of the following products that run on Linux and can open Excel files:

- Open Office (www.openoffice.org)
- GNUmeric (www.gnumeric.org)
- Star Office (wwws.sun.com/software/star/staroffice)

Solaris System Requirements

The following tables provide the recommended requirements when installing NCM on a Solaris platform. Keep in mind that the application server and the database server can be configured together or separately. If you are installing NCM on Solaris 10 and have configured a Non-global Zone on the Solaris 10 host, refer to the *Installing NCM on Solaris 10 User's Guide*.

Note: When installing NCM on Solaris, the version of Nmap distributed with NCM (Nmap 3.81) is required for Nmap scanning when running the Detect Network Devices task

Application Server	
OS	Solaris 9 and Solaris 10
CPU	Dual UltraSPARC IIIi+, 1.3+ GHz (SunFire V240)
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	14 GB, Fast SCSI

Network	100 Mbps Fast Ethernet, full duplex

Database Server	
Supported Databases	Oracle 9.2, Oracle 10.2.0.2 Enterprise (32 bit), and MySQL Max 3.23 (included)
CPU	Dual UltraSPARC IIIi+, 1.3+ GHz (SunFire V240)
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	22 GB, Single Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Application and Database Server	
OS	Solaris 9 and Solaris 10
Database	MySQL Max 3.23 (included)
CPU	Dual UltraSPARC IIIi+, 1.3+ GHz (SunFire V240)
Memory	4 GB RAM
Swap Space	8 GB Swap
Disk	36 GB, Dual Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

You will also need the following applications:

- The X Window System, X11 (also known as OpenWindows)
- Mozilla Firefox 1.0+ (refer to "Installing Web Browsers" on page 39)
- Adobe Acrobat Reader version 4.0 or higher (for viewing documentation)

Note: You must stop other Web servers, databases, and Syslog/TFTP servers running on the same system before installing NCM. You must also stop any Network Management, anti-virus (during Setup only) and WWW Publishing Server applications.

Summary Reports (Solaris)

The Summary reports are generated in the Microsoft Excel XLS format. Excel does not run on Solaris. You can either run the Summary reports from a Windows client computer connected to your NCM server or you can use one of the following products that run on Solaris and can open Excel files:

- Open Office (www.openoffice.org)
- GNUmeric (www.gnumeric.org)
- Star Office (wwws.sun.com/software/star/staroffice)

Installing Web Browsers

NCM requires a Web browser.

Installing Microsoft Internet Explorer

NCM requires Microsoft Internet Explorer version 5.5 or higher. To install the latest version of Microsoft Internet Explorer, point your browser to:

http://www.microsoft.com/windows/ie/default.asp

Follow the instructions to download and install the latest version.

Installing Mozilla Firefox on Linux

NCM requires Mozilla Firefox version 1.0 or higher. To install the latest version of Mozilla Firefox, point your browser to:

http://www.mozilla.org/releases

Follow the instructions to download and install the latest version.

Installing Mozilla Firefox on Solaris

NCM requires Mozilla Firefox version 1.0 or higher.

1. To install the latest version of Mozilla Firefox, point your browser to:

   http://www.mozilla.org/releases/#1.4

2. Scroll down to the Mozilla heading and then to Solaris SPARC. It is recommended that you download Solaris 9. Follow the instructions to download and install the latest version.
3. Mozilla Firefox needs the following compiled libraries to run properly on Solaris. From the NCM installation directory, copy the following files to your Mozilla Firefox directory:

   ```
   ./mozilla/libglib
   ./mozilla/libgtk
   ```

International Language Support

During NCM installation, you are prompted to select a Collation Type when configuring a new MS-SQL Server database. The goal is to facilitate use of NCM regardless of your native language, writing system, and cultural conventions.

MS-SQL Server collation dictates the character set that is stored in the database. For example, if you select a Chinese collation, you can only enter Chinese characters, not Japanese, Korean, and so on. Keep in mind, however, you can always enter Latin characters despite the collation type you select.

As a result of the language you select, you can enter the following information into NCM in that language:

- Comment fields
- Description fields
- Custom data labels
- Most name and text fields, such as device location and vendor (**Note**: Currently, you cannot enter a username or hostname.)

You can search on single and multibyte character sets as long as the field being searched accepts them. You can also import and export configuration policies that contain single and multibyte character sets. For more information on collation, refer to your MS-SQL Server documentation.

When using NCM internationalization support with Oracle, you must specify the appropriate database character set when creating a new Oracle database. For example, to be able to input Chinese characters, you would select one of the available Chinese character sets, such as ZHS16CGB231280, as the database character set. In addition, if the language you select is double-byte encoded, for example Chinese, Korean, or Japanese, you also need to set the NLS_LENGTH_SEMANTICS initialization parameter to CHAR. Please refer to your Oracle documentation for detailed information on setting parameters when creating a new Oracle database.

Installation CDs

There are currently three installation CDs:

- Windows Edition
- Solaris Edition
- Linux Edition

Installing on Windows

For a Windows installation, your computer should automatically run the installation application after you insert the installation CD into the CD-ROM drive. If you cannot install from the installation CD, with Admin privileges, perform the following procedure to install NCM manually:

1. On the Windows taskbar, click Start, and then click Run.
2. Enter: `<drive>:\setup.exe`, where `<drive>` is the letter of your CD-ROM drive.
3. Click OK.

Note: Setup does not work with PC Anywhere. If you attempt to run Setup through PC Anywhere, you cannot view the windows to step through the installation. This also affects uninstalling NCM.

Installing on Linux

If you are installing NCM on a Linux server, enter the following commands to mount a CD drive. It is not mounted automatically. You must login as root.

1. `#> mount /mnt/cdrom`
2. `#> cd /mnt/cdrom`
3. `#> cd linux`
4. `#> ./setup.bin`

Installing on Solaris

To install NCM on Solaris, first download the latest Solaris patches from the Sun Web site:

http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE

Enter the following commands to install NCM manually. Be sure to change to the drive on which you want to install NCM. At the shell prompt, enter:

1. `su root` [when prompted, enter the password]
2. `cd /cdrom/rendition_4_0/solaris`
3. `sh setup.bin or ./setup.bin`

Follow the instructions that appear on the screen.

Note: If you log on remotely to run setup, you may see a message like "`Warning: Cannot convert string....`" As long as you have root access, you can ignore this message and continue. If you see the message, "`It appears port 443 is in use...`," then you are not logged in to the root account. Exit Setup, log out, try logging into the root account again, and run NCM Setup when you are logged in as root.

The NCM host computer needs 2x RAM SIZE in SWAP space. In your UNIX shell, enter `swap -l` to see your current swap setting (expressed as 1k blocks). Refer to your Solaris documentation for information on increasing swap space.

Note: If you are installing NCM on Solaris 10 and have configured a Non-global Zone on the Solaris 10 host, refer to the *Installing NCM on Solaris 10 User's Guide.*

Installation Wizard

The following table guides you through the installation process.

Note: If you plan to use Oracle as your back-end database, you must create the Oracle database before installing NCM. Please refer to your Oracle documentation for information on creating and configuring an Oracle database. Cisco supports Oracle Enterprise 9.2.0.1. Keep in mind that during the NCM installation you will be prompted to create a new Oracle database, even though you have already created one. However, be sure to select the "Create a new database" option because the NCM installer needs to correctly setup the Oracle database.

Step	Install Wizard Page	Action
1	Introduction	Review the NCM database requirements information and click Next.
2	System Requirements	Confirm that you have met all system requirements and click Next.
3	License Agreement	Review the license agreement, click the "I accept the terms of the License Agreement" option, and click Next.
4	Product License Folder	Enter the path to the location of the folder that contains the product license files (.lic). Click the Choose button to browse your system for the location of the folder. If you want to copy the product license files to your CiscoWorks Network Compliance Manager install folder at a later time, click Next. If you are installing on a Linux or Solaris server, copy the product license files to a directory on the server.

Step	Install Wizard Page	Action
5	Choose Install Set	NCM works with MySQL, Oracle, or SQL Server 2000. Options include: • "Client and Server using SQL Server 2000" — Click this option and then click Next if you already have an SQL Server 2000 running on your network. Go to Step 8. (Note: You will be prompted to accept the Microsoft SQL Server license agreement.) • "Client and Server using MySQL Max" — Click this option and then Next if you would like NCM to install its own MySQL Max database, or if you already have one running on your network. Go to Step 6. • "Client and Server using Oracle" — Click this option and then Next if you already have an Oracle server running on your network. Go to Step 6. • "Client and Connector" — Click this option to install the client and LMS Connector only. Go to Step 5.5 **Note**: This option should be installed on the LMS Server. Keep in mind that if you are using an existing database server, you are prompted for the database server's hostname, port, and the username and password to create a new or existing database. When installing SQL Server: • Set Authentication to "mixed mode". • Set Collation to "SQL_Latin1_General_CP1_CI_AS" (the default). • The database must not be case-sensitive and must use local authentication. • NCM requires a working Admin password that can create new users and new databases. **Note**: NCM provides a performance monitor for the server upon which the application runs. It does not, however, monitor the database size and disk space if the database is installed on a second, separate server. If you install the database on a second, separate server, ensure that you have monitoring software that will alert you if disk space is running low or the database is running out of space.

Step	Install Wizard Page	Action
5.5	CiscoWorks Install Folder	Enter the correct folder where CiscoWorks is installed or accept the displayed folder and click Next.
6	MySQL Max Installation or Oracle Installation	If you want to install MySQL Max, click the "MySQL Max" option and click Next. If you already have a MySQL Max database installed, click the "Use existing MySQL Max" option and click Next. Go to Step 8. **Note:** If you want to use Oracle, click the "Oracle" option and click Next. If you already have an Oracle database installed, click the "Use existing Oracle" option and click Next. Go to Step 8.
7	Important: MySQL Version	The MySQL database must be 3.23.55-MAX, with InnoDB type. Click Next. **Note**: This panel does not appear if you have chosen to install a new instance of MySQL.
8	Previous Admin Settings	Click Yes to use the previous Admin settings.
9	Choose Install Folder	Enter the installation location or accept the default location, *c:\Rendition*, by clicking Next. If you are installing on a Linux or Solaris server, change to the directory where you want to install NCM, (for example: */usr/local/rendition).*
10	Database Settings	Tell NCM where the database software is installed. Either click "The database software is installed on this computer" option or "The database software is installed on another computer" option and click Next. **Note**: This panel does not appear if you are installing MySQL or are doing a client-only install.
11	Configure Email	For event notification, enter the name of the SMTP server and click Next. The default SMTP server is "mail."
12	Configure ACL Parsing	Click the check box if you want to enable the parsing of ACL configurations with each snapshot and click Next. **Note:** Parsing ACL information can increase the average time for a snapshot of a device significantly. It also increases the amount of data storage required for each snapshot.

Step	Install Wizard Page	Action
13	Choose Shortcut Folder	Click Next to accept the default location (in a new Program Group) for the product icons, or choose another location and click Next.
14	Pre-Installation Summary	Review the information for accuracy and click Install. Installation could take several minutes.
15	Database Admin Login	Enter the hostname, database server port, and the login information for the database administrator, then click Next. For example: • Hostname: MySQL1.cisco.com • Port: 3306 • Username: admin • Password: password **Note**: This panel does not appear if you are installing MySQL or are doing a client-only install.
16	Configure Database	If you are not using an existing database, make sure the "Create New Database" option is checked and click Next. If you are using an existing NCM database, click the "Use existing Network Compliance Manager database" option and click Next. **Note**: If you want to use an existing NCM database and upgrade, click the "Use existing Network Compliance Manager database" option and click Next.

Step	Install Wizard Page	Action
17	New Database/Existing Database	Enter the username and password NCM uses to connect to the database, the name of the database to create, and click Next. **Note**: For MS-SQL Server databases, you can select the collation type from the drop-down menu. For information on collation, refer to your MS-SQL Server documentation. If you uncheck the "Create Network Compliance Manager user with this username and password" checkbox, you are prompted to enter a username and password for the NCM administrator. If the checkbox is checked (the default), the username and password you entered for the database is used for the NCM administrator's username and password. **Note**: If you are using an existing database, the name provided is not the name of the database to create, but the name of the existing database.
18	Confirm Database Settings	Confirm the database information and click Next.
19	Configure Admin	Enter the first and last name of the NCM administrator, his/her email address, and click Next. Setting up the database could take several minutes.
20	Install Complete	Be sure to wait at least three minutes before launching NCM. To close the Install Wizard, click Done.

Installing Nmap on Solaris

Nmap has several installation prerequisites. Make sure you have the following installed before installing Nmap. These packages are available on the NCM Install CD or at http://sunfreeware.com.

- glib
- gtk
- openssl-0.9.7g
- pcre
- libgcc-3.3 or gcc-3.3.2 (libgcc-3.3 is preferred)

1. cd /RENDITION_HOME/server/ext/nmap
2. Unzip and add the packages using the following commands:
   gunzip <filename>
   pkgadd -d <filename>

   For example:
   cd /rendition/server/ext/nmap
   gunzip nmap-3.81-sol9-sparc-local.gz
   pkgadd -d nmap-3.81-sol9-sparc-local
3. Create a link to the nmap executable in the RENDITION_HOME/server/ext/nmap directory:

   cd /RENDITION_HOME/server/ext/nmap
   ln -s /usr/local/bin/nmap nmap

Installing Nmap on Linux

To install Nmap on Linux:

1. cd /Rendition/server/ext/nmap
2. Install the RPM package using the following command:
   rpm -i <rpm file>

   For example:
   cd /Rendition/server/ext/nmap
   rpm -i nmap-3.81-1.i386.rpm
3. Create a link to the nmap executable in the Rendition/server/ext/nmap directory:

   cd /Rendition/server/ext/nmap
   ln -s /usr/bin/nmap nmap

Installing Adobe Acrobat Reader

Cisco recommends that you install the Adobe Acrobat Reader version 4.0 or greater to view the PDF documentation. To install the latest version of Adobe Acrobat Reader, point your browser to:

http://www.adobe.com/products/acrobat/readstep.html

Follow the instructions to download and install Acrobat Reader.

Note: Third-party products mentioned in this documentation are manufactured by vendors independent of Cisco. Cisco makes no warranty, implied or otherwise, regarding the performance or reliability of these products. We provide third-party contact information to help you find technical support. However, third-party contact information is subject to change without notice and, therefore, Cisco can in no way guarantee the accuracy of this contact information.

Configuring Devices

For device-specific configuration information, refer to the *Device Driver Reference for Network Compliance Manager*.

- By default, when you add a device NCM runs a task to configure Syslog automatically. If you use Syslog, this is the most convenient way to set up new devices.
- If you use Syslog and do not want NCM to configure Syslog messaging automatically, manually configure all devices to forward syslog change notifications to the NCM Syslog server.
- If you use a Syslog relay, configure the relay to forward all Syslog notifications to NCM.
- If you use TACACS+ or RADIUS, it is recommended that you set up a new username and password to enable NCM to collect snapshots from devices.
- If access lists are configured on devices to restrict Telnet/SSH, add the NCM IP address to the list of allowed hosts.

Be sure to review the current *Release Notes* for issues that might affect your devices or overall network.

Uninstalling NCM

Uninstalling NCM requires several steps. The most significant steps are uninstalling NCM itself and removing related components from either Microsoft Windows, Solaris, or Linux. If you chose to install a MySQL Max database with NCM, you may want to uninstall that database at the same time, however, you permanently lose your historical data if you delete the database.

Note: These steps assume you installed NCM using the default folders and names. If you installed to a different folder or used different names, you must adjust accordingly.

Uninstalling from Windows

1. Click Start → Programs → CWNCM → Uninstall CWNCM.
2. Click Uninstall.
3. When the uninstall program is done, click Finish.
4. A message appears saying that not all files or folders could be removed. The folder `c:\rendition` (the installation folder) is removed when you restart the computer.
5. Shut down all your applications and restart the computer before re-installing NCM.
6. There are files left in other locations to preserve your settings, logs, and scripts in case you re-install NCM. If you want to completely purge NCM from your system, you can delete the following:

   ```
   c:\WINNT\Temp\Rendition
   c:\WINNT\site_options.rcx
   ```

Uninstalling from Linux and Solaris

As root:

1. Navigate to the InstallDirectory/UninstallerData directory (for example: `/usr/local/rendition/UninstallerData`).
2. Enter: `#./Uninstall_NCM`
3. There are files left in other locations to preserve your settings, logs, and scripts in case you reinstall NCM. If you want to completely purge NCM from your system, manually delete all files (for example: `# rm -rf /usr/local/rendition`).

Note: These steps assume you installed NCM using the default directories and names. If you installed to a different directory or used different names, you must adjust accordingly.

Uninstalling MySQL Max from Windows

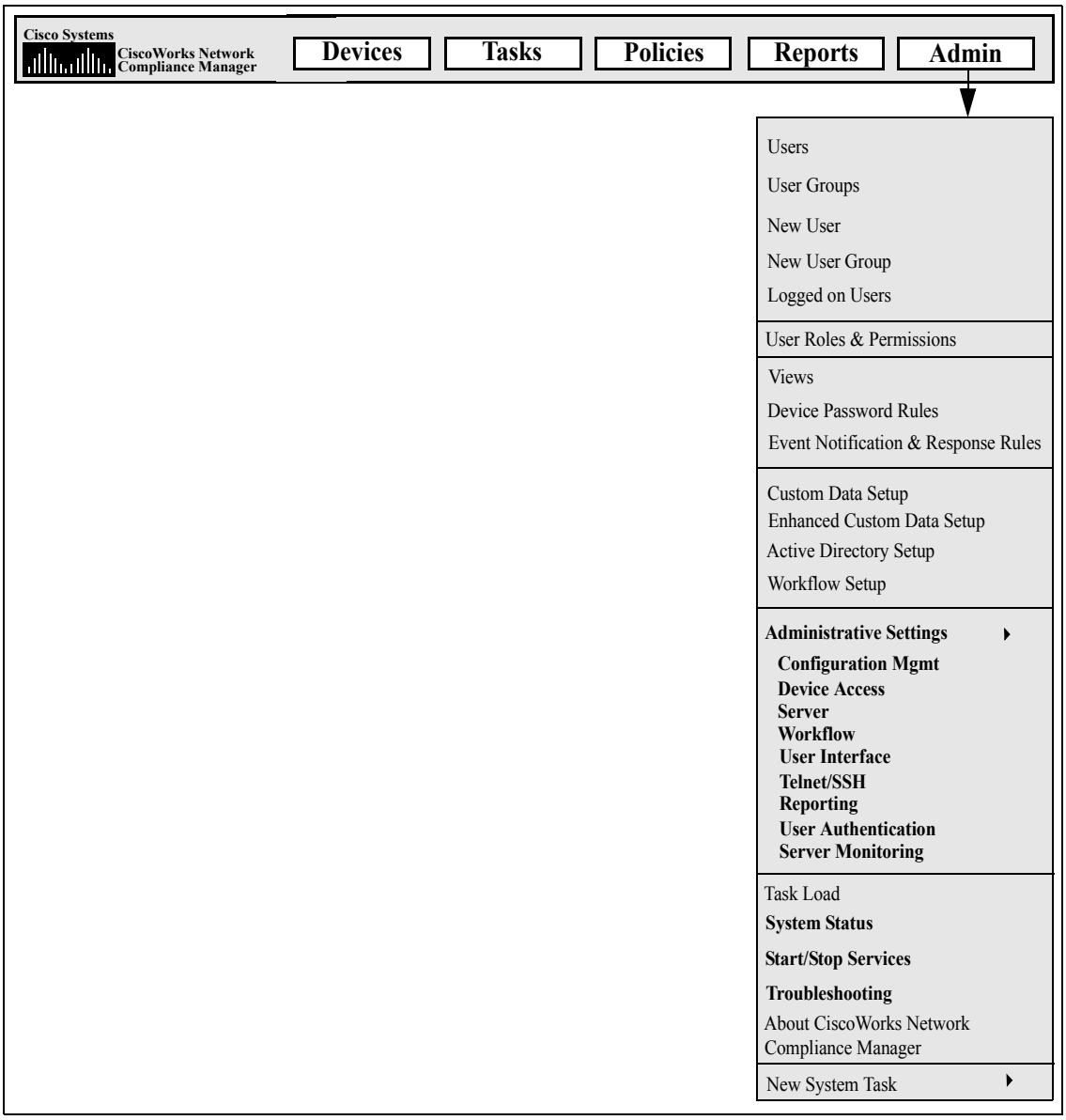
Warning: *Uninstalling the MySQL Max database permanently deletes your historical data. There is no undo*.

1. In the Windows Control Panel, double-click Add/Remove Programs. Select MySQL Servers and Clients, then click Remove.
2. Click Start → Settings → Control Panel → Administrative Tools → Services. Right-click MySQL and select Stop.
3. Click Start → Run, then enter `cmd`.
4. Enter `c:\mysql\bin\mysqld-max-nt.exe --remove`. This assumes you installed MySQL to the folder `c:\mysql`.
5. In the Services window, verify that the MySQL Service is gone. If it is still listed as disabled, close all programs and restart your computer, then check the Services window again.
6. Click Start → Run to launch a command window, then enter `cd c:\`, then enter `del c:\mysql`.

Chapter 2: Configuring Administrative Settings

Use the following table to quickly locate information.

Navigating to Administrative Settings



Getting Started

As the System Administrator, you can define values for configurable settings that affect NCM's operation. These settings receive initial values during installation, but you can change the values to customize features. For example, you can change the default values for intervals associated with various operations, or configure support for scripting languages. You can also customize the appearance and content of certain pages.

To review the configuration options and make changes, on the menu bar under Admin, select Administrative Settings. You can select the following options:

- Configuration Management
- Device Access
- Server
- Workflow
- User Interface
- Telent/SSH
- Reporting
- User Authentication
- Server Monitoring

Configuration Management

The Configuration Mgmt page enables you to configure:

- Configuration change detection
- User identification
- Startup and running configurations
- ACL parsing
- Configuration policy verification
- Pre and post task snapshots
- Topology and Duplex data gathering
- Flash storage space
- Boot Detection

To view the Configuration Mgmt page, on the menu bar under Admin select Administrative Settings and click Configuration Mgmt. The Configuration Mgmt page opens. Be sure to click Save to save your changes.

Configuration Mgmt Page Fields

Field	Description/Action
Change Detection	
Change Detection	Select one of the following options: • Enabled — NCM takes device configuration snapshots whenever changes are detected (the default). • Polling Only — NCM takes device configuration snapshots during device group snapshots, but not when changes are detected. • Disabled — Configuration snapshots are not taken in response to detected changes or during device group snapshots. Refer to "Change Detection" on page 65 for detailed information on change detection.

Field	Description/Action
Change Detection Interval	Enter the delay interval between detection of a change and the snapshot. The default is 10 minutes. When NCM detects a change, the device snapshot is delayed for the interval specified here. The subsequent snapshot reflects all change notifications sent during the interval.
Syslog Detection Patterns	If you want to add a pattern to the default patterns supplied by NCM, enter a pattern in the right-hand box and click Add Pattern <<. You can select a pattern from the left-hand box and click Delete Pattern to delete a pattern. NCM looks in the Syslog server for matches to these patterns. When NCM finds a match, it indicates a configuration change and takes a snapshot of the device configuration, if enabled above. (**Note**: Cisco provides a Syslog server. If you kept your current Syslog server when you installed NCM, you still must install the NCM Syslog server to relay Syslog messages to the NCM Syslog server.)
Syslog Patterns to Ignore	If you want to ignore a pattern, enter a pattern in the right-hand box and click Add Pattern <<. You can select a pattern from the left-hand box and click Delete Pattern to delete a pattern.
Use IP Address of sender of Syslog Messages	If checked, the IP address of the Syslog messages sender is used.
Users to Ignore for Change Detection	Indicate the users to ignore when processing Syslog or AAA change events. To add a user, enter the user name in the right-hand box and click Add Username <<. To delete a user select the username in the left-hand box and click Delete Username.
Change User Identification	
Auto-Create Users	If checked, NCM creates a new user if it does not recognize the author of a configuration change.
Auto-Create User Suffix	Enter the suffix that NCM appends to new users per the Auto-Create feature. The default is "_auto".
Syslog User Identification	If checked, NCM tries to identify users from Syslog messages.

Field	Description/Action
Syslog User Patterns	Enter a pattern in the right-hand box and click Add Pattern <<. You can select a pattern in the left-hand box and then click Delete Pattern to delete the pattern. NCM looks in the Syslog for matches to these regular expressions. When NCM finds a match, it captures the text as a user. Normally, the device drivers populate these patterns.
Resolve Workstation IP Address from Syslog	If checked, NCM resolves the IP address from the Syslog message and treats the domain as the username responsible for the related configuration change. This method is used only if the username cannot be determined in other ways from the Syslog message.
Store Unresolved IP Addresses	If checked, when a host name using DNS cannot be resolved, NCM treats the IP address as a username. Periods are replaced by dashes. For example, 10.10.1.1 becomes user 10-10-1-1.
Auto-Create Users from Syslog	If this option and Auto-Create Users are checked, NCM attempts to match users identified from Syslog messages to existing users. When there is no existing user, a new user is created.
Startup/Running Configurations	
Capture Startup Config	Select one of the following options: • Off — NCM does not capture each startup configuration. • Detect Only — NCM captures each startup configuration and compares it to the running configuration, but does not store the startup configuration. • On (the default) — NCM captures each startup configuration, compares it to the running configuration, and stores the startup configuration. Keep in mind that not all vendors and devices support the concept of a startup configuration.
Snapshot after Sync	If checked, NCM takes a snapshot after synchronizing the startup and running of configurations.
ACL Parsing	

Field	Description/Action
Parse ACL Data with each Snapshot	Select one of the following options: • Enabled — NCM parses and stores ACL data with each snapshot. • Disabled — NCM does not parse ACL data with each snapshot. Keep in mind that this option only sets the default state of this feature when adding new devices. You can use batch editing to turn on and off ACL parsing for groups of devices. (**Note**: This option can be overridden on a device-by-device basis.)
ACL Editing	
Show pre-edit application script	If checked, the script for pre-processing ACL applications is displayed when editing or creating ACLs. The pre-application script negates the existing applications of an ACL on the device. The new or updated ACL script adds the edited ACL to the device.
Show edit preparation script	If checked, the edit preparation script is displayed when editing or creating ACLs. The edit preparation script performs any necessary scripting to prepare the device to accept the edited ACL.
Show application script	If checked, the ACL application script is displayed when editing or creating ACLs. The application script is the piece of scripting used to apply an ACL, for example to a VTY connection. The application script re-applies the ACL.
Configuration Policy Verification	
Verify Before Deploy by Default	If checked, NCM checks edited configurations against defined configuration policies before deployment.
Pattern Timeout	Enter the maximum number of seconds a pattern can take to match a configuration. The default is 30 seconds.
Pre-Task and Post-Task Snapshots	

Field	Description/Action
User Override Pre/Post Task Snapshot	If checked, enables users to override the default pre-task and post-task snapshot settings when running individual tasks. If override is allowed, the pre and post task snapshot options are displayed on New Task pages, where applicable. If override is not allowed, the default setting is used. (Refer to "Configuring Pre and Post Task Snapshots" on page 67 for detailed information.)
Allow Per-Script Pre/Post Task Snapshot Setting Hints	If checked, enables individual scripts to override pre-task and post-task snapshot settings. **Note**: To override the pre-task snapshot setting, include a comment in the script with the text "tc_pre_snapshot=true" to request a pre-task snapshot or "tc_pre_snapshot=false" to request no pre-task snapshot. To override the post-task snapshot setting, include a comment in the script with the text "tc_post_snapshot=true" to request a post-task snapshot as part of the task, "tc_post_snapshot=task" to request a post-task snapshot as a separate task, or "tc_post_snapshot=false" to request no post-task snapshot. Refer to "Configuring Pre and Post Task Snapshots" on page 67 for detailed information.
Snapshot Before Run Command Script	Select one of the following options: • None • As part of task
Snapshot After Run Command Script	Select one of the following options: • None • As part of task • Scheduled as separate task
Snapshot Before Configuration Deployment	Select one of the following options: • None • As part of task

Field	Description/Action
Snapshot After Configuration Deployment	Select one of the following options: • None • As part of task • Scheduled as separate task
Snapshot Before Run Diagnostic	Select one of the following options: • None • As part of task
Snapshot After Run Diagnostic	Select one of the following options: • None • As part of task • Scheduled as separate task
Snapshot Before Delete ACL	Select one of the following options: • None • As part of task
Snapshot After Delete ACL	Select one of the following options: • None • As part of task • Scheduled as separate task
Snapshot After Synchronize Startup/Running	Select one of the following options: • None • As part of task • Scheduled as separate task
Post-Task Snapshot Delay	Enter the delay for any post-task snapshots that run as separate snapshot tasks (if any). The default is 30 seconds.

Diagnostics

Field	Description/Action
Topology Data Gathering Frequency	Topology data is included in a new class of diagnostics that requires throttling to preserve network performance. Topology data is used to render network diagrams. Gathering topology data represents a significant load on the NCM server and should be done as infrequently as possible. Enter the minimum amount of time (in hours) allowed between attempts to gather topology data. The default is 168 hours.
Stored Topology Data	Enter the allowable age (in hours) of topology data currently stored in the database. If the stored data is older than this value, data will be retrieved directly from the device. Otherwise the stored data will be used. The default is 72 hours.
Duplex Data Gathering Frequency	Duplex mismatch data is included in a new class of diagnostics that requires throttling to preserve network performance. Duplex mismatch data is used to identify a common end-to-end performance problems. Often times a duplex mismatch occurs when one machine is set at full-duplex and another at half-duplex. Gathering duplex mismatch data represents a significant load on the NCM server and should be done as infrequently as possible. Enter the minimum amount of time (in hours) allowed between attempts to gather duplex data. The default is 168 hours.
Stored Duplex Data	Enter the allowable age (in hours) of duplex data currently stored in the database. If the stored data is older than this value, data will be retrieved directly from the device. Otherwise the stored data will be used. The default is 72 hours.
Flash Storage Space	
Flash Low Event	If checked, an event is generated if the detected available flash storage space is low.
Flash Low Threshold	Enter the percentage of flash storage space that must be filled before a low space event is generated. The default is 90%.
Boot Detection	
Error Margin Factor	Enter how much clock drift (in seconds per six hours) to allow for when detecting device boots. It is recommended that the minimum frequency with which you check your devices be once every six hours.

Change Detection

NCM uses several methods for detecting changes to a device configuration, including:

- Syslog messages
- AAA log reading
- Internal proxy

From these methods, NCM uses a number of different inputs to determine who actually made a change on the device. This information provides the most likely user responsible for the change. In order of priority, the following information is used:

- User who scheduled a password change that was run on the device.
- User who scheduled a software update that was run on the device.
- User who deployed a configuration to the device.
- User who ran a script on the device.
- User who connected to the device via NCM' proxy.
- User information gathered from AAA logs.
- User information parsed out of a syslog message.

NCM assigns a change attribution to a device interaction that is higher in the priority list. For example, if a user schedules a password change while another user had proxied to the device during the same time period, if a change had been detected, that change would be assigned to the user who had scheduled the password change.

To view configuration changes on a device:

1. On the menu bar under Devices, click Inventory. A list of all currently managed devices opens.
2. Click the device for which you want to view configuration changes. The Device Details page opens.
3. From the View drop-down menu, click Configuration Changes.
4. In the User Name column, click the details link. The User Attribution Details page opens.

User Attribution Details Page Fields

Field	Description/Action
Change Event Detail	
User	Displays the name of the user who made the change.
Date	Displays the date the change was made.
Device Interaction	Displays the method used to detect the change, for example Syslog.
Additional Details	Displays additional details about the change, for example if the change was made from the console.

Configuring Pre and Post Task Snapshots

Configuring pre and post task snapshots enables you to:

- Define the pre and post snapshot behavior for various task types
- Run post snapshots as separate tasks
- Override the default pre and post snapshot behavior when running a specific task

Pre and post task snapshot options can be displayed for the following tasks:

- Deploy Config (refer to "Deploy Config Task Page Fields" on page 212)
- Run Diagnostics (refer to "Run Diagnostics Task Page Fields" on page 309)
- Delete ACL (refer to "Delete ACLs Task Page" on page 720)
- Synchronized Startup and Running (refer to "Synchronize Startup and Running Task Page Fields" on page 318)
- Run Command Script (refer to "Run Command Script Task Page Fields" on page 302)

When providing snapshot hints in command scripts, you can add a special tag to a command script to specify the pre or post task snapshot behavior when running that script. For example, suppose you have an advanced script that does not actually connect to or modify a device. The advanced script simply uses the NCM API to extract information about a device and generate a report. In that case, there is no need to take a snapshot after the task is run, so the advanced script could include a tag to indicate that no post snapshot is needed.

Keep in mind that if more than one script is selected to run against a group of devices, and more than one of the scripts contains a hint, the most conservative behavior among those specified is used.

Device Access

The Device Access page enables you to:

- Designate device connections methods
- Configure Detect Network Devices task settings
- Configure Bastion host settings
- Configure SecurID device access
- Specify what credentials should be used to access devices on a per-task basis
- Designate Nortel BayRS MIB/OS versions
- Enter Gateway Mesh information

Network environments are often protected by network firewalls. NCM provides three methods for accessing devices through firewalls:

- Open up direct access through the firewall.
- Create a Network Address Translation (NAT) on the firewall and configure NCM to use the NAT to access the device. Keep in mind that NAT addresses do not appear on the device configuration for the device using the NAT.
- Configure NCM to use an existing bastion host on the far side of the firewall to proxy management requests. Since bastion hosts are already allowed access through the firewall, the bastion host configuration enables management of a device through a proxy connectivity of the bastion host.

Keep in mind that a console server maintains a physical connection to the device using the serial link. These links are provided through Telnet to specific IP port numbers hosted on the console server. Console server connections are available even if the network device is disconnected from the network.

To view the Device Access page, on the menu bar under Admin select Administrative Settings and click Device Access. The Device Access page opens.

Device Access Page Fields

Field	Description/Action
Device Connection Methods	
Password Selection	Select one of the following options: • Always try last successful passwords first. — If checked (the default), NCM first tries the last successful password from the previous access to the device. Keep in mind that while this password is stored in the database, it is not necessarily tried first the next time the device is accessed. The "Last used rule changed" event will continue to be generated. Consequently, you can determine when devices are not using their expected password rule. • Always try passwords in defined order. — If checked, NCM always tries passwords in a defined order. Keep in mind that NCM keeps track of the most recently used authentication credentials for the next round of communications with a device. This enables you to take advantage of the Device Password Rules, while minimizing the number of connection attempts to each device. Refer to "Creating Device Password Rules" on page 145 for more information.

Field	Description/Action
Default Connection Methods	The following methods are used to connect to devices. These methods appear checked by default on the New Device page and in the Add Device wizard. Check one or more of the following options: • Telnet • SSH • SNMP • RLogin • SCP • FTP • TFTP **Note**: NCM has an integrated TFTP server and will generally access a device via SNMP or CLI to set up the transfer to and from this server. For devices that have their own TFTP server, NCM acts as a TFTP client. Typically, SCP must be used with the CLI. SCP requires a device be enabled to use SSH. SCP cannot run if the device does not have an SSH server running.
Bad Login Attempt Delay	Enter the number of seconds to delay after a bad login attempt to allow the device time to recover. The default is five seconds.
SNMP Timeout	Enter the number of seconds to delay while waiting for a device to operate on a set of SNMP commands (such as loading a config). The default is 40 seconds.
Detect Network Devices Task Settings	
Path to Nmap utility	Enter the path to the Nmap utility for scanning network devices. (**Note**: Nmap enables you to scan networks to determine which hosts are up and the services they offer. Refer to www.Insecure.Org for detailed Nmap information.)
Max Addresses to Discover Per Task	Enter the number of IP addresses to discover. Be sure to limit Detect Network Devices tasks to the maximum number of addresses (1024) to scan to reduce network traffic.

Field	Description/Action
Max SNMP Scanner Threads	Enter the maximum number of SNMP scanner threads the Detect Network Devices tasks will spawn during device discovery using the SNMP scanning method. The default is 79. Theoretically, the higher the maximum SNMP scanner thread count, the faster the task runs. However, having too many SNMP scanner threads can impact system performance due CPU overheard and network traffic that each SNMP scanner thread requires. (**Note**: When configuring the Detect Network Devices task, you have the option to have the Detect Network Devices task use SNMP to detect devices. As a result, the task will spawn many SNMP scanner threads that communicate to devices via SNMP. Refer to "Detect Network Devices Task Page Fields" on page 332 for information on other scanning methods.)
Network Discovery IP or CIDR Range Exclusions	Enter IP addresses or Classless Inter-Domain Routing (CIDR) range exclusions (for example: 192.168.1.0-192.168.2.0 or 192.168.31.0/24) in the right-hand box and click the Add Pattern << button. Ranges are inclusive. To delete patterns, select the patterns from the left-hand box and click the Delete Pattern button.
SNMP Timeout	Enter an SNMP timeout value in milliseconds for each SNMP SysOID probe. The default is 500ms.
Bastion Host Settings	
Use Bastion Host by Default	If checked, new devices use bastion host for Telnet and SSH access. (**Note**: Bastion Host settings can be overridden on a device-by-device basis.)
Default Bastion Host	Enter the hostname or IP address of the bastion host to use for Telnet and/or SSH access.
Default Bastion Host Username	Enter the username of the bastion host to use for Telnet and/or SSH access.
Default Bastion Host Password	Enter the password of the bastion host to use for Telnet and/or SSH access.
SecurID Device Access	

Field	Description/Action
SecurID License Usage	Select one of the following options: • Use Unique Tokens Per User — If checked (the default), each device access will use only the seed(s) corresponding to the user that initiated the task or Telnet/SSH proxy connection. • Use Software Token Pool — If checked, a pool of general use software token seeds are provided and used as efficiently as possible for maximum performance. Enter the username for which the pool of SecurID Software Tokens are associated. Using unique Software Tokens per user requires more tokens, and increases token maintenance. Using Software Tokens from a pool with a common user reduces the number of tokens required, and potentially increases task throughput.
Max Software Tokens	Enter the maximum number of Software Token licenses imported to the machine running NCM. The default is 1024.
Passcode Lifetime	Enter the lifetime for Software Token passcodes. The default is 60 seconds.
Task Credentials	

Field	Description/Action
Allow Standard Device Credentials	Select one or more of the following tasks. By default, all of the tasks are selected. • Configure Syslog • Delete ACLs • Deploy Configuration File • Discover Driver • Deploy Passwords • Reload Device • Run Command Script • Run Diagnostics • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software The above tasks enable users to select standard processing with device-specific passwords and/or network-wide password rules. For information on per-task credentials, refer to "Per-Task Credentials" on page 77. For information on password rules, refer to "Device Password Rule Page Fields" on page 147.

Field	Description/Action
Allow Per-Task Device Credentials	Select one or more of the following tasks. • Configure Syslog • Delete ACLs • Deploy Configuration File • Discover Driver • Deploy Passwords • Reload Device • Run Command Script • Run Diagnostics • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software If checked, the above tasks will prompt users to enter one-time use device credentials specific to that task. For information on per-task credentials, refer to "Per-Task Credentials" on page 77.

Field	Description/Action
Allow User AAA Credentials	Select one or more of the following tasks. • Configure Syslog • Delete ACLs • Deploy Configuration File • Discover Driver • Deploy Passwords • Reload Device • Run Command Script • Run Diagnostics • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software If checked, the above tasks enable users to select the task owner's AAA credentials to use when running the task. (**Note**: The user must have valid AAA credentials defined.) For information on per-task credentials, refer to "Per-Task Credentials" on page 77.
Nortel Discovery	
Nortel BayRS MIB/OS Versions	Displays a list of additional BayRS MIB versions/revisions that will discover the BayRS driver. Use <MIB Version>/<Revision> sequences separated by vertical bars, for example: 14.00/1D12|14.20/).
Gateway Mesh	
Local Gateway Host	Enter the hostname or IP address and port of the Gateway system that is in the same Realm as the NCM Core (for example: `gw-vlan10:3001)`. For information on the Gateway Mesh, refer to "Overlapping IP Networks" on page 165.

Field	Description/Action
Local Gateway Proxy Port	Enter the port name of the Gateway system that is in the same Realm as the NCM Core (for example: `gw-vlan10:3001)`. The default is 3002. For information on the Gateway Mesh, refer to "Overlapping IP Networks" on page 165.
Local Gateway Admin Port	Enter the Admin port number for the Gateway in the local Realm. This is used to fetch the Realm names from the Gateway Mesh. The default is 9090.
Gateway Admin Private Key Filename	Enter the filename of the private key for the Gateway needed to connect to the Admin port. This can be an absolute path or a relative path. A relative path is relative to the root of the NCM install tree, typically *C:\Rendition*. Keep in mind that the private key for the Gateway is created when the Gateway is installed. When using a NCM Standalone Gateway, the private key filename is `opswgw-mngt-server.pkcs8`. This file must be copied from the *saOPSWgw*/certificates* directory where the NCM Gateway was installed. This file should be copied to the root of the NCM installation, typically *C:\Rendition*. If you are integrating NCM with SAS, NCM uses the SAS Gateway Mesh. In this case, copy the `spog.pkcs` file from the SAS host to the root of the NCM installation, typically *C:\Rendition*. Be sure to change the filename in the Admin Settings to `spog.pkcs8`. **Note**: The `.pcks8` file is a PKCK#8 format file containing a private key used in a public key encryption scheme. To secure the Gateway Mesh, the private key must be used to administer the Gateway Mesh. NCM uses the Gateway Mesh administration function to list the Realm names supported by the Gateway Mesh. To test the Gateway Admin settings, open the New Device page and scroll down to the Connection Information section to see that there is a Realm name list.
Gateway Mesh Delay	Enter the number of seconds of latency to reach remote Realms through the Gateway Mesh. The default is five seconds. This number is added to the time-outs used when communicating with remote devices.

Be sure to click Save to save your changes.

Per-Task Credentials

Configuring per-task credentials enables you to specify what credentials are used to access devices by specifying unique credential handling for tasks that access devices. You can:

- Run tasks using the AAA credentials of the task owner
- Run tasks using one-time credentials specified when the task is created
- Configure which types of tasks require which types of credentials

Typically in a secure environment, you might have implemented a AAA server, such as CiscoSecure ACS TACACS+ server, that limits which commands each user is allowed to run on each device.

For example, suppose both User A and User B can run command scripts using specific commands for which they have permissions. Once NCM is implemented, both User A and User B need to be able to run commands scripts. However, you want to ensure that both User A and User B maintain credentials to run only the commands for which they have permissions.

Consequently, when using per-task credentials, you do not have to set up a new, static NCM account for User A and User B with permissions to run commands scripts. Each user can run command scripts with their current permissions. If either User A or User B uses a command for which they do not have permissions, NCM will return an error.

When using AAA credentials, NCM:

- Tries all standard credentials processing, including Last Successful Credentials, Device-Specific Credentials, Password Rules, and Device Archived Passwords.
- For each attempt, NCM replaces the username and password with the task owner's AAA username and password. If an attempt fails, NCM will retry again with the user's AAA password as both the exec and enable password. If all AAA login attempts fail, the task will fail.

Note: There is a hidden config setting proxy/auth_fallback_for_aaa_task that can be set in an .RCX file. If set to true, NCM will fall-back and attempt standard password handling.

When configuring one-time credentials, NCM uses the specified type of credential handling, based on its task type. For example, if only AAA credentials are allowed for Snapshot tasks, all snapshot task will use AAA credentials. If more than one credentials type is allowed for a given task type, the user has a choice as to which to use.

If a given task is selected to use one-time credentials, NCM uses the exact credentials specified by the user when the task was created. If the one-time credentials fail, the task fails.

Note: If the one-time credentials succeed, NCM does not update the last successful credentials information for the device.

Server

The Server page enables you to:

- Designate TFTP and SMTP servers
- Set NCM task limits
- Configure Syslog
- Configure device importing intervals
- Configure Domain Name resolution
- Configure Primary IP address reassignment and deduplication settings
- Resolve FDQN tasks
- Enable the Audit Log
- Configure database pruning
- Configure advanced scripting capabilities
- Configure server performance tuning
- Configure dynamic device group re-calculation

To view the Server page, on the menu bar under Admin, select Administrative Settings and click Server. The Server page opens.

Server Page Fields

Field	Description/Action
Servers	
TFTP Server IP	Enter the IP address of the TFTP server used by NCM (by default, the NCM server itself).
TFTP File Path	Enter the path and folder to which the TFTP server writes the configuration files. NCM requires read/write permissions to this folder. The default is *C:\<install directory\server\ext\tftp\tftpdroot.*
SMTP Server	Enter the host name or IP address of the SMTP server NCM uses to send email notifications.
SMTP From Address	Enter the From address NCM uses for email.
Tasks	
Max Concurrent Tasks	Enter the maximum number of tasks that can run simultaneously. NCM limits concurrent tasks to avoid impeding your network performance. The default is 20. Keep in mind that there is a limit to the number of database connections in the database connection pool. As a result, maximum concurrent tasks should never be larger than 50.
Max Concurrent Group Tasks	Enter the maximum number of group tasks that can run simultaneously. A group task, such as a snapshot run against the device inventory, schedules child tasks (one task for each device in the group). The Max Concurrent Group Tasks setting limits the number of child tasks that can run simultaneously. NCM limits the number of concurrent child tasks to avoid hindering system and network performance. The default is 15 concurrent child tasks. **Note**: By setting the Max Concurrent Group Tasks value less than the Max Concurrent Tasks value, you ensure that during large group operations, NCM is able to run independent tasks that are time-sensitive. For example, during a large group-wide change password task, NCM still runs snapshot tasks triggered by real-time change detection in a timely manner.
Max Task Length	Enter the maximum time a task can run before it is stopped and given a Failed status. The default is 3,600 seconds (one hour).
Syslog Configuration	

Field	Description/Action
Configure Syslog by Default	If checked, NCM automatically configures Syslog change detection on new devices.
Default Syslog Relay	Enter the default host name or IP address of the relay host for new devices.
Device Import	
Overwrite Existing Devices	Select one of the following options: • Yes — NCM overwrites existing device data stored in the NCM database with the data you import (the default). Devices not included in the import are unaffected. • No — NCM does not overwrite existing device data stored in the NCM database with the data you import.
Missing Device Interval	Devices that are missing from an import source longer than this interval are deleted, marked inactive, or left unchanged (per the Missing/Inaccessible Device Action). The default is 45 days.
Inaccessible Device Interval	Any device that NCM cannot access in this interval is deleted, inactive, or left unchanged (per the Missing/Inaccessible Device Action). The default is 45 days.
Missing/Inaccessible Device Action	Select one of the following options: • Delete device — Deletes devices that are missing or inaccessible from the database. • Mark device inactive — Marks missing or inaccessible devices as inactive (the default). In general, it is a good idea to change devices to inactive rather than deleting them from the database to preserve the configuration history • No action — No action is taken for missing or inaccessible devices.
Primary IP Reassignment and Deduplication Settings	
Primary IP Address Reassignment	If checked, NCM looks through all IP addresses associated with the device, including the primary IP address (plus all other interfaces associated with the device), and sets the primary IP address that matches a RegEx or other rule, if provided.

Field	Description/Action
Interface Name Reassignment RegEx Patterns	Enter a Regular Expression (RegEx) patterns in the right-hand box and click the Add Pattern << pattern. A regular expression is a special text string to specify the interface name (for example: Loopback.*) to which an IP address must conform. To delete patterns, select the patterns from the left-hand box and click the Delete Pattern button.
IP Address Reassignment RegEx Patterns	Enter a Regular Expression (RegEx) patterns in the right-hand box and click the Add Pattern << button. A regular expression is a special text string to match IP addresses on available interfaces (for example: 10\.1\..*). To delete patterns, select the patterns from the left-hand box and click the Delete Pattern button.
IP Reassignment Order	If more than one IP address matches the interface names or IP address patterns, select either: • Lowest IP address to assign as the primary IP address (the default) • Highest IP address to assign as the primary IP address
Duplication Detection	Select one of the following options for devices when duplicates are detected. **Note**: Devices are considered duplicates if they have the same interface and IP address information. • Leave Duplicates • Deactivate Duplicates (the default) • Delete Duplicates
Domain Name Resolution	
Overwrite Existing Domain Names	If checked, NCM overwrites manual FQDN entries with DNS-resolved FQDN entries when you run a Resolve FQDN task.
Audit Log	
Audit Logging	Select one of the following options: • Enabled — NCM stores an audit log of user actions. Click View Audit Log to see the log. • Disabled — NCM does not store an audit log of user actions (the default).
Database Pruning	

Field	Description/Action
Configurations	Enter the number of days to save configurations in the database. The default is 365 days.
Diagnostics	Enter the number of days to save diagnostics in the database. The default is 45 days.
Events	Enter the number of days to save events in the database. The default is 45 days.
Tasks	Enter the number of days to save tasks in the database. The default is 365 days.
Sessions	Enter the number of days to save proxy Telnet/SSH sessions in the database. The default is 45 days.
Log files	Enter the number of days to save server log files. The default is 30 days.
Diagram files	Enter the number of days to save diagram files. The default is 1 day.
Advanced Scripting	
Scripting Language 1	Advanced Scripting enables you to run custom scripts written in the scripting languages used in your network. You must have the language interpreter for each language installed and then associate the path with the language option via the Advanced Scripting settings. The scripting language specified here appears in a selection list on the New Command Script page when the Advanced Scripting option is enabled. By default, this setting is pre-configured for Expect. You must specify the path to the interpreter for this language in the corresponding Path to Interpreter [#] setting on this page You can configure Advanced Scripting capability for up to five languages, and you can overwrite the pre-configured defaults if you do not use those languages. Only languages that run from the command line are supported (for example, JScript and Python). **Note**: Slots 1 and 2 are pre-configured for Expect and Perl. However, NCM installs only the interpreter for Expect. You must install the interpreter for each language you specify here, and configure the path before you can run scripts written in these languages.

Field	Description/Action
Path to Interpreter 1	Enter the path to the interpreter that runs the language specified in Scripting Language 1.
Scripting Language [2-5]	Enter the language specified here appears in the Language selection list on the New Command Script page when the Advanced Scripting option is enabled. You must specify the path to the interpreter for this language in the corresponding Path to Interpreter [#] setting. **Note**: By default, Scripting Language 2 is pre-configured for Perl, but you must install the Perl interpreter for this setting to function.
Path to Interpreter [2-5]	Enter the path to the interpreter that runs the language you specified in the associated Scripting Language [#] box. **Note**: For Windows environments, by default Path to Interpreter 2 is pre-configured for Perl, but NCM does not install the Perl interpreter. Perl must be installed and the path configured for this setting to function.
Dynamic Groups	
Dynamic Group Auto-Recalculation	Enter how frequently the system re-calculates the member devices of all dynamic groups. The default is 60 minutes. Enter 0 to disable Auto-recalculation. (**Note**: Re-calculating dynamic group members means NCM will do number of queries to determine which devices belong to the dynamic group, based the group's rules and/or filters.)
Event Driven Recalculation	If checked, the system will re-calculate all dynamic group members each time a device change event occurs.

Field	Description/Action
Device Change Events	Select the device change events that will trigger dynamic group member re-calculation. This setting is n effect only when the Event Driven Recalculation option is enabled. Examples of device change events include: • Device Added • Device Configuration Change • Device Deleted • Device Edited • Device Software Change • Device Unmanaged
Performance Tuning	
For a list of events, refer to "Getting Started" on page 429.	Click the check box for each event you want to filter. This enables you to tune the performance of your system.

Be sure to click Save to save your changes.

Workflow

The Workflow page enables you to:

- Enable Workflow
- Configure event notification and response rules
- Configure the Device Reservation System
- Configure Device Reservations for the Telnet/SSH Proxy

To view the Workflow page, on the menu bar under Admin, select Administrative Settings and click Workflow. The Workflow page opens.

Workflow Page Fields

Field	Description/Action
Workflow	
Enable Workflow	If checked, approval is required for tasks for which an Approval rule is defined.
Priority Values	Defines the priority values that can be set on tasks requiring approval. The default values include: • Low • Medium • High You can add different values, such as Urgent, Normal, and so on by entering the value and clicking the Add Value << button. You can delete a value by selecting the value and clicking Delete Value button. **Note**: The NCM Scheduler does not look at the values. It is basically a visual queue for you to determine which tasks need approval in a timely manner.
Event Notification & Response Rules	

Field	Description/Action
Run Task	If checked (the default), all tasks that are scheduled due to event rules must be approved. For example, if a configuration policy non-compliance event occurs, thereby triggering a task for corrective action, the task must be approved before deployment.
Device Reservation System	
Device Reservation System	Select one of the following options: • Enabled — Enables the Device Reservation System (the default). For information on the Device Reservation System, refer to "Reserving Devices" on page 222. • Disabled — Disables the Device Reservation System.
Default Duration	Enter the number of minutes devices and/or device groups can remain reserved. The default is 60 minutes.
Max Number of Columns in Activity Calendar	Sets the maximum number of columns in the Activity Calendar. The default value is 1024. For information on the Activity Calendar, refer to "Activity Calendar" on page 223.
Minimum Overlap for Half-Hour	Set the minimum number of minutes into a half-hour a reservation must extend for it to be displayed on the Activity Calendar as reserved for that hour. The default value is 5 minutes.
Telnet/SSH Proxy Reservation	

Field	Description/Action
Device Reservations for Telnet/SSH Proxy	The NCM Telnet/SSH Proxy can be used to access and configure devices. It provides access control, keystroke session logging, and in-line commenting capabilities. Select one of the following options: • Ignore — Ignore device reservations when accessing devices via the Telnet/SSH proxy (the default). For information on the Device Reservation System, refer to "Reserving Devices" on page 222. • Warn — Warn users if an approved device reservation does not exist when connecting to a device via the Telnet/SHH proxy. • Prevent — Prevent users from connecting to a device via the Telnet/SSH proxy if an approved device reservation does not exist. If the user has Override permission, he/she is prompted as to whether or not to override non-access to the device. If Warn or Prevent is selected, NCM looks for a matching device reservation, including user, device or device group, if approved, and the time reserved for the multi-task project.
No Device Reservation Warning Message	Enter the warning message to display when an approved device reservation does not exist. The default warning message is: *WARNING: You do not have an approved reservation for this device at this time*. You have the option of deleting the default warning message.

User Interface

The User Interface page enables you to:

- Configure login security
- Set the date format shown on all pages
- Customize NCM menus
- Add slots for the View/Edit Modules pages
- Add and delete roles from the New/Edit Templates pages
- Customize the size of the text box on the Edit Command Script Diagnostic pages
- Customize the Device Selector display
- Enable enhanced custom fields

To view the User Interface page, on the menu bar under Admin, select Administrative Settings and click User Interface. The User Interface page opens. Be sure to click Save when you are done.

User Interface Page Fields

Field	Description/Action
Security	
Session Timeout	Enter the number of seconds NCM waits before terminating an inactive Web session. The default is 1800 seconds. Keep in mind that the change will not take effect until your next login.
Check Device Permissions for View Device Configuration	If checked, users can view the device configuration only if they have appropriate device permission. You must restart NCM for your change to take effect.
Auto-complete user name and password	If checked, the browser's auto-complete function is enabled on the NCM login page.

Field	Description/Action
Cross site scripting check	If checked, NCM checks user input to filter out the potential cross site scripting elements such as <script>, <object>, <img>, <input>, and so on. In other words, this option enables you to remove potentially malicious Javascript code from your scripts. An error is returned when malicious Javascript code is found.
Date/Time Display	
Date Format	This setting controls how dates appear throughout the Web interface. The default format is MMM-dd-yy HH:mm:ss. You can vary the order of the date and time elements, swap the date and time, enter a 4-digit year (yyyy), and change the month to a 2-digit numeric value (MM). Keep in mind that the elements are case-sensitive. For example HH refers to a 24-hour clock, while hh refers to a 12-hour clock.
Menu Customization	
Show Summary Reports	If checked (the default), a link to Excel Summary Reports is shown. The Summary reports include trend and long term data on system usage in a Microsoft Excel format.
Show Custom Menu Link	If checked, a user-defined name appears above the About option. You provide the menu title and link to an HTML page, such as the home page of your ticketing application.
Custom Menu Title	Enter the name you want to appear.
Custom Menu Page	If Show Custom Menu Link is selected, enter the URL to the HTML page you want to display when a user clicks the menu title. This can be a page within another HTML application.
Configuration Comparison	
Lines of Context for Visual Comparison	Enter the number of lines to display above and below each change when comparing two configurations. The default is 3.
Lines of Context for Email Comparison	Enter the number of lines to display above and below each change when comparing two configurations as text in email. The default is 3.
Software Center	

Field	Description/Action
Slots	Add and delete the slots (chassis slots for cards/blades/ modules) that users see on the View/Edit Modules pages. To add a slot, enter it in the right-hand box and click Add Slot <<. To delete a slot, select the slot in the left-hand box and click Delete Slot.
Show file compliance level	Click the checkbox to display the compliance level for each Image file in the Image Sets.
Templates	
Template Roles	Add and delete the roles that template authors choose from on the New/Edit Template pages. Roles can describe the role devices play in your network, such as Border or Core. To add a role, enter it in the right-hand box and click Add Role <<. To delete a role, select the role in the left-hand box and click Delete Role.
Scripts	
Script Text Height	Enter the size (height) of the text box on the Edit Command Script and Edit Diagnostics pages. The default is 12 rows.
Script Text Width	Enter the size (width) of the text box on the Edit Command Script and Edit Diagnostics pages. The default is 60 characters.
Device Selector	
Device Selector Maximum Count	Enter the maximum number of devices to be loaded into the Device Selector. The default is 10,000.
Device Selector Maximum Devices Per Page	Enter the number of items to be displayed on each page of the Device Selector. The default is 100. Increasing this number could impact the responsiveness of the Device Selector.
Device Selector Initial View	Select one of the following options: • All Device Groups (the default) • All Devices
Enhanced Custom Fields	

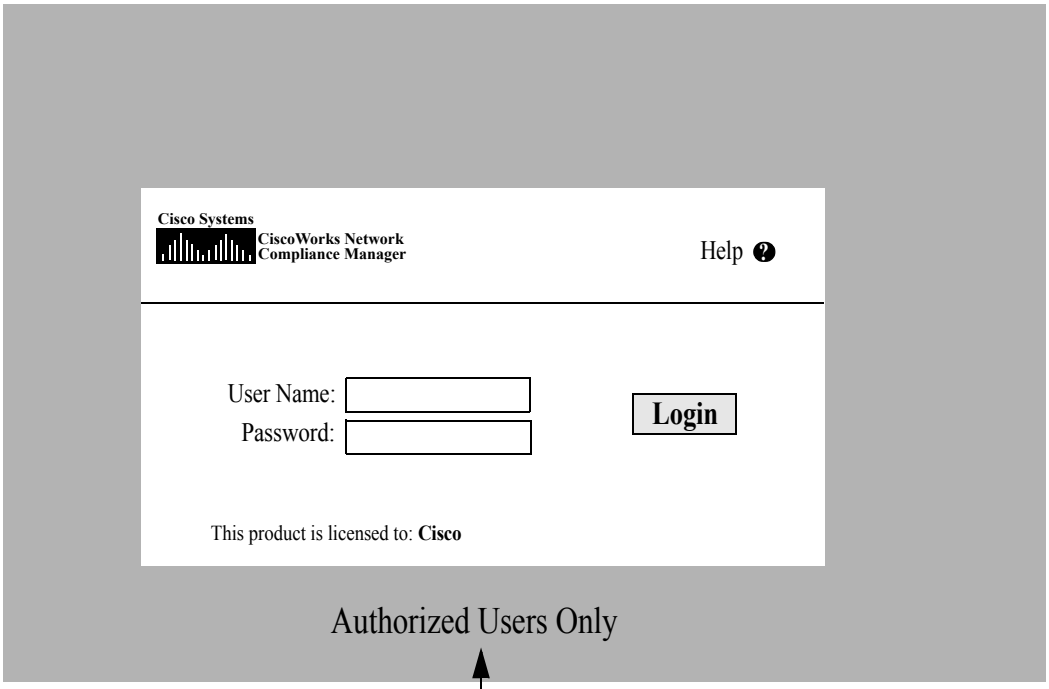
Field	Description/Action
Enable Enhanced Custom Fields	If checked, you can configure enhanced custom fields for some data sets. Custom data fields enable you to assign useful data to specific devices, configurations, users, and so on. Refer to "Custom Data Setup Page Fields" on page 539 for information.
Miscellaneous	
Task Page Refresh Interval	Enter the number of seconds for the Task List pages to refresh. The default is 60 seconds.
Config Size Threshold for Displaying as Plain Text	Enter a config size threshold for displaying a config in plain text. The default is 1,000,000 bytes. Keep in mind that certain configs are too large to provide special handling, such as line numbering, without consuming enormous server and browser resources. When a config exceeds the default value, it is displayed as plain text using <pre> and </pre> tags.
Mask Community Strings	If checked, community strings are masked.
Disable hidden stack trace output	If checked, hidden stack trace is disabled. If not checked, when a server error occurs, NCM outputs the stack trace as hidden text in the HTML page in addition to the server log. (**Note**: A full Java stack trace is provided as hidden HTML by default to aid in Support calls. If you think this might be a potential security vulnerability, check this option.

Customizing the NCM Login Page

You can customize the NCM Login page to display information, such as a warning message or company-specific information.

To customize the NCM Login page:

1. In the *$NCM_install_dir/resource* directory, open the *customer_banner.html* file. If the file does not exist, create one with that name. (Note: You may also need to create the *resource* directory.)
2. Open the file with a text editor (HTML is allowed) and enter the text to be displayed on the NCM Login page.
3. Save the file and login to NCM. The text is displayed under the Login box. There is no limitation on the number of words you can display. However, you should check the display to make sure that it fits properly on the page. The following is a sample NCM login page.



Custom Banner

Telnet/SSH

The Telnet/SSH page enables you to configure:

- Telnet/SSH logging
- The Telnet/SSH proxy
- The Telnet client
- The Telnet server
- The SSH server
- Device single sign-on

To view the Telnet/SSH page, on the menu bar under Admin, select Administrative Settings and click Telnet/SSH. The Telnet/SSH page opens.

Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issues. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task.

Telnet/SSH Page Fields

Field	Description/Action
Telnet/SSH Session Logging	
Log Commands	If checked, this option saves your commands when running a Telnet or SSH session. To view the commands, from the Device Information page, click View Telnet/SSH Sessions and then View Commands Only. The Convert to Script link on this page enables you to quickly capture the commands from a session into a script for future use.
Log Responses	If checked, this option saves the complete session logs when running a Telnet or SSH session. To view the logs, from the Device Information page, click View Telnet/SSH Sessions and the View Full Session. The Convert to Script link on this page enables you to quickly capture the commands from a session into a script for future use.
Telnet/SSH Proxy	
Enable Telnet/SSH Server	The Telnet/SSH Proxy can be used to access and configure devices. It provides access control, keystroke session logging, and in-line commenting capabilities. If checked (the default), NCM can operate as a Telnet/SSH server.
Server Inactivity Timeout	Enter the maximum time an idle Telnet or SSH session is connected to the NCM Telnet/SSH server before being disconnected. If a Telnet/SSH client connected to NCM is not active for this period of time, the session times out. The default is 30 minutes.
Default Connection Method	Select either Telent or SSH to connect to a device without Single Sign-on. This is the connection method used by the Telnet/SSH Proxy connect command when the *-method* option is not included. The method is ignored unless Use Single Sign-on is selected and the Edit Device page Supports list includes the same connection method. **Note**: When NCM is configured to use SecurID for external authentication, Single Sign-on functionality will not be enabled when connecting to the NCM proxy. You will need to authenticate again using your SecurID credentials because SecurID passcodes cannot be reused.

Field	Description/Action
Device Inactivity Timeout	Enter the number of minutes NCM keeps an idle device session open before closing the connection. The default is 30 minutes.
SSH Login Timeout	Enter the number of seconds for timeout of SSH logins using the "-login" switch in the NCM proxy. The default is 15 seconds.
Alert for Concurrent Session	Select one of the following options: • Warn of Concurrent Sessions — If checked (the default), NCM issues a warning when a second user tries to connect to a device. This helps prevent one user from inadvertently overwriting the changes of another. Only users with Admin permissions can override a warning. This is the default. • Prevent Concurrent Sessions — If checked, NCM prevents concurrent sessions for all users. • No Action — If checked, NCM ignores concurrent sessions.
Concurrent Session Handling for Distributed System	Select one of the following options: • Allow sessions to non-local devices • Prevent sessions to non-local devices Refer to the *NCM High Availability Distributed System on Oracle User's Guide* for information on Distributed Systems.
Connect to Unknown Devices	If checked (the default), NCM enables users to connect to unmanaged devices.
Max Device Connection List	Enter the maximum number of devices displayed when connecting to a device based on a wildcard search and multiple matching devices are found. The default is 20. If more devices can be returned, you are prompted to restrict the wildcard expression.
Device Single Sign-0n	
Use Single Sign-on	If checked (the default), NCM automatically authenticates a user once, then logs them into devices for which they have modify device permissions. **Note**: When NCM is configured to use SecurID for external authentication, Single Sign-on functionality will not be enabled when connecting to the NCM proxy. You will need to authenticate again using your SecurID credentials because SecurID passcodes cannot be reused.

Field	Description/Action
Sign-On To Limited Access Mode When No Modify Device Permission	If checked, NCM automatically log users in to limited access mode (e.g. exec for IOS) even if they do not have modify device permissions.
Display Sign-on Banner	If checked (the default), NCM displays the sign-on banner when it logs into a device.
Use AAA Login for Single Sign-on	If checked, NCM uses the AAA login information. This option refers to the Use AAA Login for Proxy Interface section on the New/Edit User page.
Use NCM Login when AAA Login Fails	If checked (the default) and your AAA user name and password information fails, your NCM login information is used.
Telnet Client	
Telnet Client	Select one of the following options: • Use NCM' integrated telnet client (the default) • Use standard browser telnet:// URL to NCM' telnet proxy • Use standard browser telnet:// URL directly to the indicated device
Telnet Server (changing these setting restarts the Telnet/SHH server)	
Enable Telnet	If checked (the default), NCM acts as a Telnet server.
Telnet Server Port	Enter the port on which NCM accepts client connections. The default for Windows is 23. The default for Unix is 8023.
Max Telnet Connections	Enter the maximum Telnet client connections NCM accepts simultaneously. The default is 50.
SSH Server (changing these setting restarts the Telnet/SHH server)	
Enable SSH	If checked (the default), NCM acts as an SSH server.
SHH Server Port	Enter the port on which NCM accepts client connections. The default is 22.
Max SSH Connections	Enter the maximum SSH client connections NCM accepts simultaneously. The default is 50.
SSH Fallback Option	

Field	Description/Action
SSH Fallback Order	Select one of the following options to determine the order of SSH versions to try when connecting to a device. • SSH v2 then v1 (the default) • SSH v1 then v2

Be sure to click Save to save your changes.

Reporting

The Reporting page enables you to customize the Network Status Report for your organization. There are six reporting categories:

- Policy Rule Violations
- Software Compliance Violations
- Startup vs. Running Config Mismatch
- Device Access Failure
- Configuration Change
- Email Report

For each reporting category, you can set status indicators for individual devices (and for the device group) using a combination of risk level color codes and parameters that specify a threshold for the percentage of devices that are out of compliance at each tier. For example, a higher score might be assigned to the border routers group, which control external network access and remote offices, while LAN devices might remain at the default values.

Providing settings that best reflect the significance of each event in your network can help you identify problems and keep the network in compliance with all established policies practices.

The Reporting page also provides options for the format and content of email reports sent via a user-defined email notification task and for specifying the location where you want to save the reports. You can also set diagramming parameters. For information on Diagramming, refer to "Diagramming Page Fields" on page 588.

Note: The status (risk level) of a non-complying device determines the status of the group. For example, if you set the risk level for a single non-compliant device to yellow, and one device in a group is in violation, the device group will reflect status yellow when the threshold number of devices in violation is reached.

To view the Reporting page, on the menu bar under Admin, select Administrative Settings and click Reporting. The Reporting page opens.

Reporting Page Fields

Field	Description/Action
Policy Rule Violations	
Device Status Color	Select the color to display when a single device in a device group is in violation of a configuration policy rule. The options include: • Red (the default) • Yellow • Green
Category Status Color	Enter the threshold percentage of devices that have configuration policy violations for the following device status colors: • Yellow — The default 1%. • Red — The default is 2%.
Software Compliance Violations	
Device Status Color	Select the color to display when the software for a single device in a device group is out of compliance. The options include: • Red (the default) • Yellow • Green You can select a compliance level violation from the following list: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Category Status Color	Enter the threshold percentage of devices that have software compliance violations. The options include: • Yellow — The default 1%. • Red — The default is 2%.

Field	Description/Action
Startup vs. Running Config Mismatch	
Device Status Color	Select the color to display when the startup configuration of a single device in a device group does not match its running configuration. The options include: • Red • Yellow (the default) • Green
Category Status Color	Enter the threshold percentage of devices that have startup versus run mismathes. The options include: • Yellow — The default 1%. • Red — The default is 2%.
Device Access Failure	
Device Status Color	Select the color to display when a single device in a device group reports a device access failure. The options include: • Red • Yellow (the default) • Green
Category Status Color	Enter the threshold percentage of devices that have access failures. The options include: • Yellow — The default 1%. • Red — The default is 2%.
Configuration Change	
Device Status Color	Select the color to display when the configuration of a single device in a device group has changed. The options include: • Red • Yellow (the default) • Green

Field	Description/Action
Category Status Color	Enter the threshold percentage of devices that have configuration changes. The options include: • Yellow — The default 1%. • Red — The default is 2%.
Email Report	
Email Report Format	Select the email format you want to use when sending search results as an email report. Keep in mind that this does not apply to Network Status reports. Options include: • HTML mail (the default) • CSV file attachment • Plain text • HTML mail (without links)
Include Task Results in Email Reports	If checked, complete task details are included in email reports that contain the results of a task search in comma separated value (CSV) file format. Keep in mind that this does not apply to Network Status reports.
Email Links	Select the format of addresses for HTML links in an email report. Options include: • Hostname (if resolvable) • IP Address • Canonical Name (FQDN, if resolvable) (the default) • User Defined — Enter the user-defined server address to use in email links.
SingleView	

Field	Description/Action
Device Change Events to Track	Select the device change events to track. This setting determines the default set of events to display on the Single View page. Refer to "SingleView Page Fields" on page 529. Events include: • Device Configuration Change • Device Booted • Device Diagnostic Changed • Device Password Change • Module Added • Module Changed • Module Removed • Software Change • User Message
Diagnostics to Track	Select the diagnostics to track. This setting determines which Device Diagnostic Changed events are displayed if that event type is selected on the Single View page. Refer to "SingleView Page Fields" on page 529. Default diagnostics types include: • Hardware Information • Memory Troubleshooting • NCM Detect Device Boot • NCM Device File System • NCM Flash Storage Space • NCM Interfaces • NCM Module Status • NCM OSPF Neighbors • NCM Routing Table **Note**: For detailed information on diagnostics, refer to "View Menu Options" on page 229.

Diagramming

Field	Description/Action
Maximum Nodes	Enter the maximum number of nodes to display in the diagram. The default is 250 nodes. This value can be lowered if generating the diagram is causing "Out of Memory" errors. Diagrams that include a large number of nodes result in large images. Images are generated in memory in uncompressed form before being output in JPEG format. You can increase the value if you want to include more nodes in your diagram, but keep in mind that you could run out of memory.
Label Font Size	Enter the font point size for labels in the diagram. The default is 8. Increasing this value increases the size of the labels in relation to the size of the nodes, potentially making the labels more readable.
Maximum Layout Duration	Enter the maximum time for which the layout algorithm is to run. The default is 30 seconds. The layout algorithm will stop after this maximum amount of time. Keep in mind that an accurate diagram is still generated if this limit is reached. However, the diagram might not be as optimally laid-out as possible.
Diagram Compactness	Enter the amount of space shown between nodes, from 0 to 100. The default is 90. This value controls how spread out the diagram appears. Nodes on a less compact diagram are easier to read. While a more compact diagram uses less space, compact diagrams can be hard to read. Also keep in mind that compact diagrams can take slightly longer to run, since the layout tends to take longer.
Quality-Time Ratio	Enter the preferred layout ratio from 0 to 100. The default is 100. Higher values generate a cleaner looking diagram, but take longer to layout and use more CPU cycles.
Preferred Edge Length	Enter a preferred edge length value, from 0 to 100. The default is 100. In general, longer edges provide more space between nodes in the diagram, however the layout algorithm will override this setting as needed. Larger values will cause the diagram to be more spread out, making memory consumption higher. Higher values do make edges less likely to overlap nodes and labels, thereby making the diagram more readable.
Preferred Minimal Node Distance	Enter a preferred minimal node distance value, from 0 to 100. The default is 50. This value controls how close nodes without connections are spaced. Smaller values contribute to a more compact diagram.
Other	

Field	Description/Action
Use Excel CSV Format	If checked (the default), when exporting search results to a comma separated value (CSV) file, Microsoft Excel CSV format is used.
Save report to file location	Enter the path to the location on the NCM server where you want all report files to be saved. All reports are automatically saved to this location when the user selects the "Save this report to file" option when defining the Email Report task. The default location is *C:\<install directory>/addins*.

User Authentication

User authentication enables you to centralize the authentication of users in one place and eliminate the need to maintain multiple databases. The following user authentication options are available:

- Active Directory
- SecurID
- TACACS+
- RADIUS
- Server Automation System

Keep in mind that if external authentication fails, NCM attempts to fall-back to the local user credentials in the following cases:

- When the external authentication service is down or inaccessible.
- For static user accounts that have never successfully logged in via an external authentication method.
- For the built-in Admin user account.

User authentication also enables you to configure the following security policies for built-in users within NCM:

- Define a minimum password length
- Define password complexity rules
- Lock-out users after a configured number consecutive failed login attempts

To view the User Authentication page, on the menu bar under Admin, select Administrative Settings and click User Authentication. The User Authentication page opens. Refer to "User Authentication Page Fields" on page 109 for information.

Active Directory Authentication

If your organization uses Microsoft Active Directory, you can import both your groups and users into NCM. NCM maintains active contact with your Active Directory database, remaining current on who can and cannot log into applications.

Even when external user authorization is enabled, it is possible to login to NCM if network problems make the Active Directory server unreachable. If NCM cannot connect to the designated Active Directory server, users who have previously logged in to NCM can login to NCM using their NCM user password. You can setup a NCM password on the My Profile page. Refer to "My Profile Page Fields" on page 265 for information.

Make sure that no Active Directory user has the same username as the NCM System Administrator. The default System Administrator's username is "admin," but it can be changed. If there is a name conflict between the default administrator and another Active Directory user, it may prevent the default administrator from logging in to NCM.

If a user is created in NCM and deleted in Active Directory, that user can login to NCM again using his/her NCM password (not Active Directory password).

For information on setting up external authentication for Active Directory, refer to "Active Directory External Authentication Setup" on page 112.

SecurID Authentication

The RSA SecurID® solution is designed to protect your organization by helping to ensure that only authorized users are granted access to networked resources. In general, SecurID is a two part authentication scheme, requiring a password/PIN, along with a token. The token changes every 60 seconds. Refer to "Adding SecurID Software Tokens" on page 613 for information.

TACACS+ Authentication

Cisco IOS software currently supports several versions of the Terminal Access Controller Access Control System (TACACS) security protocol, including TACACS+. TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes.

Using your TACACS+ server (typically CiscoSecure ACS) to authenticate users provides the following benefits:

- NCM users need only remember a single username and password
- NCM user administration can be centralized
- TACACS+ password restrictions can be easily enforced

Using your TACACS+ server to authenticate users into NCM enables you to:

- Configure NCM to use a TACACS+ server to authenticate user logins (i.e., to verify that the user has entered a valid username/password pair).
- Support TACACS+ authentication for the Telnet/SSH Proxy.
- Assign individual users a fallback password in NCM.
- Identify TACACS+ users so their fallback password is only used when the TACACS+ server is inaccessible (but not if any user other that Admin has entered an invalid TACACS+ password).
- Configure multiple TACACS+ servers for fail-over purposes.

Keep in mind that NCM needs to be defined in TACACS+ as an authenticating device, similar to any other router, along with a specific username. This enables users to login to NCM and NCM to login to their network devices.

Note: TACACS+ is not used for authorization/permissions. This means that the user must be added manually to NCM and assigned proper permissions before they can be authenticated via TACACS+. Once a user is identified as a TACACS+ user in NCM, you cannot remove this designation.

RADIUS Authentication

RADIUS (Remote Authentication Dial-In User Service) enables:

- A network access server to operate as a RADIUS client. The RADIUS client is responsible for passing information to designated RADIUS servers and then acting on the returned responses.
- RADIUS servers to receive connection requests, authenticate users, and then return all necessary client configuration information for proper connection.

- RADIUS servers to act as a proxy client to other RADIUS servers or others authenticating servers.

Note: RADIUS is not used for authorization/permissions. This means that the user must be added manually to NCM and assigned proper permissions before they can be authenticated via RADIUS. Once a user is identified as a RADIUS user in NCM, you cannot remove this designation.

To enable TACAC+ or RADIUS authentication:

1. On the menu bar under Admin, select Administrative Settings and click Configuration Mgmt. The Configuration Mgmt page opens.
2. Click the User Authentication tab. The User Authentication page opens. Be sure to click Save when you are done.

User Authentication Page Fields

Field	Description/Action
User Password Security	
Minimum User Password Length	Enter the minimum number of characters a password must contain. Passwords of less than this number of characters are considered invalid.
User Password Must Contain Upper and Lower Case	If checked, users must choose passwords that contain both lower-case and upper-case alphabetic characters.
Additional User Password Restriction	Select one the following options: • No additional restrictions (the default) • Must contain at least one non-alphabetic digit or special character • Must contain both at least one digit and at least one special character
Maximum Consecutive Login Failures	Enter the maximum number of allowed consecutive user authentication failures, after which the user will be disabled. A value of 0 (zero) indicates that this check should be skipped. (**Note**: This setting applies only to built-in user authentication and not to external authentication methods.)

Field	Description/Action
External Authentication Type	
External Authentication Type	Select the type of external authentication you would like to use. Options include: • None (Local Auth) • Server Automation System • TACACS+ • RADIUS • SecurID • Active Directory If you select TACACS+ or RADIUS, it can be configured in the section below. If you select Active Directory, click the Active Directory Setup link. Refer to "Active Directory External Authentication Setup" on page 112 for information. SecurID has no additional external authentication options.
TACACS+ / RADIUS Authentication	
Primary TACACS+ or RADIUS Server	Enter the host name or IP address of the primary TACACS+ or RADIUS server.
Secondary TACACS+ or RADIUS Server	Enter the host name or IP address of the secondary TACACS+ or RADIUS server. This field is optional.
TACACS+ or RADIUS Secret	Enter the shared secret for the NCM host configured on the TACACS+ or RADIUS server. A TACACS+ or RADIUS secret is the key (password) that the TACACS+ or RADIUS client (NCM) uses to encrypt communications with the TACACS+ or RADIUS server. The client and server must agree on the secret so the server can decrypt the communications.
TACACS+ or RADIUS Authentication Method	Select one of the following authentication methods used to encrypt communications between NCM and the TACACS+ or RADIUS server: • PAD (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft Challenge Handshake Authentication Protocol)
Server Automation System Authentication	

Field	Description/Action
Twist Server	Enter the host name or IP address of the Twist server.
Twist Port Number	Enter the Twist port number (typically 1032) to connect to the Twist server.
Twist Username	Enter the Twist Username to use when locating connected servers.
Twist Password	Enter the Twist Password to use when locating connected servers.
OCC Server	Enter the OCC server's host name for linking to connected servers. As a result, you can jump from the NCM Server page to the OCC Server page. Refer to "Servers Page Fields" on page 241 for information.
Default User Group	Select the name of the user group to which you can add authenticated users from the drop-down menu.

Active Directory External Authentication Setup

To enable Active Directory external authentication:

1. On the menu bar under Admin, select Administrative Settings and click User Authentication. The Administrative Settings - User Authentication page opens.
2. Scroll down to the External Authentication Type field.
3. In the External Authentication Type field, select Active Directory and click Save.
4. Click the Active Directory Setup link. The Active Directory Setup Wizard opens. If you have previously setup Active Directory authentication, the following information is displayed:
    - Active Directory Authentication Status
    - Active Directory Authentication Server Host
    - Port number
    - Connection User Name
    - Connection user password
    - Search Base
    - If you using a secure connection

The following table guides you through the setup process.

Step	Action
1	At the Welcome to the Active Directory Setup Wizard page, click Next. Enter the following information and click Next: • Server Name — Enter the host name of the Active Directory server, i.e., the host name or IP address of the AD/domain controller. • Port — Enter the LDAP request port number. Keep in mind that all Windows 2000 AD Domain Controllers listen for LDAP requests on port 389. Use port 389 or port 636 (if you are using SSL) for a single domain configuration. However, in multi-domain AD environments, you should use port 3268 or port 3269 (if you are using SSL). • Connection Type — Select either Regular Connection (the default) or Secure Connection (SSL). Be sure to select Secure Connection when connecting to the directory server. (**Note**: If you enable this option and the certificate of your directory server/domain controller server is not signed by one of the recognized CAs, you must manually import the certificate to the server where NCM is running.) For detailed information on Active Directory SSL Configuration, refer to "Active Directory SSL Configuration" on page 114.
2	Enter the following information and click Next: • Connection User Name — Enter the connection user name. Keep in mind that to query user information from the AD server, NCM should bind to the AD server with a domain user account (DN). The DN can be in the Windows 2000 LDAP format or in Windows 2000 User Principal Name (UPN) format. The Windows 2000 UPN format is a short-hand notation that uniquely identifies the DN in the Active Directory tree. Both the user account and respective domain are included in the UPN. An example of a Windows 2000 UPN DN is *jsmith@cisco.com*. • Connection User Password — Enter the connection user password • Search Base — Enter the search base. The search base is the starting point in the LDAP directory for LDAP searches. Ideally, the search base should be set to the root domain of the entire AD forest. This enables NCM to query the entire Windows 2000 AD forest. If the search base is set at a particular OU level, only child objects of that particular OU can be queried. Similarly, if the search base is set at a particular domain level, only child objects of that particular domain can be queried. For this reason, the search base should be as general as possible.
3	Indicate which security groups can access NCM. You can use the Find option to locate user groups in Active Directory and click Next.

Step	Action
4	You can verify the External Authentication setup by entering the user name and passwords then click the Test Login button. Be sure to click the Save button to save the setup information. If there are no errors, the following message is displayed and the External Authentication Setup Summary page is updated: `Successfully updated External Authentication settings.`

Active Directory SSL Configuration

For Active Directory SSL configuration:

1. Install an Enterprise Certificate Authority on a Windows 2000 or Windows 2003 Server. All Domain Controllers in the forest will automatically enroll for and install the appropriate certificate.
2. Open the Default Domain Controller Policy using the Group Policy Editor.
3. Under Computer Configuration, click Windows Settings.
4. Click Security Settings, and then click Public Key Policies.
5. Click Automatic Certificate Request Settings.
6. Use the wizard to add a policy for Domain Controllers.

For more information, see the Microsoft Knowledge Base article Q247078.

For certificate importing:

1. Start the Certificate Authority management console (usually on the Active Directory server) by clicking Start → Programs → Administrative Tools → Certification Authority.
2. Under Certificate Authority Local, find the Certificate Authority that issues certificates for your domain controllers.
3. Right-click the Certificate Authority and select Properties.
4. On the General tab, click View Certificate.
5. Select the Details tab and Copy to file.
6. Using the wizard, export the certificate to a Base64 Encoded file.
7. Copy this file to the NCM server.

8. At a Windows command prompt, go to:
   `<install directory>_Root\jre\bin`
9. Enter: keytool -import -file PATH_TO_THE_CERT_FILE -alias ADSCert -keystore ..\lib\security\cacert.

   Replace the `PATH_TO_THE_CERT_FILE` with the absolute path of the file created in step 7.

Server Monitoring

Server monitoring enables you to check on the overall health of the NCM server. Alert notification and event logging are triggered when a error is discovered. All of the server monitors are pre-packaged and shipped with NCM.

In the event that a monitor receives an error, a NCM Monitor Error event is triggered and notification of the error is sent to the System Administrator. Keep in mind that the system will not continue to send Monitor Error events for that monitor when it is checked later and is still in an error state. Once a monitor is in an error state, and an event to that effect is triggered, the system will only send a Monitor Okay event if the state changes to okay.

Note: If the system is restarted and the error condition persists, a new Monitor Error event is triggered. If the database is inaccessible, the system will attempt to email that fact to the administrator.

The Server Monitoring page enables you to configure server monitors. You also have the option of enabling all or only specific server monitors. The results of the most recent monitor runs are stored in the Monitor log file and can be viewed in the System Status page. Refer to "Server Monitoring Page Fields" on page 117 for information on the System Status page.

Note: Only Administrators have permission to change monitoring tasks settings. All users can view monitoring results.

To view the Server Monitoring page, on the menu bar under Admin, select Administrative Settings and click Server Monitoring. The Server Monitoring page opens.

Server Monitoring Page Fields

Field	Description/Action
Server Monitoring	
Enable Server Monitoring	If checked (the default), server monitoring is enabled. Email notification in the event of an NCM error is generated. The most recent results are stored in the Monitor log file and can be viewed from the System Status page.
Delay on Startup Before Starting Monitoring	Enter the number of minutes to delay starting server monitoring after startup. The default is two minutes.
Delay Between Monitoring Runs	Enter the number of minutes to delay between monitoring runs. The default is 360 minutes.
Enable the ConfigMonitor	If checked, the Config monitor is enabled. This monitor checks that the installed .rcx files and other configuration files are okay. This monitor makes a backup of the initial installed .rcx files and keeps a backup of the latest error-free installed .rcx files.
Enable the DatabaseDataMonitor	If checked, the Database Data monitor is enabled. This monitor checks that all critical system components are in the database, for example that an admin user exists, that there is only one crypto key, that one paused or pending Inventory snapshot task exists, and so on. This monitor makes a backup of the crypto key and the admin email address (for use if the database server is down).
Enable the DatabaseMonitor	If checked, the Database monitor is enabled. This monitor checks for database connectivity, for example if there are invalid credentials or too many connections.
Enable the DiskMonitor	If checked, the Disk monitor is enabled. This monitor checks for low disk space conditions.
Enable the HTTPMonitor	If checked, the HTTP monitor is enabled. This monitor ensures that the NCM Web server is running correctly.
Enable the LDAPMonitor	If checked, the LDAP monitor is enabled. This monitor checks that the Active Directory server is available.

Field	Description/Action
Enable the LicenseMonitor	If checked, the LicenseMonitor is enabled. This monitor checks if the available licenses drop below the percentage of managed devices and/or if the next license to expire is within the number of days specified. Refer to the "Monitor Configuration" section below for more information.
Enable the MemoryMonitor	If checked, the Memory monitor is enabled. This monitor checks for low memory conditions.
Enable the RMIMonitor	If checked, the RMI monitor is enabled. This monitor checks that RMI access to the NCM EJBs is working. It ensures that some other EJB container (Java application server) has not grabbed the RMI port.
Enable the RunExternalTaskMonitor	If checked, the Run External Task monitor is enabled. This monitor ensures the NCM server can run an external .bat or .sh file.
Enable the SMTPMonitor	If checked, the SMTP monitor is enabled. This monitor makes a Telnet connection to Port 25 on the configured mail server, sends an SMTP *QUIT* command, and waits for the proper *221* response code.
Enable the SSHMonitor	If checked, the SSH monitor is enabled. This monitor tests the connection to the SSH server embedded in NCM.
Enable the SyslogMonitor	If checked, the Syslog monitor is enabled. This monitor sends a Syslog message to NCM and ensures that it is received by the NCM Management Engine.
Enable the TelnetMonitor	If checked, the Telnet monitor is enabled. This monitor checks that the Telnet server embedded in NCM is running correctly.
Enable the TFTPMonitor	If checked, the TFTP monitor is enabled. This monitor TFTPs a file with a timestamp to the local machine, and then checks the file system to verify it was written correctly.
Monitor Configuration	
Check the Inventory Snapshot in the DatabaseDataMonitor	If checked, the inventory snapshot in the Database Data monitor is checked.
Warning Threshold for Free Disk Space	Enter the threshold to trigger the free disk space warning message. The default is 20 MB.

Field	Description/Action
Error Threshold for Free Disk Space	Enter the threshold to trigger the free disk space error message. The default is 10 MB.
Drives To Monitor for Disk Space	Enter a drive in the right-hand box and then click Add Drive <<. To delete a drive, select the drive in the left-hand box and click Delete Drive.
Warning Threshold for Managed Devices Count	Enter a percentage of your total licenses. If the available licenses drop below this percentage, a warning is issued. Device count threshold defaults to 10%.
Warning Threshold for License Expiration	Enter a number of days. If the next license expires within the number of days specified, a warning is issued. The expiration date threshold defaults to 30 days.
Warning Threshold for Free RAM	Enter the threshold to trigger the Free RAM warning message. The default is 20 MB
Error Threshold for Free RAM	Enter the threshold to trigger the Free RAM error message. The default is 10 MB.
Delay for SSH Thread Check	Enter the delay for the SSH Thread check. The default is 15000 milliseconds.
Delay for TFTP File Check	Enter the delay for the TFTP file check. The default is 5000 milliseconds.
Delay for Syslog message to show up	Enter the delay for the Syslog message to be displayed. The default is 45000 milliseconds.

Be sure to click Save to save your changes.

Viewing Monitor Results

The System Status page displays the results of the most recent monitor runs. To view the System Status page, on the menu bar under Admin, click System Status. The System Status page opens.

System Status Page Fields

Field	Description/Action
Run All link	Run all of the listed monitors.
Configure Server Monitoring link	Opens the Configuration Management Page. Refer to "Configuration Mgmt Page Fields" on page 58 for information.
Monitor Name	Displays the monitor name. Each monitor can return a variety of messages about the subsystem it is monitoring. Refer to "Monitor Messages" on page 121.
Status	Displays the monitor status, including: • Okay • Warning • Error • Disabled
Last Checked	Displays the date and time the monitor was last run.
Result	Displays information about the results.
Actions	You can select the following options: • Run Now — Runs the monitor immediately. • View Details — Opens the Monitor Details page, where you can view details about the monitor, including a description of the monitor, the status, results, and additional diagnostic information. • Start/Stop Service — Opens the Start/Stop Services page. Refer to "Starting and Stopping Services" on page 127 for information.

Monitor Messages

Each monitor can return a variety of messages about the subsystem it is monitoring. This section details some of these messages and possible corrective actions.

Monitor	Description/Resolution
BaseServerMonitor	<threadname> is not running. — A thread necessary for proper functioning of NCM has failed for an unknown reason. You may have to restart the NCM management engine.
ConfigMonitor	• Missing file <filename>.rcx — One of NCM' required configuration files is missing. Contact Support for assistance. • Error getting required config from <filename>.rcx — One of NCM' configuration files has become corrupted. Contact Support for assistance. • Exception parsing rcx file: <filename> — One of NCM' configuration files has become corrupted. Contact Support for assistance.
DatabaseMonitor on MySQL	• Cannot connect to the MySQL server on <servername>:3306. — There is no MySQL server running at the location where NCM is trying to connect. You can either restart the MySQL service or verify that the NCM connection information is correct. • Communication link failure: java.io.IOException — The connection to the MySQL server has been lost. You may have to restart the NCM management engine or restart the MySQL service. • Access denied for user: <username> to database <database_name> — NCM is trying to connect to the wrong database or there is some permission problem with the existing database. Verify that the NCM connection information is correct. • Invalid authorization specification: Access denied for user: <username> (Using password: YES) — NCM is trying to connect using the wrong username or password. Reset the NCM database username and password to the correct values. • General error: Table NCM.RN_CRYPTO_KEY doesn't exist — NCM can connect to the database using the credentials given, but the database is either not a NCM database or is corrupt (as it is missing the RN_CRYPTO_KEY table). Verify that the NCM connection information is correct.

Monitor	Description/Resolution
DatabaseMonitor on Oracle	• Error establishing socket. Connection refused: connect — There is no Oracle server running at the location where NCM is trying to connect. You may have to restart the Oracle service or verify that the NCM connection information is correct. • Connection reset by peer: socket write error. — The connection to the Oracle server has been lost. You may have to restart the NCM management engine or restart Oracle. • ORA-12505 Connection refused, the specified SID (<database_name>) was not recognized by the Oracle server. — NCM is trying to connect to the wrong database name. Verify that the NCM connection information is correct. • ORA-01017: invalid username/password; logon denied — NCM is trying to connect using the wrong username or password. Reset the NCM database username and password to the correct values. • ORA-00942: table or view does not exist — NCM can connect to the database using the credentials given, but the database is either not a NCM database or is corrupt (as it is missing the RN_CRYPTO_KEY table). Verify that the NCM connection information is correct.
DatabaseMonitor on SQLServer	• Error establishing socket. — There is no SQLServer running at the location where NCM is trying to connect. Either restart the SQLServer service or verify that the NCM connection information is correct. • Connection reset by peer: socket write error — The connection to SQLServer has been lost. Either restart the NCM management engine or restart SQLServer. • Cannot open database requested in login <database_name>. Login fails. — NCM is trying to connect to the wrong database name or there is some permission problem with the existing database. Verify that the NCM connection information is correct. • Login failed for user <username>. — NCM is trying to connect using the wrong username or password. Reset the NCM database username and password to the correct values. • Invalid object name RN_CRYPTO_KEY. — NCM can connect to the database using the credentials given, but the database is either not a NCM database or is corrupt (as it is missing the RN_CRYPTO_KEY table). Verify that the NCM connection information is correct.

Monitor	Description/Resolution
DatabaseDataMonitor	• Could not find an administrative user. — NCM does not have an administrative user configured. Contact Support for assistance. • Multiple crypto keys exist. — NCM contains multiple crypto keys in its database. Contact Support for assistance. • Current key does not match saved key. — NCM is now using a different crypto key. Contact Support for assistance. • More than one crypto key. — NCM is now using a different crypto key. Contact Support for assistance. • Could not find an Inventory group snapshot. — NCM does not contain a task to collect configs from all of the devices in the system. Create a Snapshot task for the Inventory group. • Could not find a reporting task. — NCM does not contain a task to generate summary reports. Create a Generate Summary Reports task. • Could not find a pruner task. — NCM does not contain a task to prune old data from the database. Create a Prune Database task.
DiskMonitor	Disk/Filesystem <filesystem> has only <space> bytes free. Error threshold is <limit> bytes. — The NCM server is close to filling up a disk drive. Delete unnecessary files from the disk drive.
HTTPMonitor	Did not get NCM login page. — An application is running on the configured HTTP/HTTPS port, but it does not appear to be the NCM web server. Stop any other web servers (e.g. IIS) running on the NCM server and then restart the NCM management engine.

Monitor	Description/Resolution
LDAPMonitor	• ActiveDirectory is not in use. — This is an informational message that reveals the NCM server is not configured to use Active Directory. • Exception in LDAPMonitor: javax.naming. CommunicationException: <hostname>:389 — The host <hostname> does not exist. Correct the Server Name setting for external authentication. • Exception in LDAPMonitor: javax.naming. CommunicationException: <hostname>:389 — The host <hostname> exists but is not accepting connections on the LDAP port (389). Check that the Server Name setting is correct. If so, check that the LDAP server is running on that host. • Exception in LDAPMonitor: javax.naming.AuthenticationException — The Connection User Name or Connection User Password setting for external authentication is incorrect. Check that these settings are correct.
LicenseMonitor	Warnings such as "License about to expire" or "Device count exceeds the current threshold of available licenses" are displayed in the Results column. If no warnings are displayed, the number of available device licenses is displayed, for example, "3454 of 3600 device licenses remaining." Click the View Details link to view details about the license, such as used and free licenses, and the license expiration date. (**Note**: If multiple licenses are used, the expiration date is the date of the next license to expire.)
MemoryMonitor	<bytes> bytes free. — This is how much memory is available to the system. It is approaching an insufficient amount for proper system functioning when an Error condition occurs. Contact Support for assistance.
RMIMonitor	Could not connect to RMI port 1099. — Another application is using the port 1099 that NCM needs for its client and API to function properly. Stop the application that is using port 1099 and restart the NCM management engine. If this is not possible, contact Support for assistance.

Monitor	Description/Resolution
RunExternalTask Monitor	• CreateProcess: <path>\tc_test.bat error=5 — NCM does not have permissions to access the test script (and possible other scripts). Check the file system permissions for NCM' directories. • CreateProcess: <path>\tc_test.bat error=2 — NCM cannot find the test script. Contact Support for assistance. • Running <path>\tc_test.bat from directory <path> Got result code: 0 Got output: <text> — The test script is corrupted. Contact Support for assistance.
SMTPMonitor	• SMTP Server name is blank. — The SMTP Server name administrative setting in NCM is blank. Verify that a mailserver is set in the Administrative Settings page. • Can't open Telnet connection to <hostname> 25 — Either NCM cannot connect to <hostname> or the host is not receiving connections on the SMTP port (25). Verify that the correct mailserver is set in the Administrative Settings page. Verify that the NCM server can access port 25 on that server. • Timeout waiting Expected: 220 Received. — An application is running on port 25 on the configured mail server, but it does not appear to be an SMTP application since it is not responding with the proper SMTP codes. Verify that the correct mailserver is set in the Administrative Settings page.
SSHMonitor	Unknown problem connecting to SSH server. — The NCM SSH server is not working correctly. Make sure no other application is listening to the SSH port that NCM is using. Restart the NCM management engine.
SyslogMonitor	Test syslog message did not get processed. — NCM' built-in Syslog server is either not running or has some problem. Contact Support for assistance.
TelnetMonitor	• Can't open Telnet connection to <hostname> 25. — The NCM Telnet server is not working correctly. Restart the NCM management engine. If this does not correct the problem, contact Support for assistance. • Timeout waiting Expected: Cisco Login: Received. — An application is running on the configured Telnet port, but it does not appear to be the NCM Telnet server. Modify the NCM Telnet server listening port.

Monitor	Description/Resolution
TFTPMonitor	• Connection timed out to the TFTP server. — The TFTP server is either not running or not accepting connections. Restart the TFTP server. • Test TFTP file was written but could not be read successfully. Check TFTP path setting. — The TFTP file was successfully written to the TFTP server, but could not subsequently be read from the filesystem. Check that the TFTP path setting is correct in the NCM management engine. • Found checkpoint file but timestamp is out of date. — The most recent file write attempt failed, and the system found a previous checkpoint attempt. This means that the TFTP server worked at some point in the past but is not working now. Restart the TFTP server.

Starting and Stopping Services

These are the four primary functional units within NCM, including:

- Management Engine
- TFTP Server
- Syslog Server
- Cisco Connection Online (CCO)

Typically, you would only stop, start, or restart a service when working with Customer Support.

To start/stop services or reload drivers or content, on the menu bar under Admin, click Start/Stop Services. The Start/Stop Services page opens.

Note: When using the Web user interface to start and stop NCM services, you could lose the ability to navigate to the previous page. If you click the Back button, you see a page with the text: null. Click your browser's Back button instead.

Start/Stop Services Page Fields

Field	Description/Action
Management Engine	Select one of the following options: • Stop — Stops the Management Engine (also referred to as the NCM server). This is the main service within NCM. • Restart — Restarts the Management Engine.
TFTP Server	Select one of the following options: • Start — Starts the TFTP server. NCM uses this primarily to retrieve and deploy configurations. (**Note**: TFTP provides the best performance. If TFTP is not available, NCM uses Telnet or SSH to process configurations.) • Stop — Stops the TFTP server. • Restart — Restarts the TFTP server.

Field	Description/Action
Syslog Server	Select one of the following options: • Start — Starts the Syslog server. NCM could be your only Syslog server, or other Syslog servers may forward messages to NCM. NCM uses Syslog messages to detect real-time change events and attribute them to users. • Stop — Stops the Syslog server. • Restart — Restarts the Syslog server.
CCO	Select one of the following options: • Reload Drivers — Enables you to reload drivers not in the product. The Reload button does not discover drivers. • Reload Content — Content is a suite of NCM enhancements and extensions available from Cisco which do not require a product upgrade. For example, NCM supports content import of software compliance policies via the NCM Alert Center (CAC). As part of CAC, you can download software compliance policies to assist you in managing network integrity.

Enabling Logging

Before changing your logging level, it is recommended that you contact Customer Support. The software components are obscure at best and some generate a significant amount of data.

To enable logging, on the menu bar under Admin click Troubleshooting. The Troubleshooting page opens. Be sure to click Submit when finished.

Troubleshooting Page Fields

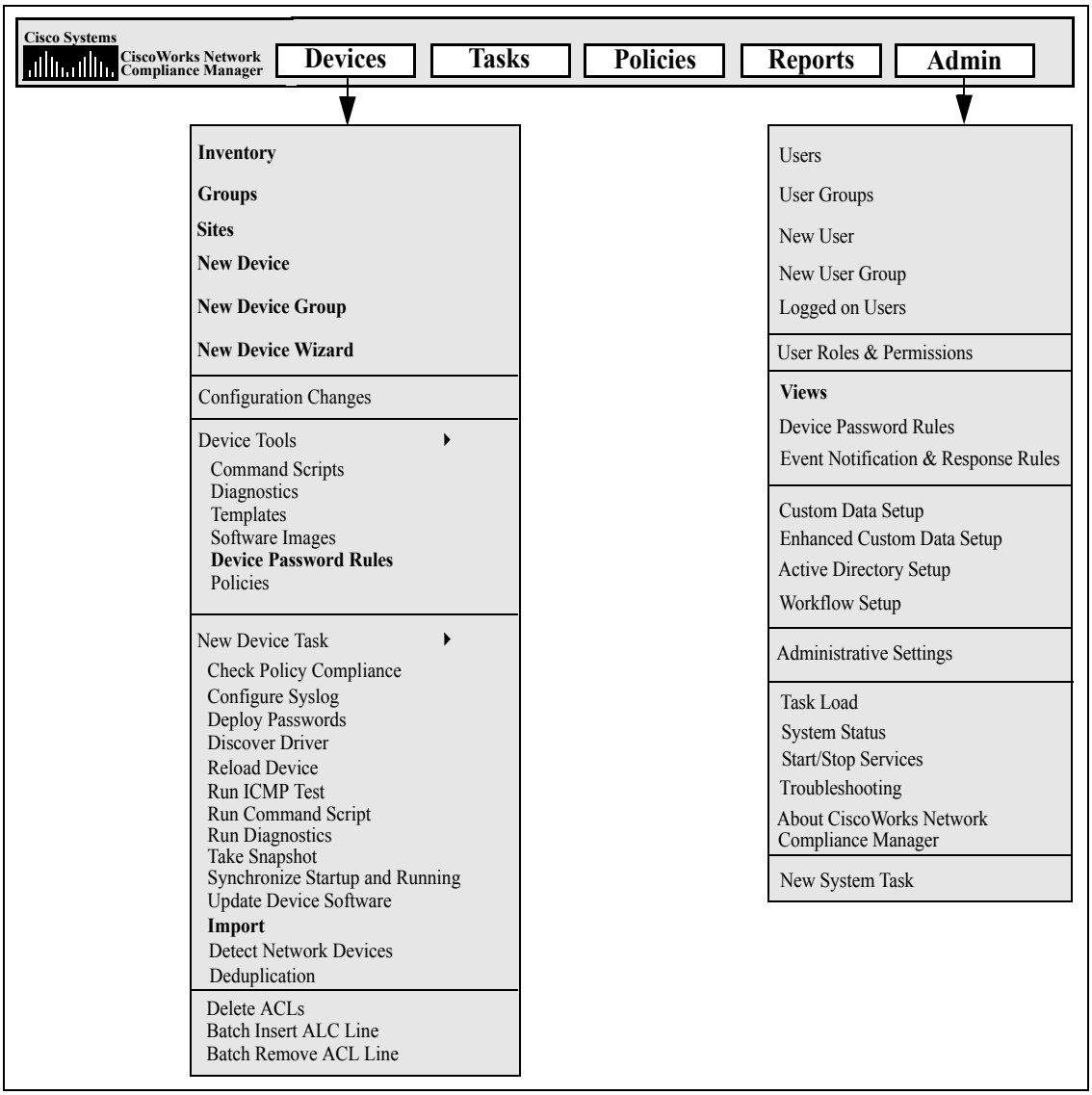
Field	Description/Action
Send Troubleshooting Information link	Opens the Send Troubleshooting Info page, where you can compose an email and send system information and logs to Customer Support. Refer to "Send Troubleshooting Page Fields" on page 23 for information.
Send Test Email to Admin User	Sends an email to the System Administrator.
Enable logging for	Select one or more components for which you want to enable logging. The current logging level follows each software component in parentheses. Example components include: • auth [Error] • changedectection [Error] • Config [Error] • deploy [Error] • user [Error]
and for	Enter any additional software components that are not on the list.

Field	Description/Action
at level < > and above	Select a logging level. Options include: • Fatal (fewest messages) • Error (default) • Warning • Info • Debug • Trace (most messages)
Keep < > days worth of logs	Enter how long you would like to keep log data. The default is two days. (**Note**: Log data can require large amounts of disk space.)
Reset	If checked, all logs are reset to the default logging level (Error) when you click the Submit button.

Chapter 3: Adding Devices and Device Groups

Use the following table to quickly locate information.

Navigating to Adding Devices



Getting Started

When you add a device, NCM:

1. Auto-detects and assigns the correct device driver to enable communication with the device. This process is called Driver Discovery.
2. Takes a snapshot of the device to collect the system information and initial configuration.
3. Runs the set of core diagnostics, such as "NCM Interfaces" and "NCM Routing Table". (Refer to "View Menu Options" on page 229 for a complete list of diagnostics.)

To successfully discover and snapshot a device, NCM requires full access to the device, and may also require SNMP read access to the device.

Keep in mind that console servers are used to provide access to devices that are not currently reachable on the IP network, and may only be reachable via a serial connection over the device's console port, for example devices with either a hardware failure, located in protected networks, or that do not run the IP protocol (IPX, ATM, and so on).

A bastion host is a host that has elevated privileges to access sections of a protected network that most other hosts cannot. This enables a management system to use a bastion host as a "hop" in managing elements on the protected network for which the bastion host has privileges. Typically, a bastion host is used for Internet and DMZ routers/switches, Extranet partners, and secured and/or private networks.

In both cases, NCM uses console servers and bastion hosts as a means of accessing a device (usually via the CLI) to perform its normal management functions when other access methods, for example Telnet, SSH, FTP/TFTP, and SNMP, are not available.

Note: If all access methods are enabled, NCM uses the following order to access devices: SSH, Telnet, SNMP, and Console. NCM also performs file transfers before screen scrapes, for example: SSH+SCP, SSH+TFTP, SSH+Screen Scrape, Telnet+SCP, Telnet+TFTP, Telnet+Screen Scrape, SNMP+TFTP, and Console+Screen Scrape).

Adding Devices

To add a new device, on the menu bar under Devices click New Device. The New Device page opens. Keep in mind that when you are editing a device's information, the Edit Device page is identical to the New Device page, except that the current device information is displayed. When you are finished, you can either click the Save Device button or the Save And Add Another button.

Note: The Detect Network Devices task enables you to locate devices on your network that you want to place under NCM management. Once you provide a range of IP addresses, NCM scans your network looking for devices. Refer to "Detect Network Devices Task Page Fields" on page 332 for information.

New Device Page Fields

Field	Description/Action
Use Wizard link	Opens the Add Device Wizard. (**Note**: The Add Device Wizard opens automatically when no devices are present.) Refer to "Using the New Device Wizard" on page 141 for information on using the New Device Wizard.
IP Address (or DNS name)	Enter the device's IP address or DNS host name.
Host Name	Enter the device's host name, if applicable.
Site	Select a Site from the drop-down menu. (**Note**: This field is only displayed if you have configured one or more Sites.) In general, a Site is a grouping of devices with unique IP addresses. Multiple Sites can be managed by a single NCM Core. A NCM Core in an installation of a NCM server, comprised of a single Management Engine, associated services, and a single database. **Note**:If a View applies to a Device/Device Group, there could be additional drop-down menus for each View. (Refer to "Segmenting Devices and Users" on page 163 for information on Views.)
Belongs to Groups	Displays the group(s) to which the device will be a member. Use Ctrl+click to select/deselect a group, or Shift+click to select a range of groups. Keep in mind that only device groups for which you have modify device permission are listed.
Change Detection & Polling	Select one of the following options: • Enabled — When checked (the default), NCM polls the device for changes as part of the regular polling task and when NCM detects change events. • Polling Only — When checked, NCM only polls the device for changes as part of the regular polling task. • Disabled — When checked, NCM ignores change events related to the device. In addition, NCM does not check the device for changes as part of the regular polling task. It a good idea to select this option during routine maintenance to exclude this device from the regular polling task.

Field	Description/Action
Management Status	Select one of the following options: • Active — When checked (the default), NCM records changes to the device. • Inactive — When checked, NCM does not record changes to the device. It is a good idea to select this options if the device is not supported or is not in active use. Making devices inactive reduces network traffic and frees resources.
Device Driver	Select one of the following options: • Auto Discover Driver — When checked (the default), NCM queries the device using SNMP or Telnet and assigns the most appropriate device driver. (**Note**: If you are editing an existing device, the option changes to Re-discover Driver.) • Specify Driver — When checked, either the driver that is currently assigned to the device is displayed, or you can select from the list of available drivers from the drop-down menu.
Comments	Enter comments about the device.
Password Information	
Use network-wide password rules	If checked (the default), NCM uses a network-wide device password rule that applies to a device. Using network-wide password rules is a highly scalable method for setting device credentials. **Note**: For large networks where groups of devices share the same credentials, use Device Password Rules. This enables you to consolidate device credentials in one place for easy manageability. Refer to "Creating Device Password Rules" on page 145 for information on creating Device Password Rules.

Field	Description/Action
Use device-specific password information	If checked, NCM uses authentication credentials that are specific to the device. Enter the following information to implement device-specific password rules. • Username — Enter the username that is used to access the device, if needed. If your devices are configured to use a AAA solution, such as TACACS+ or RADIUS, create a AAA user account and use those AAA credentials as the device credentials. • Password — Enter the password that NCM uses to access the device. • Confirm Password — Enter the password again. • Enable Password — Enter the enable password that NCM needs to access privileged mode. Most configuration changes require the enable password. (**Note**: Some devices may not require a password to access the privileged mode, for example Nortel ASN/ARN. Some devices can be configured to disable the password for the privileged mode. Please check with your network administrator for site specific configurations.) • Confirm Enable Password — Enter the enable password again. • SNMP Read-Only Community String — Enter the SNMP password that NCM uses to Read SNMP values. • SNMP Read/Write Community String — Enter the SNMP password that NCM uses to modify Read/Write SNMP values.
Show Device Access Settings (device-specific settings) Link	
Device Access Settings	NCM is designed to work with most networks and network devices. However, unique device configurations can affect NCM' ability to manage certain devices. Device access settings enable you to tailor NCM to adapt to your network configuration. Device access settings are tied to device password information. The device-specific settings you enter are applied only if you choose to use device-specific passwords. Network-wide device settings can be added to your password rules. Refer to "TACACS+ Authentication" on page 107 for information on TACACS+ authentication. Refer to "Logging In Using SecurID" on page 614 for information on using SecurID. Note: For detailed information on how to use device access settings, click the "How To Use Device Access Settings" link. The access.variables help file opens in a new browser window.
NAT Information	

Field	Description/Action
NAT IP Address	Enter the internally configured IP address of the device if it is different than the primary IP address NCM uses to access the device. (**Note**: If you are using NAT, be sure to enter the IP address that NCM should use to access the device in the Device IP box at the top of the page.)
TFTP Server IP Address	Enter the NAT'd IP address of the NCM server local to the device.
Connection Information	
Connection Method	NCM can communicate with your network devices using any combination of the following protocols. Select one or more protocols that you want to use. NCM chooses the most efficient protocol available at any given time from those you select. • SNMP • RLogin • Telnet • SSH (You can select either SSH1 or SSH2 (the default), SSH1 Only, or SSH2 only.) • Console Server (via Telnet) check box — In addition to the standard network connections, NCM can connect to a device through a console server. Also, if the standard connections fail, the Telnet/SSH Proxy automatically fails-over to the console settings when connecting users to devices. If checked, enter the IP Address or Host Name of the console server, along with the port number.
Transfer Protocol	Select one or more of the following transfer protocols: • SCP • FTP • TFTP
Bastion Host	If the "Use a Unix or Linux Bastion Host for Telnet & SSH access" check box is checked, enter the: • IP address or hostname of the bastion host. • Username (typically root) used to access the bastion host. • Password used to access the bastion host. • Password again for confirmation.

Field	Description/Action
Syslog Configuration	
Configure Syslog on Device for Configuration Change Detection	If checked (the default), and if either by driver discovery or you assigned a driver to each device, NCM takes the following steps for each device: 1. Takes a snapshot of the configuration. 2. Updates the configuration to send Syslog messages to NCM. 3. Writes a comment in the configuration indicating that the device was auto-configured to enable change detection. 4. Takes a final snapshot. You can select one of the following options: • Set Device to Log to NCM Syslog Server — Checked by default if the Configure Syslog on Device for Configuration Change Detection check box is checked. • Device Logs to a Syslog Relay, Set the Correct Logging Level — Enter the host name or IP address of the relay host. If a relay host has been entered before, it appears here by default.
ACL Parsing	
	Select one of the following options: • Enabled — If enabled (the default), ACL data is stored for the device upon each snapshot. Keep in mind that ACLs are not loaded in until a snapshot is taken. • Disabled — If disabled, ACL data is not stored for the device upon each snapshot.

Additional Information

Keep in mind that NCM populates some of the following fields automatically from the device snapshot process. If you manually populate these fields, your data is overwritten each time the device is polled.

Device Description	Enter the description you want to use to identify the device.
Model	Enter the manufacturer's model number for the device.
Domain Name	Enter the domain to which the device belongs. This is detected if the Resolve FQDN Administration option is selected.
Serial Number	Enter the manufacturer's serial number for the device.

Field	Description/Action
Vendor	Enter the vendor of the device, for example Cisco or Nortel.
Asset Tag	Enter your company's asset tag number for the device.
Location	Enter the physical or logical location of the device in your network.
Hierarchy Layer	A hierarchy layer is a device attribute. You can set a device's hierarchy layer when adding or editing a device. As a result, when configuring a network diagram, you can select which hierarchy layers on which to filter. For example, you could select to diagram your entire network (Inventory) and then filter on "Core" to get only your Core devices—devices with a hierarchy layer set to Core. Refer to "Diagramming" on page 582 for information on diagramming your network. **Note**: The options provided below are default hierarchy layers. Refer to "Editing the appserver.rcx file" on page 592 for information on adding custom hierarchy layers.) Select a hierarchy layer from the drop-down menu. Options include: • Layer not yet set • Core • Distribution • Access • Edge

Using the New Device Wizard

To add devices using the New Device Wizard, on the menu bar under Devices, click New Device Wizard. The New Device Wizard opens.

New Device Wizard Page Fields

Step	Description/Action
Step 1: Create Device	Enter the following information: • Hostname or IP — Enter the host name or IP address of the device. • Comments — Enter any comments about the device. When you are finished, click either: • Next — Opens the Authenticate page. (See below) • Finish — If the device was successfully added, the Add Device Wizard Congratulations page opens. This page provides information on any discovery issues.
Step 2: Authenticate Device	Select one of the following options: • Use network-wide password rules — If checked (the default), NCM uses a network-wide device password rule that applies to the device. You can click the Create One link to create a network-wide password rule. Refer to "Creating Device Password Rules" on page 145. • Use device-specific password — If checked, enter the following information for the device: Username, Password, Enable Password (if applicable), SNMP Read Community String, and SNMP Write Community String. When you are finished, click either: • Back — You are returned to the Create Device step. • Next — Opens the Configure page. (See below) • Finish — If the device was successfully added, the Add Device Wizard Congratulations page opens. This page provides information on discovery issues.

Step	Description/Action
Step 3: Configure Device	NCM attempts to discover the vendor and model of the device. If successful, NCM retrieves and stores the device configuration. The device is then configured for change detection. If you do not want to configure the device for change detection, uncheck the Update Syslog Configuration on Device box. If the box is checked, select one of the following options: • Log to NCM' Syslog Server — Checked by default if the Update Syslog Configuration on Device box is checked. • Log to existing Syslog Relay Host — Enter the host name or IP address of the relay host. (**Note**: NCM will set the correct logging level for change detection.) Click Finish. If the device was successfully added, the Add Device Wizard Congratulations page opens. This page provides information on any discovery issues.

Importing Devices

There are several ways to import devices from a comma-separated value (CSV) file:

- Using device password rules (usually assigned to group) and a CSV file.
- Importing device data in one CSV file and device password information in another CSV file.

To import devices using CSV files, on the menu bar under Devices, select New Device Task and click Import Devices. The Import Task page opens. Refer to "Import Task Page Fields" on page 328.

NCM can be configured to regularly import devices from a CSV file. The first time you import devices, you will have to:

- Setup the Device Password Rules and have them applied to the Inventory group (all devices). Refer to "Creating Device Password Rules" on page 145.
- Configure the default connection method. Refer to "Device Access Page Fields" on page 69.
- Prepare the device import file (Device.csv). Refer to "Import Task Page Fields" on page 328.

Keep in mind you can edit the Device.csv file or load it into a program such as Excel.

Note: The Detect Network Devices task enables you to locate devices on your network that you want to place under NCM management. Once you provide a range of IP addresses, NCM scans your network looking for devices. Refer to "Detect Network Devices Task Page Fields" on page 332 for information.

Creating CSV Device and Password Data Files

In a CSV device data file (device.csv), the first row contains the NCM database column names for the data you are importing. The most commonly used column names are listed below. Note that column names are case-sensitive.

Column Name	Description/Action
primaryIPAddress	The primary IP address for the device. This is the only required field.
deviceGroupName	The name of the group that contains the device.
hostName	The host name of the device.
consoleIPAddress	The IP address of the console associated with the device.
accessMethods	The access methods for the device. accessMethods is constructed as follows: access_methods[+connect_methods[+console]], for example: • CLI:TFTP+ssh+console • CLI:FTP+ssh:telnet • SNMP:TFTP Keep in mind access_methods can be CLI, SNMP, TFTP, or FTP, and colon-delimited if more than one access method is supported. (**Note**: connect_methods only applies if CLI is supported, and can be SSH or Telnet, and colon-delimited if more than one method is supported.)
consolePort	The port number for the console. It specifies whether or not to use the console server for device access. (**Note**: Only Telnet is used to access console server).
assetTag	The asset tag string for this device.
managementStatus	Whether NCM actively manages the device. The number 0 sets the device to Active. The number 1 sets the device to Inactive.
comments	Any descriptive text for the device.
deviceCustom1	You can create up to six custom fields in the Devices section on the Custom Data page. Be sure to create the fields before you import data.

Keep in mind that NCM populates the following fields automatically from the device configuration. If you manually populate these fields when importing device data, your data is overwritten each time the device is polled.

- Host Name
- Serial Number
- Location
- Vendor
- Model
- Operating System

Note: Do not include column names unless you are populating them. An empty value overwrites existing data if the device already exists.

To import devices using groups and device password rules, make sure you have:

1. Defined groups for the devices you are importing. Refer to "To view detailed information about a device group:" on page 161.
2. Defined network-wide password rules for each group. Refer to "Creating Device Password Rules" on page 145.
3. Imported devices, including the group to which each device belongs. Refer to "Importing Devices" on page 143.
4. Discovered drivers for the imported devices. Refer to "Discovering Device Drivers" on page 193. Refer to the *Device Driver Reference* for information on driver names.

Creating Device Password Rules

Device password rules enable you to apply the same username, password, and SNMP community strings to groups of devices, IP address ranges, or host names.

When attempting to login to a device, NCM applies the applicable Device Password Rules list sequentially until the login succeeds, and then sets that rule as the device login. If the rule fails during a future login attempt, NCM tries the applicable rules again in sequence until it finds a new valid login.

To create Device Password Rules, on the menu bar under Devices select Device Tools and click Device Password Rules. The Device Password Rules page opens.

Device Password Rules Page Fields

Field	Description/Action
New Password Rule link	Opens the Device Password Rule page. You can use this page to create and edit device password rules. Refer to "Device Password Rule Page Fields" on page 147 for information.
Check Boxes	You can use the left-side check boxes to delete device password rules. Once you have selected the rules, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all of the rules.
Change Date	Displays the date and time the rule was last changed.
Rule Name	Displays the name of the rule.
Type	Displays the type of rule, either: • IP Range • Host Name • Device Group
Devices	Displays the rule's host name, IP address, or group name.
Create By	Displays the login name of the person who modified the rule. NA means the name is not available.
Actions	You can select the following action for each rule: • Edit — Opens the Device Password Rule page, where you can edit the rule. Refer to "Device Password Rule Page Fields" on page 147 for information. (**Note:** Device Password Rules are listed in priority order. Use the arrows to move the rule up or down in the list.)

Note: The order of rules is significant. NCM applies rules in the order shown on the Device Password Rules page. If you notice a persistent performance problem when taking snapshots, consider reordering the rules to place the most commonly-used rules at the top. You should also restrict rules to fewer groups or smaller IP ranges.

Device Password Rule Page Fields

Field	Description/Action
Rule Definition	
Network-Wide Password Rule	If checked (the default), NCM uses a network-wide device password rule that applies all devices in the rule. Using a network-wide password rule is a highly scalable method for setting device credentials.
Rule Name	Enter the rule name.
Insert Before	Select an existing rule name from the drop-down menu that this rule is to be inserted above.
IP Range	If checked, enter the first and last IP addresses of the range to which the rule applies. Using wildcards (* or ?), you can apply this rule to a set of related devices.
Hostname	If checked, enter the host name for which this rule applies. Using wildcards (* or ?), you can apply this rule to a set of related devices.
Device Group	If checked, select the name of one or more groups to which this rule applies. To apply the rule to all devices, select Inventory.
Device-Specific Password Information	If checked, NCM uses authentication credentials that are specific to only one device. Enter the IP address of the device to which the rule applies.
Password Information	
Username	Enter the username that NCM uses to access the device. If your devices are configured to use a AAA solution, such as TACACS+, create a AAA user account for NCM and use those AAA credentials as the device credentials.
Password	Enter the password that NCM uses to access the device.
Confirm Password	Enter the password again

Field	Description/Action
Enable Password	Enter the enable password that NCM needs to access privileged mode. Most configuration changes require the enable password. (**Note**: Some devices may not require a password to access the privileged mode, for example Nortel ASN/ARN. Some devices can be configured to disable the password for the privileged mode. Please check with your network administrator for site specific configurations.)
Confirm Enable Password	Enter the enable password again
SNMP Read-Only Community String	Enter the SNMP read-only community string.
SNMP Read/Write Community String	Enter the SNMP read/write community string.
Show Device Access Settings	NCM is designed to work with most networks and network devices. However, unique device configurations can affect NCM' ability to manage certain devices. Device access settings enable you to tailor NCM to adapt to your network configuration. Device access settings are tied to device password information. The device-specific settings you enter are only applied if you choose to use device-specific password information Network-wide device settings can be added to your password rules. Examples include: • Exec mode prompt • Config mode prompt • Admin prompt For detailed information on how to use device access settings, click the “How To Use Device Access Settings” link.

Be sure to click the Save button when you are finished. The new rule is displayed in the Device Password Rules list.

Adding Device Groups

Creating a device group helps you categorize your devices in ways that make sense for your organization. Your devices are probably organized already, perhaps using one of the following schemes:

- Geography/physical location, such as Seattle and New York
- Business unit/department, such as Sales, Purchasing, and Manufacturing
- Role in the network architecture, such as core, edge, distribution, and access

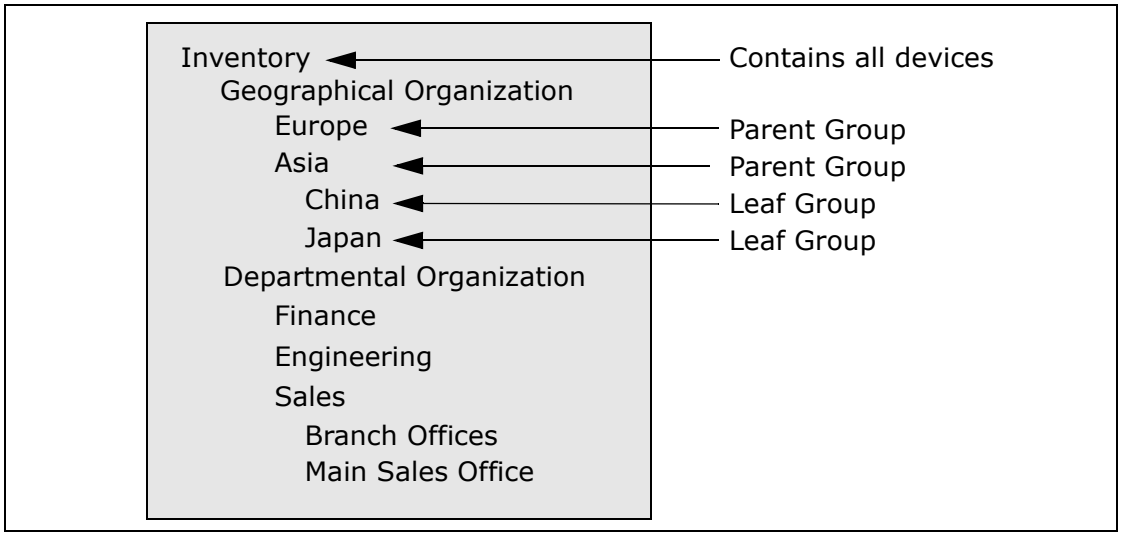
Initially, the Device Groups page includes one system group, the Inventory group. The Inventory group contains all devices added to NCM. However, any user-defined groups you create also appear on this page.

A device group hierarchy in NCM is made up of Parent groups and Leaf groups.

- A parent group can only have one Parent. Any previous association is overwritten if you add a Parent group as a Child group of a new Parent group. In addition, a Parent group can contain only device groups, not devices.
- A Leaf group can contain only devices, not other device groups.

Keep in mind that the default Inventory group is treated specially and is both a Parent and a Leaf group. It contains all devices in the system. Any Leaf groups that do not belong to a Parent group are included in the Inventory group.

Creating a device group hierarchy enables you to easily run tasks and reports against a set of device groups. An example device group hierarchy is shown below.



With this device group hierarchy, for example, you can run tasks and reports against the Japan devices or against the Asia devices (which would include all of the China and Japan devices).

New Group Page Fields

To add new device groups, on the menu bar under Devices click New Device Group. The New Group page opens.

Field	Description/Action
Group Name	Enter a group name
Description	Enter a description of the group.
Site	Select a Site from the drop-down menu, if applicable. The options depend on how many Views have been defined.
Owner	Select a name from the drop-down menu. Admin is the default.

Field	Description/Action
Sharing	Select either Public or Private. All users can see Public groups, while only the group owner and the System Administrator can see Private groups. **Note**: With private device groups, multiple users can setup their own device groups. When they log into NCM, they only see their device groups, as well all public device groups. As a result, users can customize NCM for ease-of-use and scalability.
Parent Device Group	The Inventory group appears in the drop-down menu, but you can select another group. Keep in mind that your selection is ignored if you make the group private. Private groups cannot be part of the group hierarchy.
Devices	Select one of the following options: • Use Device Selector to select a fixed device set (static group) — All current device groups are displayed in the left-hand box of the Device Selector, with the Inventory device group listed first. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • Use filters to define a dynamic device set (dynamic group) — Refer to "Dynamic Device Groups" on page 154 for information.

Adding Parent Groups

To add a new Parent group:

1. On the menu bar under Devices click Groups. The Device Group page opens. Refer to "Device Groups Page Fields" on page 159.
2. Click the New Parent Group link at the top of the page. The New Parent Group page opens.

Note: You must have the correct permissions to create Parent groups. Also, the device group hierarchy is shared and all Parent groups must be made public.

New Parent Group Page Fields

Field	Description/Action
Group Name	Enter the name of the Parent group.
Description	Enter a description of the Parent group, which usually differentiates this from other groups.
Sharing	Parent groups are always public.
Parent Device Group	Inventory is displayed by default in the drop-down menu.
Child Device Groups	• All device groups — Displays a list of all current device groups. Select the device groups you want to include as children of the Parent group and click Copy >>. Keep in mind that a group can only be a child of one parent group. If the group you are adding already belongs to a parent group, the group will be removed from the former parent group. • Children of this group — Displays a list of device groups that are assigned to the Parent group as children. Select the Child groups you want to remove from this Parent group and click << Remove.

When you are finished, click the Save button. The New Parent Group opens.

Parent Group Page Fields

Field	Description/Action
Groups link	Opens the Device Groups page, where you can view all of the device groups. Refer to "Device Groups Page Fields" on page 159 for information.
New Group link	Opens the New Device Group page. Refer to "Adding Device Groups" on page 149 for information.
New Parent Group link	Opens the Add Parent Group page. Refer to "New Parent Group Page Fields" on page 152 for information.
Group Name	Displays the user-defined name of the device group. Clicking a group name opens the Device Group Details page. Refer to "Device Group Details Page Fields" on page 161 for information.
Description	Displays a description of the group, which usually differentiates this from other groups.
Number of devices	Displays the number of devices in the group.
Owner	Displays the user name that created the device group.
Sharing	Displays whether the group is Public or Private. All users can see Public groups, while only the group owner and the System Administrator can see Private groups.
Actions	You can select the following options: • Edit — Opens the Edit Group page, where you can change the name and comments for a user-defined group. You can also add and delete devices from the group. Refer to "Edit Group Page Fields" on page 190 for information. • Delete — Permanently deletes a group. • Make Public/Private — Toggles a device group between Public and Private modes.

Dynamic Device Groups

A dynamic device group is very similar to a static device group, except the devices included in a dynamic device group are not fixed. Rather, the system determines which devices are included in a dynamic device group by doing a query using predefined criteria associated with the group.

As with static device groups, dynamic device groups are displayed in all group lists, including Run Device tasks pages, Search pages, Diagrams, Device Software reports, and so on. The following table outlines the differences between static and dynamic device groups.

Static Device Groups	Dynamic Device Groups
Created by selecting devices. Refer to "New Group Page Fields" on page 150.	Created by defining a set of search criteria and/or rules. The maximum search criteria is 10. The steps for creating a dynamic device group are listed below.
Devices remain fixed unless manually added or removed.	Devices can change when network and/or device configuration events occur.
Can manually remove devices from the group.	Cannot manually remove devices from the group.

Note: A dynamic group can only be a child group in the group hierarchy. In addition, dynamic groups do not appear on the Edit Device page or the Import Device Task page, where you specify to which group devices belong.

Creating Dynamic Device Groups

There are two ways to create a dynamic device group:

- Using the Device Search Results page
- Using the New Group page

To create a dynamic group using the Device Search page:

1. On the menu bar under Reports, select Search For and click Devices. The Search For Device page opens.
2. Enter search criteria. For example, check the Device Vendor field and enter Cisco.
3. Click the Search button. The Device Search Results page opens displaying all of your Cisco devices.
4. Scroll down to the bottom of the page until you see the yellow "Search Criteria" section.
5. Enter the name of the dynamic group, check the "Create as a dynamic group" option, and click the Create Group button.
6. The "Successfully created new device group: <name>" message is displayed at the top of the Device Search Results page.

To create a dynamic group using the New Group Page:

1. On the menu bar under Devices, click New Device Group. The New Group page opens.
2. Enter the name of the dynamic group in the Group Name field.
3. Complete the Description, Owner, Sharing, and Private Device fields as needed. Refer to "New Group Page Fields" on page 150 for details on these fields.
4. Scroll down to the Devices field.
5. Click the "Use filters to define a dynamic device set (dynamic group)" option. The display changes to enable you:
   - Configure searches using one or more search criteria, for example Device IP, Domain Name, Policy Compliance, and so on. (**Note**: You must specify at least one search filter and/or rule to create a dynamic device group.)
   - Use Boolean expressions (and/or) to filter searches, if necessary.
   - Limit a search by device group. Using this option, you can create a dynamic group based on other groups.
6. Once you have defined your dynamic device group, click the Save button. The new dynamic device group is displayed.

To change a dynamic device group to a static device group, open the Edit Group page and scroll down to the Device field. Click the "Use Device Selector to select a fixed device set (static group)" option. When you change a dynamic device group to a static device group, the current device set will become the members of the new static device group.

Calculating Dynamic Device Groups

A dynamic device group's members are calculated when:

- You first configure the dynamic device group.
- You click the "Update device list" link on the Dynamic Device Group page.
- A background process periodically re-calculates all of the dynamic device groups.
- Pre-defined device change events occur.

Refer to "Server" on page 79 for information on the Dynamic Group Auto-Recalculation and Event Driven Recalculation parameters.

Device Selector

The Device Selector enables you to easily navigate group trees to select devices and device groups for a variety of applications.

By default, all current device groups are displayed in the left-hand box of the Device Selector, with the Inventory device group listed first. The All Groups option is displayed in the shaded area above the list of device groups. To view a list of all devices in a device group, double click the name of the device group in the Group Name column.

Note: If you are modifying a device group, the Device Selector displays the current devices in the group in the Added Devices box.

The initial Device Selector view is set to All Groups by default, except when modifying an existing list of devices. When the list of devices for a group exceeds 100 in the left-hand box, the devices are displayed on multiple pages. The number of pages is indicated below the left-hand box. The maximum list size is 10,000 devices. To reconfigure these parameters, refer to "User Interface" on page 89.

If you double click a parent device group, the list is updated to display the device groups that belong to that parent device group. If you double click a child device group, the list is updated to display the devices belonging to that child device group. As a result, you can easily navigate each group tree. To return to the previous level, click the All Groups option or the currently displayed device group name that appears in the shaded area above the device list.

The following table lists the Device Selector options.

Option	Result
Select All	Selects all of the device groups and/or devices. Once highlighted, you can move the items to the Added Devices box using the right arrows button [>>>] or remove them from the Added Devices box using the left arrows button [<<<]. (**Note**: You can use the Shift or Ctrl keys for multi-selection.) If you want to add only specific device groups or devices to the Added Devices box, simply click the item to highlight it and then click the right arrows button [>>>]. Keep in mind that the right arrows button [>>>] is grayed-out if the group is not allowed.

Option	Result
Select None	De-selects the highlighted device groups and/or devices.
Sorting	You can sort the device list by clicking the Host Name or IP Address column titles.
Limit by name or IP	Enables you to narrow your search for a specific device group or device by entering a portion of the group name, host name, or IP address.

Viewing Device Groups

Initially, the Device Groups page includes one system group: the Inventory group. The Inventory group contains all devices. However, any user-defined groups you create also appear on this page.

To view device groups, on the menu bar under Devices, click Groups. The Device Groups page opens. Keep in mind that Public device groups are visible to all users. Private device groups are visible only to the group owner and NCM administrators.

Device Groups Page Fields

Field	Description/Action
New Group link	Opens the New Group page, where you can create a new device group. Refer to "Adding Device Groups" on page 149 for information.
New Parent Group link	Opens the New Parent Group page, where you can add a new Parent group. Refer to "New Parent Group Page Fields" on page 152 for information.
Group Name	Displays the user-defined name of the device group. Parent groups are not indented, unless they are also children of other Parent groups. Groups that belong to a Parent group are indented beneath their parent. Clicking a group name opens the Device Group page, where you can view detailed information about the device group. Refer to "Device Group Details Page Fields" on page 161 for information.
Description	Displays a description of the group.
Number of devices	Displays the number of devices in the group.
Owner	Displays the user name that created the device group.
Sharing	Displays whether the group is Public or Private. All users can see Public device groups, while only the group owner and the NCM Administrator can see Private device groups.

Field	Description/Action
Actions	The Actions field for the Inventory group is empty until you select a group name. User-defined groups display the following actions: • Edit — Opens the Edit Group page, where you can change the name and comments for a user-defined group. You can also add and delete devices from the group. Refer to "Edit Group Page Fields" on page 190 for information. • Delete — Permanently deletes the group. • Make Public/Private — Toggles a device group between Public and Private modes.

To view detailed information about a device group:

1. On the menu bar under Devices, click Groups. The Device Groups page opens.
2. Click the group name on which to view detailed information. The Device Group Details page opens.

Device Group Details Page Fields

Field	Description/Action
Groups link	Opens the Device Groups page, where you can view all of the devices. groups. Refer to "Device Groups Page Fields" on page 159 for information.
New Device link	Opens the New Device page where you can add a new device. Refer to "Adding Devices" on page 134 for information.
New Group link	Opens the New Group page, where you can add a new group. Refer to "Adding Device Groups" on page 149 for information.
New Parent Group link	Opens the New Parent Group page, where you can add a new Parent group. Refer to "Adding Parent Groups" on page 152 for information.
Edit Group link	Opens the Edit Group page, where you can edit the device group. Refer to "Edit Group Page Fields" on page 190 for information.
Current Working Group	Shows the current working group in the drop-down menu. You can select a different group from the drop-down menu.
List Active Devices Only check box	If checked, the list of devices is restricted to actively managing devices.
Run Task on this Group	You can select a task from the drop-down menu to run on this group. Refer to "What Are Tasks?" on page 278 for information on running tasks.

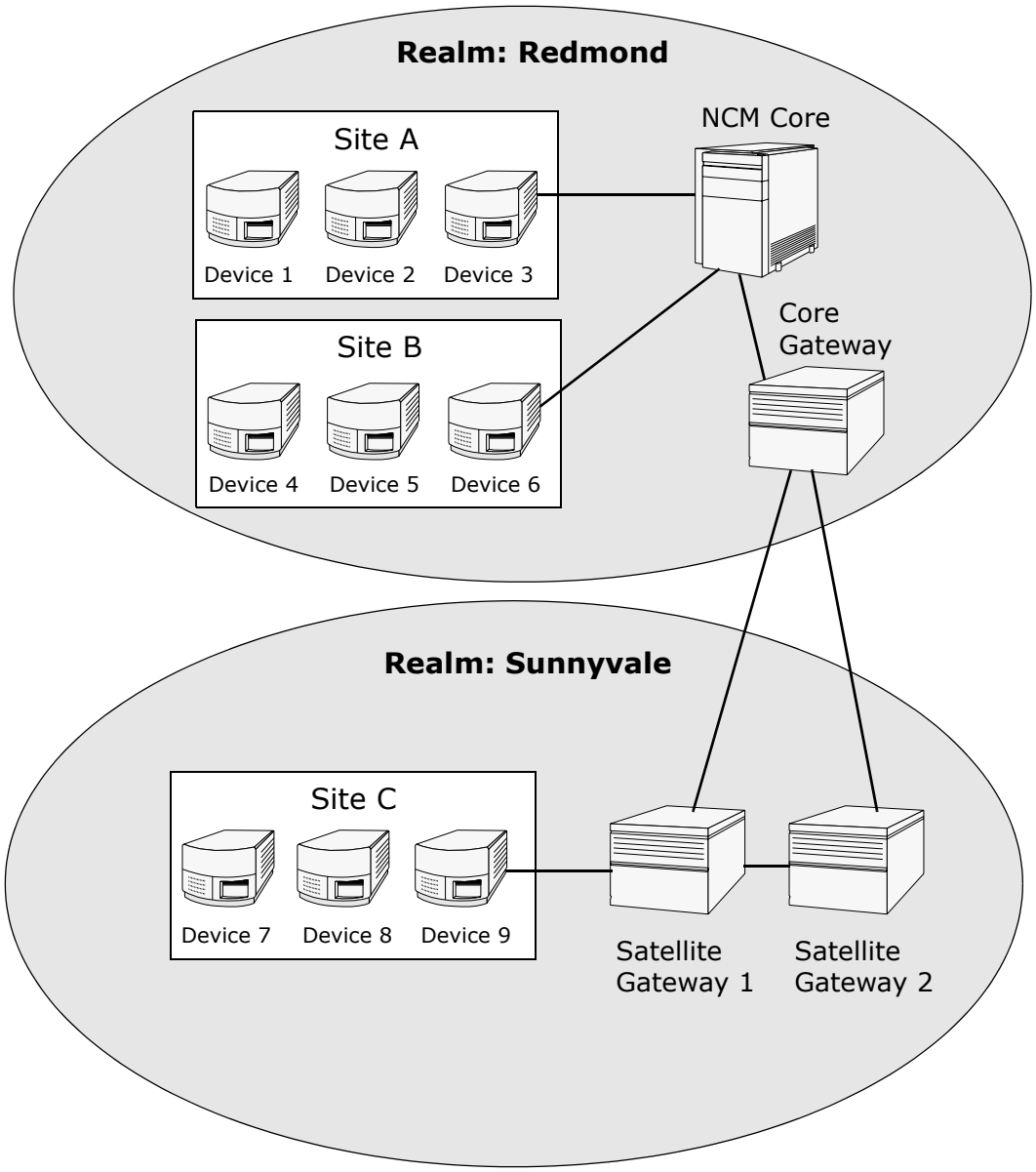
Field	Description/Action
Check Boxes	You can use the left-side check boxes to manage devices. Once you have selected the devices, click the Actions drop-down menu. Options include: • Activate — Instructs NCM to manage the selected devices. • Deactivate — Instructs NCM not to manage the selected devices. • Batch Edit Device — Opens the Batch Edit Device page, where you can assign a driver and set the connection methods for all the checked devices at once. Refer to "Batch Edit Device Page Fields" on page 191 for information. • Delete — Deletes the selected devices. • Select a task to run against the device group. The adjacent Select drop-down menu enables you to select or deselect all of the devices.
Host Name	Displays the host name of the device. Clicking a host name opens the Device Detail page, where you can view information about the device and its configuration history.
Device IP	Displays the IP address of the device. Devices in red failed the last snapshot attempt. Inactive devices are marked with an icon beside the IP address. Clicking an IP address opens the Device Detail page, where you can view information about the device and its configuration history.
Vendor	Displays the name of the device manufacturer.
Model	Displays the model designation of the device.
Last Changed Time	Displays the date and time the device's configuration was last changed.
Actions	You can select the following actions: • Edit Device — Opens the Edit Device page, where you can edit the information for this device. • Telnet — Opens a Telnet window. • SSH — Opens an SSH Window. • View Config — Opens the Device Configuration Details page, where you can view the latest configuration and add comments.

Segmenting Devices and Users

NCM provides the ability to manage overlapping IP networks and partition both devces (and device groups) and users (and user groups). The following terms are used in this section.

- **NCM Core** — A single NCM Management Engine, associated services (Syslog and TFTP), and a single database. A NCM Core can manage multiple Sites (set of devices). Multiple NCM Cores can be connected in a Distributed System configuration. Refer to the *NCM High Availability Distributed System on Oracle User's Guide* for detailed information on installing and configuring a Distributed System.
- **View** — A set of one or more partitions that separates objects in NCM into specific partitions within the View. Currently, the maximum number of Views you can configure is three.
- **Device View** — A View that applies to devices and device groups.
- **User View** — A View that applies to users and user groups.
- **Partition** — A set of objects that is part of a View. An object can only be in one partition within a View. The set of all partitions in a View *partitions* the objects. If there is more than one View, each object is in one (and only one) partition within each View that applies to the object.
- **Site** — A device partition. Each Site belongs to only one Realm and one NCM Core. As a result, a Site is managed by one (and only one) NCM Core. Each device belongs to one and only one Site. Sites can be used in conjunction with a Permissions model, group hierarchy, distribution of devices across NCM Cores, and network diagramming.
- **Realm** — A network segment. In general, a Realm is identified by a set of unique IP addresses. For example, a Realm cannot contain two devices numbered as 10.255.111.128. Instead, the devices must be broken out into separate Realms. A Site is not required to be in the same Realm as its managing NCM Core. Keep in mind that a Realm is a large area that can include many Sites. While a Realm does not have to include any NCM Cores, typically a NCM Core manages devices in its local Realm. A NCM Core can manage devices in remote Realms via the Gateway Mesh. The Gateway Mesh is used to proxy IP traffic between Realms. Refer to the *NCM Gateway User's Guide* for detailed information.

The following figure illustrates the various components of a multi-site configuration. Keep in mind that Realms and Sites cannot overlap and a device cannot be in more than one Realm or Site, as shown in the figure. However, there can be multiple Sites and NCM Cores in a Realm. There can also be multiple Gateways in a Realm.



Overlapping IP Networks

Every Site must have a managing NCM Core. However as shown in the previous figure, the managing NCM Core does not have to be in the same Realm as the Site it is managing.

When accessing devices, if the NCM Core is in the same Realm, for example Device 3, NCM directly connects to the device to manage it. If the NCM Core is in a different Realm than a device it is managing, for example Device 9, NCM connects to Satellite Gateway 1 in its Realm, which then communicates through the other Gateways to Device 9.

The collection of Gateways is called a *Gateway Mesh*. A Gateway in the same Realm as a NCM Core is called a *Core Gateway*. A Gateway in a Realm without a NCM Core is called a *Satellite Gateway*. The Gateway Mesh enables a NCM Core to manage devices in different Realms. Currently, only Telnet/SSH is used for remote access. (Refer to "Device Access Page Fields" on page 69 for information on configuring the Gateway Mesh.)

Keep in mind that installing and configuring an Cisco Gateway is only required if you want to manage devices and networks that use duplicate and/or overlapping IP addresses. The Cisco Gateway is a standalone product and not bundled with NCM. If you need to install and configure an Cisco Gateway to use with NCM, refer to the *NCM Gateway User's Guide*.

You can configure multiple:

- Realms — Enables you to use overlapping IP addresses. That is, more than one device with the same IP address.
- Sites (in the same Realm) — Enables you to restrict view access for users to devices that are in the same Realm. Refer to "Restricted Device Views" on page 166 for information.
- Gateways (in the same Realm)— Enables you to improve up-time in the event that one Gateway fails.
- NCM Cores (in the same Realm) — Enables you to share access to device information in the NCM system. The NCM Distributed System on Oracle is a multimaster system where data from each NCM Core in a Gateway Mesh is accessible to all other NCM Cores. This allows for redundant data and failover in the event of a NCM Core crash. (Refer to the *NCM Distributed System on Oracle User's Guide* for more information.)

NCM Gateway

The NCM Gateway enables a NCM Core to manage servers that are behind one or more NATed devices or firewalls. It does this by creating persistent TCP tunnels between Gateway instances, much like SSH tunnels. Unlike SSH, however, the NCM Gateway supports tunneled HTTPS proxy CONNECTs. This enables any client that supports HTTPS proxy CONNECT, such as a Web browser, to use the NCM Gateway.

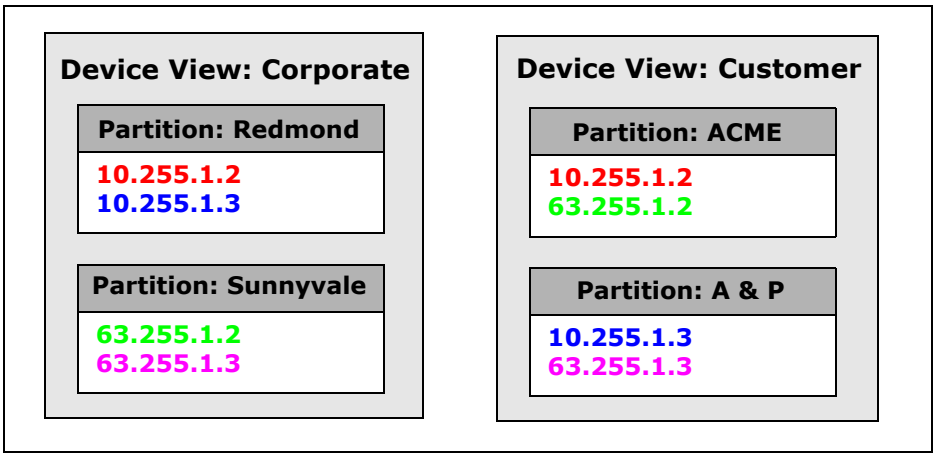
The NCM Gateway also supports tunneled TCP port forwarding, similar to SSH, as well as UDP port forwarding. In addition, the NCM Gateway provides bandwidth management. This is important when a tunnel is transmitting over a low-bandwidth link and you need to limit usage of the bandwidth to a fixed amount that is less than the maximum link speed.

For detailed information on configuring the Gateways, refer to the *NCM Gateway User's Guide*.

Restricted Device Views

NCM provides the ability to restrict which devices a user can see. As a result, you can segment access to device information in the NCM system. For example, if your organization has a three-tier hierarchy, including Corporate, Regional, Customer views, you can ensure that certain users can only view parts of the network for which they are authorized. Refer to "Adding User Roles" on page 261 for information on granting permissions.

The following figure illustrates the relationship between Device Views and Partitions. In this example, there are a total of four devices in NCM and two defined Device Views (Corporate and Customer). Keep in mind that the Device Views are independent of each other and all four devices are in one and only one Partition within each Device View.



In a multi-core NCM installation, when a task is run, NCM locates:

1. The device the task will run against.
2. The Site that the device is in.
3. The NCM Core that manages that Site. This is the NCM Core that executes the task.

Note: If the NCM Core and Site are in different Realms, the NCM Core must use the Gateway Mesh to communicate to the devices. For detailed information on the Gateway mesh, refer to the NCM *Gateway User's Guide*. The NCM Gateway is a standalone product and not bundled with NCM.

If you have View permission for one or more devices included in a Device View Partition, but no View permission for a second Device View, you do have implicit View permission for any devices for which you have View permission that are included in both Device Views. Using the above figure, if you have View permission in the Redmond Partition of the Corporate Device View, but you do not have View permission for any Partitions in the Customer Device View, you will be able to view 10.255.1.2 even though the device is in a Device Partition for which you do not have View permission. This is because you have View permission to it through the Redmond Partition.

For an example of how to segment devices, refer to "Editing Device Groups" on page 190.

Restricted User Views

NCM provides the ability to restrict which users can view other users. As a result, Views and Partitions can *partition* users and user groups in the NCM system. For example, if a Managed Service Provider is managing a large banking institution, the users working for the Manager Service Provider can be rendered invisible to the bank's users.

Note: Users will not be able to grant permissions to other users unless they have the permission to do so. Refer to "Adding User Roles" on page 261 for information on user permissions.

Views Page Fields

Sites and Partitions are always public groups. They can be placed within the device group hierarchy. If an object (i.e., Device, Device Group, User, or User Group) is added to one Site or Partition, it is automatically removed from the Site or Partition to which it previously belonged.

If a Site or Partition is deleted, all objects are automatically placed in the Default Site or Partition. This is done to ensure that any object appears in only one Site and one Partition for each of the defined Views. Any reference to an IP address without an explicit Site uses the default Site in the Site View. (Refer to "Segmenting Devices and Users" on page 163 for detailed information on Sites and Partitions.)

To open the Views page, on the menu bar under Admin click Views. The Views Page opens.

Field	Description/Action
New View Link	Opens the New View page, where you can create a new Device View or User View. **Note**: The maximum number of Views is three, including the default View labeled "Site". The Site View is needed by the system to connect to devices via the Gateway Mesh. Any reference to an IP address without an explicit Site uses the Site View.
Name	Displays the default Site View and any other Views that you have created.
Description	Provides a description of the View.

Field	Description/Action
Number of Partitions	Displays the number of partitions in the View.
Actions	You can select the following actions: • Edit — Opens the Edit View page. Refer to "Edit View Page Fields" on page 170 for information. • Delete — Enables you to delete a View. Keep in mind that you cannot delete the default Site View.

New View Page

To add a new View:

1. On the menu bar under Admin, click Views. The View page opens.
2. Click the New View link at the top of the page. The New View page opens.
3. Enter the View name and a description.
4. In the Applies to field, select if the View applies to "Devices & Device Groups" and/or "Users & User Groups." Keep in mind that you can select both options. As a result, a Partition can apply to both devices and users. If the View applies to users, on the Edit User page you have the option of setting the Partition in that View. If the View applies to devices, on the Edit Device page you have the option setting the Partition in that View.
5. Click the Save View button. The Views page opens displaying the current Views. Keep in mind there is one default View named *Site*. This View contains all of the discovered devices in your network. (Refer to "Segmenting Devices and Users" on page 163 for detailed information on Views.)

Edit View Page Fields

To edit an existing View:

1. On the menu bar under Admin, click Views. The Views page opens.
2. For the View you want to edit, click the Edit option in the Actions column. The Edit View page opens.

Field	Description/Action
Views Link	Opens the Views page. Refer to "Views Page Fields" on page 168 for information.
New <View Name> Link	Opens the New <View Name> page where you can add devices and/or users to the Site. Refer to "New Site Page Fields" on page 171 for information.
Description	Provides a description of the View.
Applies to	Indicates the type of objects (Devices & Device Groups or Users & User Groups) that applies to the View. Keep in mind that the View can contain both devices and users.

When editing the default Site View, the following fields are displayed:

- Core — In a Distributed System installation, this field is displayed. It specifies which NCM Core will be used to manage devices in this Site.
- Realm Name — If a Gateway Mesh has been configured in the NCM Administrative Settings under Device Access, this field is displayed. (Refer to "Device Access" on page 68 for information.) Select a Realm from the drop-down menu. This specifies what Realm the devices in this Site are in. If the NCM Core is not in the same Realm, NCM uses the Gateway Mesh to connect to the devices in this Site.

New Site Page Fields

To add a new Partition to a Site:

1. On the menu bar under Admin, click Views. The Views page opens.
2. In the Name column, click the View you want to edit. The Partition in <View> page opens.
3. In the Actions column, click the Edit option for the View you want to edit. The Edit <View> page opens. (Refer to "Segmenting Devices and Users" on page 163 for detailed information on Sites and Partitions.)

Field	Description/Action
Name	Enter the Site name.
Description	Enter a description of the new Site.
Core	In a distributed NCM installation, this specifies which NCM Core will be used to manage devices in this Site. **Note**: This option is not displayed if there is only one NCM Core. (Refer to *Multimaster Distributed System on Oracle User's Guide* for more information.)
Realm Name	Select a Realm from the drop-down menu. This specifies what Realm the devices and/or users in this Site are in. **Note**: This option is not displayed if there is only one Realm (i.e., no Gateway Mesh). If the NCM Core is not in the same Realm, NCM uses the Gateway Mesh to connect to the devices in this Site.
Devices	Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector.

Be sure to click the Save button when you are done.

Adding Devices to a Site

To add devices to a Site:

1. On the menu bar under Admin click Views. The Views page opens.
2. In the Name column, click the View you want to edit.
3. In the Site Name column, click the Site you want to edit. The Site page opens. This page is similar to the Inventory page, where you can view a list of the managed devices in the Site. However, there are two added links at the top of the page: Edit Group and Partitions. Clicking the Partitions link returns you to the Sites page. (Refer to "Inventory Page Fields" on page 217 for information.) **Note**: You can navigate directly to this page by clicking the Sites option under the Device menu option on the menu bar.
4. Click the Edit Group link to open the Edit Partition page, where you can edit the devices in the Site. Be sure to click the Save button when you are finished. (Refer to "Segmenting Devices and Users" on page 163 for detailed information on Sites and Partitions.)

Field	Description/Action
Group Name	Displays the name of the Site.
Description	Displays the description of the View.
Sharing	Displays whether the device group is Public or Private, if applicable. Keep in mind that Partition groups are always public.
Parent Group Device	Select a parent group from the drop-down menu, if applicable.
Devices	A list of devices is displayed in the Device Selector's Added Devices box, if applicable. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector.

Be sure to click the Save button when you are done.

Viewing Partition Details

A Partition is set of devices and/or users that is part of a View. A device and/or user can only be in one partition within a View. If there is more than one View, each device and/or user is in one (and only one) Partition within each View.

To view and/or edit Partition information:

1. On the menu bar under Admin click Views. The Views page opens.
2. Click the name of the View for which you want to view information. The Partitions for that View page opens.

Field	Description/Action
Name	Displays the name of the Partition. (**Note**: If you click the Partition name, the Device Details page opens. Refer to "Inventory Page Fields" on page 217 for information.)
Description	Displays the description of the Partition. Refer to "Segmenting Devices and Users" on page 163 for detailed information on Partitions.)
Number of Devices	Displays the number of devices in the Partition.
Actions	You can select the following actions: • Edit — Opens the Edit Partitions page, where you can add or delete devices from the Partition. • Delete — Enables you to delete the Partition.

Edit View Page Fields

To edit a Site (or Partition):

1. On the menu bar under Admin, click Views. The Views page opens.
2. For the View you want to edit, click the Edit option in the Actions column. The Edit View page opens. The following table includes the fields when editing the default Site View.

Field	Description/Action
View Name	Displays Default Site.
Description	Provides a description of the partition.
Core	This field is only displayed for partitions in the default Site View. In a distributed NCM installation, this specifies which NCM Core will be used to manage devices in this Site. (Refer to "Overlapping IP Networks" on page 165 for more information on NCM Cores.)
Realm Name	Select a Realm from the drop-down menu. This field is only displayed for partitions in the default Site View. This specifies what Realm the devices in this Site are in. If the NCM Core is not in the same Realm, NCM uses the Gateway Mesh to connect to the devices in this Site.
Devices	A list of devices is displayed in the Device Selector's Added Devices box. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. Keep in mind that you can only add a device to a partition (which automatically removes the device from its previous partition). In addition, to delete a partition, you must move all the devices from it into a different partition before the system can delete it.

Site List

The Site List provides a list of your current Sites. A Site is set of devices. Each Site belongs to only one Realm and one NCM Core. As a result, a Site is managed by one (and only one) NCM Core. Sites can be used in conjunction with a Permissions model, group hierarchy, distribution of devices across NCM Cores, and network diagramming.

To view the Sites List, on the menu bar under Devices click Sites. The Site List page opens.

Field	Description/Action
Views link	Opens the Views page. Refer to "Views Page Fields" on page 168 for information.
New Site link	Opens the New Site page. Refer to "New Site Page Fields" on page 171 for information.
Site Name	Displays the name of the Site.
Description	Displays the description of the Site.
Number of Devices	Displays the number of devices in the Site.
Realm	Displays the name of the Realm. A Realm is a network segment. In general, a Realm is identified by a set of unique IP addresses. While a Realm does not have to include any NCM Cores, typically a NCM Core manages devices in its local Realm. A NCM Core can manage devices in remote Realms via the Gateway Mesh. The Gateway Mesh is used to proxy IP traffic between Realms. Refer to the *NCM Gateway User's Guide* for detailed information.
Actions	You can select the following actions: • Edit — Opens the Edit Site page, where you can add or delete devices from the Site. • Delete — Enables you to delete the Site.

Segmenting Devices Example

In the following example, you will:

- Create a new View named *Corporate*.
- Add a partition to the Corporate View named *Redmond* and specify two devices to be included in the partition.
- Make sure that the View Partition Permission is configured properly so that users can view the devices in the Redmond partition.

1. Login to NCM as Admin.
2. On the menu bar under Admin, click Views. The Views page opens. (**Note**: There is one default View named *Site*. A site is a physical partitioning of your network's devices that contains all of the discovered devices in your network.)
3. Click the New View link at the top of the page. The New View page opens.
4. Enter "Corporate" for the View Name.
5. Enter "Partitions devices by location" in the Description field.
6. Click the Save View button. The Views page opens. You should see "Corporate" in the Name column. By default, there is one partition. This partition includes all of the devices in your network.
7. For the Corporate View, click Edit in the Actions column. The Edit View page opens.
8. Click the New Corporate link at the top of the page. The New Corporate page opens.
9. Enter "Redmond" in the Corporate Name field.
10. Enter "Partitions devices by location" in the Description field.
11. Using the Device Selector, double click Inventory.
12. While pressing the Shift key, select the first two devices in the left-hand device list.
13. Click the right arrows (>>>) button. The devices are displayed in the right-hand Added Devices box.

14. Click the Save button. The Partitions In The Corporate View page opens, displaying the number of devices in the Redmond partition.
15. On the menu bar under Admin, click the User Roles & Permissions. The User Roles & Permissions page opens.
16. Click the New User Role link at the top of the page. The New User Role page opens.
17. From the Type drop-down menu, select View Partition Permission.
18. Enter “Redmond” in the Name field and “Redmond Role” in the Description field.
19. In the View By drop down menu, select Corporate.
20. Select Redmond from the list of views.
21. Click the Save button.

Defining Partitions Case Study

You can use Views and Partitions to define View Partition permissions. View Partition permissions restrict:

- Specific users to only view specific sets of devices
- Specific users to only view specific sets of users
- Specific users to only view specific sets of user groups
- Specific users to only view specific sets of device groups

In the following case study, Acme Service Provider uses NCM to manage their customers' devices and users. They've configured NCM as follows.

Partitioning Devices

Customer 1: Cortland Electronics

Routers:

- A (10.255.1.20)
- B (10.255.1.22)

Firewalls:

- A (10.255.1.190
- B (10.255.1.173)

Users:

- Palmer
- Opal
- Pete

User Groups:

- Cortland
- Cortland Security
- Cortland Management

Device Groups:

- Cortland Development
- Cortland QA

Customer 2: Chandler Enterprises

Routers:

- C (10.255.1.36)
- D (10.255.1.72)

Firewalls:

- C (10.255.1.190)
- D (10.255.1.173)

Users:

- Adam
- Colby

User Groups:

- Chandler
- Chandler Security

The following devices exist in the system.

Cortland Electronics **Chandler Enterprises**

	A	B	C	D
Router	**10.255.1.20**	**10.255.1.22**	**10.255.1.36**	**10.255.1.72**
Firewall	**10.255.1.190**	**10.255.1.173**	**10.255.1.152**	**10.255.1.151**

The following steps describe how the IT folks at Acme Service Provider were able to configured NCM in such a way.

1. Login to NCM.
2. On the menu bar under Admin, select Views. The Views page opens.
3. Click the New View option at the top of the page. The New View page opens.
4. Enter **Device Type** in the View Name field.
5. Enter **Network Security** in the Description field.
6. Click the Save View button. The Views page opens listing the current Views.
7. In the Name column, click Device Type. The Partitions in Device Type View page opens.
8. Click the New Device Type link at the top of the page. The New Device Type opens.
9. Enter **Routers** in the Device Type Name field.
10. Enter **Routers A, B, C, and D** in the Description field.
11. Using the Device Selector, select Routers A (10.255.1.20), B (10.255.1.22), C (10.255.1.36), and D (10.255.1.72) from the left-hand box, add them to the right-hand box, and click the Save button. The Partitions in Device Type View opens displaying the newly created partition.
12. Click the New Device Type link at the top of the page. The New Device Type opens.
13. Enter **Firewalls** in the Device Type Name field.
14. Enter **Firewalls A, B, C, and D** in the Description field.
15. Using the Device Selector, select Firewalls A (10.255.1.190), B (10.255.1.173), C (10.255.1.152) and D (10.255.1.151) from the left-hand box, add them to the right-hand box, and click the Save button. The Partitions in Device Type View opens displaying the newly created partition.

16. Repeat Steps 2 through 15 with the following parameters:
    - Step 4: Enter **Customer**
    - Step 9: Enter **Cortland Electronics**
    - Step 10: Enter **Router C (10.255.1.136)** and **D (10.255.1.72)**
      Firewall A (10.255.1.190) and **B (10.255.1.173)**
    - Step 13: Enter **Chandler Enterprises**
    - Step 14: Enter **Router A (10.255.1.20)** and **B (10.255.1.22)**
      Firewall C (10.255.1.152) and **D (10.255.1.151)**

The following table shows the devices and their Partition assignments.

Device	View		
	Site	Device Type	Customer
10.255.1.20 (Router A)	—	Router	Chandler Enterprises
10.255.1.22 (Router B)	—	Router	Chandler Enterprises
10.255.1.36 (Router C)	—	Router	Cortland Electronics
10.255.1.72 (Router D)	—	Router	Cortland Electronics
10.255.1.190 (Firewall A)	—	Firewall	Cortland Electronics
10.255.1.173 (Firewall B)	—	Firewall	Cortland Electronics
10.255.1.152 (Firewall C)	—	Firewall	Chandler Enterprises
10.255.1.151 (Firewall D)	—	Firewall	Chandler Enterprises

Now that the Device Partitions are configured, the IT folks at Acme Service Provider want to configure permissions for viewing devices, users, and user groups, and device groups.

Palmer is Cortland Electronics' network engineer. Pete their the security expert. Adam is Chandler Enterprises' network engineer. Colby is their security expert.

The Acme Service Provider IT folks want security boundaries for:

- Chandler Enterprises' routers
- Chandler Enterprises' devices
- Cortland Electronics routers
- Cortland Electronics' devices
- Chandler Enterprises firewalls
- All routers
- All firewalls
- All devices

Creating User Groups

The following steps describe how the IT folks at Acme Service Provider were able to create user groups and assign view permissions in NCM for each security boundary.

I. Create the Cortland Group

1. Login to NCM as either the NCM Administrator or a user with Administrator privilege.
2. On the menu bar under Admin, click New User Group. The New User Group page opens.
3. Enter **Cortland** in the Group Name field.
4. Enter **Security boundaries** in the Description field.
5. Select "Routers" from the Partition drop-down list for Device Type.
6. Select "Cortland" from the Partition drop-down list for Customer.
7. Scroll down to the View Partition Permission field and select the "Customized View Permission Role (specific to this user group)" option.
8. Select "Routers" from the Device Type box and "Cortland" from the Customer box. Then, click the Save button.

II. Create The Cortland Security Group

1. On the menu bar under Admin, click New User Group. The New User Group page opens.
2. Enter **Cortland Security** in the Group Name field.
3. Enter **Security boundaries** in the Description field.
4. Select "Firewalls" from the Partition drop-down list for Device Type.
5. Select "Cortland" from the Partition drop-down list for Customer.
6. Scroll down to the View Partition Permission field and select the "Customized View Permission Role (specific to this user group)" option.
7. Select "Firewalls" from the Device Type box and "Cortland" from the Customer box. Then, click the Save button.

III. Create the Chandler Group

1. On the menu bar under Admin, click New User Group. The New User Group page opens.
2. Enter **Chandler** in the Group Name field.
3. Enter **Security boundaries** in the Description field.
4. Select "Routers" from the Partition drop-down list for Device Type.
5. Select "Chandler" from the partition drop-down list for Customer.
6. Scroll down to the View Partition Permission field and select the "Customized View Permission Role (specific to this user group)" option.
7. Select "Routers" from the Device Type box and "Chandler" from the Customer box. Then, click the Save button.

IV. Create the Chandler Security Group

1. On the menu bar under Admin, click New User Group. The New User Group page opens.
2. Enter **Chandler Security** in the Group Name field.
3. Enter **Security boundaries** in the Description field.
4. Select "Firewalls" from the Partition drop-down list for Device Type.
5. Select "Chandler" from the Partition drop-down list for Customer.
6. Scroll down to the View Partition Permission field and select the "Customized View Permission Role (specific to this user group)" option.

7. Select “Firewalls” from the Device Type box and “Chandler” from the Customer box. Then, click the Save button.

Note: Steps 5, 6, 12, 13, 19, 20, 25, and 26 are not mandatory. A user group does not have to be in a specific partition to assign view permission to its users. The example includes these steps to illustrate the isolation of user groups mentioned later.

The following table shows the user groups and partitions for which the user groups can provide permissions.

User Group	Partitions Assigned Per View		
	Site	Device Type	Customer
Cortland	—	Router	Cortland Electronics
Cortland Security	—	Firewall	Cortland Electronics
Chandler	—	Router	Chandler Enterprises
Chandler Security	—	Firewall	Chandler Enterprises

Creating Users

The following steps describe how the IT folks at Acme Service Provider created users for each security boundary.

I. Create the Palmer User

1. On the menu bar under Admin, click New User. The New User page opens.
2. Enter **Palmer** in the User Name field.
3. Select “Cortland” in the User belongs to selected groups field.
4. Enter Palmer’s password and confirm the password.
5. Select “Routers” from the Partition drop-down list for Device Type.
6. Select “Cortland” from the Partition drop-down list for Customer.
7. Click the Save button. The All Users page opens.

II. Create the Pete User

1. On the menu bar under Admin, click New User. The New User page opens.
2. Enter **Pete** in the User Name field.
3. Select “Cortland Electronics” and “Cortland Electronics Security” in the User belongs to selected groups field.
4. Enter Pete’s password and confirm the password.
5. Select either “Firewalls” from the Partition drop-down list for Device Type.
6. Select “Cortland” from the Partition drop-down list for Customer.
7. Click the Save button. The All Users page opens.
8. On the menu bar under Admin, click New User. The New User page opens.

III. Create the Adam User

1. Enter **Adam** in the User Name field.
2. Select “Chandler” in the User belongs to selected groups field.
3. Enter Adam’s password and confirm the password.
4. Select “Routers” from the Partition drop-down list for Device Type.
5. Select “Chandler” from the Partition drop-down list for Customer.
6. Click the Save button. The All Users page opens.

IV. Create the Colby User

1. On the menu bar under Admin, click New User. The New User page opens.
2. Enter **Colby** in the User Name field.
3. Select “Chandler” and “Security” in the User belongs to selected groups field.
4. Enter Colby's password and confirm the password.
5. Select “Firewalls” from Partition drop-down list for Device Type
6. Select “Chandler” from Partition drop-down list for Customer.
7. Click the Save button. The All Users page opens.

Acme Service Provider Users

Ryan is Acme Service Provider's system engineer. Norm is responsible for maintaining all of Cortland Electronics and Chandler Enterprise routers. Annie is Acme Service Providers security expert.

I. Create the Ryan User

1. On the menu bar under Admin, click New User. The New User page opens.
2. Enter **Ryan** in the User Name field.
3. Select "Cortland," Cortland Security," "Chandler," and "Chandler Security" in the User belongs to selected groups field.
4. Enter Ryan's password and confirm the password.
5. Select either "Firewalls" or "Routers" from the Partition drop-down list for Device Type.
6. Select either "Cortland Electronics" or "Chandler Enterprises" from the Partition drop-down list for Customers.

   Note: The selections you make in Steps 5 and 6 will impact the users listed in the "Partitioning Users" section on page.

7. Click the Save button. The All Users page opens.

II. Create the Annie User

1. On the menu bar under Admin, click New User. The New User page opens.
2. Enter **Annie** in the User Name field.
3. Select "Cortland Security" and "Chandler Security" in the User belongs to selected groups field.
4. Enter Annie's password and confirm the password.
5. Select "Firewalls" from the Partition drop-down list for Device Type.
6. Select either "Cortland Electronics" or "Chandler Enterprises" from the Partition drop-down list for Customer. (The selection you make will impact the users listed in the "Partitioning Users" section on page.)
7. Click the Save button. The All Users page opens.

III. Create the Norm User

1. On the menu bar under Admin, click New User. The New User page opens.
2. Enter **Norm** in the User Name field.
3. Select "Cortland" and "Chandler" in the User belongs to selected groups field.
4. Enter Norm's password and confirm the password.
5. Select "Routers" from Partition drop-down list for Device Type.
6. Select either "Cortland Electronics" or "Chandler Enterprises" from Partition drop-down list for Customer. (The selection you make will impact the users listed in the "Partitioning Users" section on page.)
7. Click the Save button. The All Users page opens.

The following table shows all users and the user groups in which they are included. In addition, the table shows the view permissions for each user groups and the devices each user can view.

User	User Groups	Partitions	Devices	Total
Palmer	Cortland	Routers & Cortland Electronics	10.255.1.72 10.255.1.36	2
Pete	Cortland	Routers & Cortland Electronics	10.255.1.72 10.255.1.36	
	Cortland Security	Firewalls & Cortland Electronics	10.255.1.190 10.255.1.173	4
Adam	Chandler	Routers & Chandler Electronics	10.255.1.20 10.255.1.22	2
Colby	Chandler	Routers and Chandler Enterprises	10.255.1.20 10.255.1.22	
	Chandler Security	Firewalls & Chandler Enterprises	10.255.1.152 10.255.1.151	4
Ryan	All	All	All	8
Annie	Cortland Security	Firewalls & Chandler Enterprises	10.255.1.190 10.255.1.173	

User	User Groups	Partitions	Devices	Total
	Chandler Security	Firewalls & Chandler Enterprises	10.255.1.152 10.255.1.151	4
Norm	Cortland	Routers & Cortland Electronics	10.255.1.20 10.255.1.36	
	Chandler	Routers & Chandler Enterprises	10.255.1.20 10.255.1.22	4

Partitioning Users

The following table shows the partitions each user can view.

User	View		
	Site	Device Type	Customer
Palmer	—	Router	Cortland Electronics
Pete	—	Firewall	Cortland Electronics
Adam	—	Router	Chandler Enterprises
Colby	—	Firewall	Chandler Enterprises
Ryan	—	Router	Cortland Electronics
Annie	—	Firewall	Chandler Enterprises
Norm	—	Router	Chandler Enterprises

The following table shows each user and the user group they are in, the partitions the user groups are in, and the devices each user can view.

User	User Groups	Partitions	Users Can View	Total
Palmer	Cortland	Routers & Cortland	Palmer and Ryan	2
Pete	Cortland Cortland Security	Routers & Cortland Firewalls & Cortland	Palmer and Ryan Pete	3
Adam	Chandler	Routers & Chandler	Adam and Norm	2
Colby	Chandler Chandler Security	Routers and Chandler Firewalls & Chandler	Adam and Norm Colby and Annie	4
Ryan	All	All	Ryan	7
Annie	Cortland Security Chandler Security	Firewalls & Chandler Firewalls & Chandler	Pete Colby and Annie	3
Norm	Cortland Chandler	Routers & Cortland Routers & Chandler	Palmer and Ryan Adam and Norm	4

Editing Device Groups

To edit an existing device group:

1. On the menu bar under Devices, click Groups. The Device Groups page opens.
2. Click Edit in the Actions column for the device group you want to edit. The Edit Group page opens. Be sure to click Save when you are done.

Edit Group Page Fields

Field	Description/Action
Group Name	Displays the name of the device group.
Description	Displays a description of the device group.
Owner	Select an owner from the drop-down menu.
Sharing	Either informs you that the device group you are editing is public or private, or that the device group is a parent group. If you are editing a leaf group, you are informed that the device group has a parent.
Parent Device Group	Displays the name of the parent device group in the drop-down menu.
Devices	Select one of the following options: • Use Device Selector to select a fixed device group (static group) — For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • Use filters to define a dynamic device set (dynamci group) — The display changes to enable you configure searches using one or more search criteria, use Boolean expressions (and/or) to filter searches, or limit a search by device group.
Child Device Groups	• All device groups — Displays a list of all current device groups. Select the device groups you want to include as children of the Parent group and click Copy >>. • Children of this group — Displays a list of device groups that are assigned to the Parent group as children. Select the Child groups you want to remove from this Parent group and click << Remove.

Editing a Batch of Devices

The batch edit functionality enables you to make changes to device settings. You can:

- Assign a driver
- Set connection methods (SNMP, Telnet, SSH)
- Set transfer protocols (SCP, TFTP, FTP)
- Set bastion host information
- Reset the last used password
- Set ACL parsing

1. On the menu bar under Devices, click Inventory. A list of all currently managed devices opens.
2. Check the check boxes for the devices you want to edit in one batch operation.
3. On the Actions drop-down menu, click Batch Edit Device. The Batch Edit Device page opens. Be sure to click the Save button when you are finished.

Batch Edit Device Page Fields

Field	Description/Action
Devices	Lists the selected devices.
Assign Driver	If checked, select the driver to assign to the batch of devices.

Field	Description/Action
Set Connection Methods	If checked, select the access methods for the batch edit from the following connection methods and transfer protocols: Connection Methods (checked by default): • SNMP • Telnet • SSH — Select either SSH1 or SSH2 (the default), SSH1 Only, or SSH2 Only. Transfer Protocols (checked by default): • SCP • FTP • TFTP
Set Bastion Host Information	If checked, enter the following information: • Check uses Unix or Linux bastion host for Telnet & SSH access, if applicable • IP address or Host Name of the bastion host • Bastion Host Username • Bastion Host Password • Confirm the password
Reset Last Used Passwords	If checked, reset last used passwords.
Set ACL Parsing	If checked, select one of the following options: • Enable ACL parsing and storage with each snapshot. • Disable ACL parsing and storage with each snapshot.

Discovering Device Drivers

Discovery matches an appropriate device driver to any device. The device driver translates proprietary commands for each device to the universal format that NCM uses to manage heterogeneous networks.

Discovery queries each new device using SNMP or Telnet/SSH and assigns the appropriate device driver. If this process fails, the result appears on the Recent Tasks page. NCM cannot actively manage a device configuration until the correct driver is assigned. If driver discovery fails, you can assign a driver manually. For a list of supported drivers, refer to the *Device Driver Reference*.

To initiate the device driver discovery process, on the menu bar under Devices, select New Device Task and click Discover Driver. The New Task - Discover Driver page opens. Refer to "Discover Driver Task Page Fields" on page 289. Keep in mind that device driver discovery is also initiated by the Deploy Software task. After software is successfully uploaded (and the device is rebooted, if this option is selected), a device driver discovery task is initiated.

Accessing Devices Using Telnet

Launching Telnet and SSH sessions from NCM offers several benefits:

- Simplify logins — Users login using their NCM account. NCM verifies the user's permissions. The user can enter NCM CLI commands or connect directly to a device. The user can exit from one device, then connect to another, and so on, in one session. The user must remember only one login, regardless of device vendors, types, and so on. If the requested login method does not work, NCM automatically tries backup login methods.
- Organize by groups and permissions — Organizing devices into groups and assigning permissions per group ensures that users access just the devices they care about and have permissions for.
- Store configurations, even without AAA — The Telnet/SSH Proxy enables you to store modified configurations, in-line comments, and who made changes. The Telnet/SSH Proxy automatically associates audit logs of sessions to the configurations.
- Reduce ACLs — You need an Access Control List (ACL) only for the NCM server, rather than one ACL per device.
- Increase security — Identifying who is changing devices on your network makes it easier to detect an unauthorized user and track unauthorized changes. NCM also makes it easy to deploy a stable configuration stored prior to the unauthorized changes, correcting potential damage and restoring network service quickly.

In addition, you can connect your Telnet/SSH client to devices through NCM, and track the sessions. NCM has been tested with connections from the following clients (though others may also work):

- SecureCRT
- Windows Telnet
- Putty

There are a number of Admin Settings related to the Telnet/SSH Proxy interface. Refer to "Telnet/SSH" on page 94 for information.

To initiate a Telnet session using NCM, on the menu bar under Devices, click Inventory. A list of all currently managed devices opens. Select the Telnet option in the Actions column for the device. You are logged into the device and you see the device prompt in the Telnet window.

Note: If your computer does not already have the Java Runtime Environment (JRE) installed, your browser initiates a download from the Sun Website the first time you use Telnet or SSH. This is expected and you should approve the download and installation of the JRE.

The first time you run a Telnet or SSH session from NCM, you may see a security window asking you to download a certificate from Cisco. Click Grant always to continue. This verifies that you trust content from Cisco.

You can enter whatever device commands you like. Enter *quit* when finished. This logs you out of the Telnet session, but you remain in a NCM Telnet/SSH Proxy session. The Proxy session uses the `NCM>` prompt.

In a Telnet/SSH Proxy session, you can connect to another device or enter NCM CLI commands. You can initiate a Proxy session directly by clicking Connect at the top of any page. In a Telnet Proxy session, you can connect to another device or enter NCM CLI commands.

Accessing Devices Using SSH

To initiate an SSH session, on the menu bar under Devices, click Inventory. A list of all currently managed devices opens. Select the SSH option in the Actions column for the device. You can enter whatever device commands you like. Enter *quit* when you are finished. This logs you out of the SSH session, but you remain in a NCM Telnet/SSH Proxy session.

Note: You can initiate a Proxy session directly by clicking Connect at the top of any page. In a SSH Proxy session, you can connect to another device or enter NCM CLI commands.

Listing Telnet/SSH Sessions

To list Telnet and SSH sessions, on the menu bar under Devices, click Inventory. A list of all currently managed devices opens. Click the device. The Device Details page for that device opens. From the View drop-down menu, click Telnet/SSH Sessions. The Telnet/SSH Session page opens with the device host name or IP address at the top.

Telnet/SSH Session List Page Fields

Field	Description/Action
User Name	Displays user name of the person who ran the session.
Start Date	Displays the date and time the session began.
End Date	Displays the date and time the session ended.
Status	Displays the status of the session, either Open or Closed.
Type	Displays the type of session, either Telnet or SSH.
<Custom Fields>	All custom fields defined for Telnet/SSH sessions appear on this page.
Actions	You can select from the following options: • View Full Session — Opens the Telnet/SSH Session page, where you can view the commands entered and the device responses during this session. • View Commands Only — Opens the Telnet/SSH Session page, where you can view only the commands entered during this session. This is useful for recording scripts to replay on this or other devices. Click any command to view the device response to that command.

Note: Selecting text with the left mouse button highlights the text in reverse video. You can then press the Enter key to paste the text onto the clipboard. Pressing the right mouse button inside the Telnet/SSH applet pastes the text from the clipboard to the applet.

A shortcut when using connect is adding wildcards to the host name or IP address, such as `connect *.sfo`. This returns a list of devices (or a message to narrow your search). Enter the number of the device you want to connect to. The Shell interface supports the following control characters.

Control Character	Description
^A	Moves the cursor to beginning of the input line.
^B, Left Arrow	Moves the cursor back one character.
^C	Cancels the input line and returns a new prompt.
^D	Erases the character under the cursor.
^F, Right Arrow	Moves the cursor right one character.
^H, Backspace, Delete	Erases the character to the left of the cursor.
^J, ^M	Sends a CRLF.
^K	Kills from the cursor to end of line and places text in the kill buffer.
^L, ^R	Echoes a command on new command line (simulates screen redraw).
^N, Down Arrow	Moves to the next command in the command history.
^P, Up Arrow	Moves to the previous command in the command history.
^T	Transposes the character under the cursor with the previous character.
^U, ^X	Deletes from the cursor to the beginning of line, and places the deleted characters in the kill buffer.
^W	Deletes from the cursor to the beginning of word, and places the deleted characters in kill buffer.
^Y	Yanks from the kill buffer to the current location.
^\	Closes the current device connection (useful for access through a console server).
ESC-b	Moves the cursor backwards one word.
ESC-f	Moves the cursor forwards one word.

Making Configuration Changes Using The Telnet/SSH Proxy

Do the following to make configuration changes via the Telnet/SSH Proxy.

1. Telnet or SSH to the NCM server and login using your NCM credentials.
2. Use the *connect* command to connect to devices. You can enter `connect*` to view the devices available for connection through NCM. If there are too many devices to display, narrow the field by entering the first few letters of the hostname (or digits of the IP address), followed by an asterick, for example: `connect bor*`.
3. Enter the number from the list of numbers displayed in the Telnet/SSH Proxy of the device to which you want to connect. NCM automatically logs you into the device after checking your access credentials.
4. Assuming that this is a Cisco IOS device, enter `Config T` mode on the device make the change and add any relevant comments.
5. Exit out of Configure Terminal mode and enter `Exit`.
6. To exit the NCM Telnet/SSH Proxy, enter `Exit` at the prompt.

Keep in mind when using the Telnet/SSH Proxy, in-line commenting occur as you are logged into the device.

Using a Bastion Host

A bastion host is a gateway between a private network and a public network. Used as a security measure, a bastion host can act as a barrier between private and public networks to prevent attacks by hackers.

Using a bastion host with NCM enables you to have lockdown capability over Telnet or SSH access. You can:

- Specify a bastion host on a per device basis.
- Specify username (optional) and password as login credentials for the bastion host.
- Telnet or SSH to the bastion host and then Telnet or SSH through to the target device.

Note: When using a bastion host, all CLI access will be routed through the bastion host rather than directly to the device. When connecting via the Telnet/SSH Proxy to a device configured to use a bastion host, NCM connects via the bastion host, and applies the user's AAA credentials, if indicated, to both the bastion host and the target device.

Keep in mind that access to a bastion host will not go through the normal NCM password rules processing. If the bastion host credentials are invalid, there is no fallback. After logging into the bastion host, access from there to the device will follow the normal password processing in NCM.

Note: Multiple bastion hosts cannot be specified for an specific device. However, you can simulate this by load-balancing across multiple bastion hosts that share a DNS name.

To designate a Unix or Linux bastion host for Telnet & SSH access:

1. On the menu bar under Devices, click Inventory. A list of all currently managed devices opens.
2. Click the New Device link at the top of the page. The New Device page opens.
3. Scroll down to the middle of the page to locate the Connection Information section. Refer to "New Device Page Fields" on page 135 for information.

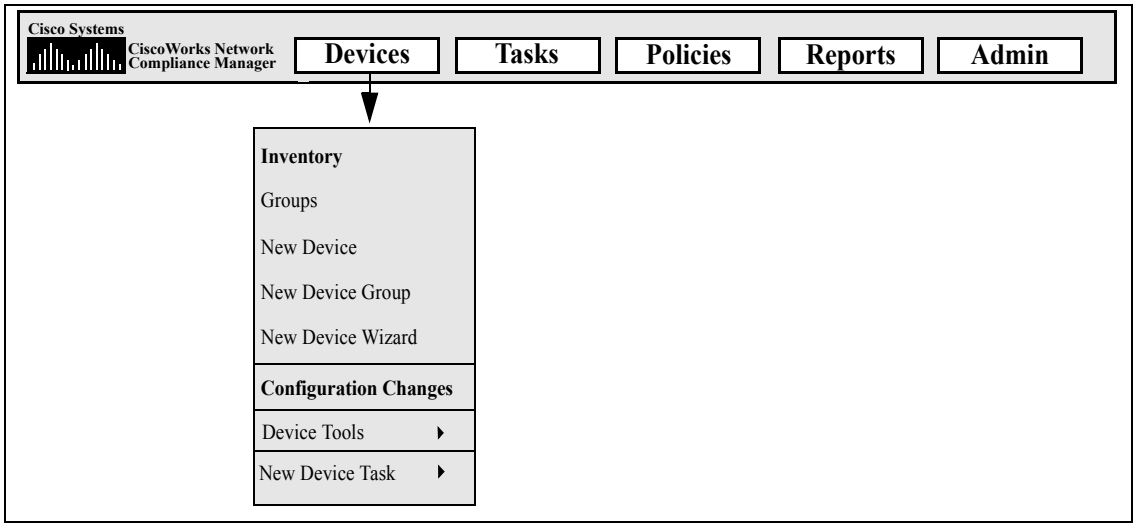
To designate if new devices should use a bastion host by default for Telnet and SSH access, on the menu bar under Admin, select Administrative Settings and click Device Access. Refer to "Device Access Page Fields" on page 69 for information.

Chapter 4: Managing Device Configurations

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 202
Viewing Device Configuration Changes	"Viewing Device Configuration Changes" on page 203
Comparing Device Configurations	"Comparing Device Configurations" on page 209
Deploying Device Configurations	"Deploying Device Configurations" on page 211

Navigating to Device Configuration Changes



Getting Started

CiscoWorks Network Compliance Manager (NCM) detects and records device configuration changes. As soon as a device configuration change occurs, NCM downloads the configuration into its centralize repository. NCM supports multiple real-time changed detection and alerting systems that enable you to immediately identify what changes were made and by whom.

For devices that support user attribution via Syslog, such as Cisco IOS devices, NCM extracts the username and associates it with a configuration change. If NCM cannot associate the username with an NCM user, a new user account is created with a randomly generated password. By default, NCM appends the term "_auto" to the new user to distinguish it as auto-generated. This enables NCM to report ownership for all changes, including ones made by unregistered users. NCM uses several methods, including AAA accounting logs, Syslog messages, and Proxy logs to discover the author of a given configuration change.

Access Control Lists (ACLs) are part of the configuration on many devices. They filter network traffic by controlling whether routed packets are accepted or blocked at the router's interfaces.

In general, the definition of an ACL is a collection of configuration statements. These statements define addresses and patterns to accept or deny. ACLs can be used to restrict the contents of routing updates and to provide network security.

NCM retrieves configuration information from devices and extracts the ACL statements from the configuration. NCM then stores the ACLs independent of the configuration. Refer to Chapter 20, "Working with ACLs" for detailed information on creating ACLs.

Viewing Device Configuration Changes

The Configurations Changes page enables you to view configurations that have changed. Devices that appear in red text failed the last snapshot attempt. Inactive devices are indicated with an icon next to the IP address.

With configuration changes shown in different colors, you can easily scan two configurations and quickly identify the areas that have changed. To identify a misconfigured device manually, you must connect to the device, call up the configuration, and identify if there is anything anomalous about the configuration.

To view a complete list of all recent configuration changes, on the menu bar under Devices, click Configuration Changes. The Configuration Changes page opens. You can click a device to view specific device configuration information.

To view configuration changes for a specific device:

1. On the menu bar under Device, click Inventory. A list of all currently managed devices opens.
2. Click the device for which you want to view configuration changes. The Device Details page for that device opens.
3. From the View drop-down menu, click Configuration Changes. The Device Configurations page opens.

Device Configurations Page Fields

Field	Description/Action
Hostname	Displays the device's host name. Clicking the device's host name opens the Device Details page, where you can view information about this device.
Device IP	Displays the device's IP address. Clicking the device's IP address opens the Device Details page, where you can view information about this device.
Last Access Time	Displays the date and time the device was last accessed.
Last Snapshot Result	Displays the last snapshot result, for example "Configuration unchanged."
View menu	Refer to "View Menu Options" on page 229 for information.
Edit & Provision menu	Refer to "Device Events Page Fields" on page 233 for information.
Connect menu	Refer to "Connect Menu Options" on page 248 for information.
Scheduled Deployments for Device link	Opens the Task Search Results page, where you can view if there are any deployments scheduled for the device.
Edited Configurations link	Opens the Config Search Results page. Refer to "Configuration Search Results Page Fields" on page 464 for information.
Check Boxes	You can use the left-side check boxes to compare two device configurations and/or delete device configurations. Once you have selected the devices, click the Actions drop-down menu and click either: • Compare — Opens the Compare Device Configurations page, where you can compare the two selected configurations side-by-side. The differences are highlighted in different colors to make them easy to view. • Delete — Deletes the checked device configurations. The adjacent Select drop-down menu enables you to select or deselect all of the device configurations.
Date	Displays the date and time the configuration was added or changed.

Field	Description/Action
Changed By	Displays the login name of the person who changed the configuration, device, or task. N/A means not applicable.
Comments	Displays any comments about the configuration.
Actions	You can select the following actions: • Compare to Previous — Opens the Compare Device Configuration page, where you can view the selected configuration and the next previous configuration side-by-side. The differences are highlighted in different colors to make them easy to view. • View Config — Opens the Device Configuration Detail page, where you can view the entire configuration, deploy this version of the configuration to the device running configuration, edit the configuration, retrieve diagnostics, and compare the configuration to the previous configuration. Refer to "Device Configuration Detail Page Fields" on page 206 detailed information. • Diagnostics — Opens the Diagnostics page, where you can view diagnostic information for this configuration. Diagnostics include Basic IP, Device Information, CWNCM Detect Device Boot, CWNCM Interfaces, CWNCM Module Status, CWNCM OSPF Neighbors, and CWNCM Routing Table. For detailed information on diagnostics, refer to "View Menu Options" on page 229.

If the Startup and Running Configurations differ, the following links are displayed at the top of the Device Configurations page:

- View Startup — Opens the Device Configuration page, where you can view the current configuration. Refer to "Device Configuration Detail Page Fields" on page 206 for information.
- Compare Startup with Running — Opens the Compare Device Configurations page, where you can compare the Startup and Running Configurations. Refer to "Compare Device Configurations Page Fields" on page 209 for information.
- Synchronize — Opens the New Task - Synchronize Startup and Running page, where you can synchronize the Startup and Running Configurations. Refer to "Synchronize Startup and Running Task Page Fields" on page 318 for information.

Device Configuration Detail Page Fields

The Device Configuration Detail page enables you to:

- Examine the details of a particular configuration.
- Enter comments about the configuration.
- Deploy this version of the configuration to the device. For example, you could deploy a stable configuration to roll back an incorrect change to the device.

To view the Device Configuration Details page for a specific device:

1. On the Device Details page, click the View drop-down menu and then click Configuration Changes. The Device Configurations page opens.
2. In the Actions column, click the View Config option. The Device Configuration Detail page opens.

Field	Description/Action
Hostname	Displays the device's host name. Clicking the device's host name opens the Device Details page, where you can view information about this device.
Device IP	Displays the device's IP address. Clicking the device's IP address opens the Device Details page, where you can view information about this device.
Last Access Time	Displays the date and time the device was last accessed.
Last Snapshot Result	Displays the last snapshot result, for example "Configuration unchanged."
View menu	Refer to "View Menu Options" on page 229 for information.
Edit & Provision menu	Refer to "Device Events Page Fields" on page 233 for information.
Connect menu	Refer to "Connect Menu Options" on page 248 for information.
Deploy to running configuration link	Opens the New Task - Deploy Config page, where you can deploy the configuration to the running config. (**Note**: This action may not be available for all devices.) Refer to "Deploy Config Task Page Fields" on page 212 for information.

Field	Description/Action
Deploy to startup configuration and reboot link	Opens the New Task - Deploy Config page, where you can deploy the configuration to the startup config and reboot the device (so the startup and running configurations remain synchronized). (**Note**: This action may not be available for all devices.) Refer to "Deploy Config Task Page Fields" on page 212 for information.
Text Version link	Displays the configuration in plain text in a new browser window so you can copy it to the clipboard and paste it into other applications.
Download Binary Configuration link	Displays the configuration in Binary format in new browser window so you can copy it to the clipboard and paste it into other applications.
Compare to previous link	Opens the Compare Device Configurations page, where you can view the older and newer configurations side-by-side. The differences are highlighted in different colors to make them easy to view.
Changed By	Displays the login name of the person whose change triggered the snapshot.
Create Date	Displays the date and time of the last configuration change.
<custom fields>	Displays any custom fields defined for device snapshots and diagnostics.
Configuration Comments	Enter comments to differentiate this configuration from others, especially the previous configuration. Click Edit Comments. The Edit Comments option enables you to edit the custom fields and comments for this configuration. Refer to "Editing Device Configuration Data" on page 208 for information on editing device configuration data.
Line/Configuration Text	Displays the configuration file.

Editing Device Configuration Data

On the Device Configuration Detail page, you can add or edit configuration comments by clicking Edit Comments to open the Edit Device Configuration Detail page. For information on adding custom data, refer to "Custom Data Setup Page Fields" on page 539.

When editing in-line comments:

- Whenever a line in a configuration changes, the comment for that line is removed. For example, if you change the host name, NCM also removes any comment immediately above the host name command because NCM cannot be sure the comment remains valid after the command is changed.
- Be careful adding or removing blank lines. Because blank lines can be significant for some devices, NCM treats added or removed blank lines as configuration changes. You can add blank comment lines (lines that begin with a double comment character, usually !! or ##).
- In-line comments are not versioned in the same way as configuration files. A comment block applies to the next command in the configuration. If a deployment does not affect the next command line, the comment does not change. If you deploy an old configuration (to overwrite a new one), the comments from the newer configuration may be applied to the deployed configuration, even though the comments might end up in the wrong places.
- If you are concerned about losing comments in a file that requires significant editing, it is recommended that you copy the configuration file with the comments before saving, so you can restore comments if necessary.

Comparing Device Configurations

The Compare Device Configuration page displays two configurations for the same device side-by-side. Additions, deletions, and changes are highlighted in two columns with line numbers on the left. Each configuration is identified by its unique IP address and the date/time on which the configuration snapshot was taken.

To compare two configurations:

1. On the menu bar under Devices, click Configuration Changes. The Configuration Changes page opens.
2. Using the left-side check boxes, click any two devices.
3. On the Actions drop-down menu, click Compare. The Compare Device Configurations page opens.

Compare Device Configurations Page Fields

Field	Description/Action
Lines Changed	Displays the number of lines changed, highlighted in charcoal grey.
Lines Inserted	Displays the number of inserted lines, highlighted in light blue.
Lines Deleted	Displays the number of lines deleted, highlighted in pink.
Show differences with context	If selected (the default), only changes with three lines before and after each change are displayed.
Show full text	If checked, the complete configuration file is displayed.
Show UNIX-style diff	If checked, the configuration file is displayed in UNIX diff format.
Deploy to Running configuration link	Opens the Deploy Configuration page, where you can deploy this configuration to the running config on the device. (**Note**: This action may not be available for all devices.)
Deploy to startup configuration and reboot	Opens the Deploy Configuration page, where you can deploy the configuration to the startup config and reboot the device (so the startup and running configurations remain synchronized). (**Note**: This action may not be available for all devices.)

Field	Description/Action
Configuration #1/ Configuration #2	Clicking the Configuration #1 or Configuration #2 link opens the Device Configuration Detail page. Refer to "Device Configuration Detail Page Fields" on page 206 for information.
Device	Displays the host name and IP address for the device. Clicking the device's host name and IP address opens the Device Details page, where you can view information about this device and its configuration history.
Date	Displays the date and time of the last configuration change.
Changed By	Displays the login name of the person whose change triggered the snapshot.
Configuration Comments	Displays any comments about the configuration.

Deploying Device Configurations

There are two ways to deploy a configuration:

- To the running configuration — When deployed, the configuration file remains in use until the device is rebooted. Rebooting the device might cause the startup configuration to overwrite the running configuration.
- To the startup configuration — When deployed, the device is rebooted and the new configuration becomes both the running and startup configuration.

To deploy a configuration:

1. On the menu bar under Devices, click Configuration Changes. The Configuration Changes page opens.
2. In the Actions column for a device, click View Config. The Device Configuration Detail page opens. Select one of the following options (if applicable):
   - Deploy to running configuration — Opens the New Task - Deploy Config page, where you can deploy this configuration to the running config on the device.
   - Deploy to startup configuration and reboot — Opens the New Task - Deploy Config page, where you can deploy the configuration to the startup config and reboot the device (so the startup and running configurations remain synchronized).

Deploy Config Task Page Fields

Field	Description/Action
Task Name	Displays Deploy Config. You can enter a different task name if applicable.
Applies to	Displays the device's Host Name or IP address.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored.) The "Verify that changes are compliant with all policies that apply to the device" option is checked by default.
Configuration	Displays the configuration.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Server page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Server Page Fields" on page 80 for information on enabling Device Credentials.)

Field	Description/Action
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Pre-Task / Post-Task Snapshot Options
Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 58 for information.)

Pre-Task Snapshot	Select one of the following options: • None (the default) • As part of task
Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.

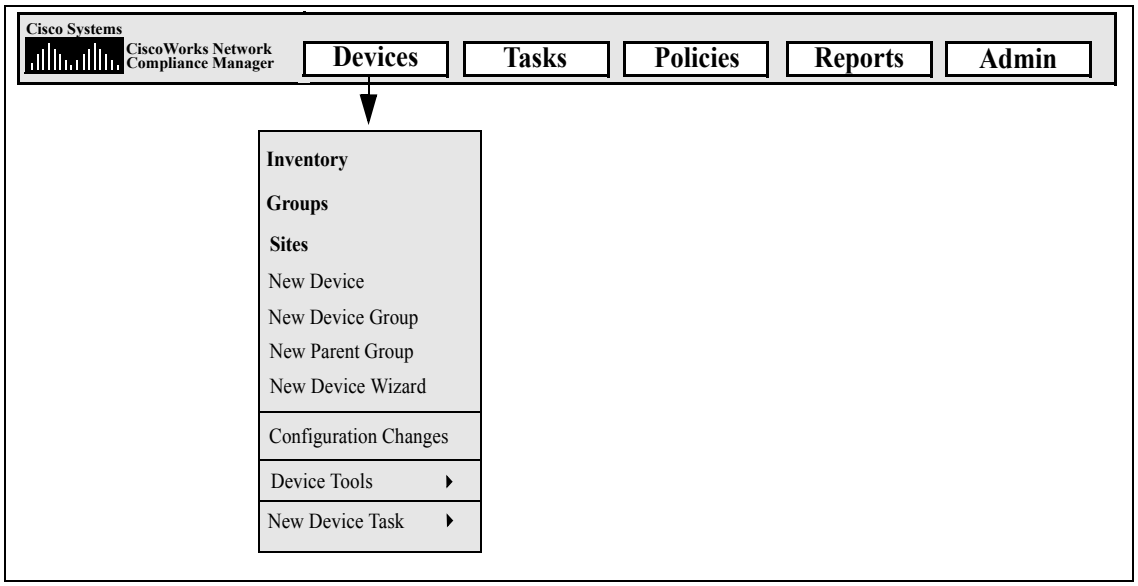
Field	Description/Action
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Links	You can select the following links: • View Configuration • Edit Configuration • All Pending Deploy Config Tasks For This Device • Cancel All Pending Deploy Config Tasks

Be sure to click Save Task when you are finished.

Chapter 5: Viewing Devices

Use the following table to quickly locate information.

Navigating to Device Information



Viewing Devices

To view a list of the managed devices, on the menu bar under Devices click Inventory. Inventory is the default working group. It lists all of the currently managed devices. Refer to "Adding Devices" on page 134 for information on adding new devices.

Inventory Page Fields

Field	Description/Action
Groups link	Opens the Device Groups page, where you can view a list of current device groups. Refer to "Viewing Device Groups" on page 220 for information.
New Device link	Opens the New Device page, where you can add a new device. Refer to "Adding Devices" on page 134 for information.
New Group link	Opens the New Device Group page, where you can add a new device group. Refer to "Adding Device Groups" on page 149 for information.
New Parent Group link	Opens the New Parent Group page, where you can add a new Parent group. Refer to "Adding Parent Groups" on page 152 for information.
Current Working Group	Displays Inventory, the default group. You can select a different group from the drop-down menu, if applicable.
List active devices only check box	Check this box if you want the inventory list to include only active devices. Inactive devices are not actively managed.
Run Task on this Group	You can select a task from the drop-down menu to run on this group. Refer to "What Are Tasks?" on page 278 for information on running tasks.

Field	Description/Action
Check Boxes	You can use the left-side check boxes to manage devices. Once you have selected devices, click the Actions drop-down menu. Options include: • Activate — Instructs NCM to manage the selected devices. • Deactivate — Instructs NCM not to manage the selected devices. • Batch Edit Device — Opens the Batch Edit Device page, where you can assign a driver and set the connection methods for all the selected devices at once. Refer to "Batch Edit Device Page Fields" on page 191 for information. • Delete — Deletes the selected devices. • Select a task to run against the checked devices. Refer to "Running Tasks Against Ad-hoc Device Groups" on page 278 for information. The adjacent Select drop-down menu enables you to select or deselect all of the devices.
Host Name	Displays the host name of the device. Devices in red failed the last snapshot attempt. Inactive devices are marked with an icon beside the IP address. Clicking the Host Name link opens the Device Details page, where you can view basic information about the device and its configuration history. Refer to "View Menu Options" on page 229 for information on the Device Details page.
Device IP	Displays the IP address of the device. Clicking the Device IP link opens the Device Details page, where you can view basic information about the device and its configuration history. Refer to "View Menu Options" on page 229 for information on the Device Details page.
Device Vendor	Displays the device manufacturer's name.
Device Model	Displays the device's model designation.
Site	Displays the site to which the device belongs. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

Field	Description/Action
Actions	You can select the following actions for each device: • Edit — Opens the Edit Device page, where you can edit the information for this device. • Telnet — Opens a Telnet window. • SSH — Opens an SSH window. • View Config — Opens the Current Configuration page, where you can view the latest configuration, deploy to running configuration, and/or add comments.

Viewing Device Groups

A device group is a method for categorizing your devices in ways that make sense for your organization, for example:

- Geography/physical location
- Business unit/department
- Role in the network architecture
- Activation state

Once created, device groups can be used to direct various features, such as searching, authenticating rules, and updating passwords.

Initially, the Device Groups page includes one system group: the Inventory group. The Inventory group contains all devices. However, any user-defined groups you create also appear on this page.

To view a list of the device groups, on the menu bar under Devices, click Groups. The Device Groups page opens. Keep in mind that Public device groups are visible to all users. Private device groups are visible only to the owner and NCM administrators.

Device Groups Page Fields

Field	Description/Action
New Group link	Opens the New Device Group page, where you can create a new device group. Refer to "Adding Device Groups" on page 149 for information on creating new device groups.
New Parent Group link	Opens the New Parent Group page, where you can add a new Parent group. Refer to "Adding Parent Groups" on page 152 for information.
Group Name	Displays the user-defined name of the device group. Parent groups are not indented unless they are also children of other Parent groups. Groups that belong to a Parent group are indented beneath their parent. Clicking a group name opens the Device Group page, where you can view detailed information about the device group. Refer to "Device Groups Page Fields" on page 220 for information. (**Note**: Group names that are preceded by the cloud icon are included in Partitions. Refer to "Segmenting Devices and Users" on page 163 for information on Partitions.)

Field	Description/Action
Description	Displays a brief description of the group.
Number of devices	Displays the number of devices in the group.
Owner	Displays the user name that created the device group.
Sharing	Displays whether the device group is Public or Private. All users can see Public device groups, while only the owner and the System Administrator can see Private device groups.
Actions	The Actions field for the Inventory group is empty until you select a Group Name. User-defined device groups display the following actions: • Edit — Opens the Edit Group page, where you can edit the information for the device group. • Delete — Enables you to delete the device group. • Make Private/Make Public — Enables you to designate the device group as Public or Private. All users can see Public device groups, while only the owner and the System Administrators can see Private device groups.

Reserving Devices

For organizations with large networks, managing who is working on which devices and at what times is important. The Device Reservation System enables you to reserve a device or a group of devices for a specific period of time. Device Reservation conflict notification prevents you from accidentally working on devices that are already under maintenance and allows a large IT group to schedule and work on the network in a controlled, organized fashion. (Refer to "Workflow" on page 86 for information on configuring the Device Reservation System and the Activity Calendar.)

Keep in mind that devices and/or device groups affected by sub-tasks of a multi-task project are automatically reserved for the duration of the tasks. In addition, when a multi-task project is approved, and one or more scheduled tasks include the following read-write tasks (see below), a check is done to determine if the read-write task affects a currently reserved device. If it does, a device reservation conflict event is created. A device reservation conflict does not prevent you from running the task against the device or device group, however.

- Deploy Configuration
- Run Command Script
- Deploy Passwords
- Reload Device
- Synchronize Startup and Running
- Update Device Software

If a multi-task project reserves a device or group of devices, you are informed when a device configuration change is detected on any of the devices.

For information on setting up multi-task projects, refer to "Scheduling Multi-Task Projects" on page 360.

Activity Calendar

The Activity Calendar enables you to view the activity that is taking place on your network. It provides a list of the tasks and device reservations that have been scheduled for any given day, including:

- All tasks scheduled to run on the day being viewed.
- The start time and date of the task.
- The duration of the task.
- The reserved devices and/or device groups on which the tasks are being run against.
- If the task has an uncleared Device Reservation Conflict event.

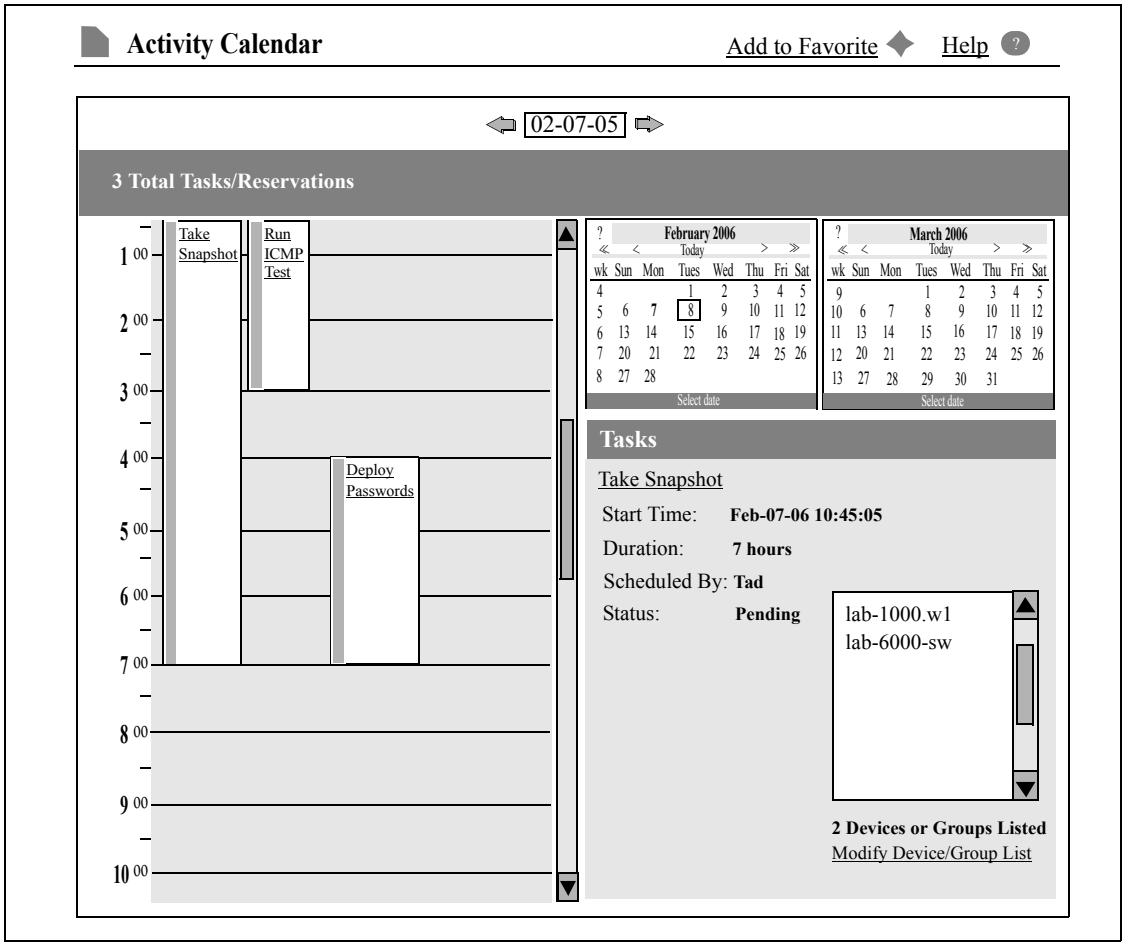
All task blocks start and end on hour or half hour demarcations. Consequently, if a task starts at 22 minutes after the hour, it will be displayed within the row that represents the hour.

The left-hand calendar displays the current month. The right-hand calendar displays the next month. The selected day is highlighted on the appropriate calendar. You can select a specific day by clicking the day listed on the calendar. The page is re-drawn with the appropriate day's events.

Task Details are displayed below the calendars in the right-hand pane. The following task information is provided:

- Start time
- Duration
- The name of the user who scheduled the event
- The status of the event, for example Pending, Running, and Success.

To view the Activity Calendar, on the menu bar under Tasks, click Activity Calendar. The Activity Calendar opens. The following figure shows a sample Activity Calendar display.



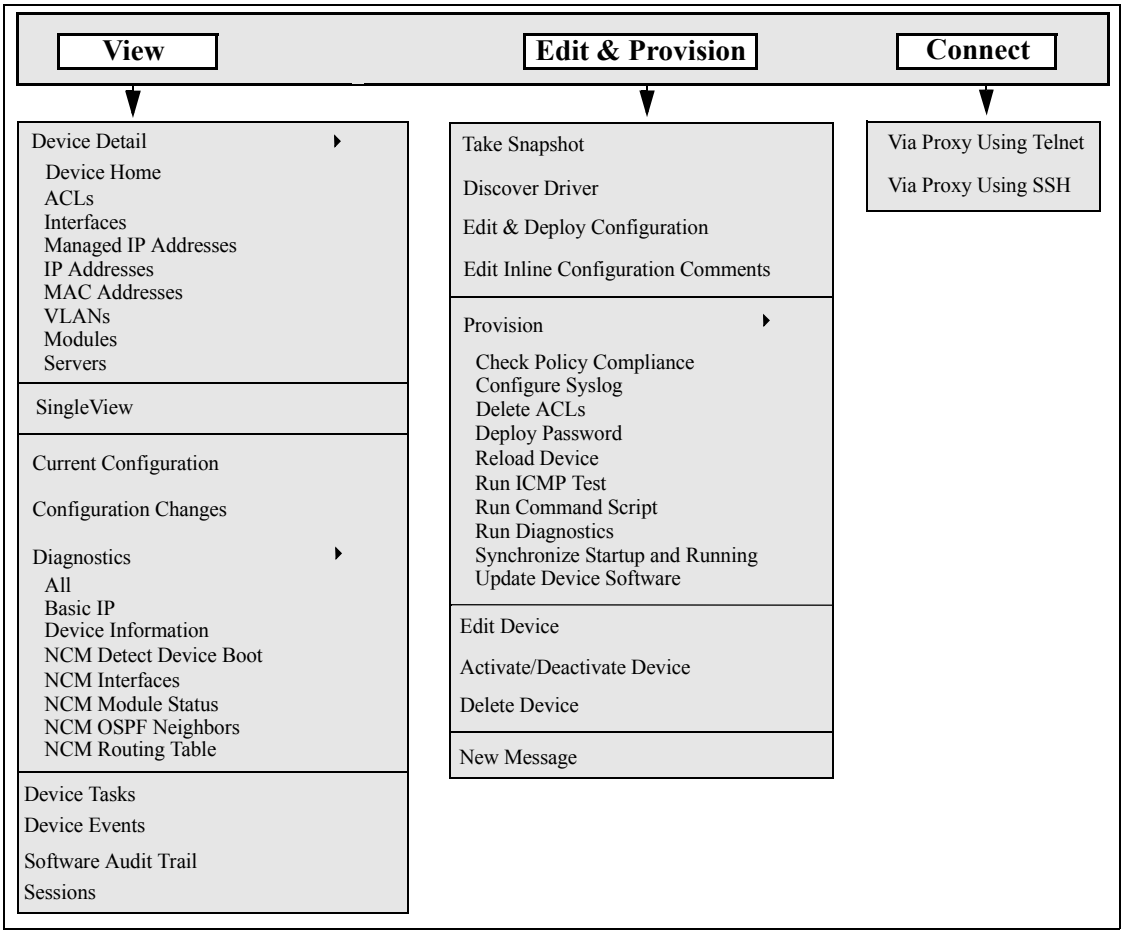
If you click the link displayed in a cell, the information in the Tasks panel is updated. If a multi-task project has an uncleared device reservation conflict, the cell is highlighted in yellow. For information on configuring a multi-task project, refer to "Scheduling Multi-Task Projects" on page 360.

Viewing Device Details

The Device Details page enables you to perform device-specific tasks. To view the Device Details page:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, click a device. The Device Details page opens for that device. (Keep in mind that you can view the Device Details page from most other pages using the Search feature.)

The following figure provides an overview of the tasks you can perform from the Device Details page.



Device Details Page Fields

Field	Description/Action
Hostname	Displays the device's host name. Clicking the device's host name opens the Device Details page, where you can view information about this device.
Device IP	Displays the device's IP address. Clicking the device's IP address opens the Device Details page, where you can view information about this device.
Last Access Time	Displays the date and time the device was last accessed via NCM (such as taking a snapshot or deploying a configuration).
Last Snapshot Result	Displays the status of the last snapshot of this device's configuration. If the snapshot failed, there is a link to that Task Result page.
Watch Device Link	If you click the Watch Device option for the first time, a Watch Group is created, along with a Watch Devices event rule, that includes the device. Any changes to the device will trigger an email notification for the user watching the device. The Watch Devices event rule will send an email notification for a variety of events, such as: • Device Access Failure • Device Booted • Device Configuration Change • Device Deleted • Device Diagnostic Changed • Device Edited • Device Software Change • Software Vulnerability Detected **Note**: You can edit the Watch Devices event rule to change events. All future watched devices will use the same event rule name. Refer to "New Event Notification & Response Rules Page Fields" on page 436. To remove a device from the Watch Group, click Stop Watching Device.
View menu	Opens the View menu. Refer to "View Menu Options" on page 229 for information.

Field	Description/Action
Edit & Provision menu	Opens the Edit & Provision menu. Refer to "Device Events Page Fields" on page 233 for information.
Connect menu	Opens the Connect menu. Refer to "Connect Menu Options" on page 248 for information.
Device Description	Displays the user defined description of the device, if applicable.
Comments	Displays the user-defined comments about the device. If you want to add comments, enter comments in the Comments box and click Update Comment.
Vendor	Displays the device vendor, such as Nortel or Cisco.
Model	Displays the manufacturer's model number.
Software Version	Displays the version of operating system software running on the device.
Driver Name	Displays the driver assigned to the device.
Device Type	Displays the type of device, such as a router, switch, or firewall.
Serial Number	Displays the manufacturer's serial number for the device.
Asset Tag	Displays your company's asset tag number for the device.
Location	Typically, the location is obtained in the Configuration file.
Device Origin	Displays the name of the import source if the device was imported into NCM and the source was named. If the import source was not named, it states Added to NCM on <date>. If the device was added manually, it states Manually added by <user name> on <date>.
Last Successful Snapshot	Displays the date and time the last snapshot succeeded.
Last Configuration Change	Displays the date and time the device's configuration was last changed.
Change Detection & Polling	Displays either: • Enabled — Indicates that NCM periodically polls the device to verify the stored configuration against the device's actual configuration. • Disabled — Indicates the device is not polled periodically or otherwise managed by NCM.

Field	Description/Action
Management Status	Displays either: • Active — Indicates that NCM records changes to the device's configuration. • Inactive — Indicates that NCM does not record changes and that you cannot change the device through NCM.
Ticket Number	Displays the ticket number, if applicable. You can click the Update Ticket button to update the ticket if you have installed one of the NCM Connectors.

View Menu Options

Menu Option	Description/Action
Device Detail	You can select the following options: • Device Home — Opens the Device Details page for that device. • ACLs — Opens the Device ACLs page, where you can view a list of all ACLs associated with this device. Refer to "Viewing ACLs" on page 706 for information. • Interfaces — Opens the Device Interfaces page, where you can view the device's interfaces and a list of upstream and downstream devices connected via each interface. When a connected device is actively managed, there is a link to that device. This enables you to traverse the Layer 3 topology when troubleshooting without having to look up your network diagrams. (**Note**: The Device Interfaces page is updated when you run the Interfaces diagnostic. By default, this diagnostic runs when NCM detects a configuration change.) Refer to "Device Interfaces Page Fields" on page 234 for information. • Managed IP Addresses — Opens the Device Managed IP Addresses page, where you can view and modify all IP addresses that might be used to access the device. Keep in mind that there must be one primary IP address that uniquely identifies each device. However, you can add alternate IP addresses to increase the odds that NCM can connect to the device. Alternate IP addresses reduce administration overhead and increase the quality of device data. (**Note**: If NCM fails to access a device by the primary IP address, it tries the alternate addresses in the order listed. To ensure network efficiency, move the IP addresses that are most likely to be accessed to the top of the list.) Refer to "Device Managed IP Addresses Page Fields" on page 236 for information.

Menu Option	Description/Action
Device Details (*Cont.*)	• IP Addresses — Opens the Device IP Addresses page, where you can view all IP addresses that are associated with the device. This includes the IP addresses of interfaces on the device, as well as IP addresses on the network that are visible to the device. Refer to "Device IP Addresses Page Fields" on page 237 for information. • MAC Addresses — Opens the Device MAC Addresses page, where you can view a list of all MAC addresses known to NCM that are associated with the device. Refer to "Device MAC Addresses Page Fields" on page 238 for information. • VLANs — Opens the VLANs page, where you can view VLAN information as it is configured on the device. Refer to "Device VLANs Page Fields" on page 239 for information. • Modules — Opens the Device Blade/Modules page, where you can view a list of the modules (blades, cards) installed on the device. By default, the module data is updated weekly by the Module Status diagnostic. Refer to "Device Blades/Modules Page Fields" on page 240 for information. • Servers — Opens the Servers page, where you can view a list of servers that are connected to the device. Refer to "Servers Page Fields" on page 241 for information.
SingleView	Opens the SingleView page, where you can track events that indicate changes to either a single device or all of your devices on one page. Refer to "Consolidated View of Events (SingleView)" on page 528 for information.
Current Configuration	Opens the Current Configuration page, where you can deploy the configuration to the running configuration on the device. Refer to "Device Configurations Page Fields" on page 204 for information.
Configuration Changes	Opens the Device Configurations page, where you can view two device configurations side-by-side. Refer to "Comparing Device Configurations" on page 209 for information.

Menu Option	Description/Action
Diagnostics	Select an option from the Diagnostics list. Each option shows a historical list of diagnostics specific to the device. The most frequently employed diagnostics include: • All — Displays all of the diagnostics on one page. • Basic IP — Displays the basic IP information, such as the default gateway, DNS servers, Domain list, and the IP addresses assigned to installed interfaces. • Memory Troubleshooting — This diagnostic is a sample custom diagnostic that is implemented for some devices. It is included as a standard diagnostic after a device configuration change. • Device Information — Displays basic device information, such as software and hardware versions, the model and host name of the device, and interface descriptions. Although this information appears with the default diagnostics, it is updated only when NCM runs a snapshot task on the device. • NCM Detect Device Boot — Displays information on when the device was last booted. • NCM Device File System — Records what files (generally software image files) are currently on the device's flash cards or hard drive. This data is used by the Deploy Software task. • NCM Flash Storage Space — This diagnostic is special-purpose diagnostic used only against Nortel BayRS devices to trigger a low-flash space event, which then causes a compression script to run. • NCM Interfaces — Displays the interfaces information for the device, such as state, IP address, errors, I/O rate, and VLAN information. • NCM Module Status — Displays the module diagnostics for this device. • NCM OSPF Neighbors — Displays a list of the OSPF neighbor tables stored in the NCM database. • NCM Routing Table — Displays all the routing tables for this device stored in the NCM database. If BGP is running, it shows the Routing Table summary information, when available. • NCM Topology Data Gathering — This diagnostic is used to populate the tables used for diagramming and topology reports. It does not have any viewable diagnostic output.

Menu Option	Description/Action
Device Tasks	Opens the Device Tasks page, where you can view a list of all tasks associated with this device. You can also view details about the task or rerun the task from this page. Refer to "Device Tasks Page Fields" on page 242 for information on the Device Tasks page.
Device Events	Opens the Device Events page, where you can view recent system events for the device, including their success/failure status, and access detailed information about the event by clicking the link in the Summary field. Refer to "Device Events Page Fields" on page 233 for information on the Device Events page fields.
Software Audit Trail	Opens the Device Software Audit Trail page, where you can view what software is loaded on the device. Refer to "Device Software Audit Trail Page Fields" on page 243 for information on the Device Loaded Software page fields.
Sessions	Opens the Device Session page, where you can view a list of the Telnet and SSH sessions associated with the device. Sessions can include only the commands or the keystroke logging for the entire session. Refer to "Device Sessions Page Fields" on page 245 for information on the Device Session page fields.

Keep in mind that most of the NCM diagnostics are standard diagnostics that are shipped with the product and cannot be edited, with the exception of the following sample diagnostics:

- Memory Troubleshooting
- Hardware Information

Device Events Page Fields

The Device Events page enables you to view recent system events for the device, including their success/failure status, and access detailed information about the event.

Field	Description/Action
Check Boxes	You can use the left-side check boxes to delete selected events. Once you have selected events, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all of the events.
Date	Displays the date and time the event occurred.
Summary	Displays a brief summary of the event. If you click the Summary link, the Event Detail page opens, where you can view detailed information about the event.
Added By	Displays the person or process that initiated the event.

Device Interfaces Page Fields

The Device Interfaces page enables you to view the device's interfaces and a list of upstream and downstream devices connected via each interface. Keep in mind that although a Port is a Layer 2 term and Interface is a Layer 3 term, NCM does not make that distinction.

Field	Description/Action
Port Name	Displays the name of the port, such as Ethernet0 or Serial1.
Port Status	Displays if the interface is Configured Up or Administratively Down. (**Note**: This does not reflect the protocol state of the interface, only the configured state.)
IP Address	Displays the primary IP address for the interface. NCM parses the IP address from the device configuration.
Description	Displays a brief description of the interface. NCM parses the description from the device configuration.
Actions	You can select the following actions for each interface: • Edit Interface — Opens the Edit Interface page, where you can edit the details about this interface and any custom data fields. • View Interface — Opens the Interface Detail page, where you can view details about this interface and custom data, view alternate IP addresses, the connected servers, and view or edit comments. Refer to "Interface Detail Page Fields" on page 235. • Interfaces in Subnet — Opens the Device Interfaces page, where you can view all the interfaces in the same subnet as this interface. This enables you to traverse the devices linked within the subnet, as long as the devices are actively managed.

Interface Detail Page Fields

The Interface Detail page enables you to view details for a specific interface. Keep in mind that although a Port is a Layer 2 term and Interface is a Layer 3 term, NCM does not make that distinction.

Field	Description/Action
Device	Displays the name and IP address of the device.
Name	Displays the interface name, for example: Ethernet0/1
Type	Displays the type of interface, for example: Ethernet
Status	Displays the status of the interface, for example: Configured Up
Primary IP	Displays the interface's Primary IP address. If you click the Interfaces in Subnet link, the Device Interfaces page opens, where you can view all the interfaces in the same subnet as this interface. This enables you to traverse the devices linked within the subnet, as long as the devices are actively managed.
Description	Displays a description of the interface.
MAC Address	Displays the MAC address of the interface, for example: 00-50-10-F6-41
Duplex	Network interfaces identify the Ethernet port, speed, duplex settings, devices connected, and VLAN name. A duplex mismatch is a configuration mismatch between the speed and duplex of a managed server and a connected network device.
Speed	Network interfaces identify the Ethernet port, speed, and duplex settings, devices connected, and VLAN name. A duplex mismatch is a configuration mismatch between the speed and duplex of a managed server and a connected network device.
Configuration	Displays the current configuration of the interface. If you click the View Configuration link, the Current Configuration page opens.
Comments	Displays any comments about the interface. If you click the Edit Detail link, the Edit Interface Detail opens.

Device Managed IP Addresses Page Fields

The Managed Device IP Addresses page enables you to view and modify all IP addresses that might be used to access the device. Keep in mind that there must be one primary IP address that uniquely identifies each device.

Field	Description/Action
New IP Address link	Opens the New IP Address page, where you can add new IP addresses. It is recommended that when using NAT or other addressing schemes you add IP addresses that are not automatically detected by NCM. The addresses you add here are labeled "custom".
IP Address	Displays the device's IP address, either Primary, Alternate, or Custom.
Use To Access Device	Displays Yes or No. NCM tries to access the device first by its primary IP address, then by its console server address (if any), and finally by any alternate IP addresses that states Yes in this field (No is the default).
Type	Displays the type of IP address: Primary, Alternate, or Custom. The IP Address from the New/Edit Device page is always the primary IP address. Additional IP addresses detected are alternate addresses. If IP addresses are added using the New IP Address link, they are considered custom IP addresses.
Actions	You can select the following actions for each device: • Edit — Opens the Edit IP Address page, where you can modify the IP address and subnet mask, insert the new IP address before the primary IP address for a new access order, and comment the change. • Move Up — When multiple alternate IP addresses appear in the list, this option moves the IP address up in the list. NCM tries the alternate addresses in the order listed. • Move Down — When multiple alternate IP addresses appear in the list, this option moves the IP address down in the list. NCM tries the alternate addresses in the order listed.

Device IP Addresses Page Fields

The Device IP Addresses page enables you to view all IP addresses that are associated with the device. This includes the IP addresses of interfaces on the device, as well as IP addresses on the network that are visible to the device.

Field	Description/Action
Port Name	Displays the port name associated with the device's IP address.
IP Address	Displays the IP address.
Type	Displays the description of the IP address, for example: "Address of Port" or "Seen from Port".
VLAN ID	Provides a link to the VLAN, if any, containing this IP address if the type is "Address of Port".
Remote Location	Provides links to the remote location if the type is "Seen from Port". The remote location is a device and port known to NCM.
First Seen	Displays the date and time the IP address was first identified.
Last Seen	"Current" is displayed if the IP address was seen the last time NCM gathered topology data. If not current, this is the date and time when NCM last saw the IP address on the network. Keep in mind that the IP address is possibly no longer on the network, for example an IP address of a laptop or other transient device. In addition, the routing traffic could change such that the IP address is no longer in the main flow.
Actions	You can select the following actions for each device: • View Details — Opens the IP Address Details page, where you can view details on the following information: Device, Device Port, IP address, Type, First Seen, and Last Updated. • View MAC - Opens the MAC address details page that is cross-referenced with this IP address. Cross-referencing means that when NCM gathers data, the IP address and MAC address were indicated as coming from the same source. This is only available on "seen from port" records.

Device MAC Addresses Page Fields

The Device MAC Addresses page enables you to view a list of all MAC addresses that are associated with the device.

Field	Description/Action
Port Name	Displays the port name associated with the device's IP address.
MAC Address	Displays the device's MAC address.
Type	Displays the description of the MAC address, for example: "Address of Port" or "Seen from Port".
VLAN ID	Provides links to the VLAN, if any, containing this MAC address if the type is "Address of Port".
Remote Location	Provides links to the remote location if the type is "Seen from Port". The remote location is a device and port known to NCM. This could alternately be a server and interface.
First Seen	Displays the date and time the MAC address was first identified.
Last Seen	"Current" is displayed if the MAC address was seen the last time NCM gathered topology data. If not current, this is the date and time when NCM last saw the MAC address on the network. Keep in mind that the MAC address is possibly no longer on the network, for example a MAC address on a laptop or other transient device. In addition, the routing traffic could change such that the MAC address is no longer in the main flow.
Actions	You can select the following actions for each device: • View Details — Opens the MAC Address Details page, where you can view details on the following information: Device, Device Port, MAC address, Type, First Seen, and Last Updated. • View MAC - Opens the MAC address details page that is cross-referenced with this IP address. Cross-referencing means that when NCM gathers data, the IP address and MAC address were indicated as coming from the same source. This is only available on "Seen from Port" records.

Device VLANs Page Fields

The Device VLANs page displays a list of all ports on the device that are configured as part of a VLAN on that device.

Field	Description/Action
Port Name	Displays the port belonging to the VLAN. If you click the port, the Interface Detail page opens. Refer to "Interface Detail Page Fields" on page 235.
VLAN ID	Displays the name of the VLAN. If you click the VLAN ID, the Interface Details page opens to show the full details of the VLAN configuration. Refer to "Device Interfaces Page Fields" on page 234.
VLAN Description	Displays information about the VLAN pulled from the device.

Device Blades/Modules Page Fields

The Device Blade/Modules page list of the modules (blades, cards) installed on the device. By default, the module data is updated weekly by the Module Status Diagnostic task.

Field	Description/Action
Slot	Displays the slot on the device in which the module is installed.
Description	Displays a brief description of the module. NCM parses the description from the device configuration.
Model	Displays the model identifier.
Serial	Displays the module's serial number.
Actions	You can select the following actions for each module: • Edit Module — Opens the Edit Blade/Module Detail page, where you can view the module inventory details and edit the custom data fields. • View Module — Opens the Blade/Module Detail page, where you can view the module inventory details and edit the comments.

Servers Page Fields

The Servers page displays the name of each server that is connected to the device on which you are displaying details. If you click a server's hostname, the Server Detail page opens. Keep in mind that NCM only infers the location of Layer 1 wiring. NCM's reduction algorithm reduces (as best it can) all connections between devices and/or servers.

Field	Description/Action
Network Device Interface	The network device interface used by the server, for example FastEtherner1/0.
Server Host Name	Displays the server's host name. Clicking the server's hostname opens the Server Detail page.
Server Interface	The server interface name as reported by the operating system.
Customer	Displays the customer name.
Facility	Displays the customer's facility.
Server Use	Displays server use.
Deployment Stage	Displays the Deployment Stage.

Device Tasks Page Fields

The Device Tasks page lists of all tasks associated with the device. You can also view details about the task or rerun the task from this page.

Field	Description/Action
Refresh this page every 60 seconds	Uncheck this box if you do not want the display to refresh every 60 seconds. Refer to "User Interface Page Fields" on page 89 for information on setting this value.
Check Boxes	You can use the left-side check boxes to delete selected tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all of the tasks.
Scheduled Date	Displays the date and time the task ran or is scheduled to run.
Task Name	Clicking the task name opens the Task Information page, where you can view task details, such the originator of the task, when the task was created, and the devices affected by the task. You can also view detailed task history information.
Task Status	Displays the status of the task. Statuses include: • Succeeded — The task succeeded. • Failed — The task failed. • Duplicate — The task duplicated another task, therefore it did not run. • Skipped — The task was skipped because an identical task was already running when the time arrived for this task to run. • Warning — A group task containing some failed sub-tasks, but not all tasks failed.
Scheduled By	Displays the login name of the person who scheduled the task (or the last user to modify the task).
Comments	Displays comments about the task.
Actions	You can select the following actions for each task: • Detail — Opens the Task Detail page, where you can view details about the task. • Run Again — Opens the Edit Task page, where you can edit and rerun a task. This link appears only when you can rerun the task.

Device Software Audit Trail Page Fields

The Device Software Audit Trail page enables you to view what software is currently loaded on a device.

Field	Description/Action
Hostname	Displays the device's hostname. Clicking the device's hostname opens the Device Details page, where you can view information about the device.
Device IP	Displays the device's IP address. Clicking the device's IP address opens the Device Details page, where you can view information about the device.
Last Access Time	Displays the date and time the device was last accessed (such as taking a snapshot).
Last Snapshot Result	Displays the status of the last snapshot of the device's configuration. If the snapshot failed, there is a link to the Task Result page.
View menu	Opens the View menu. Refer to "View Menu Options" on page 229 for information.
Edit & Provision menu	Opens the Edit & Provision menu. Refer to "Device Events Page Fields" on page 233 for information.
Connect menu	Opens the Connect menu. Refer to "Connect Menu Options" on page 248 for information.
Change Date	Displays the date and time the software was last deployed.
Changed By	Displays the name of the person who last deployed the software to the device.
Change To	Displays the current software version running on the device.
Changed From	Displays the software version that was running on the device prior to the software deployment.
Software Compliance	Displays the software compliance rating. Refer to "Adding a New Software Compliance" on page 403 for more information.

Field	Description/Action
Importance	Displays the importance of the compliance rule that was violated, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours (the default). • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Image Set	Displays the name of the last Image Set deployed to the device. An image set is a grouping of images that can be deployed to a device simultaneously. An image set can contains one or more images.

Device Sessions Page Fields

The Device Session page lists the Telnet and SSH sessions associated with the device. Sessions can include only the commands or the keystroke logging for the entire session.

Field	Description/Action
Start Date	Displays the date the session began.
End Date	Displays the date the session ended.
Status	Displays if the session is Open or Closed.
Type	Displays if the session is via Telnet or SSH.
Created By	Displays the login name of the person who opened the session.
Actions	You can select the following actions for each session: • View Session — Opens the Telnet/SSH Session page, where you can view the commands and system responses for that session. There is also a link to the configuration (if any) created by this session. • View Commands Only — Opens the Telnet/SSH Session page, but limits the display to only the commands entered during the session. This can be useful when you want to create a script from the commands.

Edit & Provision Menu Options

Menu Option	Description/Action
Take Snapshot	Opens the New Task - Snapshot page. The Snapshot task enables you to schedule a snapshot. A snapshot refreshes the copy of the device configuration and related data stored in the NCM database. Specifically, a snapshot checks whether the stored configuration matches the running configuration on the device. If not, the snapshot task replaces the copy of the device configuration and related data stored in the NCM database. Refer to "Take Snapshot Task Page Fields" on page 314 for more information.
Discover Driver	Opens the New Task - Discover Task page. Driver discovery creates a task to check whether a driver is assigned to the device. If not, discovery overwrites the current driver with the most appropriate driver in the NCM database. (**Note**: NCM requires a driver to communicate with each device.) Refer to "Discover Driver Task Page Fields" on page 289 for information.
Edit & Deploy Configuration	Opens the Edit Configuration page with the current configuration, where you can edit the configuration and then deploy it. When you click the "Deploy to Device" option, you can schedule a configuration deployment or initiate an immediate configuration deployment. NCM will deploy the configuration change to the device and capture the resulting configuration. The Task Result page for this task will automatically refresh while the task runs. Refer to "Deploy Config Task Page Fields" on page 212 for information.
Edit Inline Configuration Comments	Opens the Edit Configuration page, where you can enter comments, often times prefixed with two exclamation points (!!). Keep in mind that the persistent comment character is only two characters. However, some devices use multiple comment characters as delimiters. This can cause the comment engine to have difficulties parsing persistent comments.

Menu Option	Description/Action
Provision	You can select from the following options: • Check Policy Compliance — Opens the New Task - Check Policy Compliance page, where you can view devices whose configurations and software are or are not in compliance with current policies. Refer to "Check Policy Compliance Task Page Fields" on page 342. • Configure Syslog — Opens the New Task - Configure Syslog page, where you can automatically configure Syslog on this device for real-time change detection. Refer to "Resolve FQDN Task Page Fields" on page 351. • Delete ACLs — Opens the New Task - Delete ACLs page, where you can delete ACLs. Refer to "Deleting ACLs" on page 719. • Deploy Password — Opens the New Task - Deploy Passwords page, where you can setup a task to deploy password changes to the device. Refer to "Deploy Passwords Task Page Fields" on page 284. • Reload Device — Opens the New Task - Reload Device page, where you can reload devices into the NCM database. Refer to "Reload Device Task Page Fields" on page 293. • Run Command Script — Opens the New Task - Run Command Scripts page, where you can edit and schedule a command script for the device. Refer to "Run Command Script Task Page Fields" on page 302. • Run Diagnostics — Opens the New Task - Run Diagnostics page, where you can schedule diagnostics for the device. Refer to "Run Diagnostics Task Page Fields" on page 309. • Synchronize Startup and Running — Opens the New Task - Synchronize Startup and Running page, where you can synchronize the startup and running of configurations for a device. Refer to "Synchronize Startup and Running Task Page Fields" on page 318. • Update Device Software — Opens the New Task - Update Device Software page, where you can schedule the deployment of software to one or more devices. Refer to "Update Device Software Task Page Fields" on page 322.
Edit Device	Opens the Edit Device page, where you can edit the information for the device. Refer to "Adding Devices" on page 134 for information.

Menu Option	Description/Action
Activate/Deactivate Device	Manages or unmanages the device.
Delete Device	Opens a dialog box, where you can confirm that you want to remove the device entirely from the NCM database. If you permanently delete a device from the NCM database, you will lose the configuration history for that device. Instead, consider editing the device to make it inactive, which preserves the configuration history.
New Message	Opens the New Message page, where you can post a message to all NCM users referring to this device. You can also track the event using SingleView. Refer to "Consolidated View of Events (SingleView)" on page 528 for information.

Connect Menu Options

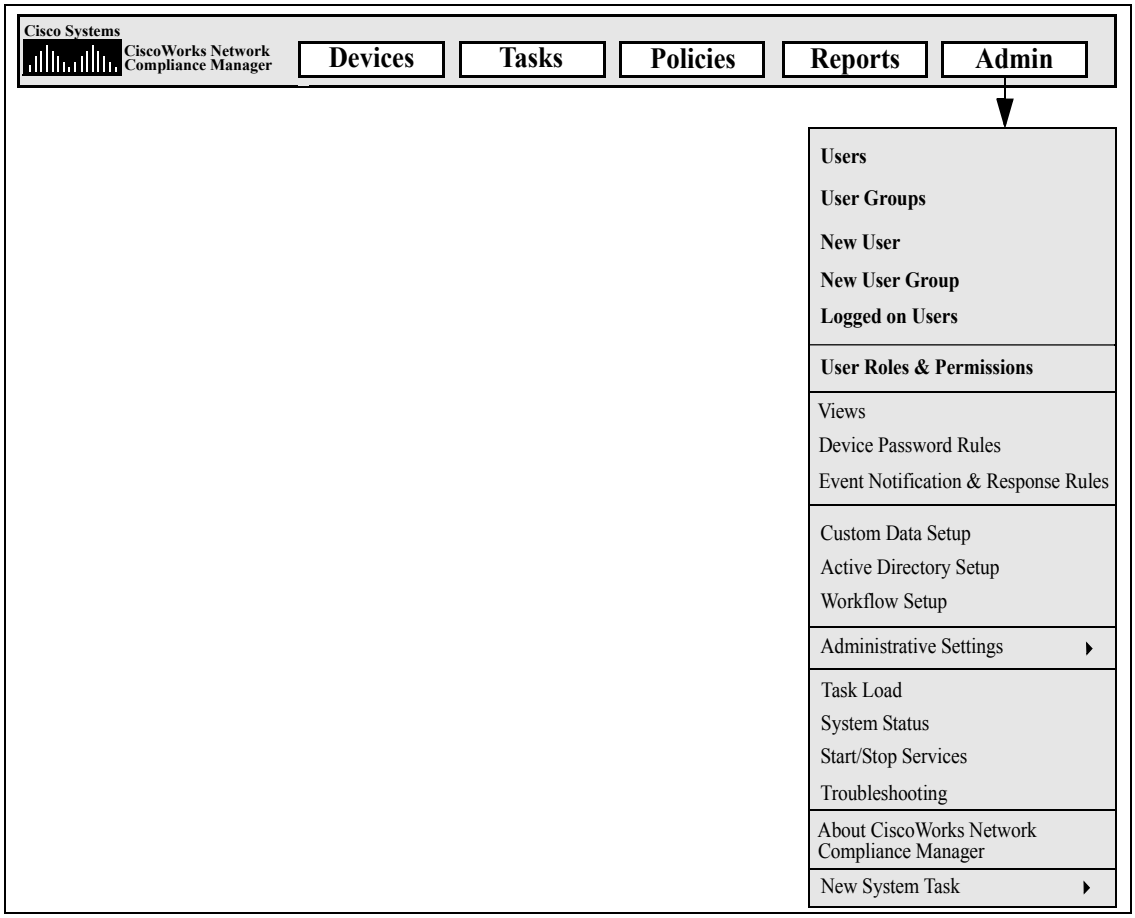
NCM supports single sign-on to network devices using the Telnet or SSH protocol. The NCM server acts as a Telnet/SSH proxy. The data transferred is in clear text format. Keep in mind that if you do not use the NCM server as a Telnet/SSH proxy, you can login directly to the device through a secured URL or by using standard Telnet commands.

Menu Option	Description/Action
Via Proxy Using Telnet	Opens a Telnet window, where you can enter Telnet commands to this device.
Via Proxy Using SSH	Opens an SSH window, where you can enter SSH commands to this device.

Chapter 6: Managing Users

Use the following table to quickly locate information.

Navigating to Managing Users



Adding Users

Designing user authentication and authorization is a challenging task. The choices you make affect how CiscoWorks Network Compliance Manager (NCM) is used. Adopting a proper authentication and authorization design helps alleviate many security risks.

Best practices in both information security and IT departments generally include the concept of “least privilege”, which means that each user should be assigned the least amount of rights necessary to perform their job duties. In addition, the nature of some organizations creates an environment where it is appropriate for the tasks that each user can perform to be separated by each user’s role.

The following terms are used in this section:

- Role - Roles are used to partition users into groups that share the same security privileges. A user assigned to a role is granted permissions defined by the role. For example, if a user is authorized to perform certain operations, such as adding devices, managing configuration policies, or deploying software, NCM uses fixed role identities with which to access resources.Creating a new user role from scratch, rather than using an existing role as a starting point, creates a template with default deny permissions on every action type. This allows roles to be easily created in line with the “least privilege” security best practice.
- User Group — A user group is a logical container for the purpose of user management. The System Administrator can assign users to user groups, which in turn map to specific roles. Keep in mind that a user group can be assigned one or more roles.
- Protected Entity — Protected entities are devices and custom scripts that are subject to extra permission checks.

To add a new user, on the menu bar under Admin click Users. The All Users page opens. When you are first adding users, this page is empty except for your Admin account information.

All Users Page Fields

Field	Description
New User link	Opens the New User page, where you can add users. Refer to "New User Page Fields" on page 254 for information. Keep in mind that only the System Administrator can add users.
Search for Users link	Opens the Search For Users page, where you can search for users by first name, last name, email address, and/or AAA user name. Refer to "Searching for Users" on page 495 for information.
Logged on Users link	Opens the Logged On Users page, where you can view who is currently logged in, including their user name, user host, and the last access time. Keep in mind that this only shows users who logged in using the Web UI, not the Command Line Interface (CLI). (NOTE: You can also select the Logged On Users option from the Admin drop-down menu to view this page.)
User Groups link	Opens the User Groups page, where you can add and edit user groups. Refer to "User Groups Page Fields" on page 256 for information.
User Roles & Permissions link	Opens the User Roles & Permissions page, where you can edit user permissions. Refer to "User Roles & Permissions Page Fields" on page 261 for information.
Users in this group	Displays the following icons: • Regular User Account • Disabled User Account
User Name	Displays the user's full name.
First Name	Displays the user's first name.
Last Name	Displays the user's last name.
Email	Displays the user's email address.

Field	Description
Actions	You can select the following options: • Edit — Opens the Edit User page. If the account is your own account, the page is entitled My Profile. You can make changes to your user profile and click save. The changes are shown on the User List page. Refer to "New User Page Fields" on page 254 for information. • Delete —You can delete a user (with Admin privileges). • Permissions — Opens the User Permissions page. If you click the Edit User Profile option at the top of the page, the Edit User page opens. You can make changes to the user profile and click Save. The changes are shown on the User List page. Refer to "New User Page Fields" on page 254 for information. • Config Changes — Opens the Config Search Results page. This page displays what configuration changes, if any, the user made. Refer to "Viewing Device Configuration Changes" on page 203 for information.

New User Page Fields

Field	Description/Action
User Information	
User Name	Enter the NCM user name of the user. This name is used to login to NCM, such as Operator or Administrator. (**Note**: Do not include spaces in the user name.)
User belongs to selected groups	Select one of the following default user groups to which the user belongs. These groups provide user roles and all associated permissions for the user. Keep in mind that NCM does not assign a group by default. A user that does not belong to a group can only perform limited tasks, such as viewing devices and configuration changes. (**Note**: If you created a new group, it is displayed in the list.) • Limited Access User — Limited Access users are typically operators that do not have passwords to configure network devices. While they have permission to view devices, they cannot modify most information in the NCM database, or run batch operations or operations which would reconfigure network devices. • Full Access User — Full Access users are typically network engineers trusted with passwords to configure some, if not all, devices in the network. They have permission to modify most information in the NCM database, and can reconfigure devices one-at-a-time, but not in batch mode. Often times they are restricted as to which devices they have permission to reconfigure. • Power User — Power users are typically expert engineers allowed to perform most actions. They can reconfigure and otherwise act on groups of devices. • Administrator — Administrators are responsible for administering NCM, including managing users, setting policy, and running network-wide operations. They have permission to take any action on any device.
Password	Enter the password for the user. This is the password used when logging into NCM.
Confirm Password	Enter the NCM password of the user for confirmation.
First Name	Enter the first name of the user.

Field	Description/Action
Last Name	Enter the last name of the user.
Email Address	Enter the email address of the user.
Status	Select one of the following options: • Enabled — The account is enabled (the default). • Disabled — The account is disabled. You can use this option to disable an account while still keeping the account on the system.
External Auth Failover	If external authentication fails for this user, you can enable authentication failover to local authentication.
Comments	Enter comments about the account.
AAA	
AAA User Name	Enter the AAA (TACACS+ or RADIUS) username for this user. This enables NCM to associate AAA usernames with NCM usernames.
AAA Password	Enter the AAA password for this user.
Confirm AAA Password	Enter the AAA password again for verification.
Use AAA Login for Proxy Interface check box	If checked, NCM checks the user's AAA credentials when logging the user into the Telnet/SSH Proxy.
SecurID	
After a new user has been added, a link to the Manage Software Tokens page is displayed when you edit the user's information. The Manage Software Tokens page enables you to add Software Token licenses associated with the user's login. Refer to "Adding SecurID Software Tokens" on page 613.	

Be sure to click the Save button when you are finished.

Adding User Groups

To add a new user group, on the menu bar under Admin click User Groups. The User Groups page opens. Keep in mind that by default, a user group will use the most permissive Command Permission as defined by the union of roles applied to the user group. To ensure the appropriate lockdown of permissions, assign the most restrictive roles possible to the user group.

Note: You can also navigate to this page from the All Users page by clicking the User Groups link.

User Groups Page Fields

Field	Description/Action
New User Group link	Opens the New User Group page, where you can add user groups. Refer to "New User Group Page Fields" on page 258 for information.
Users link	Opens the All Users page, where you can edit user groups. Refer to "All Users Page Fields" on page 252 for information.
User Roles & Permissions link	Opens the User Roles & Permissions page, where you can edit user permissions. Refer to "User Roles & Permissions Page Fields" on page 261 for information.
Group Name	Displays the name of the user group. Clicking any of the Group Name links opens User Details page, where you can view all of the current users in the group. Refer to "All Users Page Fields" on page 252 for information on adding users and editing user profiles.
Description	Displays a brief description of the group.
User Roles	Displays the user roles that have been assigned to the group. Clicking a user role opens the User Role Information page, where you can view details about the user role. Refer to "Adding User Roles" on page 261 for information.

Field	Description/Action
Actions	You can select the following options: • Edit — Opens the Edit User Group page. Refer to "User Groups Page Fields" on page 256 for information. • Delete —You can delete the group (with Admin privileges). • Permissions — Opens the View Permissions page. Refer to "New User Group Page Fields" on page 258 for information. • Config Changes — Opens the Config Search Results page. This page displays what configuration changes, if any, the users in the group made. Refer to "Device Configurations Page Fields" on page 204 for information.

New User Group Page Fields

Field	Description/Action
General Information	
Group Name	Enter the name of the user group.
Description	Enter a description of the user group.
Command Permissions	
Existing Command Permission Role	Users in the user group must be explicitly granted the corresponding command permission for every action they attempt to perform. If checked (the default), select one or more of the following options: • Administrator — Administrators are responsible for administering NCM, including managing users, setting policy, and running network-wide operations. They have permission to take any action on any device. • Power — Power users are typically expert engineers allowed to perform most actions. They can reconfigure and otherwise act on groups of devices. • Full Access — Full Access users are typically network engineers trusted with passwords to configure some, if not all, devices in the network. They have permission to modify most information in the NCM database, and can reconfigure devices individually, but not in batch mode. Often times they are restricted as to which devices they have permission to reconfigure. • Limited Access — Limited Access users are typically operators that do not have passwords to configure network devices. While they have permission to view devices, they cannot modify most information in the NCM database, or run batch operations or operations which would reconfigure network devices. **Note**: If you have defined a role other than the default roles, it is displayed in the list.

Field	Description/Action
Customized Command Permission Role	If checked, you can customize command permission roles specific to this user group. For each command, click a button to grant or deny permission to this role. For a complete list of Command permissions, refer to "Appendix B: Command Permissions" on page 741. You can click Grant All to grant permission to all commands. This is useful for Admin users and when you want to deny permission to only a few commands. Click Deny All to deny permission to all commands. By default, all commands are denied. The following icons to the right of certain commands indicate that you may need to modify device permissions or script permissions. • Modify Device Permission required icon — NCM can control permissions on a per-device basis. Modify Device Per Permission specifies whether you can modify a device. You must have Modify Device Permission for the specific device(s) you want to run this command against. See "Modify Device Permissions" below. • Script Permission required icon — NCM can control permissions on a per Command Script basis. Script Permission specifies whether you can run a Command Script. You must have Script Permission for the specific Command Script you want to run. See "Script Permissions" below. **Note**: Custom scripts are presumed to modify device configurations. Therefore, they are checked against the user's Modify Device Config permissions.
Modify Device Permissions	
All Devices	Enables users in the group to modify all devices.
None	No device can be modified. This is the default setting.
Existing Modify Device Permission Role	Enables you to select existing Modify Device permission roles for the users in the group. If there are no existing roles configured, the following message is displayed: No existing roles found.
Customized Modify Device Permission Role	Enables you to select Device Permission roles from the list specific to this user group.
Script Permissions	
All Scripts	Enables the users in the group to modify all scripts.

Field	Description/Action
None	No scripts can be modified. This is the default setting.
Existing Modify Device Permission Role	Enables you to select existing Script permission roles for users in the group. If there are no existing roles configured, the following message is displayed: No existing roles found.
Customized Modify Device Permission Role	Enables you to select one of the Script Permission roles from the list specific to this user group.
Customized Script Permission Role	Enables you to select customized Script permission roles from the list.
View Device Permissions	
All Sites/All Devices	Enables the users in the user group to view all Sites. A site is a physical partitioning of devices. When segmenting devices, the Default Site contains all of your devices. Refer to "Segmenting Devices and Users" on page 163 for information. **Note**: If you are not using View Permissions, new users are placed in the View All Sites group, giving them View Permission to all devices. If you create View Permissions, new users are not implicitly granted any View Permissions.
None	No sites are viewable. This is the default setting.
Existing View Permission Role	Enables you to select an existing View permission role for users in the user group. If there are no existing roles configured, the following message is displayed: No existing roles found.
Customize View Permission Role	Enables you to select View permission roles from the list.
Users	
Users in Group/All Users	To add a user, select the user from the right-hand box and click << Add. To remove a user, select the user in the left-hand box and click Remove.

Be sure to click the Save button when you are finished.

Adding User Roles

Users must be explicitly granted the corresponding command permission for each action they want to perform, such as viewing a Web page or executing a command. A set of command permissions creates a command permission role. You can then apply the role to a user group to set the command permissions for that given user group. For example, the network operations staff could have permission to access device records and view changes, but not to script changes on devices or remove devices.

Note: If you are not using View Permissions, new users are placed in the View All Sites group, giving them View Permission to all devices. If you create View Permissions, new users are not implicitly granted any View Permissions.

To add a new user role:

1. On the menu bar under Admin, click either the Users or User Groups option.
2. On either the All Users page or the User Groups page, click the User Roles & Permissions link. The User Roles & Permissions page opens.

User Roles & Permissions Page Fields

Field	Description/Action
New User Role link	Opens the New User Role page, where you can select a user role. Refer to "New User Role Page Fields" on page 263 for information.
Users link	Opens the All Users page, where you can view current users and add new additional ones. Refer to "All Users Page Fields" on page 252 for information.
User Groups link	Opens the User Groups page, where you can view current user ground and add new additional ones. Refer to "User Groups Page Fields" on page 256 for information.
Network Compliance Manager Default Roles	
Role Name	Displays the role name. You can select any role to view information for the role, including a list of command permissions for the role.

Field	Description/Action
Role Type	Displays the role type, including Command Permission, Modify Device Permission, Script Permission, and View Permission.
Description	Displays a description of the role.
Actions	You can select the following options: • Edit — The Edit User Role page opens. Refer to "Adding User Roles" on page 261 for information. • Create Copy — Opens the Edit User Role page, where you can add a new user role. Refer to "New User Role Page Fields" on page 263 for information. • Delete — You can delete the role (Admin privileges only).
User Defined Roles	
Role Name	Displays the role name. You can select any role to view information for the role, including a list of command permissions for the role.
Role Type	Displays the role type, for example Command Permission, Modify Device Permission, and Script Permission.
Description	Displays a description of the role.
Actions	You can select the following options: • Edit — The Edit User Role page opens. Refer to "New User Role Page Fields" on page 263 for information. • Create Copy — Opens the Edit User Role page, where you can add a new user role. Refer to "New User Role Page Fields" on page 263 for information. • Delete — You can delete the role (with Admin privileges only).

New User Role Page Fields

Field	Description/Action
New User Role	Select a user role from the drop-down menu. The display is modified depending on your selection. The options include: • Command Permission — Enter the name and description of the user role. For each command, click a button to grant or deny permission to this role. For a complete list of Command permissions, refer to "Appendix B: Command Permissions" on page 741. You can click Grant All to grant permission to all commands. This is useful for Admin users and when you want to deny permission to only a few commands. Click Deny All to deny permission to all commands. • Modify Device Permission — Enter the name and description of the user role. Select the device group(s) from the list. This role will have Modify Device permission for all devices that are members of the selected device groups. • Script Permission — Enter the name and description of the user role. Select the scripts from the list. This role will have Script permission to all selected scripts. • View Permission — Enter the name and description of the user role. Select the sites from the list. This role will have View permission for all devices that are members of the selected partition's device groups. For information on segmenting devices, refer to "Segmenting Devices and Users" on page 163.

Be sure to click the Save button when you are finished.

Keep in mind that user groups are not automatically assigned to user roles. To assign a user group to a user role:

1. On the menu bar under Admin, click User Groups. The User Groups page opens.
2. Click the Edit option in the Actions column for the group you want to add to the new role. The Edit User Group page opens. Refer to "New User Group Page Fields" on page 258 for information.

Editing User Preferences and Profiles

On the Home page, the My Workspace tab includes the following:

- Current Device — Displays the current device, if applicable.
- Current Device Group — Displays the current device group, if applicable.
- My Favorites — Displays a list of your favorite devices, URLs, and/or NCM pages. You can add items to this list by clicking the Add To Favorites link at the top of most NCM pages.
- My Settings — Enables you to change your settings.

My Settings

You can select the following options under My Settings:

- My Profile — Refer to "My Profile Page Fields" on page 265.
- My Workspace — Refer to "My Workspace Page Fields" on page 266.
- My Preferences — Refer to "My Preference Page Fields" on page 267.
- My Permissions — Refer to "My Permissions Page Fields" on page 268.
- Change Password — Refer to "Change Password Page Fields" on page 268.

My Profile Page Fields

The My Profile page enables you to change your user settings, such as your user name, password, and email address.

On the Home page under My Settings click My Profile. The My Profile page opens. Be sure to click the Save button when you are finished.

Field	Description/Action
User Information	
User Name	Enter a new NCM username.
User belongs to groups	Displays the groups to which you belong. Clicking a group opens the current list of users that belong to the group.
Password	Enter a new NCM password.
Confirm Password	Enter the new NCM password again for confirmation.
First Name	Enter a new first name.
Last Name	Enter a new last name.
Email Address	Enter a new email address.
External Auth Failover check box	Check if in the event external authentication fails, authentication automatically fail-overs to local authentication.
Comments	Enter any comments about the user account.
AAA	
AAA User Name	Enter a new AAA (TACACS+ or RADIUS) username.
AAA Password	Enter a new AAA password.
Confirm AAA Password	Enter your new AAA password again for confirmation.
Use AAA Login for Proxy Interface check box	If checked, your AAA login information is used with each NCM Telnet and SSH session.
SecurID	

Field	Description/Action
Manage Software Token licenses link	NCM can be configured to log into devices using SecurID credentials. Clicking this link opens the View SecurID Tokens page. Refer to "Adding SecurID Software Tokens" on page 613 for information. (**Note**: This link is not displayed if software tokens are not supported on your platform or SecurID is not properly configured.)

My Workspace Page Fields

To edit your workspace, on the Home page under My Settings click My Workspace. The My Workspace page opens.

Field	Description/Action
Favorite Links	Displays your favorite links. Links can be devices, NCM pages, or other URLs. To remove a link, click the red Delete icon next to the link you want to remove. You can also rename a link by entering a new name and then clicking the Rename button. You can use the up and down arrows to move a favorite link up or down in the list.
Add Customized Favorite Link	Enter a link name in the Link Name field. The maximum number of characters is 25. You can also enter a link URL address. Be sure to click the Add Favorite Link button when you are done.
Workspace Settings	You can use any of the links as your default Home page by selecting the link from the drop-down menu. To change the number of links allowed on your My Favorites list, select a number from the drop-down menu. The default is 10. (**Note**: This option is not available until you add a shortcut.)

My Preference Page Fields

To edit current your Home page preferences, on the Home page under My Settings click My Preferences. The My Preference page opens.

Field	Description/Action
Show My Tasks and Approval Requests (when Workflow is enabled) on the home page	Select Yes (the default) or No.
Show Recent Changes on the home page	Select Yes (the default) or No.
Show Recent Events on the home page	Select Yes (the default) or No.
Show System Reports on the home page	Select Yes or No (the default).
Show My Favorite Reports on the home page	Select Yes (the default) or No.
Show My Device Groups on the home page	Select Yes (the default) or No.

Be sure to click the Save button when you are finished.

My Permissions Page Fields

The View Permissions page displays the permissions you have due to the groups to which you belong. Keep in mind that there are also assigned roles. Refer to "New User Role Page Fields" on page 263 for information.

Note: If you are not using View Permissions, new users are placed in the View All Sites group, giving them View Permission to all devices. If you create View Permissions, new users are not implicitly granted any View Permissions.

To view your current permissions, on the Home page under My Settings click My Permissions. The My Permissions page opens.

Field	Description/Action
User Groups and Roles	Displays all of the groups you belong to and the roles assigned to each group. Refer to "Adding User Roles" on page 261 for information.
Command Permissions Granted	Displays the permissions you have relative to commands. Refer to "Granting Command Permissions" on page 741 for information.
Modify Device Permissions Granted	Displays the permissions you have to modify devices.
Script Permissions Granted	Displays the permissions you have to run and modify scripts.
View Permissions Granted	Displays the permissions you have to view devices. Refer to "Segmenting Devices and Users" on page 163 for information.

Change Password Page Fields

To change your current NCM password, on the Home page under My Settings click Change Password. The Change Password page opens.

Field	Description/Action
New Password	Enter a new password.
Confirm New Password	Enter the new password again for confirmation and click the Submit button.

Customizing the Home Page

The Home page opens whenever you login to NCM. You can also return to the Home page by clicking the Home link in the upper left-hand corner of each page.

You can customize the Home page to include:

- Workflow approvals
- List of tasks
- Recent configuration changes (what device changed and when)
- Recent system events (such as device access failures)
- Selected device groups
- Selected favorite reports
- Selected system reports

My Homepage Fields

Field	Description/Action
Workflow Approvals (if applicable)	
Tasks Awaiting My Approval link	Displays the tasks awaiting your approval, including: • Task Name — Displays the task name. If you click the task name, the Task Information page opens, where you can approve the task. Refer to "Task Information Page Fields" on page 698 for information on the Task Information page. • Approve By — Displays the date and time by which the task must be approved. Refer to "Approval Requests" on page 695 for information on task approval. • Approval — Displays the Approval status. • Schedule Date — Displays when the task was scheduled. • Status — Displays the current status. Click the View All link to open the Approval Requests page, where you can view a list of your approval requests. Refer to "Approval Requests" on page 695 for information on the Approval Requests page.
My Tasks	
Task Name	Displays a list of your tasks. Refer to "What Are Tasks?" on page 278 for information. When you first configure NCM, a list of default tasks are displayed, including Take Snapshot, Generate Summary Reports, Run Diagnostics, and Data Pruning.
Scheduled Date	Displays the date and time the task was scheduled.
Status	Displays the current task status. For a list of task statuses, refer to "Task Information Page Fields" on page 376.
View All link	Opens the My Tasks page, where you can view all of your tasks. Refer to "What Are Tasks?" on page 278 for information.
Recent Changes	

Field	Description/Action
Time frame	The default time frame is the past 24 hours. You can select the following time frames: • Past 1, 2, 4, 8, 12, 24, and 48 hours • Past 1 and 2 weeks • Past 1 month • All Configs
Date	Displays the date and time of the configuration change.
Device	Displays the host name or IP address of the device that was changed. Clicking the device link opens the Device Details page.
Changed By	Displays the login name of the person who changed the configuration, device, or task. N/A means not applicable.
Comments	Displays any comments about the configuration.
Action	You can select the following actions: • Compare to Previous — Opens the Compare Device Configuration page, where you can view the selected configuration and the next previous configuration side-by-side. The differences are highlighted in different colors to make them easy to view. • View Config — Opens the Device Configuration Detail page, where you can view the entire configuration, deploy this version of the configuration to the device running configuration, edit the configuration, retrieve diagnostics, and compare the configuration to the previous configuration.
View All link	Opens the Configuration Changes page, where you can view all the configuration changes and adjust the time frame in which you view changes. Refer to "Viewing Device Configuration Changes" on page 203 for information.

Recent Events

Field	Description/Action
Time frame	The default time frame is the past 24 hours. You can select the following time frames: • Past 1, 2, 4, 8, 12, 24, and 48 hours • Past 1 and 2 weeks • Past 1 month • All Configs
Event Summary	Displays the type of event. Click the link to view a complete list of events of this type. Refer to "Consolidated View of Events (SingleView)" on page 528 for information.
Count	Displays the number of events of this type.
Event List Page link	Opens the System & Network Events page, where you can see a longer list of events and adjust the time frame in which you view events. Refer to "Consolidated View of Events (SingleView)" on page 528 for information.
My Device Groups (if applicable)	
Device Group links	Opens the Device Groups page, where you can view the current device groups.
My Favorite Reports (if applicable)	
All Favorite Reports link	Opens the User & System Reports page, where you can view the reports you created from custom searches as well as the System reports.

Statistics Dashboard Tab Page Fields

The Statistics Dashboard tab provides information on the following reports:

- Top 5 Vendors — Refer to "Summary Reports" on page 601 for information.
- Top 5 OS Versions — Refer to "Summary Reports" on page 601 for information.
- Number of Configuration Change - Last 7 Days — Refer to "User & System Reports" on page 568 for information.
- Change History by Time of Day — Refer to "Summary Reports" on page 601 for information.
- Top 10 Most Accessed Devices — Refer to "Summary Reports" on page 601 for information.
- System Status — Refer to "Network Status Report" on page 572 for information.

Search/Connect Function

The Home page (and every page) includes a Search Tab on the left-side of each page that enables you to find devices by Hostname or IP address and connect to them via Telnet or SSH. The search function accepts wildcards, so you can quickly find a group of related devices, or at least narrow your search until you find the target device. Refer to "Searching for Devices" on page 449 for information on the Search For Devices page fields.

You can also use the Search For drop-down menu to search for specific:

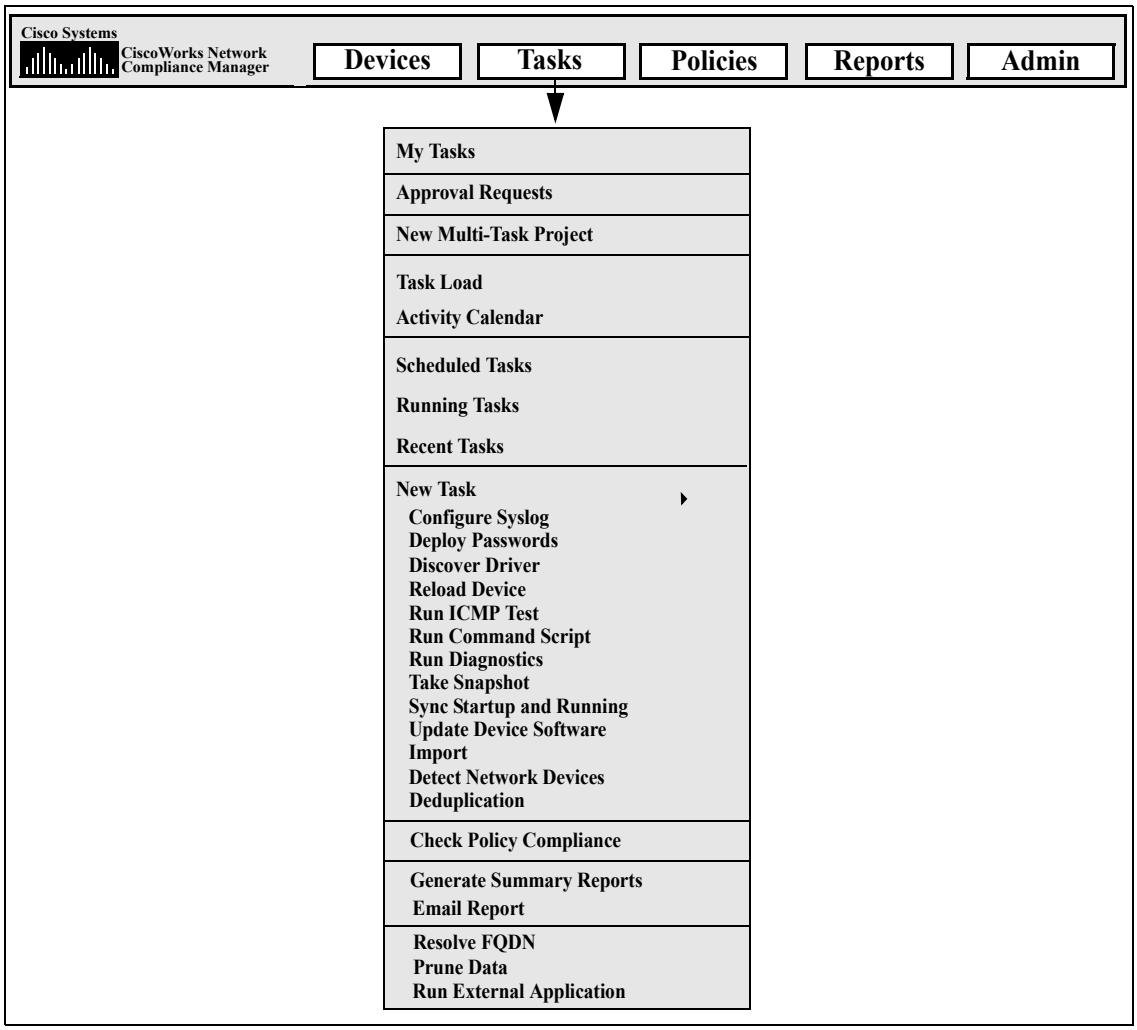
- Devices
- Modules
- Configurations
- Diagnostics
- Tasks
- Sessions
- Events
- Users
- SingleSearch
- ACLs
- MAC addresses
- IP addresses
- VLANs
- Advanced Search

Chapter 7: Scheduling Tasks

Use the following table to quickly locate information.

Topic	Refer to:
Scheduling Multi-Task Projects	"Scheduling Multi-Task Projects" on page 360
Viewing My Tasks	"My Tasks Page Fields" on page 365
Viewing Scheduled Tasks	"Viewing Scheduled Tasks" on page 369
Viewing Running Tasks	"Viewing Running Tasks" on page 371
Viewing Recent Tasks	"Viewing Recent Tasks" on page 373
Viewing Task Load	"Viewing Task Load" on page 379

Navigating to Task Pages



What Are Tasks?

Tasks are the primary mechanism by which NCM interacts with your network. Tasks are specific actions you can either schedule or run immediately. The Task Information page provides the results of performed tasks, such as snapshots to identify device and configuration changes and software policy compliance to identify devices that are or are not in compliance.

Running Tasks Against Ad-hoc Device Groups

You can run a task or set of tasks (Multi-Task Project) against a temporary group of devices by creating ad-hoc device groups. You can create ad-hoc device groups by using either:

- The check boxes on the Device List page to select devices and then selecting the task you want to run against the devices using the Actions drop-down menu. Refer to "Viewing Devices" on page 217 for detailed information.
- Importing a CSV file that contains an ad-hoc list of devices. For example, let's say you have 200 devices in your network and there is one DNS server for each group of 50 devices. Instead of creating four device groups (each with 50 servers), you can generate a CSV file that maps the devices to DNS servers. You then can load the CSV file into a command script and run one task to update all of the DNS servers. For information on running command scripts, refer to "Run Command Script Task Page Fields" on page 302.

For information on Multi-Task Projects, refer to "Multi-Task Project Page Fields" on page 361.

To open the New Task page, on the menu bar under Tasks, select New Task and click the task you want to schedule. The New Task page opens for that task. The following table lists the tasks from which you can choose.

Task	Refer to...
Configure Syslog	"Configure Syslog Task Page Fields" on page 280
Deploy Passwords	"Deploy Passwords Task Page Fields" on page 284
Discover Driver	"Discover Driver Task Page Fields" on page 289
Reload Device	"Reload Device Task Page Fields" on page 293
Run ICMP Test	"Run ICMP Test Task Page Fields" on page 296
Run Command Script	"Run Command Script Task Page Fields" on page 302
Run Diagnostics	"Run Diagnostics Task Page Fields" on page 309
Take Snapshot	"Take Snapshot Task Page Fields" on page 314
Sync Startup & Running	"Synchronize Startup and Running Task Page Fields" on page 318
Update Device Software	"Update Device Software Task Page Fields" on page 322
Import Device	"Import Task Page Fields" on page 328
Detect Network Devices	"Detect Network Devices Task Page Fields" on page 332
Deduplication	"Deduplication Task Page Fields" on page 339
Check Policy Compliance	"Check Policy Compliance Task Page Fields" on page 342
Generate Summary Reports	"Generate Summary Reports Task Page Fields" on page 346
Email Report	"Email Report Task Page Fields" on page 348
Resolve FQDN	"Resolve FQDN Task Page Fields" on page 351
Prune Data	"Data Pruning Task Page Fields" on page 354
Run External Application	"Run External Application Task Page Fields" on page 357

Configure Syslog Task Page Fields

The Configure Syslog task enables you to schedule the automatic configuration of one or more devices to send Syslog messages. NCM uses Syslog messages to help detect real-time configuration changes. After discovery (or when you assign a driver to each device), NCM:

1. Takes a snapshot of the configuration.
2. Updates the configuration to send Syslog messages to NCM.
3. Writes a comment in the configuration indicating that the device was auto-configured to enable change detection.
4. Takes a final snapshot.

Field	Description/Action
Task Name	Displays Configure Syslog. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against (the default). • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.

Field	Description/Action
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored.)
Syslog Configuration	Select one of the following options: • Set Device to Log to the NCM Syslog Server (the default). • Device Logs to a Syslog Relay, Set the Correct Logging Level. — Enter a Relay Host.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Field	Description/Action
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times

Field	Description/Action
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Deploy Passwords Task Page Fields

The Deploy Passwords task enables you change the password settings and SNMP community strings for a single device or for a device group from a central location. Keep in mind that if your network uses AAA with NCM, you should change passwords through your AAA server, not through NCM. Otherwise, NCM might lose contact with the devices. In addition, NCM does not actually manage AAA passwords, nor does NCM manage device-maintained user accounts. NCM only manages what is prompted for when you schedule a password deploy for a single device, or the output of the "what this means" links if you schedule a group password deploy.

NCM supports password and community string changes for most devices, including menu-driven devices such as the Nortel Baystack 450. For information on which devices support Password Management, refer to the *CiscoWorks Network Compliance Manager (NCM) Device Driver Reference*.

Upon a successful change, NCM performs a device snapshot and downloads the changed configuration. To quickly view all recent password or SNMP community string changes, navigate to the Configuration Changes page. Refer to "Viewing Device Configuration Changes" on page 203 for information.

Note: If you use AAA and attempt to change the device password with the password deployment functionality, NCM might attempt to connect to the device using the new password, not AAA. However, the device could still expect an AAA login. If necessary, you would have to manually reconfigure the device to use AAA (in case that changed), and reconfigure NCM to login to the device using the correct AAA credentials.

Field	Description/Action
Task Name	Displays Deploy Passwords. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	

Field	Description/Action
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored.).
Limited Access Username	Enter the limited access username that NCM needs to access the device. Keep in mind that usernames vary depending on the device's vendor and operating system. Click k the "What this means" link for device-specific information. (**Note**: A blank username means that the associated field will not be changed on the device.)
Limited Access Password	Enter the limited access password that NCM needs to access the device. Keep in mind that passwords vary depending on the device's vendor and operating system. Click the "What this means" link for device-specific information. (**Note**: A blank password means that the associated field will not be changed on the device.)
Confirm Password	Enter the password again to confirm it.
Full Access Username	Enter the full access username that NCM needs to access the device. Keep in mind that usernames vary depending on the device's vendor and operating system. Click the "What this means" link for device-specific information. (**Note**: A blank username means that the associated field will not be changed on the device.)
Full Access Password	Enter the full access password that NCM needs to access the device. Keep in mind that passwords vary depending on the device's vendor and operating system. Click the "What this means" link for device-specific information. (**Note**: A blank password means that the associated field will not be changed on the device.)
Confirm Password	Enter the password again to confirm it.
SNMP Read Community Strings	To add an SNMP Read Community String, enter the string in the right-hand box, then click << Add Read Community String. To remove an SNMP Read Community String, select the name in the left-hand box, then click Delete Read Community String. Select "Append to existing community strings on device" (the default) or "Replace existing community strings on device."

Field	Description/Action
SNMP Write Community Strings	To add an SNMP Write Community String, enter the string in the right-hand box, then click << Add Write Community String. To remove an SNMP Write Community String, select the name in the left-hand box, then click Delete Write Community String. Select "Append to existing community strings on device" (the default) or "Replace existing community strings on device."
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.

Field	Description/Action
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	Not Available

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Discover Driver Task Page Fields

The Discover Driver task enables you to schedule driver discovery.

Field	Description/Action
Task Name	Displays Discover Driver. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	

Field	Description/Action
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored.)
Options	If there is no driver set, check the "Only if No Driver is set" check box (the default).
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Field	Description/Action
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Reload Device Task Page Fields

The Reload Device task enables you to reboot devices.

Field	Description/Action
Task Name	Displays Reload Device. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that large amounts of data could be stored. This option is recommended for device troubleshooting only.

Field	Description/Action
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.

Field	Description/Action
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	Not available.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Run ICMP Test Task Page Fields

The Run ICMP (Internet Control Message Protocol) Test task enables you to schedule either a ping or traceroute test from a device to one or more devices.

Traceroute attempts to trace the path a packet takes through the network. Traceroute transmits packets with small Time-To-Live (TTL) values. TTL is an IP header field that is designed to prevent packets from running in loops, also known as *hop-limit*. Traceroute depends on devices sending an ICMP Time Exceeded message back to the sender. Traceroute causes devices along a packet's normal delivery path to generate these ICMP messages that identify the path.

Packet INternet Groper (Ping) sends a single packet and listens for a single packet in reply. Ping is implemented using the required ICMP Echo function.

In general, the traceroute option performs its action by going from one device to the next along routes that the device knows about. Alternatively, ping goes to each device along the route individually.

Keep in mind that the traceroute and ping commands are not functions that NCM completes. The devices do these. NCM must be able to login to the source device and then issue the appropriate command for that device to trace to the destination devices. Each device could implement the functionality differently (or not at all). What you see in the ICMP Test Results page is a dump of what the device displays on the screen.

Both ping and traceroute are excellent networking troubleshooting tools. For example, with ping you can test 100 devices to see if they can access a specific device. Or if you see that 20 devices are having a problem accessing a specific device, you can run an automated remote traceroute and check the path each device is taking to that destination.

Field	Description/Action
Task Name	Displays Run ICMP Test. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	

Field	Description/Action
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored.)
Test Type	Select either ping or traceroute.
Target Host List	To add a host, enter the name in the right-hand box, then click << Add Host. To remove a host, select the host name in the left-hand box, then click Remove Host.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Field	Description/Action
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The ICMP Test Result page opens if the task is scheduled to run immediately.

Note: What you see in the ICMP Test Results page is a dump of what the device displays on the screen.

If the task is successful and you selected the ping option, the following information is displayed, depending on the device and the information you entered on the Run ICMP Test Task page:

- Create Date
- Command Run
- Result
- Command Output (for example: `Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms`)

If you selected the traceroute option, the following information is displayed, depending on the device and the information you entered on the Run ICMP Test Task page:

- Create Date
- Command Run
- Result
- Command Output (for example:
```
1 1ms 1ms 1ms 10.255.111.2
2 4ms 4ms 4ms 10.255.111.3
3  *  *  *  *
```

The first column displays the hop. The next three columns show the time it took for the device to respond. If the time the device takes to respond is longer than the designated time-out value, asterisks are displayed.). The last column is the host that responded.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for information.

Run Command Script Task Page Fields

The Run Command Script task enables you to run command scripts.

Field	Description/Action
New Command Script link	Opens the New Command Script page. Refer to "New Command Script Page Fields" on page 560 for information on writing scripts.
Command Scripts link	Opens the Command Scripts page. Refer to "Command Scripts Page Fields" on page 556 for information.
Task Name	Displays the Run Command Script name. You can enter a different task name, if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	

Field	Description/Action
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that large amounts of data could be stored.
Command Script to Run	Select the command script to run. The options will change depending on the type of script you select. Standard command scripts include: • One-time use script • Cisco IOS Insert Line into ACL by ACL id • Cisco IOS Insert Line into ACL by Handle • Cisco IOS Remove Line from ACL by ACL id • Cisco IOS Remove Line from ACL by Handle • Compress Flash • Contivity 1100 Deploy SNMP Community Strings • Extended Ping • Full Duplex • ios_7k_reboot • ios_generic_reboot • Passport 8xxx - Deploy Community Strings • Passport 8xxx - Deploy User Passwords • ios_13switch_reboot • Sample - Provision FastEther Interface • Set Banner • Set Banner Only If Needed • Set Location • Set NTP Server • Turn off directed broadcast
Limit to script types	Select all (the default) or select one of the following: • ACL Advanced Script • ACL Application Script • ACL Creation Script • ACL Edit Script

Field	Description/Action
Depending on the command script you select, the following options could be displayed.	
Mode	Displays the device access mode, such as Cisco Exec or Nortel Manager. This is similar to the device platform.
Variables	If the script has variable fields to fill in, enter the values. When finished, you can click Update Scripts to view the script that will run with these variable values.
Device Family	(Advanced Scripting) Displays the name of the device family on which this script runs. A device family is a collection of devices that share a similar configuration CLI command syntax.
Parameters	Enter the parameters for the script.
Script	Displays the device-specific commands to run. You can edit this instance of the script, however your changes are not saved after this instance runs. If there are multiple modes, one instance of the script appears for each mode. **Note:** The height and width of the Script box is controlled by settings in the Administrative Settings page, User Interface tab. If you use the scripting feature extensively, you may want to adjust these settings so that you can see the script without scrolling.
Deploy option	To run scripts line-by-line rather than deploying in bulk, check the "Run scripts line-by-line..." check box. Keep in mind that devices that are able to run scripts through a bulk deployment method (such as Cisco IOS configuration scripts) do so whenever possible. The default is that the entire contents of the script is deployed and run in a single batch. If an error occurs, the script keeps going. Running a script line-by-line in such cases will result in the script capturing the error and stopping execution.
Wait Option	Checked by default. If you uncheck this option, the task is allowed to run even if there is already another task running against the same device.
Language	(Advanced Scripting) Displays the language in which the script was written.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Field	Description/Action

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Pre-Task / Post-Task Snapshot Options
Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 58 for information.)

Pre-Task Snapshot	Select one of the following options: • None (the default) • As part of task
Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Field	Description/Action
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.

Field	Description/Action
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Run Diagnostics Task Page Fields

The Run Diagnostics task enables you to schedule the running of diagnostics.

Field	Description/Action
New Diagnostic link	Opens the New Diagnostics page. Refer to "New Diagnostic Page Fields" on page 534 for information.
Diagnostic link	Opens the Diagnostics page. Refer to "Diagnostics Page Fields" on page 532 for information on managing diagnostics.
Task Name	Displays Run Diagnostics. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	

Field	Description/Action
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that large amounts of data could be stored.
Diagnostics to Run	Select the diagnostic to run. Use Ctrl+click to select/deselect additional diagnostics. Diagnostics include: • Memory Troubleshooting • NCM Detect Device Boot • NCM Device File System • NCM Flash Storage Space • NCM Interfaces • NCM Module Status • NCM OSPF Neighbors • NCM Routing Table • NCM Topology Data Gathering **Note**: For detailed information on diagnostics, refer to "View Menu Options" on page 229.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options

Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Field	Description/Action
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Pre-Task / Post-Task Snapshot Options
Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 58 for information.)

Pre-Task Snapshot	Select one of the following options: • None (the default) • As part of task
Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.

Field	Description/Action
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Take Snapshot Task Page Fields

The Take Snapshot task enables you to schedule a snapshot. A snapshot checks whether the stored configuration matches the running configuration on the device. If not, the task stores a new copy of the device configuration and related data in the NCM database. However, if you select the "Make Snapshot a Checkpoint" option, the NCM database is updated even if NCM does not detect a difference.

Field	Description/Action
Task Name	Displays Take Snapshot. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	

Field	Description/Action
Session Log	Check the "Store complete device session log" box to store a debugging log. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored.)
Options	Select one or both of the following options: • Make Snapshot a Checkpoint — Copies the running configuration to the NCM database rather than checking first whether the stored configuration differs from the running configuration. • Retrieve Binary Configuration — Copies the binary configuration, if any, as well as any text information to the NCM database.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Field	Description/Action
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Synchronize Startup and Running Task Page Fields

The Synchronize Startup and Running task enables you to synchronize the startup and running of configurations for a device. NCM will overwrite the startup configuration with the current running configuration. This task ensures that when the device reboots, the current configuration will continue to run.

Field	Description/Action
Task Name	Displays Synchronize Startup and Running. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	

Field	Description/Action
Session Log	Check the "Store complete device session log" box to store a debugging log. This is useful when debugging a failed snapshot, however large amounts of data can be stored.
Options	Select the "Bypass if in sync" box if you want NCM to skip the task if the configurations are already synchronized.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Pre-Task / Post-Task Snapshot Options
Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 58 for information.)

Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task

Field	Description/Action
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Update Device Software Task Page Fields

The Update Device Software task enables you to schedule the deployment of software to one or more devices. Refer to "Software Images" on page 417 for more information. Keep in mind that:

- Total memory is the total physical memory on the device.
- Free memory is the free memory available for uploads at the time of the last memory diagnostic.
- Net memory is the estimate of free memory after the Update Device Software task is run, taking into account any files you marked to be added or removed from the device (but not taking into account the squeeze pre or post processing task).

Field	Description/Action
Task Name	Displays Update Device Software. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.

Field	Description/Action
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Session Log	Check the "Store complete device session log" box to store a debugging log. This is useful when debugging a failed snapshot, however large amounts of data can be stored.
Deployment Table	If you are deploying software to a single device, the Deployment Table opens. Refer "Deployment Table" on page 326 for information.
Image Set	Select the name of the software images you are deploying.
Slot	Select the slot to which you want to deploy the software. NCM lists all the slots currently in the NCM database.
Memory Preparation	Select one of the following options: • None — Do not prepare the device memory before updating the software. You should manually ensure that the device has enough memory to receive the new software, otherwise the task will fail. • Compact device memory on selected slot — Before deploying software, NCM executes a command to compact memory, such as the Cisco IOS squeeze command, if one is supported by the device. No files are removed from the device. You should still ensure that sufficient memory will be available for the update. • Delete files from selected slot, then compact memory — Before deploying software, NCM deletes all files from the slot, then compacts the memory, if the device supports a compact command. (**Note**: If the deploy software task fails, followed by a device power failure or reboot, the device might not be bootable.)
Reboot	Check the "Reboot device after deploying software" box to run a script to reboot the device after software deployment. Enter the number of seconds to pause after rebooting before taking a snapshot of the configuration in the "Pause after Reboot" box. The default is 60 seconds.

Field	Description/Action
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options
Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 69 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.

Field	Description/Action
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Deployment Table

The Deployment Table provides advanced options for deploying software to a single device. The data is based on the last File System diagnostic.

Field	Description/Action
Run a File System Diagnostic link	Opens the New Task - Run Diagnostics page, where you can schedule a File System diagnostic to be run on the device. (Refer to "Run Diagnostics Task Page Fields" on page 309 for information.)
Preprocessing tasks	Before deploying software, NCM executes a command to compact memory, such as the Cisco IOS squeeze command, if one is supported by the device. No files are removed from the device. You should still ensure that sufficient memory will be available for the update.
Name	Displays the name of the device.
Size	Displays the size of the software image to be downloaded.
Compliance	Displays the compliance level of the software image, such as Security Risk, Pre-production, Obsolete, and so on. Keep in mind that this field is not displayed by default. Refer to "User Interface Page Fields" on page 89 for information.
File System Name (for example Flash)	Displays the total amount of free free memory on the file system.
PostProcessing tasks	After deploying software, NCM executes a command to compact memory, such as the Cisco IOS squeeze command, if one is supported by the device. No files are removed from the device. You should still ensure that sufficient memory will be available for the update.
Checkbox	Files that exist on the device are highlighted. Select this checkbox if you do not want to deploy these files to the device.
Adding	Displays the File, Image Set, and Destination of the software deployment.
Deleting	Displays if any files are to be deleted.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Note: If the images you have selected to deploy do not fit in the device's available free disk space, an error message is displayed. You can either return to the task and make changes or deploy the software. It is possible that the disk space calculation is in error.

Import Task Page Fields

The Import task enables you to import device and device password data using a comma-separated value (CSV) format. It is recommended that you create network-wide device password rules first, then import devices. You can also import a set of device-specific data from one file, then import the device password data from a second file.

Field	Description/Action
Device Import Admin Settings link	Opens the Administrative Settings page (Server tab), where you can set NCM task limits, enable Workflow, Configure Syslog, and so on.
Task Name	Displays Import. You can enter a different task name if applicable.
Site	Provides a drop-down menu where you can select a Site. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.) In general, a Site is a set of devices that is managed by one (and only one) NCM Core. A NCM Core is a single NCM Management Engine, associated services (Syslog and TFTP), and a single database. A NCM Core can manage multiple Sites.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Import File	Enter the name of the Comma Separated Value (CSV) file you are importing. If the file is on the local system, you can use the Browse button to locate the file. Be sure to include the full path to the file on the NCM server. If you are using a template to create a new CSV file in the Data Type field (see below), be sure to save the file on your local hard drive.

Field	Description/Action
Data Type	Select one of the following options and enter the data you are importing: • Devices — The Device CSV Template contains various fields that allow for network devices to be entered into NCM, including IP addresses, host names, and device group names. • Passwords — The Device Passwords CSV Template is only required if you are not using Device Password Rules. If you are using a template to create a new CSV file, click the link for either a devices or password CSV template file. Once the file is open, save it under a different name on your local hard drive, then modify the saved file to fit your device data or passwords.
Syslog Configuration	Select one of the following options: • Set Device to Log to the NCM Syslog Server • Device Logs to a Syslog Relay, set the correct logging level • Do not configure syslog Check the "Run Discover Drivers on newly imported Devices" box if you want NCM to discover device drivers for the devices associated with the CSV file you are importing. This option requires valid device passwords and community strings. Therefore, you should only use the option when you already have passwords and device password rules set up and debugged for your network or when you import the second file containing device password information. Check the Deactivate inactive or missing devices check box if you want NCM to deactivate devices that have not been accessed or imported successfully in the last 45 days.
Preprocess Command	To automate and schedule the entire process within NCM, enter the name (and path) of the script file to run before importing the data. This field needs the full executable command which runs in the command/shell console on the server. For example, "perl" needs to be specified if the filter is a PERL script for Windows: `perl c:/filter.pl`
Log filename	Enter the name of the file to which NCM will write information about the import task. The log file is helpful when debugging import problems. Check the "Append to log file" if you want NCM to append this data to the existing log file. Otherwise, NCM will overwrite any existing data in the log file.

Field	Description/Action
Device Origin	Enter the name you want to give this import file. This is useful when you import data on a recurring basis and need to differentiate different data sources and dates.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.

Field	Description/Action
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Detect Network Devices Task Page Fields

Detecting network devices enables you to locate devices on your network that you want to place under NCM management. Once you provide a range of IP addresses, NCM scans your network looking for devices. Newly discovered devices are automatically added, along with the appropriate device drivers. In addition, if the Primary IP Address Reassignment option is checked on the Administrative Settings — Server page, NCM automatically assigns the correct IP address to a device if the device has multiple IP addresses and interfaces. Consequently, a device is only entered into the system once. Refer to "Device Access Page Fields" on page 69 and "Server Page Fields" on page 80 for task settings.

If you select Driver Discovery on the task page, after NCM adds the device to the system, it polls the device to see what type of device it is and subsequently assigns the appropriate device driver to manage the device. NCM then takes a snapshot of the device and downloads the configuration and asset information from the device into the database.

For unsupported hosts, a group is also created and added to the system (Inventory). To make sure that unsupported devices are not added as active (and therefore count towards the device's license) and to prevent any operation performed against Inventory that would include these devices, all devices from unsupported hosts are set to inactive by default.

If you want to perform tasks against these devices, you must first activate them. You can activate devices from either the:

- Device Details page, using the Edit & Provision menu (Activate Device option).
- Group Device page, where you can select devices using the check boxes and then select the Activate option from the Actions drop-down menu.

When running the Detect Network Devices task, the Task Information page shows:

- Active nodes — Active nodes are IP addresses that responded to either an SNMP scan or an Nmap scan. A node is considered active if it can be managed by NCM. Refer to the *Device Driver Reference* for a list of supported devices.

- Non-active nodes — Non-active nodes are IP addresses that did not respond to either an SNMP scan or an Nmap scan, or both. A device might not respond to an SNMP scan if an incorrect community string is use by NCM to query the device.
- Unsupported hosts — Unsupported hosts are IP addresses that responded to either an SNMP scan or an Nmap scan. However in the case of SNMP, it returned a SysOID that NCM does not support. In the case of Nmap, the operating system fingerprint returned no matches that NCM supports.
- Existing devices — Existing devices indicate that the device's IP address is already known to NCM and exists in the system as either the primary IP address of the device or the IP address appears in the database as a result of the BasicIP diagnostic.

Scanning Methods

There are two types of Internet Protocol (IP) traffic:

- User Datagram Protocol (UDP) — UPD is a simple message-based connectionless protocol. With UDP, packets are sent across the network in chunks. In general, UDP is rather unreliable and the order of arriving packets is not guaranteed.
- Transmission Control Protocol (TCP) — TCP is a connection-oriented protocol. TCP is very reliable and the order in which packets are received along a connection is guaranteed.

SNMP scanning uses UDP. SNMP attempts connections to systems using known SYSOIDs to identify network devices. The SNMP scanning method has less impact on your network because it does not require multiple connections to each system. In addition, SNMP is fast, however it can be bogged down if there are a lot of password rules, since all password rules are tried for every IP address scanned. Also, SNMP requires login credentials (community strings) to be successful.

Nmap Scanning uses TCP, although it can be configured to use UDP for some tasks. Because Nmap is a port scanner, if you do not want your network scanned, you should opt for the SNMP scanning method. In addition, Nmap makes many connections to devices so as to test the various ports.

Keep in mind that Nmap does not login to devices, and therefore does not need login credentials. Nmap can range from fast to slow, depending on the network configuration and the IP addresses being scanned. Scanning IP addresses, for example 192.168.0.0, can be very slow. It is highly recommended that you only scan IP address ranges that are within your own organization.

Note: Many organizations have monitoring systems that will send alarms if they detect a network scan in progress. If you are using Nmap to detect network devices, make sure your IT team is fully aware of the scheduled activity.

Defining IP Address Ranges

You must specify at least one IP address inclusion range. You can define ranges two ways:

- CIDR (Classless InterDomain Routing) notation — CIDR denotes a block or range of IP addresses, for example 10.255.1.0/24. This represents an IP address range from 10.255.1.0 to, and including, 10.255.1.255. In total, 256 IP addresses. The /24 in the 10.255.1.0/24 CIDR notation represents how many bits make up the CIDR block's prefix. In this case, it is 24 bits. The balance of the block (the final eight bits) are considered wildcards. Other examples include:
  - 192.168.100.1/32 is a single host 192.168.100.1. (Note all 32 bits make up the prefix without any wildcard bits.)
  - 172.16.0.0/16 is an extremely large range from 172.16.0.0 to 172.16.255.255. It is recommended not to discover ranges this large.
  - 10.255.0.0/23 is a moderately large range. This range goes from 10.255.0.0 to 10.255.1.255, and includes 512 IP addresses.

- Ranged input — IP address blocks are represented with a lowest-highest notation, for example 10.255.1.0 - 10.255.1.255. You can enter a single IP address, for example 192.168.100.1. Exclusion ranges can also be specified. This enables you to mask out certain addresses, or ranges of addresses, from network device detection. For example, you can scan the range 10.255.1.0/24. However, if there are printers from 10.255.1.10 to 10.255.1.20 that you do not want to scan, the inclusion range is 10.255.1.0/24. The exclusion range is 10.255.1.10 - 10.255.1.20.

Field	Description/Action
Task Name	Displays Detect Network Devices. You can enter a different task name if applicable.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Max Nodes	Enter the number of IP addresses to discover. The maximum is 1024. Keep in mind that tasks with more nodes than the maximum allowed will cause the task to fail.
Inclusions	Enter IP addresses or Classless Inter-Domain Routing (CIDR) range inclusions (for example: 192.168.1.0-192.168.2.0 or 192.168.31.0/24) in right-hand box and click the << Add Discovery Range button. Ranges are inclusive. You can use the Delete Discovery Range button to delete ranges.
Exclusions	Enter IP addresses or Classless Inter-Domain Routing (CIDR) range exclusions (for example: 192.168.1.0-192.168.2.0 or 192.168.31.0/24) in the right-hand box and click the << Add Exclusion Range button. Ranges are inclusive. You can use the Delete Exclusion Range button to delete ranges.

Field	Description/Action
Scanning Methods	Select one or both of the following scanning methods: • SNMP (the default) • Nmap (Note: Careful consideration should be taken when identifying the network range you are going to scan. Some network topologies can result in very long scans. In addition, it is recommended that you do not scan Internet addresses.) For detailed information on scanning methods, refer to "Scanning Methods" on page 333.
Password rule fallback	If selected (the default), SNMP scans the require community strings. Password rule fallback is used for those community strings.
Sites	Select a Site from the drop-down menu. Refer to "Segmenting Devices and Users" on page 163 for information on Sites.
Device Group Name	Select one of the following options: • Use the default group name (DetectedNetworkDevices<*nnn*>, where *nnn* is the task ID) or select a device group from the drop-down menu. • Enter a device group name for added devices (the default). **Note**: When using the Detect Network Devices task, a new group could be created from devices that responded to the network scan, but did not return a known OS.
Driver Discovery	If checked (the default), device drivers are discovered after the device has been detected.
Device Credentials Options	
Device Credentials	Select one of the following options: • Use network-wide password rules • Use task specific credentials — Enter the username, password, and SNMP community string information.

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Field	Description/Action
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished.

The Task Information page opens if the task is scheduled to run immediately. The Task Information page displays detailed information about the discovered nodes. Refer to "Task Information Page Fields" on page 376 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Deduplication Task Page Fields

If you import devices into NCM using either the CSV (Comma Separated Value) file or Connectors, it is possible to have duplicate devices created in the NCM database. For example, if you are importing devices from different management systems, such as HP OpenView or CiscoWorks, they could use different management IP addresses to refer to the same device. The Deduplication task enables you to resolve device duplication issues. Keep in mind that the Detect Network Devices task does this automatically. Refer to "Detect Network Devices Task Page Fields" on page 332 for information.

Field	Description/Action
Task Name	Displays Deduplication. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.

Field	Description/Action
Comments	Enter comments about the task.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.

Field	Description/Action
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Check Policy Compliance Task Page Fields

The Check Policy Compliance task enables you to determine if devices are in compliance with either configuration policies or software compliance policies. You should only need to run the Check Policy Compliance task when you create or update policies. By doing so, you can quickly determine if a device is out of compliance with the newly created policy.

Note: By default, NCM runs a compliance check on a device's configuration whenever a configuration change is detected. If configured, you are notified if a configuration change violates applied policies. In addition, you can configure a number of automated reactions, such as emailed alerts, SNMP traps, and even run a command script to force the device to return to a compliant state.

Field	Description/Action
Task Name	Displays Check Policy Compliance. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.

Field	Description/Action
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Action	Select one or both of the following options: • Check configuration policy compliance (the default) — Checks to see if the selected device(s) are in compliance with configuration policies. • Check software compliance — If checked, the software compliance is checked, resulting in text output showing the compliance level and any identified security vulnerabilities. Software Vulnerability events are generated if appropriate. Refer to "Software Vulnerability Report Fields" on page 595 for more information.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	

Field	Description/Action
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status.

Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Generate Summary Reports Task Page Fields

The Generate Summary Reports task enables you to update the Summary reports (which by default are updated by a recurring task each Sunday). If you want to permanently change the schedule for updating Summary reports, you can edit the existing recurring task.

Field	Description/Action
Task Name	Displays Generate Summary Reports. You can enter a different task name if applicable.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	

Field	Description/Action
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Email Report Task Page Fields

The Email Report task enables you to email NCM reports.

Field	Description/Action
Task Name	Displays Email Report. You can enter a different task name if applicable.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Report to run	Select a report to email. Keep in mind that each time this task runs, the last saved report is overwritten with the new information. (**Note**: Summary reports cannot be emailed using this task.) Refer to "Navigating to Reports" on page 566 for a list of reports.
Applies to	This field is displayed for the Network Status report only. Select the device group against which you want to run the report.
Email Recipients	Enter one or more email addresses. Be sure to separate addresses with commas.
Email Subject	Enter the subject line of the email message.
Sender Email	Enter the return address to include in the email.
	Select the "Save a copy of this report to file at location <path> to automatically save the report to the location shown. This location is configured by the System Administrator. (**Note**: This option is available for all reports except Summary reports.)
Email Format	Select one of the following options from the drop-down menu: • Default format • HTML mail • CSV file attachment • Plain text • HTML mail (without links)

Field	Description/Action
File Export	Click the check box to save a copy of the report to file.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.

Field	Description/Action
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Resolve FQDN Task Page Fields

The Resolve FQDN task enables you to set the FQDN (Fully Qualified Domain Name) for each device in the system by running a reverse DNS lookup on the device's primary IP address.

Field	Description/Action
Task Name	Displays Resolve FQDN. You can enter a different task name if applicable.
Applies to	Select one of the following options: • Single Device — Enter the device's Host Name or IP address on which to run the task against. • Single Group — Select a device group on which to run the task against. • Multiple Devices/Groups — Opens the Device Selector. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options (not available)	

Field	Description/Action
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Data Pruning Task Page Fields

Data pruning is a system task that requires a system administrator or someone with similar permissions to configure the system. Data pruning removes obsolete files, diagnostics, events, and tasks. The following files are not removed by data pruning:

- Current configuration
- Configurations scheduled for deployment

When the NCM server is configured for pruning, you can specify how long the files should be kept. The default settings for these files include:

- Configurations — 365 days
- Tasks — 365 days
- Diagnostics — 45 days
- Events — 45 days
- Sessions — 45 days
- Log files — 30 days

Field	Description/Action
Task Name	Displays Data Pruning. You can enter a different task name if applicable.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.

Approval Options
Approval options are only displayed if the task is part of a Workflow Approval Rule.

Field	Description/Action
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status.

Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Run External Application Task Page Fields

The Run External Application task enables you to schedule an external application to run from NCM, such as the "ping" command or an external language interpreter. This task can be used to enable integration with external Help Desk and NMS solutions.

Note: On a Windows platform, the path should use the Windows file separator character, which is a backslash (\). The short names (those with ~<*n*>) are only needed when a file name includes spaces. For example, *C:\Rendition* is fine, but *C:\Program Files* is not. Keep in mind that short names are only needed when you are passing parameters, for example: *C:\Program Files\Internet Explorer\iexplore.exe* is fine. However, *C:\Program Files\Internet Explorer\iexplore.exe someFilename.html* will not work. You would need to use *C:\Progra~1\Intern~1\iexplore.exe someFilename.html*.

Field	Description/Action
Task Name	Displays Run External Application. You can enter a different task name if applicable.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Run	Enter the command line utility or script you want to execute. Be sure to provide the fully-qualified path and filename for the executable file. You can supply parameters to an external application by supplying both the name of the application to run, followed by its parameter(s). For example, to run an external command "foo" with parameters "bar" and "bat", you would enter "foo bar bat" without the quotes.
Start in	Enter the path of the external application and the startup directory for that application.
Task Result	Check the "Treat non-zero result code as fail task" box if you want to treat non-zero result code as a failed task.

Field	Description/Action
Text Output	Select one of the following options: • Results from stdout (the default) — After the application runs, its standard text output to the console is stored in the Task Details. This is used for most applications, such as command line utilities. • Results from file — For no output, select this option, but leave the filename blank. After the application runs, NCM reads this file and includes the contents in the Task Details. This is useful for commands that write output to a file instead of stdout. Be sure to enter the fully-qualified path to the result file, if applicable.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.

Field	Description/Action
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Be sure to click Save Task when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 376 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 365 for more information.

Scheduling Multi-Task Projects

You can configure a multi-task project to run several different tasks sequentially joined together under a single project. For example, you might want to perform a software upgrade and then push an updated configuration to the device. Consolidating the tasks together under one project simplifies the management approvals by authorizing work at the project level rather than the task level. It also enables you to coordinate sets of disparate tasks and manage them as one unit.

Each task included in the multi-task project is run in the order you specify. For example, you can schedule driver discovery, a snapshot, run a custom script, and so on, for a group of devices. Keep in mind that as far as the NCM Scheduler is concerned, the multi-task project is considered one task. When the multi-task project is scheduled to run, the NCM Scheduler runs all the tasks in the order specified. If for some reason one of the tasks in the multi-task project does not run, the multi-task project fails. If the multi-task project requires approval, when the multi-task project is approved, all of the tasks included in the multi-task project are automatically approved.

Note: You can reserve devices and/or device groups using the Multi-Task Project page.

To create a multi-task project, on the menu bar under Tasks, click New Multi-Task Project. The New Task - Multi-Task Project page opens.

Multi-Task Project Page Fields

Field	Description/Action
Task Name	Displays Multi-Task Project. You can enter a different task name if applicable.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Add any comments about the multiple task job.
Task Options	
Sub Tasks	Select a subtask from the drop-down menu. Depending on the subtask you select, the new task page for that task opens, where you can configure the task. For example, if you select the Configure Syslog task, the New Task - Configure Syslog page opens. As you add tasks, they are displayed on the Edit Task - Multiple Task Project page. You can edit or delete the task if necessary. When you click Save Task, the Pending Tasks page opens. Refer to "Scheduled Tasks Page Fields" on page 369.
Reserved Devices	Use the Device Selector to reserve devices. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that the tasks are to run against. The default is 60 minutes.
Approval Options	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.

Field	Description/Action
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	Not available

When you are finished, be sure to click Save Task.

How to Configure a Multi-Task Project

This section steps you through the process of setting up a multi-task project, including reserving devices and/or device groups for your project and using the Activity Calendar to view your project's reserved devices and/or device groups.

1. On the menu bar under Tasks, click New Multi-Task Project. The New Task - Multi-Task Project page opens.
2. In the Task Name field, enter a name for your project, for example Pine Valley Office. It is assumed that you have already added specific devices and/or device groups to a parent group named *Pine Valley Office*. If not, refer to "Adding Device Groups" on page 149 for information.

3. In the Start Date field, either check Start As Soon As Possible (the default) or click the calendar, from which you can select a date and time you want your project to start.
4. In the Comments field, enter comments about your project.
5. In the Sub Tasks field under Task Options, select a sub-task you want to include in your project from the drop-down menu. For example, if you select the Deploy Passwords task, the New Task - Deploy Passwords page opens.
6. Using the Deploy Passwords page, in the Applies To field, select Pine Valley Office from the drop-down menu. You could also enter the name or browse for a CSV file containing a list of the devices and/or device groups in Pine Valley Office.
7. Complete the Task Options section. The options displayed in this section differ from task to task. For information on the Deploy Password task, refer to "Deploy Passwords Task Page Fields" on page 284.
8. Click Save Task. You are returned to the Multi-Task Project page, where you can add additional sub-tasks to your project.
9. To reserve all of the devices in the Pine Valley Office, in the Reserved Devices field, click Modify. The Device Selector opens.
10. Double click Pine Valley Office. All devices in the Pine Valley Office are displayed.
11. If you want to reserve all of the devices in the Pine Valley Office, click Select All and then click the right arrows (>>>). The devices are listed in the Selected Devices box. To add only specific devices, you can narrow your search by entering a portion of the host name or IP address of the device or select only devices you want to add, and then click the right arrow.
12. Enter the Estimated Duration time for which you want to reserve the devices. The default is one hour.
13. Click Save Task. The list of reserved devices is included in the Reserved Devices field.
14. Click Save Task. The My Tasks page opens, where you can edit, delete, pause, or run your project immediately.
15. On the menu bar under Tasks, click Activity Calendar. The Activity Calendar opens.

16. Using the calendar, select the day on which your project has reserved the Pine Valley Office devices. Your project, Pine Valley Office, is displayed in the time slot you selected.
17. Click Pine Valley Office. The Task Information page opens, where you can view detailed information about your project.

Viewing My Tasks

The My Tasks page shows tasks originated by the currently logged in user, including the task approval status, if applicable, and if the task has not yet run.

To view the My Task page, on the menu bar under Tasks, click My Tasks. The My Task page opens.

My Tasks Page Fields

Field	Description/Action
My Drafts link	If applicable, opens the My Drafts page.
Approval Requests link	If the task requires approval, opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. By default, the page shows tasks that have not completed, including tasks that are: • Not approved • Waiting Approval • Waiting to run Refer to "Approval Requests" on page 695 for information.
Scheduled Tasks link	Opens the Scheduled Tasks page, where you can view scheduled tasks that are in the queue, but have not yet run. Refer to "Scheduled Tasks Page Fields" on page 369 for information.
Running Task link	Opens the Running Task page, where you can view all running tasks. Refer to "Running Tasks Page Fields" on page 371 for information.
Recent Tasks link	Opens the Recent Tasks page, where you can view all recent tasks. Refer to "Recent Tasks Page Fields" on page 373 for information.

Field	Description/Action
Show Tasks Check Boxes	If the task requires approval, you can select the following display options: • Approved • Not Approved • Waiting Approval • Overridden • Draft • No Approval Required
Check Boxes	You can use the left-side check boxes to delete tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Schedule Date	Displays the date and time the task was created.
Approved By Date	If applicable, displays the date and time the task must be approved. If a task is not approved by its approval date, its status is set to "Not Approved." (**Note**: Approval options are only displayed if the task is part of a Workflow Approval Rule.)
Task Name	Displays the task name. Clicking a task opens the Task Details page. Refer to "What Are Tasks?" on page 278 for information.
Approval Status	If applicable, displays the task's approval status. Approval status is only displayed if the task is part of a Workflow Approval Rule. Approval statuses include: • Awaiting Approval • Approved • Not Approved • Overridden • No Approval Required

Field	Description/Action
Task Status	Displays the status of the task. Statuses include: • Warning — A group task containing some failed sub-tasks, but not all tasks failed. • Draft — NCM will not run the task, nor is the task sent out for approval, when in Draft status. • Duplicate — The task was not started because an identical task is already running. • Failed — The task failed. • Paused — Someone paused the task. It will not run when its scheduled time arrives. • Pending — The task is queued and waiting for its scheduled time. • Running — The task has started, but has not yet finished. • Skipped — The task was skipped due to errors, for example incorrect permissions, unmanaged devices, and so on. • Succeeded — The task succeeded. • Waiting — Although the scheduled time has arrived, the task is waiting because the "Max Concurrent Tasks" limit has been reached.
Task Type	Displays the task type, for example: • Deploy Password • Deploy Config • Discover Driver • Reload Device • Take Snapshot • Synchronize Startup and Running Configurations For a complete list of tasks, refer to "What Are Tasks?" on page 278. (**Note**: Multi-Task Project tasks may or may not be displayed on the My Tasks results page. It depends on whether the Multi-Task Project task includes at least one of the task types listed above as a sub-task.)

Field	Description/Action
Actions	You can select one of the following options: • Edit — Opens the Edit Task page. • Delete — Enables you to delete the task. • Pause — Pauses the task so it does not run at its scheduled time. (**Note**: You can select Resume if you want to resume the task.) • Run Now — Runs the task as soon as possible. If the maximum number of concurrent tasks has not been reached, the task runs immediately.
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

Viewing Scheduled Tasks

To view scheduled tasks that are in the queue, but have not yet run, on the menu bar under Tasks click Scheduled Tasks. The Scheduled Tasks page opens.

Note: To change the task page refresh interval, on the menu bar under Admin, select Administrative Settings and click User Interface. On the User Interface page, scroll down to the Miscellaneous section and enter a task page refresh interval.

Scheduled Tasks Page Fields

Field	Description/Action
My Tasks link	Opens the My Task page. Refer to "My Tasks Page Fields" on page 365 for information.
My Drafts link	Opens the My Drafts page. Refer to "My Tasks Page Fields" on page 365 for information.
Approval Requests link	If the task requires approval, opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. Refer to "Approval Requests" on page 695 for information.
Running Task link	Opens the Running Task page. Refer to "Running Tasks Page Fields" on page 371 for information.
Recent Tasks link	Opens the Recent Tasks page. Refer to "Recent Tasks Page Fields" on page 373 for information.
Current Working Group	Displays the name of the current working group. You can select a different group from the drop-down menu and click the Refresh button.
Show Group/Parent Tasks Only	If checked, only group and parent tasks are shown.
Check Boxes	You can use the left-side check boxes to delete scheduled tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Schedule Date	Displays the date and time when NCM is scheduled to run the task.
Task Name	Displays the task name.

Field	Description/Action
Host/Group	Displays the host or group name of the network device(s) associated with the task. You can click the link to open the Device Information page, where you can view basic information about the devices in the group.
Task Status	Displays the status of the task, for example: • Pending — The task is queued, but has not yet run. • Paused — Polling is paused. To resume polling, enter the "resume polling" CLI command. • Draft — The task is in Draft mode and will not run. For a complete list of task statuses, refer to "Task Information Page Fields" on page 376.
Scheduled By	Displays the login name of the person who scheduled the task (or the last user to modify the task).
Comments	Displays comments about the pending task.
Actions	You can select the following actions for each entry in the Pending Tasks table: • Edit — Opens the Edit Task page, where you can edit and rerun the task that is recurring or has not yet occurred. • Delete — Deletes the task. • Pause — Pauses the task so it does not run at its scheduled time. (**Note**: You can select Resume if you want to resume the task.) • Run Now — Runs the task as soon as possible. If the maximum number of concurrent tasks has not been reached, the task runs immediately.
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

Viewing Running Tasks

To view running tasks, on the menu bar under Tasks click Running Tasks. The Running Tasks page opens.

Note: To change the task page refresh interval, on the menu bar under Admin, select Administrative Settings and click User Interface. On the User Interface page, scroll down to the Miscellaneous section and enter a task page refresh interval.

Running Tasks Page Fields

Field	Description/Action
My Tasks link	Opens the My Task page. Refer to "My Tasks Page Fields" on page 365 for information.
My Drafts link	Opens the My Drafts page. Refer to "My Tasks Page Fields" on page 365 for information.
Approval Requests link	Opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. Refer to "Approval Requests" on page 695 for information.
Scheduled Task link	Opens the Scheduled Task page. Refer to "Scheduled Tasks Page Fields" on page 369 for information.
Recent Tasks link	Opens the Recent Tasks page. Refer to "Recent Tasks Page Fields" on page 373 for information.
Current Working Group	Displays the current working group. Use Ctrl+click to select/deselect more than one group.
Show Group/Parent Tasks Only	If checked, only the group/parent tasks are displayed.
Refresh this page every 60 seconds	Uncheck this box if you do not want the display to refresh every 60 seconds. Refer to "User Interface Page Fields" on page 89 for information on setting this value.
Check Boxes	You can use the left-side check boxes to delete tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Start Date	Displays the date and time NCM began running the task.

Field	Description/Action
Task Name	Displays the task type.
Host/Group	Displays the host or group name of the network device(s) associated with the task. You can click the link to open the Device Information page, where you can view basic information about the devices in the group.
Task Status	Displays the status of the task (running). If the maximum number of concurrent tasks has been reached, the task is waiting for another task to finish. Consequently, the Running Tasks page returns "No Tasks Found." (**Note**: The number of tasks could exceed the Max Concurrent Tasks value because group parent tasks are not included in the setting.)
Scheduled By	Displays the login name of the person who scheduled the task (or the last user to modify the task).
Comments	Displays comments about the pending task.
Actions	You can select the following action for each entry in the Running Tasks table: • Edit — Opens the Edit Task page where you can edit the task. • Detail — Opens the Task Information page, where you can view details about the task. • Delete — Enables you to delete the task.

Viewing Recent Tasks

To view recent tasks, on the menu bar under Tasks click Recent Tasks. The Recent Tasks page opens. The Recent Tasks page shows all recent tasks, regardless of their status.

Note: To change the task page refresh interval, on the menu bar under Admin, select Administrative Settings and click User Interface. On the User Interface page, scroll down to the Miscellaneous section and enter a task page refresh interval.

Recent Tasks Page Fields

Field	Description/Action
My Tasks link	Opens the My Task page. Refer to "My Tasks Page Fields" on page 365 for information.
My Drafts link	Opens the My Drafts page. Refer to "My Tasks Page Fields" on page 365 for information.
Approval Requests link	Opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. Refer to "Approval Requests" on page 695 for information.
Scheduled Task link	Opens the Scheduled Task page. Refer to "Scheduled Tasks Page Fields" on page 369 for information.
Running Tasks link	Opens the Running Tasks page. Refer to "Running Tasks Page Fields" on page 371 for information.
Current Working Group	Displays the group name of the network device(s) associated with the task. Use Ctrl+click to select/deselect more than one group.

Field	Description/Action
Show Filters	Click the Show Filters option to display the following filters: • Show tasks within — Select the time frame for which you want to view recent tasks. • Show Detail — Click the Show Detail box and then Refresh to view task details for each task in the Recent Tasks page. • Show Group/Parent Tasks Only — Click to show only group/parent tasks. • Task Status — Check one or more task statuses to display. Be sure to click Refresh if you change the status.
Check Boxes	You can use the left-side check boxes to delete tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Complete Date	Displays the date and time NCM began running the task.
Task Name	Displays the task type.
Host/Group	Displays the host or group name of the network device(s) associated with the task. You can click the link to open the Device Information page, where you can view detailed information about the devices in the group.
Task Status	Displays the status of the task, for example: • Succeeded — The task succeeded. • Failed — The task failed. • Duplicate — The task duplicated another task. • Skipped — The task was skipped because an identical task was already running when the time arrived for this task to run. For a complete list of task statuses, refer to "Task Information Page Fields" on page 376.
Scheduled By	Displays the login name of the person who scheduled the task (or the last user to modify the task).
Comments	Displays comments about the task.

Field	Description/Action
Actions	You can select the following action for each task in the Recent Tasks table: • Detail — Opens the Task Information page, where you can view details about the task. • Run Again — Opens the Rerun Task page, where you can edit the task and run it again. (**Note**: This option only appears if the task can be rerun.)
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

Task Information Page Fields

The Task Information page includes detailed information on tasks, including:

- Task status
- Originator
- Devices affected
- Duration
- Approval information
- Result details
- Task history

The Task information page also provides links to more detailed information in the event of a warning or failure. Keep in mind that a task can be successfully completed but still contain errors. For example, you could successfully deploy to a running configuration but have invalid commands within the configuration.

To open the Task Information page:

1. Select a device from the Inventory page. The Device Details page opens.
2. From the View drop-down menu, click Device Tasks. The Device Tasks page opens.
3. Click the Detail option in the Actions column for the task on which you want detailed information. The Task Information page opens.

Field	Description/Action
Edit Task link	Opens the task page so that you can edit the task. This link is only displayed for pending tasks. Refer to "What Are Tasks?" on page 278.
Run Again link	Opens the task page so that you can re-run the task. This link is only displayed for completed tasks. Refer to "What Are Tasks?" on page 278.
Return to List link	Opens the My Tasks page. Refer to "Viewing My Tasks" on page 365.
General Information	

Field	Description/Action
Task Name	Displays the task name.
Task Status	Displays the task status, including: • Draft • Duplicate • Failed • Paused • Pending • Requested (Note: Requested means the task is waiting for Approval. Refer to "Approving Tasks" on page 698.) • Running • Skipped • Succeeded • Synchronous (**Note**: NCM typically runs tasks by creating a thread and letting the task run asynchronously in the background. The CLI and API enable synchronous tasks where they are run in the current thread and the command blocks until the command completes.) • Waiting • Warning **Note**: Multi-task projects will continue processing when a warning is encountered. The warning status is shown in the parent task.
Comments	Displays any comments about the task.
Originator	Displays the username or process that scheduled the task.
Create Date	Displays the date and time the task was created.
Devices Affected	Displays the host name and/or IP address of the affected device.
Schedule Date	Displays the date and time the task was scheduled to run.
Start Date	Displays the task's start date.
Complete Date	Displays the task's complete date.

Field	Description/Action
Duration	Displays the task's duration.
Repeat Type	Displays the repeat type, for example: non-recurring.
Approval Information	
Approver(s)	Displays a list of task approvers.
Approval Status	Displays the task approval status.
Priority	Displays the task priority.
Approved By	Displays the date and time the task must be approved.
New Comments	Enter additional comments about the task.
Approve Button	Click the Approve button to approve the task.
View Task Details link	Clicking the View Tasks link opens the Diagnostics History page.
Additional Information	
Result Details	Displays the diagnostics that were automatically run (depending on the device type), for example: • Diagnostic "NCM Module Status" completed • Diagnostic "NCM Routing Table" completed • Diagnostic "NCM Interfaces" completed • Diagnostic "NCM OSPF Neighbors" completed
Task History	
Task History Information	Displays task history information, such as when the task was run, the repeat type, and status.

Viewing Task Load

The Task Load page shows the number of tasks currently in the system. Tasks are divided into three categories:

- Tasks scheduled to start in the next 15 minutes
- Tasks waiting to execute
- Currently running tasks

Keep in mind that the Task Load page includes all tasks in the system, even those where the current user may not have permission to view. Consequently, the task count will not necessarily match the task count on the Search for Tasks page.

To view the Task Load page, on the menu bar under Tasks, click Task Load. The Task Load page opens. (You can also access this page under Admin.)

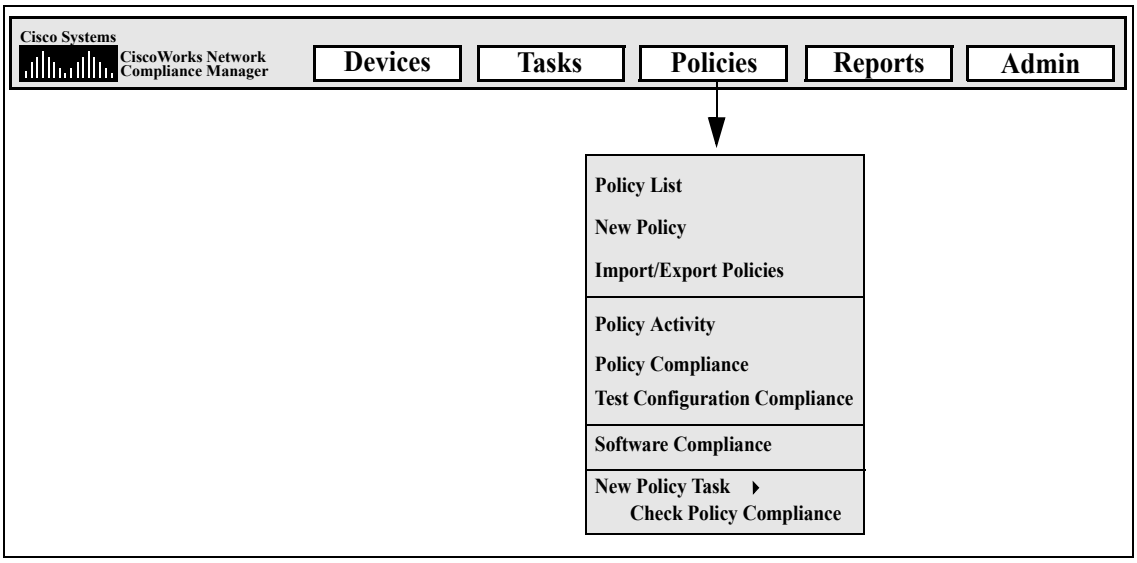
Task Load Page

Field	Description
Tasks Starting in < 15 minutes	Displays the number of task scheduled to start in the next 15 minutes.
Tasks Waiting	Displays the number of waiting tasks. If the maximum number of concurrent tasks has been reached, the task is waiting for another task to finish.
Tasks Running	Displays the number of running tasks.

Chapter 8: Managing Policy Assurance

Use the following table to quickly locate information.

Navigating to Policy Assurance



Getting Started

The NCM Policy Manager enables you to establish network configuration policies and best practices to ensure maximum uptime and reliability. In addition, you can designate standardized device configurations, thereby decreasing individual configuration variances. The NCM Policy Manager ensures that all infrastructure change activity is reported by comparing a device's configuration against a set of approved configuration policies.

The NCM Policy Manager applies a set of rules, or filters, to each device configuration change that NCM detects. If a change to a device (or group of devices) is non-compliant, the NCM Policy Manager generates an event and triggers a notification rule. As a result, you can correct the non-compliant change, preserving both compliance and network availability.

You can summarize policy compliance status for all of your managed devices. This enables you to provide a risk-rated snapshot of your policy compliance status and quickly identify and resolve high-risk configuration and software compliance violations.

The following terms are used in this section:

- Configuration Policy — A configuration policy is a set of configuration rules applied to a device or group of devices. Each of the rules is checked against the device’s configuration to ensure that the device is in compliance.
- Configuration Rule — A configuration rule is part of a Configuration Policy. It is written as a regular expression, for example *ip name-server* or *interface FastEthernet*. This expression is matched against a device's configuration to which the configuration rule is applied. Each configuration rule applies only to a selected device family, such as BayStack or Cisco IOS.
- Configuration Rule Exception — A configuration rule exception is part of a configuration rule. Like a configuration rule, it is a regular expression. However, its purpose is to exclude text it matches in the device configuration from consideration by the configuration rule it's part of.

Note: Administrator or Power User permissions are required to create both configuration rules and exceptions.

Creating a Configuration Policy

Before you can create configuration rules, you need to create a configuration policy. To create a configuration policy, on the menu bar under Policies click Policy List. The Policies page opens. The page is empty until you create a configuration policy.

NCM ships with several default policies, including the NSA Router Best Practices policy. Some examples of policies you might want to configure include:

- All configurations in a device group must have Access List 110 defined.
- All Fast Ethernet interfaces must have duplex set to Auto Negotiate.
- All border routers must have certain DNS servers.

Note: You can navigate directly to the New Configuration Policy page by clicking the New policy option, or you can view the existing polices on the Policies page and then click the New Configuration Policy link at the top of the page.

Policies Page Fields

Field	Description
New Configuration Policy link	Opens the New Configuration Policy page, where you can create a new configuration policy. Refer to "New Configuration Policy Page Fields" on page 387 for information.
Check Policy Compliance link	Opens the Check Policy Compliance task page, where you can check for policy compliance. Refer to "Check Policy Compliance Task Page Fields" on page 342 for information. (**Note**: You can also navigate to the Check Policy Compliance task page by clicking the Check Policy Compliance option under Policies/New Policy Task on the menu bar.)
Import/Export link	Opens the Import/Export Policies page, where you can import a pre-configured configuration policy or export a configuration policy to a file. Refer to "Importing/Exporting Configuration Policies" on page 393 for information. (**Note**: You can also navigate to the Import/Export Policies page by clicking the Import/Export Policies option.)
Check Boxes	You can use the left-side check boxes to manage configuration policies. Once you have selected the policies, click the Actions drop-down menu and click either: • Activate — Instructs NCM to check the compliance configurations against the selected policies. • Deactivate — Instructs NCM not to check the compliance configurations against the selected policies. • Delete — Deletes the selected polices. The adjacent Select drop-down menu enables you to select or deselect all of the polices.
Policy Name	Displays the policy name.
Description	Displays a description of the policy.
Actions	You can select the following action: • View & Edit — Opens the Edit Configuration Policy page, where you can edit the configuration policy. Refer to "Editing a Configuration Policy" on page 394 for information. • Test — Opens the Test Policy Page, where you can test the policies against a device or group of devices. Refer to "Test Policy Page Fields" on page 386 for information.

Test Policy Page Fields

The Test Policy page enables you to test a policy against a device or group of devices. When you have selected the devices, click the Perform Test button.

Field	Description/Action
Select the policies to be tested	Select a policy from the drop-down menu.
Select the devices to test against	For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector.

New Configuration Policy Page Fields

To open the New Configuration Policy page, on the menu bar under Polices, click New Policy. The New Configuration Policy page opens.

Field	Description/Action
Policy Name	Enter the policy name. A policy is a set of configuration rules applied to a device or a group of devices.
Policy Description	Enter a description of the policy.
Scope	Select one of the following options: • Select the device groups to which this policy applies — Select one or more device groups from the list. You can use Shift+click or Ctrl+click to select multiple device groups. • Use filters to define a dynamic policy scope — A policy scope includes the devices a policy can potentially affect. Keep in mind that the policy scope can only affect a given device if the policy has a policy rule that affects the device family containing the device. When defining a policy, you can define the policy scope the same way you define a Dynamic Group. As a result, you can create a private Dynamic Group in conjunction with a policy. (Refer to "Dynamic Device Groups" on page 154 for information on creating Dynamic Groups.)
..but not these devices	Enter the IP address or hostname of the device in the right-hand box and then click Add Exception <<. To remove a device, select the IP address or hostname of the device in the left-hand box and click Remove Exception.
Configuration Rules	The configuration rules table displays all configuration rules that will be applied by the configuration policy. The configuration policy applies all configuration rules to each configuration saved by NCM from the devices selected for this configuration policy. Keep in mind that configuration rules are applied in no particular order.
New Rule button	To create a new rule for this configuration policy, click the New Rule button. The New Configuration Rule page opens. Refer to "New Configuration Rule Page Fields" on page 389 for information.
Detailed Description	Enter a detailed description of the configuration policy. Keep in mind that a short description of the configuration policy appears in any list in which the policy appears. This field enables you to add a detailed description of the configuration policy.

Field	Description/Action
Policy Status	Click one of the following options: • Active — Marks the configuration policy active (the default). • Inactive — Deactivates the configuration policy.

Be sure to click the Save when you are finished.

New Configuration Rule Page Fields

When you click the New Rule button on the New Configuration Policy page, the New Configuration Rule page opens.

A configuration rule is part of a Configuration Policy. It is written as a regular expression, for example *ip name-server* or *interface FastEthernet*. This expression is matched against a device's configuration to which the configuration rule is applied. Each configuration rule applies only to a selected device family, such as BayStack or Cisco IOS.

Note: NCM uses Regular Expressions, or RegEx (an expression that describes a set of strings) to define configuration rules.

Field	Description/Action
New Configuration Rule	
Rule Name	Enter the configuration rule name.
Rule Description	Enter a description of the configuration rule.
Applies to configurations from devices with these drivers	
Device Family	Select the device family to which the configuration rule applies from the drop-down menu, for example BayStack, Cisco IOS or Nortel ASF. Select one of the following options: • All applicable drivers — If checked (the default), NCM chooses all applicable drivers. Keep in mind that a configuration rule applies only to the configuration for devices that are assigned a specific driver. • Select specific drivers — If checked, select one or more drivers from the list. Keep in mind that a configuration rule applies only to the configuration for devices that are assigned a specific driver.

Field	Description/Action
Apply Rule To	Select one of the following options: • Entire Configuration File — Applies the configuration rule to the entire configuration file (the default). • Each Instance of a Block Within the Configuration File — Applies the configuration rule to specific blocks within the configuration file, such as a single interface in a Cisco IOS device. A block is defined by two regular expressions: The "block start pattern" and the "block end pattern." If you are applying the configuration rule to each instance of a specific block within the configuration file, enter the block start pattern, for example *interface .** and the block end pattern, for example *!*.
Each Configuration <must contain> or <must not contain> text that matches the pattern	Enter the desired pattern and if it <must contain> or <must not contain> text that matches the pattern. "Must contain" specifies that the configuration files to which this rule applies must contain text that matches the text you enter. "Must not contain" specifies that the configuration files to which this rule applies must not contain the text you enter. (**Note**: The Get Help link provides information and examples on how to use Regular Expressions.)
Each Configuration must contain these lines in any order	Enter the desired lines from the configuration. The NCM Policy Manager looks at each line in the text area independently. The NCM Policy Manager searches the configuration for a match of that line. If a match is not found, the configuration is considered out-of-compliance with the Policy Rule. (**Note**: The NCM Policy Manager performs the search in no particular order.)

Field	Description/Action
Importance	Select the importance level. This indicates the non-compliance risk rating for the configuration policy rule. NCM can sort violations based on their severity. For example, Critical violations can automatically open a trouble ticket in the Change Management system, while Informational violations can be identified in a daily report. Options include: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours (the default). • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Detailed Description	Enter a description of the configuration rule.
Rule Exceptions	Displays a list of rule exceptions, if applicable. A configuration rule exception is part of a configuration rule. Its purpose is to exclude text it matches in the device configuration from consideration by the configuration rule it's part of. To add an Exception Rule, click the New Exception link. The New Configuration Rule Exception page opens. (Refer to "Adding a Configuration Rule Exception" on page 396 for information.)
Auto-Remediation	Displays a list of Auto-remediation scripts, if applicable. An Auto-remediation script enables you to define variables in the script that reference data from the configuration that caused a configuration rule to fail. Keep in mind that variables obtain their values from capturing groups in the rule pattern. For a variable to reference a capturing group from the rule pattern, its name must be the same number as the capturing group from the pattern. For example, the *1* variable in an Auto-remediation script will be replaced with the value of the first capturing group from the rule pattern when the script is run. To add a new Auto-remediation script, click the New Auto-Remediation Script link. The New Command Script page opens. (Refer to "Adding Command Scripts" on page 558 for information on running command scripts.)

When you are finished, you can either click the Save button to save the configuration rule, the Save And Add Another button to save the current rule and add a new one, or the New Exception button to add a new configuration rule exception.

Importing/Exporting Configuration Policies

You can import pre-defined configuration policies or export configuration policies to a file. This enables you to easily share configuration policies.

To import or export a configuration policy, on the menu bar under Policies, click Import/Export Policies. The Import/Export Policies page opens.

Import/Export Policies Page Fields

Field	Description/Action
Import Policy	Enter the policy file to import or click the Browse button to locate the policy file. When the policy file is displayed, click the Import button. If the policy file already exists, you are prompted to rename it.
Export Policy	Displays a list of the current configuration policies. Click the configuration policies you want to export and then click the Export button. Keep in mind that the device groups associated with the configuration policy, if applicable, are not exported. Also, any configuration policy exception rules are not exported. Example policies include: • Ensure Logging • Ensure Passwords • No Delay on Interfaces • NSA Router Security Best Practices

Editing a Configuration Policy

To edit a configuration policy:

1. On the menu bar under Policies, click Policy List. The Policies page opens.
2. Click the View & Edit action for the configuration policy you want to edit. The Edit Configuration Policy page opens. Be sure to click Save when finished.

Edit Configuration Policy Page Fields

Field	Description/Action
Policy Name	Displays the policy name.
Policy Description	Displays a description of the policy.
Scope	Select one of the following options: • Select the device groups to which this policy applies — Select one or more device groups from the list. You can use Shift+click or Ctrl+click to select multiple device groups. • Use filters to define a dynamic policy scope — A policy scope includes the devices a policy can potentially affect. Keep in mind that the policy scope can only affect a given device if the policy has a policy rule that affects the device family containing the device. When defining a policy, you can define the policy scope the same way you define a Dynamic Group. As a result, you can create a private Dynamic Group in conjunction with a policy. (Refer to "Dynamic Device Groups" on page 154 for information on creating Dynamic Groups.)
..but not these devices	To add an IP address or hostname of the device, enter the Host name or IP address in the right-hand box and then click Add Exception <<. To remove a device, select the IP address or hostname of the device in the left-hand box and click Remove Exception.

Field	Description/Action
Configuration Rules	Displays all configuration rules that will be applied by the configuration policy. The configuration policy applies all configuration rules to each saved configuration from the devices selected for this configuration policy. Keep in mind that configuration rules are applied in no particular order. The importance column displays either Informational, Low, Medium, High, or Critical. This indicates the non-compliance risk rating for the configuration policy rule. Click the View & Edit link in the Actions column to edit the configuration rule.
New Rule button	To create a new rule for this configuration policy, click the New Rule button. The New Configuration Rule page opens. Refer to "New Configuration Rule Page Fields" on page 389 for information.
Detailed Description	Displays a detailed description of the configuration policy.
Policy Status	Click one of the following options: • Active — Marks the configuration policy active (the default). • Inactive — Deactivates the configuration policy.

Adding a Configuration Rule Exception

A configuration rule exception is part of a configuration rule. Like a configuration rule, it is a regular expression. However, its purpose is to exclude text it matches in the device configuration from consideration by the configuration rule it is part of.

An exception rule typically excludes either a text pattern or a specific device configuration from the configuration rule. Exceptions are usually created when one or more device configurations do not comply with a rule, but you cannot alter the rule to fit all similar configurations.

To add a configuration rule exception to an existing configuration rule:

1. On the menu bar under Policies, click Policy List. The Policies page opens.
2. Select the policy to which you want to add the exception rule and click View & Edit. The Edit Configuration Policy page opens.
3. Click the New Rule button. The New Configuration Rule page opens.
4. Click the New Exception button at the bottom of the page. The New Configuration Rule Exception page opens.

New Configuration Rule Exception Page Fields

Field	Description/Action
Expires on	If checked, choose the month, day, year, hour, and minute after which this exception is disregarded by the rule. An exception rule's expiration date is the date after which the exception ceases to have any effect on the rule it is part of. Although the exception rule continues to exist after its expiration date, the configuration policy applies the rule as if the exception rule does not exist.
Ignore this device entirely when checking the configuration rule	If checked, NCM skips this device when checking the configuration rule.
Ignore text matching this pattern when checking the configuration rule	If checked, enter a regular expression. All text in a configuration rule that matches the regular expression is not subject to this configuration rule. (**Note**: The Get Help option provides examples.)
Device	Enter the IP address or hostname of the device to which this exception rule applies.

Be sure to click the Save button when you are finished.

Viewing Configuration Policy Activity

You can view events that show a device's configuration was not in compliance with the configuration rules contained in one or more configuration policies. The events indicate when NCM detected and recorded that a device's configuration was non-compliant.

To view the Configuration Policy Activity page, on the menu bar under Policies, click Policy Activity. The Configuration Policy Activity page opens.

Configuration Policy Activity Page Fields

Field	Description/Action
For the (time frame)	Select the time frame in which you want to view non-compliance events. The default is the past hour.
Current Working Group	Select the group for which you want to view non-compliance events. The default is Inventory, which includes all other groups.
Event Date	Displays the date the configuration policy was found to be in non-compliance.
Policy Name	Displays the name of the configuration policy. Click this link to open the Edit Configuration Policy page. You can edit the configuration policy and any included configuration rules. Refer to "Editing a Configuration Policy" on page 394 for information.
Host Name	Displays the host name of the device. Click this link to view basic information about the device and its configuration history.
Device IP	Displays the IP address of the device. Click this link to view basic information about the device and its configuration history.
Summary	Displays the event type (Configuration Policy Non-Compliance). Click this link to open the System Event Detail page, where you can view details of the non-compliance event.

Field	Description/Action
Importance	Indicates the importance of the compliance rule that was violated, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Added By	Displays the person or process that added the configuration policy.

Viewing Policy Compliance

The Policy Compliance page enables you to view the devices whose configurations are or are not in compliance with configuration policies. To view the Policy Compliance page, on the menu bar under Policies, click Policy Compliance. The Policy Compliance page opens.

Policy Compliance Page Fields

Field	Description/Action
Check Policy Compliance link	Opens the Check Policy Compliance task page, where you can check for configuration compliance. Refer to "Check Policy Compliance Task Page Fields" on page 342 for information.
Current Working Group	Select the group for which you want to view device compliance status.
Display only devices that are not in compliance	If checked, devices that are in compliance are not displayed.
Host Name	Displays the host name of the device. Click this link to view basic information about the device and its configuration history.
Site	Displays the Site to which the device belongs.
Policy Compliance	• Yes — Indicates that the device's configuration is in compliance with all configuration polices. • No — Indicates that the device's configuration is not in compliance with all configuration policies.
Device IP	Displays the IP address of the device. Click this link to view basic information about the device and its configuration history.
Importance	Displays the highest importance of all configuration policy rules currently violated by the device. • Critical — Red • Medium — Blue • Low — Yellow
Last Changed Time	Displays the date and time the device's configuration was last changed.

Field	Description/Action
Actions	You can select the following options: • Policy Events — Opens the Configuration Policy Activity page, where you can view the details of the non-compliance event. • Policies Applied — Opens the Configuration Policies that Apply to Device page, where you can view the configuration polices and rules for a specific device. Refer to "Configuration Policies That Apply to Device Page Fields" on page 402 for information.

Configuration Policies That Apply to Device Page Fields

To view the Configuration Policies That Apply to Device page:

1. On the menu bar under Policies, click Policy Compliance.
2. In the Actions column for the device on which you need information, click the Policies Applied link. The Configuration Policies That Apply to Device page opens.

Field	Description/Action
Policy Name	Displays the name of the configuration policy applied to the device.
Rule Name	Displays the name of the configuration rule applied to the device.
Out of compliance key	Displays if the device is currently out of compliance, including: • Critical Importance (red) • High Importance (red) • Medium Importance (amber) • Low Importance (yellow) • Informational (yellow)
Actions	You can select the following options: • Host name or IP address — Opens the Device Information page, where you can view basic information about the device and its configuration history. • Policy Name — Opens the Edit Configuration Policy page, where you can edit the policy and add/edit configuration rules. Refer to "Editing a Configuration Policy" on page 394. • Rule Name — Opens the Edit Configuration Rule page, where you can edit the configuration rule. Refer to "Adding a Configuration Rule Exception" on page 396.

Adding a New Software Compliance

As network device security alerts and notifications about security vulnerabilities continue to increase, many organizations are faced with tracking which OS version is present on each device and whether that OS version is vulnerable to security issues. NCM enables you to specify OS versions that are susceptible to security problems and then generate alerts or automated responses when those versions are detected. Keep in mind that you can group images into categories, such as "pre-production" or "Obsolete." Images can also classified, for example "Security Risk," based on recently discovered vulnerabilities.

To add a new software compliance or review existing compliance definitions:

1. On the menu bar under Polices, click Software Compliance. The Software Compliance page opens. (Refer to "Software Compliance Page Fields" on page 406 for information on the Software Compliance page.)
2. Click the Add Compliance link. The Add Compliance page opens. Be sure to click Save when you are finished.

Add Compliance Page Fields

Field	Description/Action
Add Compliance	
Policy Name	Enter the policy name.
Status	Displays one of the following options: • Active — Marks the configuration policy active (the default). • Inactive — Deactivates the configuration policy. Inactive policies do not generate non-compliance events.

Field	Description/Action
Compliance Level	Select a compliance rating name. You can use any of the compliance definitions given depending on your requirements and validation procedures. Options include: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Description	Enter a description of the compliance. To improve awareness of security issues, any security risk description should include a short title of the vulnerability, any applicable CVE/CAN or CERT designations, and a link to the vendor notice, if available.
Matching Criteria (Matching criteria can use wildcard operators: * and ?.)	
Software Version	Enter the software version currently running on the device.
Device Driver	Select a device driver used to access the device from the drop-down menu. (Any is the default.)
Device Model	Enter the device model.
Configuration Contains	Enter a pattern to match against the current device configuration to determine if the compliance applies to a given device.
Software Vulnerability Information (for Security Risk compliance level)	
Discloser Date	Enter the date when the software vulnerability was flagged in the following format: *yyyy-MM-dd*.

Field	Description/Action
Importance	Select the severity of the security vulnerability from the drop-down menu, including: • Informational • Low • Medium • High • Critical
CVE Name	Enter the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures. (For more information, refer to www.cve.mitre.org.)
Solution	Enter detailed solution information.
Advisory Link	Enter the URL to an external reference for advisory information on a vulnerability.
Solution Link	Enter the URL to an external reference for more information on possible solutions to the vulnerability.

Software Compliance Page Fields

The Software Compliance page enables you to review existing software compliance definitions.

Field	Description/Action
Add Compliance link	Opens the Add Compliance page, where you can add a compliance. Refer to "Add Compliance Page Fields" on page 403.
Device Software Report link	Opens the Device Software report, where you can view the software version and compliance rating currently assigned to each device. Refer to "Device Software Report Fields" on page 593.
Software Vulnerabilities Report link	Opens the Software Vulnerabilities report, where you can view the software version and compliance rating currently assigned to each device, along with any security violation events sorted by importance. Refer to "Software Vulnerability Report Fields" on page 595.
View	Select either "User-define policies" or "Security Alert Service alerts" from the drop-down menu. Security Alert Service alerts are events originating from the Security Alert Service. (**Note**: The Security Alert Service is a subscription-based service.)
Checkboxes	You can use the left-side check boxes to manage software compliance definitions. Once you have selected the compliance definitions, click the Actions drop-down menu and click either: • Activate — Instructs NCM to activate the software compliance definition. • Deactivate — Instructs NCM to deactivate the software compliance definition. • Delete — Deletes the software compliances definition. The adjacent Select drop-down menu enables you to select or deselect all of the polices.
Name	Displays compliance's name.
Version	Displays the software version.
Driver	Displays the driver name.
Model	Displays the model designation of the device.

Field	Description/Action
Filename	You can provide a filename (wildcards are allowed), that the system can use to determine compliance. For example, you can tag all images that begin with router5*.bin as Obsolete.
Compliance	Displays the compliance rating name. Ratings include: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Importance	Displays either Informational, Low, Medium, High, or Critical. This indicates the importance of the compliance rule that was violated. • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Comments	Displays a description of the compliance.
Actions	You can select the following options: • Edit — Opens the Edit Compliance page where you can edit the compliance. • Delete — Enables you to delete the compliance.

Editing a Software Compliance

To edit a software compliance:

1. On the menu bar under Policies, click Software Compliance. The Software Compliance page opens.
2. Click the Edit action for the software compliance you want to edit. The Edit Compliance page opens. Be sure to click Save when finished.

Edit Compliance Page Fields

Field	Description/Action
Edit Compliance	
Policy Name	Displays the policy name.
Status	Displays one of the following options: • Active — Marks the configuration policy active (the default). • Inactive — Deactivates the configuration policy. Inactive policies do not generate non-compliance events.
Compliance Level	Displays the compliance rating name. You can use any of the compliance definitions given depending on your requirements and validation procedures. Options include: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Description	Displays a description of the compliance.
Matching Criteria	
Software Version	Displays the software version currently running on the device.

Field	Description/Action
Device Driver	Displays the device driver used to access the device.
Device Model	Displays the device model.
Configuration Contains	Displays the pattern used to match against the current device configuration to determine if the compliance policy applies to a given device.
Software Vulnerability Information (for Security Risk compliance level)	
Discloser Date	Displays the date when the software vulnerability was flagged.
Importance	Displays the severity of the security vulnerability, including: • Informational • Low • Medium • High • Critical
CVE Name	Displays the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures. (For more information, refer to www.cve.mitre.org.)
Solution	Displays solution information.
Advisory Link	Displays a URL to an external reference for advisory information on a vulnerability.
Solution Link	Displays a URL to an external reference for more information on possible solutions to the vulnerability.

Testing Configuration Compliance

You can test device configurations for compliance against one or more configuration policies or test your configuration policies against one or more configurations. This enables you to test a device's configuration compliance or test a configuration policy before deployment.

On the menu bar under Policies click Test Configuration Compliance. The Test Configuration Compliance page opens.

Test Configuration Compliance Page Fields

Field	Description/Action
Policy List link	Opens the Polices page, where you can view a list of your policies. Refer to "Policies Page Fields" on page 385 for information.
Select the policies to be applied	You can select one of the following options: • All Policies — If checked (the default) all of your configuration policies are tested. • Polices that are applicable to selected device groups — Select a device group for which to run the test against. To select multiple device groups, press the Shift key while selecting device groups. • Selected policies — Select a specific policy. To select multiple policies, press the Shift key while selecting policies.
Test policy against existing devices	If you select this option, the Device Selector opens. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector.
Test policy against configuration	If you select this option, enter or paste the configuration text in the box and select the device family for the configuration text you entered from the drop-down menu.

When you are finished, click Perform Test. If the configuration policy check passes, the "The configuration is in compliance with all selected policies" message is displayed at the bottom of the page. If the configuration policy check fails, a list of each violation is displayed at the bottom of the page with links, such as "View the entire configuration," to detailed information.

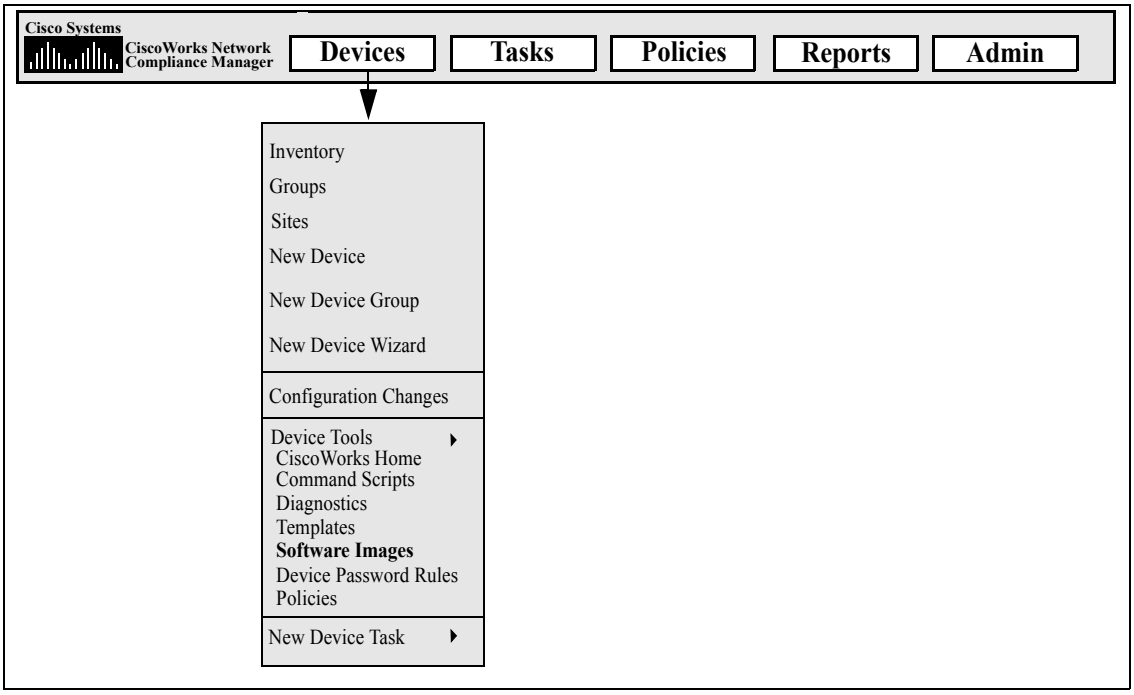
Note: You can also test a policy against configuration text by clicking the Test option in the Actions column on the Policies page. The Test Policy page opens. Refer to "Test Configuration Compliance Page Fields" on page 410 for information.

Chapter 9: Deploying Software

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 414
Software Images	"Software Images" on page 417
Adding Image Sets	"Adding Image Sets" on page 419
Deploying Software	"Deploying Software" on page 422
Adding a New Compliance	"Adding a New Compliance" on page 423
Viewing Device Software Versions	"Viewing Device Software Versions" on page 426

Navigating to Software Images



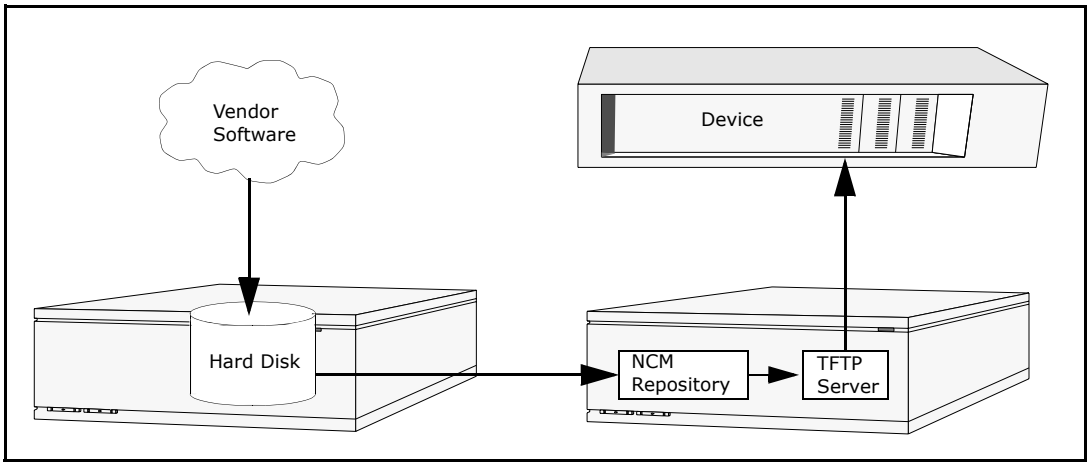
Getting Started

CiscoWorks Network Compliance Manager (NCM) provides a central repository of device software, including operating system (OS) images, that you can deploy to one or more devices that share the same software. Having a central storage location guarantees that the last known good software is available in-house.

You can:

- Load software image sets into the system. An image set is a grouping of images that can be deployed to a device simultaneously. An image set can contains one or more images. When you initiate a software upload, you select an image set to be uploaded. Each image in the image set is uploaded in turn. If the device has a problem (e.g. out of memory), the rest of the upload is aborted.
- Define the minimum requirements for an image set, such as the device family, device model, minimum volatile RAM available, processor, or boot ROM version required to run the image successfully.
- Prepare a device prior to deploying an image by deleting files to free up flash memory space, and/or compacting the flash memory.
- Reboot a device after deploying an image.
- Schedule updates through NCM. For example, you might deploy a new image to one device successfully during the day shift, then schedule updates to many more devices during off-peak hours.
- Define multiple compliance ratings to identify software versions and upgrade devices as resources permit.

The figure below illustrates the download process.



There are several best practices that you should follow when using the software update feature. Cisco recommends the following practices when deploying software images:

- Follow your standard change control and approval processes. Any time you modify the state of a device some risk is entailed. To minimize the impact this could have on your network, adhere to all defined change processes in the organization, such as approvals, notifications, change windows, and so on.
- Research and understand the proper steps for updating a given device and OS version. On some devices, multiple images may be required to upgrade. In addition, there may be firmware or hardware dependencies.
- Test the functionality of a given OS version before deploying it on a production network. When upgrading (or particularly when downgrading) OS versions, the device configuration may be altered or may need to be updated prior to or after the change. Before deploying a given version in production test it thoroughly in a test-lab environment to ensure the configuration upgrades successfully and the device functions as expected.
- Backup your current device images. Use the NCM repository to store the existing images on your devices before upgrading them. This way you can quickly recover should a new image exhibit any unexpected results.

- Whether upgrading a device, it is a good idea to have out-of-band management access to the device via a console server.
- Provide image requirements and verify them carefully. NCM enables you to specify the requirements for each software image.
- When deploying images to business critical devices, do not use the auto-reboot function. Rather, use the software update feature to prepare the devices and load the images, then manually inspect each device to be sure it is in a clean state before rebooting it.
- Update a single device first before updating a group of devices.

Software Images

Before you upgrade a device's software, you should view a list of your devices, along with the currently installed software on each device, including:

- Image set
- Filenames
- Required driver
- Hardware requirements

On the menu bar under Devices, select Device Tools and click Software Images. The Software Images Page opens.

Software Images Page Fields

Field	Description/Action
Add Image Set link	Opens the Add Software Image Set page, where you can add an Image Set. Refer to "Adding Image Sets" on page 419 for information.
Software Compliance link	Opens the Software Compliance page, where you can add a new compliance or view the Device Software report. Refer to "Adding a New Software Compliance" on page 403 for information on adding a new compliance. Refer to "Device Software Report" on page 593 for information on the Device Software report.
Image Set	Displays the name of the Image Set.
Driver Required	Displays the name of the NCM driver required for this platform.
Model Required	Displays the name of the required model.
Hardware Required	Displays hardware requirements, if applicable.
Added By	Displays the name of the person who downloaded the software.

Field	Description/Action
Actions	You can select the following options: • Edit — Opens the Edit Software Image page, where you can edit existing software information. Refer to "Edit Software Image Page Fields" on page 421 for information. • Software Images — Opens the Manage Images in Set page, where you can edit the image set, add images, and deploy software. Refer to "Add Software Image Set Page Fields" on page 419, "Edit Software Image Page Fields" on page 421, or "Deploying Software" on page 422. • Delete — Enables you to delete the image. • Update Device — Opens the Update Device Software Task page. Refer to "Deploying Software" on page 422 for information.

Adding Image Sets

To add Image Sets:

1. On the menu bar under Devices, select Device Tools and click Software Images. The Software Images page opens.
2. Click the Add Image Set link at the top of the page. The Add Software Image Set page opens. Be sure to click the Save Software button when finished.

Add Software Image Set Page Fields

Field	Description/Action
Image Set Name	Enter the Image Set Name. All images in a particular Image Set are applied to the same file system location on the device.
Image 1... 5	You can enter up to five new images or configuration files for the Image Set.
Vendor MD5 Checksum	Enter the vendor's MD5 checksum. Checksum is a 128-bit checksum computed using the MD5 algorithm. MD5 is a cryptographically secure algorithm. It is very difficult for someone to intentionally change a file and still obtain the same checksum for the file. Frequently, a vendor supplies these checksums along with the software images for their devices. If you compute the checksum on the image (or NCM computes it for you), it should match what the vendor supplied. If it does not match, you probably have a corrupted image file which should not be deployed or the vendor may have calculated a checksum using a different algorithm.
ZIP with multiple images	Specify a ZIP compressed file which will be uncompressed.

Field	Description/Action
Image Set Requirements	Image Set requirements include: • Driver — The driver information to save with the software. The list includes all known drivers. For example, if you want to upload software on a Cisco Aironet 1100 Access Point, select the "Cisco Aironet access points, 350, 1100, and 1200 series, IOS version 12.2" drivers. • Model — The model information to save with the software. The list includes all known models. For example, if you have a Cisco Aironet 1200 series Access Point, select "AIR-AP1220-IOS-UPGRD (C1200 Series)." • System Memory (in bytes) >= — The minimum RAM the image set requires to operate successfully. On most devices, the image resides in processor memory, also known as System Memory or DRAM. The amount of processor memory physically present is calculated for each device using the File System diagnostic. For example, 16,384 bytes equals 16k. Note that not all devices support the File System diagnostic. On those devices, the RAM requirement is ignored. • Processor — The CPU on the device. For example, if you have a Cisco Aironet 1200 series Access Point, select "AIR-AP1220-IOS-UPGRD (PowerPC405GP)." • Boot ROM — The ROM on the device.
Description	Enter a brief description to differentiate this software download from others.

Edit Software Image Page Fields

To edit software images:

1. On the menu bar under Devices, select Device Tools and click Software Images. The Software Images page opens.
2. For the image set you want to edit, click the Edit option in the Actions column. The Edit Software Image Set page opens.

Field	Description/Action
Image Set Name	Displays the name for this image set. You can also specify an existing image set, in which case NCM adds the new image to the existing image set. All images in a particular image set are applied to the same file system location on the device.
Image Set Requirements	• Driver — The driver information to save with the software. The list includes all known drivers. For example, if you want to upload software on a Cisco Aironet 1100 Access Point, select the "Cisco Aironet access points, 350, 1100, and 1200 series, IOS version 12.2" drivers. • Model — The model information to save with the software. The list includes all known models. For example, if you have a Cisco Aironet 1200 series Access Point, select "AIR-AP1220-IOS-UPGRD (C1200 Series)." • Device RAM Required >= — The minimum RAM of the device. • Processor — The CPU on the device. For example, if you have a Cisco Aironet 1200 series Access Point, select "AIR-AP1220-IOS-UPGRD (PowerPC405GP)." • Boot ROM — The ROM on the device. • Description — A brief description, to differentiate this software download from others.

Be sure to click Save Software when finished.

Deploying Software

The Update Software option enables you to automatically upgrade the current software images installed on your devices. This significantly reduces the time it takes to manually roll out network-wide software upgrades and provides an audit trail for software upgrades to ensure that all policies and procedures are being followed.

To automatically upgrade the current software image on your devices:

1. On the menu bar under Devices, select Device tools and click Software Images. The Software Images page opens.
2. For the image set you want to deploy, click the Update Software option in the Actions column. The Update Device Software task opens. Refer to "Update Device Software Task Page Fields" on page 322 for information.

Keep in mind that:

- Total memory is the total physical memory on the device.
- Free memory is the free memory available for uploads at the time of the last memory diagnostic.
- Net memory is the estimate of free memory after the Update Device Software task is run, taking into account any files you marked to be added or removed from the device (but not taking into account the squeeze pre or post processing task).

Adding a New Compliance

It is very important that your devices are running the latest approved software. Network administrators can group images into categories, such as Pre-production or Obsolete. Images can also classified, for example Security Risk, based on recently discovered vulnerabilities.

To add a new compliance or review existing compliance definitions:

1. On the menu bar under Devices, select Device Tools and click Software Images. The Software Images page opens.
2. Click the Software Compliance option at the top of the page. The Software Compliance page opens.
3. Click the Add Compliance option. The Add Compliance page opens. Be sure to click Save when finished.

Add Compliance Page Fields

Field	Description/Action
Add Compliance	
Policy Name	Enter the policy name.
Status	Displays one of the following options: • Active — Marks the configuration policy active (the default). • Inactive — Deactivates the configuration policy. Inactive policies do not generate non-compliance events.

Field	Description/Action
Compliance Level	Select a compliance rating name. You can use any of the compliance definitions given depending on your requirements and validation procedures. Options include: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Description	Enter a description of the compliance.
Matching Criteria (Matching criteria can use wildcard operators: * and ?.)	
Software Version	Enter the software version currently running on the device.
Device Driver	Select a device driver used to access the device from the drop-down menu. (Any is the default.)
Device Model	Enter the device model.
Configuration Contains	Enter a pattern to match against the current device configuration to determine if the compliance applies to a given device.
Software Vulnerability Information (for Security Risk compliance level)	
Discloser Date	Enter the date when the software vulnerability was flagged in the following format: *yyyy-MM-dd*.
Importance	Select the severity of the security vulnerability from the drop-down menu, including: • Informational • Low • Medium • High • Critical

Field	Description/Action
CVE Name	Enter the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures. (For more information, refer to www.cve.mitre.org.)
Solution	Enter detailed solution information.
Advisory Link	Enter the URL to an external reference for advisory information on a vulnerability.
Solution Link	Enter the URL to an external reference for more information on possible solutions to the vulnerability.

Viewing Device Software Versions

The Device Software report enables you to view the software version and compliance rating currently assigned to each device.

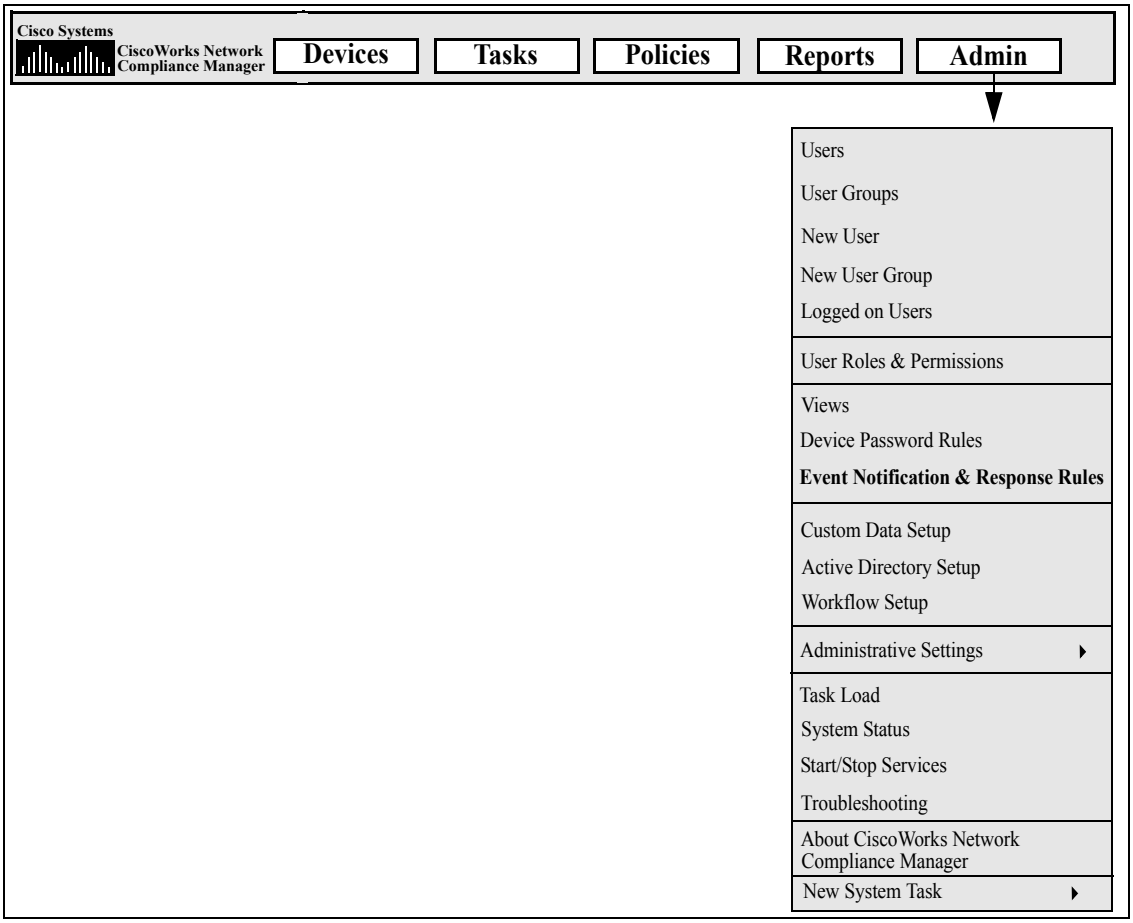
1. On the menu bar under Devices, select Device Tools and click Software Images. The Software Images page opens.
2. Click the Software Compliance option at the top of the page. The Software Compliance page opens.
3. Click the Device Software Report option at the top of the page. The Device Software Report opens. Refer to "Device Software Report Fields" on page 593 for information.

Note: You can also navigate to the Device Software report from the Reports drop-down menu.

Chapter 10: Event Notification Rules

Use the following table to quickly locate information.

Navigating to Event Notification Rules



Getting Started

CiscoWorks Network Compliance Manager (NCM) enables you to trigger many different actions when events occur in the system, including:

- Running tasks, such as snapshots or diagnostics
- Sending Email notification
- Sending Email digests
- Sending SNMP traps
- Sending Syslog messages

Event rules can be limited to specific device groups and/or times of day. The following table describes the available events from which you can select. The events are listed in alphabetical order.

Event	Description
Approval Denied	A user has denied an approval request.
Approval Granted	A user has approved a task.
Approval No Longer Required	A task approval is no longer required.
Approval Override	A user has overridden the approval of a task allowing the task to run without approval.
Approval Request	A user has created a task that requires approval before it can run.
Approval Task Changed	A user has made a change to a task that requires approval before it can run.
Approval Task Deleted	A user has deleted a task that was earmarked for approval.
Approval Task Timeout	A task was not approved in the time allotted.
Command Authorization Error	A user tried to run a command that he/she is not authorized to use.
Concurrent Telnet/SSH Session Override	A user ignored the restriction on simultaneous logins. The user logged-in to a device via the Proxy despite another user's prior login.
Configuration Policy Added	A user has added a new configuration policy.

Event	Description
Configuration Policy Changed	A user has changed a configuration policy.
Configuration Policy Non-Compliance	A configuration change violated a policy rule.
Configuration Policy Pattern Timeout	A policy pattern took more than 30 seconds to match.
Configuration Rule Added	A user has added a new configuration rule.
Configuration Rule Changed	A user has changed a configuration rule.
Device Access Failure	NCM cannot access a device. This could be due to a bad password or there was no route to the host.
Device Added	A user added a device.
Device Booted	A device was rebooted.
Device Command Script Completed Successfully	A device command script succeeded.
Device Command Script Failed	A device command script failed.
Device Configuration Change	NCM detected a configuration change while running a Snapshot task.
Device Configuration Change - No User	NCM detected a configuration change by an unknown user.
Device Configuration Deployment	NCM successfully deployed a configuration to a device. This event will return a warning status if the snapshot after deployment does not succeed.
Device Configuration Deployment Failure	NCM failed to deploy a configuration to a device.
Device Data Failure	NCM failed to save a configuration or diagnostic output to the database.
Device Deleted	A user permanently removed a device.

Event	Description
Device Diagnostic Changed	The Device Diagnostic Changed event currently indicates that a user changed the diagnostic script. This is a known bug. The Device Diagnostic Changed event should indicate that the results of running a diagnostic differ from the last time the diagnostic was run.
Device Diagnostic Completed Successfully	A device diagnostic succeeded.
Device Diagnostic Failed	A device diagnostic failed.
Device Edited	A user modified a device's information.
Device Flash Storage Running Low	A device’s flash storage is running low.
Device Inaccessible	A device is inaccessible.
Device Managed	A user marked a device as Active.
Device Missing From Import	When the Import task is run periodically and given a file of devices to import, this event occurs when a device was included in the file the last time the import occurred, but is no longer included in the file during the current import.
Device Password Change	A user deployed a password change.
Device Password Change Failure	NCM failed to deploy a device password change.
Device Permissions - Modified	A device was added to or removed from a group, which changed permissions such that users can modify the device.
Device Permissions - New Device	Someone added a new device to a device group, changing the permissions for users associated with that device group.
Device Reservation Conflict	There was a device reservation conflict.
Device Snapshot	NCM checked a device for a configuration change.
Device Software Change	NCM detected a new OS version on a device (for example: from IOS 11 to IOS 12).

Event	Description
Device Startup/Running Config Difference	NCM detected a difference between the Startup and Running configurations.
Device Unmanaged	A user marked a device as Inactive. Imported devices can also be Inactive if unreachable for a certain time of period.
Email Report Saved	A user has saved an email report.
External Directory Server Authentication Error	NCM could not connect to an external LDAP authentication server.
Group Added	A user has added a group.
Group Deleted	A user has deleted a group.
Group Modified	A user modified a device group.
Last Used Device Password Changed	The password last used for access to a device was changed.
License Almost Exceeded	The devices exceed 90% of the total number of licensed nodes.
License Almost Expired	Your NCM license expires soon (date-based licenses only).
License Exceeded	The devices exceed the total number of licensed nodes. NCM allows a 20% excess.
License Expired	Your license has expired. NCM will no longer allow logins, but will continue to take scheduled snapshots and record changes.
Module Added	Someone added a module/blade/card to a device.
Module Changed	Someone changed the attributes of a module/blade/card installed in a device.
Module Removed	Someone removed a module/blade/card from a device.
Monitor Error	A server monitor failed to run.
Monitor Okay	A server monitor ran successfully.

Event	Description
Pending Task Deleted	A user deleted a scheduled task before it ran.
Reserved Device Configuration Changed	A user has changed the device configuration on a reserved device.
Scheduled for Deploy Configuration Edited	A user modified a configuration that was scheduled to be deployed.
Scheduled for Deploy Password Modified	A new password was deployed, and there is another Password Deploy task scheduled. This indicates that the new password that was just deployed will be changed again (when the pending Password Deploy task executes).
Scheduled for Deploy Script Modified	Currently not used.
Server Startup	The NCM Management Engine was started.
Session Data Captured	The Proxy saved a connect session to the database.
Software Update Failed	NCM failed to update the OS software on a device.
Software Update Succeeded	NCM successfully updated the OS software on a device.
Software Vulnerability Detected	If you setup a Software Compliance with the Compliance set to “Security Risk,” when NCM snapshots devices and detects an OS version that is tagged as a “Security Risk,” this event is generated.
Summary Reports Generated	A user has generated Summary reports.
Task Started	A task has started.
Ticket Created	When using the Remedy AR System Connector to interact with a 3rd party Ticketing systems, this event indicates that NCM created a ticket in that 3rd party Ticketing system.
User Added	A user has been added.
User Authentication Error	A user entered an incorrect password when logging into NCM.

Event	Description
User Authentication Lockout	A user is locked out due to too many consecutive failed login attempts.
User Deleted	A user has been deleted
User Disabled	A user record was edited and the user's status changes from Enabled to Disabled.
User Enabled	A user record was edited and the user's status changes from Disabled to Enabled.
User Login	A user logged-in to NCM.
User Logout	A user has logged-out of NCM.
User Message	A user created a message by clicking the New Message link.
User Permission Changed	A user's permission has been changed.

Adding Event Rules

To add event notification rules, on the menu bar under Admin, click Event Notification & Response Rules. The Event Notification & Response Rules page opens. This page lists currently defined rules that are triggered by NCM events. Event rules marked with a pound sign (#) are inactive.

Note: Admin users see all event rules; other users see only their own event rules.

Event Notification & Response Rules Page Fields

Field	Description/Action
New Event Notification & Response Rule link	Opens the New Event Notification & Response Rule page. Refer to "New Event Notification & Response Rules Page Fields" on page 436 for information.
Rule Name	Displays the name of the event rule.
Action	Displays the action performed by the event rule. Actions include: • Run Task • Send Email • Send SNMP Trap • Add to Email Digest • Send Syslog Message
User Name	Displays the event rule's owner.
Actions	You can select from the following options: • Edit — Opens the Edit Event Notification & Response Rule page, where you can edit an event rule. Refer to "New Event Notification & Response Rules Page Fields" on page 436 for information. • Delete — Opens a confirmation window, where you are prompted to confirm the deletion. This option appears only when you have permission to delete the event rule.

New Event Notification & Response Rules Page Fields

The New Event Notification & Response Rule page enables you to add/edit a new Event Notification & Response rule.

1. On the menu bar under Admin, click Event Notification & Response Rules. The Event Notification & Response Rules page opens.
2. Click the New Event Notification & Response Rule link at the top of the page. The New Event Notification & Response Rule page opens.

Field	Description/Action
Add Email & Event Rule named	Enter the event rule name.
To take this action	Select one of the following options. (**Note**: Depending on the option you select, the page will refresh and provide specific fields for the action.) • Run Task — Refer to "Run Task Action" on page 438. • Send Email Digest — Refer to "Send Email Digest Action" on page 438. • Send Email Message — Refer to "Send Email Message Action" on page 439. • Send SNMP Trap — Refer to "Send SNMP Trap Action" on page 440. • Send Syslog Message — Refer to "Send Syslog Message Action" on page 441. • Create/Add to Ticket — Refer to "Create/Add to Ticket" on page 441.

Field	Description/Action
When the following events occur	Select one or more of the events from the events list. You can select multiple events using Ctrl+click or Shift+click. Refer to "Getting Started" on page 429 for a description of the event rules. Select one of the following options (if applicable): • of any importance — If selected (the default) the event rule will trigger regardless of the importance of any violated configuration policy rules. Refer to "New Configuration Rule Page Fields" on page 389 for information on how to set configuration policy rule importance. • of at least < > importance — You can select either Critical, High, Medium (the default), Low, or Informational. The event rule will trigger only if the event was generated due to the failure of a configuration policy rule with an importance equal to or greater than the importance selected. Refer to "New Configuration Rule Page Fields" on page 389 for information on how to set configuration rule importance. If you select the Configuration Policy Non-Compliance event, select one of the following options: • For all policies — If selected (the default) all configuration polices are checked. • For selected policies — Select one or more configuration policies from the list. You can use Shift+click or Ctrl+click to select multiple configuration polices. If you select the Device Command Script Completed Successfully or Device Command Script Failed event, you can select a command script from the drop-down menu. If you select the Device Diagnostic Changed or the Device Diagnostic Completed Successfully event, you can select a diagnostic from the drop-down menu. (Note: The Device Diagnostic Changed event currently indicates that a user changed the diagnostic script. This is a known bug. The Device Diagnostic Changed event should indicate that the results of running a diagnostic differ from the last time the diagnostic was run.)
Rule Status	Select one of the following options: • Active — If checked (the default), the event rule is run when the event occurs. • Inactive — If checked, the event rule is not run. This option can be used to temporarily turn off an event rule.

Field	Description/Action
Between	If checked, specify a time range and select the hours to start and end the event rule.
On devices in these groups	If checked, select one or more groups from the list.

Depending on the action you select, the bottom portion of the New Event Notification & Response Rules page will be different.

Run Task Action

When an event occurs, you can have it trigger any NCM task. You can have NCM take a snapshot, store diagnostics, run a command script, or even launch an external application. You can even feed event variables into the command line for external applications. This enables you to customize NCM and tailor its operations to your needs.

Wait	Enter the number of seconds, minutes, hours, or days to wait before running the task.
Task	Select a task to run from the drop-down menu.

Send Email Digest Action

Email digests combine multiple NCM events into a single email report that is sent periodically. Email digests can be used to inform users of common system events, such as configuration changes or device add, delete, and change activity.

You can quickly scan digests for events of interest, while minimizing email volume. Each user can have one email digest. A user can set up multiple event rules. Each rule feeds a different set of events into their digest.

NOTE: If you want multiple email digests with different schedules or recipient lists, you can create users whose only purpose is to define appropriate digest rules.

Send all my digests starting at (hour)	Enter the hour of the day when you want NCM to send your email digests.
And repeating every (hours)	Enter the interval at which you want NCM to send your email digests. For example, if you enter 6, the digests are sent every six hours.
From	Enter the email address of the sender. This default is NCM.

Field	Description/Action
To	Enter the email address of the recipient. Be sure to separate multiple addresses with commas. Note: If the variable is set to $EventUserEmail$, the email address is derived from the user who created the Email Digest. As a result, if the user's email address changes, the new email address is used.
Subject	Enter a brief subject line of the message.
Message Header	Enter a message header. This is the text that begins the header or summary section of the message. For HTML messages, this is often an ordered list tag .
End Summary	Enter the text that ends the header or summary section of a message. For HTML messages, this is often an ordered list end tag .
Message Footer	Enter the message footer. You can tailor this to your needs. For example, you could provide contact information or indicate this message is sent by the NCM server.
Text Message or HTML Message	Check either Text Message or HTML Message (the default). If you select HTML Message, NCM sends the appropriate mail headers so that the mail reader can interpret the HTML in the message. If you select Text Message, NCM sends a plain text message, and any HTML tags are displayed as is.
Event Summary	This field provides the summary text, briefly describing the event. The specific message content is unique to the rule. For HTML messages, this line often begins with a list item tag and may contain additional HTML tags and NCM variables. If you click the Display Variable Names link, the Event Rule Variables window opens, listing all the variables you can use.
Event Details	This field includes the text, variables, and optional HTML tags that describe the event in detail.

Send Email Message Action

You can send email messages to users or distribution lists when NCM events occur. One email message is sent for each event. For example, you can use this action to alert all users when a core device's configuration changes, to notify a system administrator when a device is inaccessible, or to keep an archive of system events in a public folder. You could also define a text-only event rule with a brief message to email your pager.

Field	Description/Action
From	Enter the person or process and email address the email message is from. If you click the Display Variable Names link, the Event Rule Variables window opens, which lists all the variables you can use. Refer to "Event Rule Variables" on page 443 for more information.
To	Enter the email address the message is to. Be sure to separate multiple addresses with commas. To send email to the user associated with the event, use the variable $EventUserEmail$.
Subject	Enter the subject line of the email message. You can use variables to include system information on the subject line.
Text Message	If checked, NCM sends a plain text message. Any HTML tags are displayed as is.
HTML Message	If checked, NCM sends the appropriate mail headers so that the mail reader can interpret the HTML in the message.
Both Text and HTML	If checked (the default), both a text message and an HTML message is sent. Keep in mind that NCM sends a multi-part email message. The email client displays whichever format is appropriate. For example, Outlook displays HTML by default. If messages are received on a pager, PDA, or similar device, Cisco recommends using short text-only messages.

Send SNMP Trap Action

An SNMP Trap is a network status message (defined by RFCs 1155 and 1215). This action is used to send SNMP traps when NCM events occur. For example, you can send an SNMP trap to your Network Management System (NMS) every time a snapshot is taken. To display the trap correctly, you may first need to load the NCM Management Information Base (MIB), which defines the message format. NOTE: The network must be configured to permit SNMP traffic to travel through routers, firewalls, and other network devices.

SNMP Trap Receiver Hostname	Enter the DNS name or IP address of the host.
SNMP Trap Receiver Port	Enter the host port that receives the SNMP trap. If you click the User Default Port link, the default port number is entered. 162 is the standard SNMP port.
SNMP Community String	Enter the community string to use when sending the SNMP trap. The recipient must be configured to accept this string. If you click the Use Default Community String link, the default community string, Public, is entered.

Field	Description/Action
SNMP Version	Select the version of SNMP to use, either v1 (the default) or v2.
Event Description	Enter a description of the event. You can include NCM variables. If you click the Display Variable Names link, the Event Rule Variables window opens, which lists all the variables you can use. Refer to "Event Rule Variables" on page 443 for more information.
Subsystem	Enter the subsystem name, such as User Login Control or Device Diff Engine. The maximum length is 256 characters.
Severity	Select one of the following options to identify the severity of the event. Note that there is no intrinsic security level associated with each event, so you can assign any value that makes sense. • Alert • Critical • Debug • Emergency • Error • Info • Notice • Warning

Send Syslog Message Action

You can use syslog messages to forward any NCM event to an external management system. For example, you might notify your CA UniCenter system when NCM detects a device configuration change so that an alert appears on your operations console.

Syslog Hostname	Enter the host name of the Syslog server.
Syslog Port	Enter the port used by Syslog. If you click the Use Default Port link, the default Syslog port, 514, is entered.
Syslog Message	Enter the Syslog message, including variables. If you click the Display Variable Names link, the Event Rule Variables window opens, which lists all the variables you can use. Refer to "Event Rule Variables" on page 443 for more information.

Create/Add to Ticket

Ticketing System Hostname	Enter the ticketing system hostname.

Field	Description/Action
Event Description	Enter the event description.

Be sure to click Save Rule when you are finished.

Event Rule Variables

Several event rule variables are available for:

- Device events
- Device configuration events
- Device diagnostics events
- All events

Device Events Variables

Note: Variables are case-sensitive. You must enter them exactly as shown.

You can use these variables only for device event rules:

Variable	Description
$DeviceID$	NCM's identification number for the device.
$HostName$	The device's host name.
$IPAddress$	The devices primary IP address.
$FQDN$	The devices fully-qualified domain name.
$Vendor$	The device's manufacturer.
$Model$	The device's model number.

Variables for Device Configuration Events

Note: Variables are case-sensitive. You must enter them exactly as shown.

You can use these variables only for device configuration event rules:

Variable	Description
$DataID$	NCM's identification number for the latest configuration
$Comments$	Configuration comments.
$Diff$	Textual differences of the configuration changes.

Variables for Device Diagnostic Events

Note: Variables are case-sensitive. You must enter them exactly as shown.

You can use these variables only for device diagnostics event rules:

Variable	Description
$CurrentDiag$	The text of the current diagnostic.
$PreviousDiag$	The text of the previous diagnostic.
$Diff$	The textual difference of the changes between current and previous diagnostic.
$DataID$	Indicates that it is also for diagnostic events.

Variables for All Events

You can use the following variables in all event rules. Keep in mind Variables are case-sensitive. You must enter them exactly as shown. (NOTE: For a complete list of variables, click the Display Variable Names link on the New Event Notification & Response Rule.)

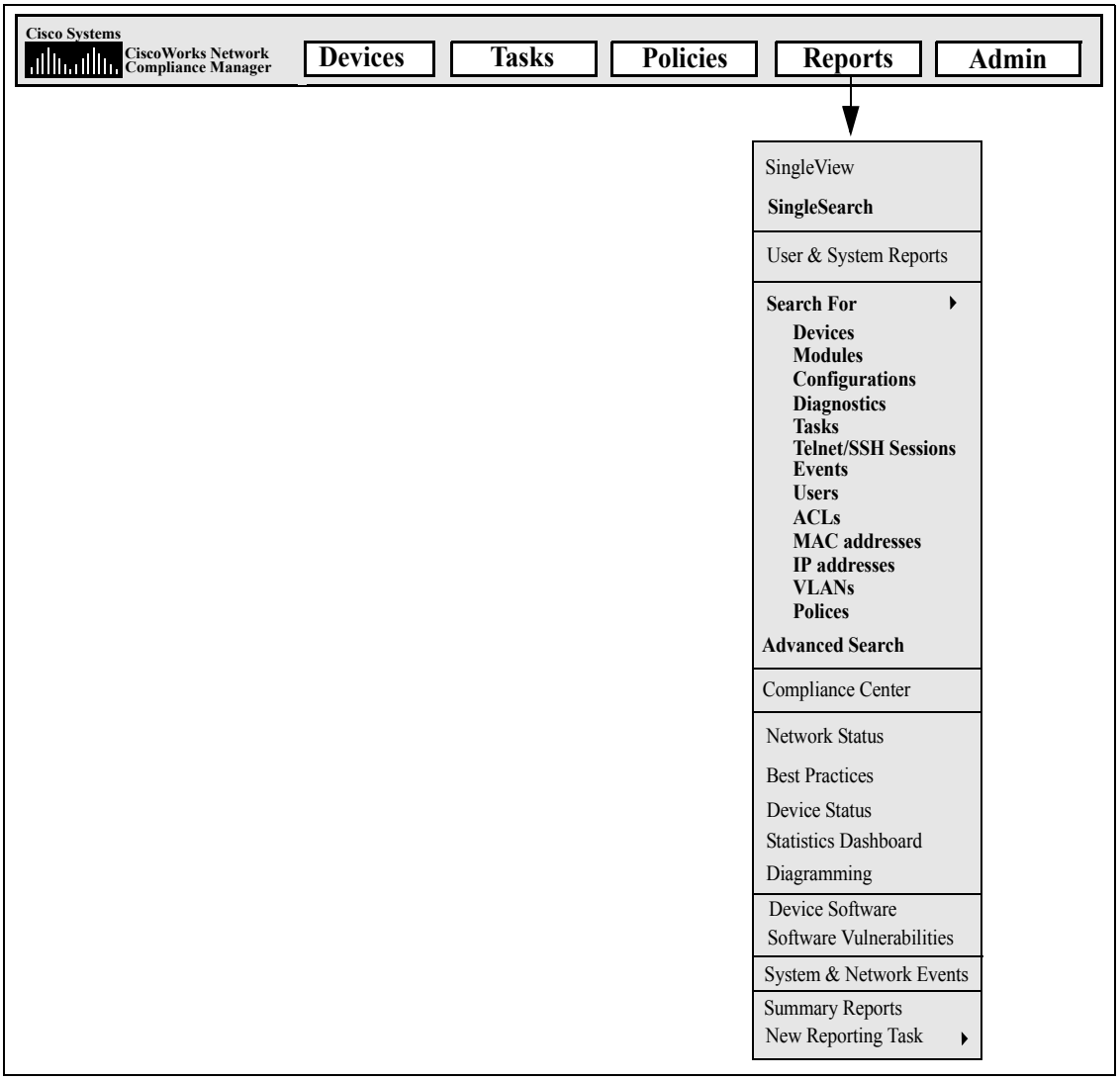
Variable	Description
$ApprovalPriority$	Task approval priority.
$ApprovalDate$	Task approval date.
$ApproverEmails$	Comma separated list of email addresses of the task approvers.
$AppURL$	NCM's application URL (such as *https://host/*) used to put links to NCM directly into email messages.
$EventID$	NCM's identification number for this event.
$EventType$	The type of event.
$EventDate$	The date the event occurred.
$EventText$	The event details.
$EventUserFirstName$	The first name of the NCM user associated with this event. (Note: If no user is associated with this event or if no First Name is set for the user, this will be an empty string.)
$EventUserLastName$	The last name of the NCM user associated with this event. (Note: If no user is associated with this event or if no Last Name is set for the user, this will be an empty string.)
$EventUserName$	The NCM user name associated with this event (indicates "no user" when appropriate).
$EventUserEmail$	Email address of the user associated with this event.
$FyiEmails$	Comma separated list of email addresses of the task FYI recipients.
$LocalHostName$	The hostname of the NCM server.
$LocalHostAddress$	The IP address of the NCM server.
$OriginatorFirstName$	The first name of the task originator.

Variable	Description
$OriginatorLastName$	The last name of the task originator.
$OriginatorName$	The name of the task originator.
$TaskName$	The task name.
$TaskComments$	The task comments.
$TaskDevices$	A list of devices affected by the task.
$TaskFrequency$	The frequency of the task.
$TaskID$	A null string if the event is not associated with a task.

Chapter 11: Performing Searches

Use the following table to quickly locate information.

Navigating to Search Pages



Searching for Devices

Device searches enable you to search for devices using a combination of criteria and operators. All search criteria are joined by the Boolean operators AND/OR and the results match all criteria. You can also search for devices that are out of compliance with specified policies or rules. (Refer to "Creating a Configuration Policy" on page 384 for information on Policies.)

To search for devices, on the menu bar under Reports select Search For and click Devices. The Search For Devices page opens. When you are finished entering search criteria, click the Search button. NCM returns a list of devices containing all the specified search criteria on the Device Search Results page. Refer to "Device Search Results Page Fields" on page 455 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Devices Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to select the information you want to include in the Device Search Results page.
Host Name	Select an operator and enter the Host Name. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the device's IP address.
Secondary IP Address	Select an operator and enter the device's secondary IP address.
Device Vendor	Select an operator and enter the name of the vendor who manufactured the device.
Device Model	Select an operator and enter the model designation of the device.
Device Type	Select the type of network device, such as router, switch, firewall, VPN, DialUp, DSL_ISDN, or load balancer from the scroll-down menu.
Device Status	Select one of the following options for the device: • Any (the default) • Active • Inactive (Inactive devices are not actively managed by NCM.)
Driver Name	Select one or more drivers associated with the device from the scroll-down menu. To select multiple drivers, click the first driver, then Ctrl+click to select additional drivers.

Field	Description/Action
Domain Name	Select an operator and enter the domain name.
Policy Compliance	Select one of the following options for the device: • Any (the default) • Device in compliance • Device not in compliance • Device not in compliance with rule of at least Medium importance — You can select Critical, High, Medium, Low, or Informational. This enables you to filter the search to include only devices that are in violation of configuration rules above a given importance. (Refer to "New Configuration Rule Page Fields" on page 389 for information on importance ratings for configuration policy rules.) • Device has no applicable policy • Device not in compliance with the following policies — Select one or more policies from the list. • Device not in compliance with the following rules — Select one or more policy rules from the list. (Refer to "New Configuration Rule Page Fields" on page 389 for information on policy rules.)
Access Methods	Select an access method from the scroll-down menu: • Telnet • SSH • SNMP • SCP • FTP • TFTP
Device Location	Select an operator and enter the location of the device.
Serial Number	Select an operator and enter the serial number of the device.
Asset Tag	Select an operator and enter information from the device asset tag.
Device Software Version	Select an operator and enter the version number of the operating system running on the device.

Field	Description/Action
Device Firmware Version	Select an operator and enter the version number of the firmware running on the device.
Comments	Select an operator and enter a unique portion of the comment for the device.
Free Ports	Select an operator (equals, is less than, or is greater than) and enter the number of free ports. You can enter either a percentage or an absolute number ports.
Total Ports	Select an operator (equals, is less than, or is greater than) and enter the total number of ports on the device.
Ports In Use	Select an operator (equals, is less than, or is greater than) and enter the number of ports in use. You can enter either a percentage or an absolute number of ports.
System Memory	Select an operator (equals, is less than, or is greater than) and enter the total amount of RAM (MB) on the device.
Configuration Text	Select an operator (contains or does not contain) and enter a unique portion of the current device configuration. You can select the Boolean operators AND/OR and enter an additional portion of the current device configuration for more complex searches. If the search operator is "contains,", you can provide a value in the "Show <#> context lines around the matched line when displaying Current Configuration" check box. You can include up to five lines above and below the search text in the results page. The default value is three. (**Note**: This can significantly slow performance if there are a large number of results to load.)
Different Startup/ Running	If checked, search devices with different startup and running configuration.
Last Changed Time	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.

Field	Description/Action
Create Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
ACL ID	Select an operator (contains or does not contain) and enter an ACL ID.
ACL Handle	Select an operator (contains or does not contain) and enter an ACL handle.
ACL Type	Select an operator (contains or does not contain) and enter an ACL type.
ACL Configuration	Select an operator (contains or does not contain) and enter an ACL type.
ACL Application	Select an operator (contains or does not contain) and enter an ACL application.
Module Slot	Select an operator (contains or does not contain) and enter a module slot.
Module Description	Select an operator (contains or does not contain) and enter a module description.
Module Model	Select an operator (contains or does not contain) and enter a module model.
Module Memory	Select an operator (equals, is less than, or is greater than) and enter module memory.
Module Firmware Version	Select an operator (contains or does not contain) and enter the module's firmware version.
Module Hardware Version	Select an operator (contains or does not contain) and enter the module's hardware version.

Field	Description/Action
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups Note: Use Shift+click to select/deselect multiple device groups.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)
Device Custom Data	Select an operator and enter the unique text that might appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields.)

When you click the Search button, NCM returns a list of devices containing all the specified search criteria on the Device Search Results page. Refer to "Device Search Results Page Fields" on page 455 for information.

Device Search Results Page Fields

The Device Search Results page display depends on the search criteria that you selected on the Search For Devices page. Refer to "Search For Devices Page Fields" on page 450 for information on search criteria. The following table describes the available options on the Device Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For Devices page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	You can use the left-side check boxes to manage devices. Once you have selected the devices, click the Actions drop-down menu and click either: • Activate — Instructs NCM to manage the selected devices. • Deactivate — Instructs NCM not to manage the selected devices. • Batch Edit Device — Opens the Batch Edit Device page, where you can assign a driver and set the connection methods for all of the selected devices. • Delete — Deletes the selected devices. • Check Policy Compliance — Refer to "Check Policy Compliance Task Page Fields" on page 342. • Configure Syslog — "Configure Syslog Task Page Fields" on page 280. • Deploy Passwords — "Deploy Passwords Task Page Fields" on page 284. • Discover Driver — "Discover Driver Task Page Fields" on page 289. • Reload Device — "Reload Device Task Page Fields" on page 293. The adjacent Select drop-down menu enables you to select or deselect all of the devices.

Option	Description/Action
Actions	You can select the following actions for each entry in the Device Search Results table: • Edit — Opens the Edit Device page, where you can edit information about this device. • Telnet — Opens a Telnet window, where you can enter Telnet commands. • SSH — Opens an SSH window, where you can enter SSH commands to this device. • View Config — Opens the Current Configuration page, where you can edit and add comments to the selected configuration. You can also deploy the modified configuration from this page.
Search Criteria	Displays the search criteria used in the search. You can: • Save result devices as a new device group — Enter the name of the new group and click Create Group. (**Note**: For information on creating a Dynamic Group, refer to "Dynamic Device Groups" on page 154.) • Add result devices to existing device group — Select a group using the drop-down menu and click Add. • Save the search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform).

Searching for Modules

You use module searches to search the NCM database for information on the cards, blades, or modules installed in your devices.

To search for modules, on the menu bar under Reports, select Search For and click Modules. The Search For Modules page opens. When you are finished entering search criteria and click the Search button, NCM returns a list of modules containing all the specified search criteria on the Module Search Results page. Refer to "Module Search Results Page Fields" on page 460 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Modules Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Module Search Results page to show only the selected information.
Host Name	Select an operator and enter the Host Name. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the device's IP address.
Slot	Select an operator and enter the slot on the device in which the module is installed.

Field	Description/Action
Description	Select an operator and enter a unique portion of the module's description.
Model	Select an operator and then enter the model of the module. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Serial	Select an operator and enter the module's serial number.
Memory	Select an operator and enter the total amount of RAM (MB) on the module.
Firmware Version	Select an operator and enter the version number of the firmware loaded on the module.
Hardware Revision	Select an operator and enter a portion of the module's hardware revision designation.
Comments	Select an operator and enter a portion of the module's comment.
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.

Field	Description/Action
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)
Module Custom Data	Select an operator and enter unique text that will appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields defined for this card or module.)

Module Search Results Page Fields

The Module Search Results page display depends on the search criteria that you selected on the Search For Module page. Refer to "Search For Modules Page Fields" on page 457 for information. The following table describes the available options on the Module Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search for Module page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following actions for each entry in the Module Search Results table: • Edit Module — Opens the Edit Blade/Module Detail page, where you can edit information about this module. • View Module — Opens the Blade/Module Detail page, where you can view module details.
Search Criteria	Displays the search criteria used in the search. You can: • Save result devices as a new device group — Enter the name of the new group and click Create Group. (**Note**: For information on creating a Dynamic Group, refer to "Dynamic Device Groups" on page 154.) • Add result devices to existing device group — Select a group using the drop-down menu and click Add. • Save the search as a user report — Enter the name of the user report, then click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform).

Searching for Configurations

Configuration searches enable you to search configuration files using a combination of criteria and operators. All search criteria are joined by the Boolean operators AND/OR and the results match all criteria.

To search for configuration files, on the menu bar under Reports, select Search For and click Configurations.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

When you are finished entering your search criteria and click the Search button, NCM returns a list of configurations containing all the specified search criteria on the Configuration Search Results page. Refer to "Configuration Search Results Page Fields" on page 464 for information.

Search For Configuration Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Configuration Search Results page to show only the selected information.
Host Name	Select an operator and then enter the host name of the device. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and then enter the IP address of the device.

Field	Description/Action
Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Changed By	Select an operator and then enter the login name of a user who might have changed a device's configuration.
Device Status	Select one of the following options for the device: • Any (the default) • Active • Inactive (Inactive devices are not actively managed by NCM.)
Comments	Select an operator (contains or does not contain) and then enter the comment text you want to find. This searches only text that appears in the Configuration Comment box in the Device Configuration Detail page.
Configuration Text	Select an operator (contains or does not contain) and enter a unique portion of the current device configuration file. If the search operator is "contains,", you can provide a value in the "Show <#> context lines around the matched line when displaying Current Configuration" check box. You can include up to five lines above and below the search text in the results page. The default value is three. (**Note**: This can significantly slow performance if there are a large number of results to load.) **Note:** Historical configurations are not searched.
Search Scope	If checked, only the current configuration is searched.
Different Startup/Running	If checked, search devices with different startup and running configuration.

Field	Description/Action
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)
Configuration Custom Data	Select an operator and enter unique text that might appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields.)

Configuration Search Results Page Fields

The Configuration Search Results page display depends on the search criteria you selected on the Search For Configuration page. Refer to "Search For Configuration Page Fields" on page 461 for information. The following table describes the available options on the Configuration Search Results page.

Field	Description/Action
Modify this search link	Returns you to the Search For Configuration page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	You can use the left-side check boxes to compare and delete configuration from the NCM database. Once you have selected the configurations, click the Actions drop-down menu and click either: • Compare — Opens the Compare Device Configurations page, where you can compare any two configurations. The differences are highlighted for easy reference. You can also deploy configurations from this page. • Delete — Deletes the selected configuration from the NCM database. The adjacent Select drop-down menu enables you to select or deselect all of the devices.
Actions	You can select the following actions for each entry in the Configuration Search Results table: • Compare to Previous — The Compare Device Configurations page opens, where you can view this and the previous configurations side by side. The differences are highlighted in different colors to make them easy to read. • View Config — Opens the Device Configuration Detail page, where you can edit and add comments to the selected configuration. You can also deploy the selected configuration from this page. • Diagnostics — Opens the Diagnostics page, where you can view diagnostic information for this configuration.

Field	Description/Action
Search Criteria	Displays the search criteria used in the search. You can: • Save result devices as a new device group — Enter the name of the new group and click Create Group. • Add result devices to existing device group — Select a group from the drop-down menu and click Add. (**Note**: For information on creating a Dynamic Group, refer to "Dynamic Device Groups" on page 154.) • Save the search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform).

Searching for Diagnostics

Diagnostic searches provide access to your device diagnostic information based on search criteria you define. Results match all search criteria. The type of information provided by each diagnostic is device-specific.

To search for diagnostics, on the menu bar under Reports select Search For and click Diagnostics. The Search For Diagnostics page opens.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

When you are done entering your search criteria and click the Search button, NCM returns a list of diagnostics containing all the specified search criteria on the Diagnostics Search Results page. Refer to "Diagnostic Search Results Page Fields" on page 470 for information.

Search For Diagnostics Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Diagnostics Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and then enter the IP address of the device.
Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.

Field	Description/Action
Diagnostic Type	Select the type of diagnostic data on which you want to search from the scroll-down menu. To select or deselect multiple types, use Ctrl+click. Diagnostic types include: • Hardware Information • ICMP Test • Memory Troubleshooting • NCM Detect Device Boot • NCM Device File System • NCM Flash Storage Space • NCM Interfaces • NCM Module Status • NCM OSPF Neighbors • NCM Routing Table **Note**: For detailed information on diagnostics, refer to "View Menu Options" on page 229.
Device Status	Select one of the following options for the device: • Any (the default) • Active • Inactive (Inactive devices are not actively managed by NCM.)
Diagnostic Text	Select an operator (contains or does not contain) and enter a unique portion of the diagnostics you want to search for or exclude from the search results.
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.

Field	Description/Action
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)
Diagnostic Custom Data	Select an operator and enter unique text that might appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields.)

Diagnostic Search Results Page Fields

The Diagnostics Search Results page display depends on the search criteria you selected on the Search for Diagnostics page. Refer to "Search For Diagnostics Page Fields" on page 467 for information. The following table describes the available options on the Diagnostic Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For Diagnostics page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	You can use the left-side check boxes to delete Diagnostics from the NCM database. Once you have selected the diagnostics, click the Actions drop-down menu and click: • Compare — Opens the Compare diagnostics page, where you can compare any two diagnostics of the same type. • Delete — Deletes the selected configuration from the NCM database. The adjacent Select drop-down menu enables you to select or deselect all of the diagnostics.
Actions	You can select the following actions for each entry in the Diagnostics Search Results table: • View Detail • Compare to Previous

Option	Description/Action
Search Criteria	Displays the search criteria used in the search. You can: • Save the search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. • Save result devices as a new device group — Enter the name of the new group and click Create Group. • Add result devices to existing device group — Select a group from the drop-down menu and click Add. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform).

Searching for Tasks

Task searches enable you to search the NCM database for tasks scheduled on your network.

To search for tasks, on the menu bar under Reports select Search For and click the Tasks. The Search For Tasks page opens. When you click the Search button, NCM returns a list of tasks containing all the specified search criteria on the Task Search Results page. Refer to "Task Search Results Page Fields" on page 477 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Tasks Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Tasks Search Results page to show only the selected information.
Task Name	Select an operator and then enter the task name. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal
Host Name	Select an operator and then enter the host name of the device. You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Scheduled By	Select an operator and enter the name of the person who scheduled the task.

Field	Description/Action
Scheduled Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Task Status	Choose one or more statuses from the scroll-down list. Use Ctrl+click to select more than one item. The available statuses include: • Pending • Succeeded • Failed • Running • Paused • Draft • Waiting • Duplicate • Skipped • Completed • Warning • Requested

Field	Description/Action
Task Type	Select the type of task on which you want to search. To select or deselect multiple task types, use Ctrl+click. Task types include: • Check Policy Compliance • Configure Syslog • Data Pruning • Deduplication • Delete ACLs • Deploy Config • Deploy Passwords • Detect Network Devices • Discover Driver • Email Report • Generate Summary Reports • Import • Multi-task Project • Reload Device • Resolve FQDN • Run Command Script • Run Diagnostics • Run External Application • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software

Field	Description/Action
Failure Type	Choose one or more failure types from the scroll-down list. Use Ctrl+click to select more than one item. The available failure types include: • Unsupported device • Insufficient privileges • Incorrect password • Device unreachable • No password found • Unrecognized device
Comments	Select an operator (contains or does not contain) and enter the a unique portion of the comment for the task.
Result	Select an operator (contains or does not contain) and enter the unique text from the task result you are searching for. To show the task information in the Task Search Results page, check the Include this column in Search Results box. If the search operator is "contains" you can provide a value in the <#> context lines box. You can include up to five lines above and below the search text. (**Note**: This feature can significantly slow performance if there are a large number of results to load.)
Device IP	Select an operator and enter the IP address of the device.
Approve By Date	Select the following operators: • Since • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.

Field	Description/Action
Approval Status	Select one or more approval status from the scroll-down list. Options include: • Approved • Draft • Not Applicable • Not Approved • Overidden • Waiting Approval
Exclude Child Tasks	If checked, Child tasks are excluded from the search.
Device belongs to	Select one or more device groups from the scroll-down menu: **Note**: Use Shift+click to select/deselect multiple device groups.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)

Task Search Results Page Fields

The Tasks Search Results page display depends on the search criteria you selected on the Search for Tasks page. Refer to "Search For Tasks Page Fields" on page 472 for information. The following table describes the available options on the Task Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For Tasks page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	You can use the left-side check boxes delete tasks from the Task Search Results table. Once you have selected the tasks, click the Actions drop-down menu and click: • Delete — Deletes the selected tasks. The adjacent Select drop-down menu enables you to select or deselect all of the tasks.
Actions	You can select the following actions for each entry in the Tasks Search Results table: • Edit — The Edit Task page opens, where you can edit and rerun a task that is recurring or has not yet occurred. This link appears only when you can edit the task. • Delete — Deletes the task. This link appears only when the task has not yet run. • Pause — Pauses the task. This link appears only when the task has not yet run. • Run Now — Runs the task. This link appears only when the task has not yet run.

Option	Description/Action
Search Criteria	Displays the search criteria used in the search. You can: • Save the search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. • Save result devices as a new device group — Enter the name of the new group and click Create Group. • Add result devices to existing device group — Select a group from the drop-down menu and click Add. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform).

Searching for Sessions

NCM' script execution and management capabilities provide tremendous benefits when it comes to pushing out changes to multiple devices simultaneously. However, for those with little scripting experience, creating command scripts can be difficult. As a result, NCM' ScriptMaster enables NCM to automatically generate error-free scripts based on Telnet or SSH sessions recorded through the Telnet/SSH Proxy.

You can use session searches to find Telnet/SSH Proxy sessions. In addition, you can configure the Session Search Results page to include session data that appears before and after the matching session data to provide a context for interpreting the results.

Note that there is an Admin Setting that determines whether NCM saves just the commands or the full Telnet/SSH command session. Refer to "Telnet/SSH Page Fields" on page 95.

To search for sessions, on the menu bar under Reports, select Search For and click Sessions. The Search For Sessions page opens. When you are finished entering search criteria and click the Search button, NCM returns a list of Telnet/SSH sessions containing all the specified search criteria on the Session Search Results page. Refer to "Session Search Results Page Fields" on page 483 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Sessions Page Fields

Field	Description/Action
Host Name	Select an operator and enter the host name of the device associated with the session. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device associated with the session.
Device Status	Select one of the following options for the device: • Any (the default) • Active • Inactive (Inactive devices are not actively managed by NCM.)
Created By	Select an operator and enter the login name of the person who might have created a session.
Start Date	Select the following operators: • Since • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.

Field	Description/Action
End Date	Select the following operators: • Since • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Status	Select one or more of the following status options: • Failed • Open • Closed
Type	Select one or more of the following type options: • Any • Telnet • SSH
Session Data	Select an operator (contains or does not contain) and enter a unique portion of the session you want to find. If the search operator is "contains," you can provide a value in the <#> context lines box. You can include up to five lines above and below the search text in the results. (**Note**: This feature can significantly slow performance if there are a large number of results to load.)
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.

Field	Description/Action
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)
Session Custom Data	Select an operator and type unique text that might appear in any of the custom fields that are listed here. (**Note**: This section is blank if there are no custom fields defined for session data.)

Session Search Results Page Fields

The Session Search Results page display depends on the search criteria you selected on the Search for Sessions page. Refer to "Search For Sessions Page Fields" on page 480 for information. The following table describes the available options on the Session Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For Sessions page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following actions for each entry in the Tasks Search Results table: • Host Name — Opens the Device Information page, where you can view basic information about the device and its configuration history. • Device IP — Opens the Device Information page, where you can view basic information about the device and its configuration history. • View Full Session — Opens the Telnet/SSH Session page, where you can see the commands and system responses for that session. This page includes the Convert to Script link that simplifies creation of a script from commands run during the current session. There is also a link to the configuration (if any) created by this session. • View Commands Only — Opens the Telnet/SSH Session page, where you can see just the commands for that session. This page includes the Convert to Script link that simplifies creation of a script from commands run during the current session. There is also a link to the configuration (if any) created by this session.

Option	Description/Action
Search Criteria	Displays the search criteria used in the search. You can: • Save the search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform). You have the option of include task result details in the file.

Searching for Events

You can search for system and user events, such as a device access failure. Refer to "Event Descriptions" on page 489 for a description of NCM events.

To search for events, on the menu bar under Reports, select Search For and click Events. The Search For Events page opens. When you are finished entering search criteria and click the Search button, NCM returns a list of events containing all the specified search criteria on the Event Search Results page. Refer to "Event Search Results Page Fields" on page 488 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Events Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Events Search Results page to show only the selected information.
Event Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Summary	Select the name of one or more events. Use Ctrl+click to select/deselect additional events. Refer to "Event Descriptions" on page 489 for detailed information on each event.
Added By	Select an operator and provide the login name of the person who created the event.

Field	Description/Action
Importance	Select one or more of the following options: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Host Name	Select an operator and enter the host name of the device associated with these events. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device associated with these events.
Description	Select an operator (contains or does not contain) and enter the unique text from the event you are searching for. To show the text in the results page, you can include up to five lines above and below the search text in the results. (**Note**: This feature can significantly slow performance if there are a large number of results to load.)

Field	Description/Action
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)

Event Search Results Page Fields

The Event Search Results page display depends on the search criteria you selected on the Search for Events page. Refer to "Search For Events Page Fields" on page 485 for information. The following table describes the available options on the Event Search Results page.

Field	Description/Action
Modify this search link	Returns you to the Search For Events page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	The check boxes for each event enable you to delete events. Once you have selected the events, click the Actions drop-down menu and click: • Delete — Deletes the selected events. The adjacent Select drop-down menu enables you to select or deselect all of the tasks.
Actions	You can select the following actions for each entry in the Events Search Results table: • Summary — Opens the Event Detail page, where you can view the detailed result of this event. • Host Name — Opens the Device Details page, where you can view basic information about the device and its configuration history.

Field	Description/Action
Search Criteria	Displays the search criteria used in the search. You can: • Save result devices as a new device group — Enter the name of the new group and click Create Group. • Add result devices to existing device group — Select a group from the drop-down menu and click Add. • Save the search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform).

Event Descriptions

The following table describes the NCM events. The events are listed in alphabetical order.

Event	Description
Approval Denied	A user has denied an approval request.
Approval Granted	A user has approved a task.
Approval No Longer Required	A task approval is no longer required.
Approval Override	A user has overridden the approval of a task allowing the task to run without approval.
Approval Request	A user has created a task that requires approval before it can run.
Approval Task Changed	A user has made a change to a task that requires approval before it can run.
Approval Task Deleted	A user has deleted a task that was earmarked for approval.

Event	Description
Approval Task Timeout	A task was not approved in the time allotted.
Command Authorization Error	A user tried to run a command that he/she is not authorized to use.
Concurrent Telnet/SSH Session Override	A user ignored the restriction on simultaneous logins. The user logged-in to a device via the Proxy despite another user's prior login.
Configuration Policy Added	A user has added a new configuration policy.
Configuration Policy Changed	A user has changed a configuration policy.
Configuration Policy Non-Compliance	A configuration change violated a policy rule.
Configuration Policy Pattern Timeout	A policy pattern took more than 30 seconds to match.
Configuration Rule Added	A user has added a new configuration rule.
Configuration Rule Changed	A user has changed a configuration rule.
Device Access Failure	NCM cannot access a device. This could be due to a bad password or there was no route to the host.
Device Added	A user added a device.
Device Booted	A device was rebooted.
Device Command Script Completed Successfully	A device command script succeeded.
Device Command Script Failed	A device command script failed.
Device Configuration Change	NCM detected a configuration change while running a Snapshot task.
Device Configuration Change - No User	NCM detected a configuration change by an unknown user.
Device Configuration Deployment	NCM successfully deployed a configuration to a device.
Device Configuration Deployment Failure	NCM failed to deploy a configuration to a device.

Event	Description
Device Data Failure	NCM failed to save a configuration or diagnostic output to the database.
Device Deleted	A user permanently removed a device.
Device Diagnostic Changed	The results of a diagnostic differ from the previous results.
Device Diagnostic Completed Successfully	A device diagnostic succeeded.
Device Diagnostic Failed	A device diagnostic failed.
Device Edited	A user modified a device's information.
Device Flash Storage Running Low	A device’s flash storage is running low.
Device Inaccessible	A device is inaccessible.
Device Managed	A user marked a device as Active.
Device Missing From Import	When the Import task is run periodically and given a file of devices to import, this event occurs when a device was included in the file the last time the import occurred, but is no longer included in the file during the current import.
Device Password Change	A user deployed a password change.
Device Password Change Failure	NCM failed to deploy a device password change.
Device Permissions - Modified	A device was added to or removed from a group, which changed permissions such that users can modify the device.
Device Permissions - New Device	Someone added a new device to a device group, changing the permissions for users associated with that device group.
Device Reservation Conflict	There was a device reservation conflict.
Device Snapshot	NCM checked a device for a configuration change.
Device Software Change	NCM detected a new OS version on a device (for example: from IOS 11 to IOS 12).

Event	Description
Device Startup/Running Config Difference	NCM detected a difference between the Startup and Running configurations.
Device Unmanaged	A user marked a device as Inactive. Imported devices can also be Inactive if unreachable for a certain time of period.
Email Report Saved	A user has saved an email report.
External Directory Server Authentication Error	NCM could not connect to an external LDAP authentication server.
Group Added	A user has added a group.
Group Deleted	A user has deleted a group.
Group Modified	A user modified a device group.
Last Used Device Password Changed	The password last used for access to a device was changed.
License Almost Exceeded	The devices exceed 90% of the total number of licensed nodes.
License Almost Expired	Your NCM license expires soon (date-based licenses only).
License Exceeded	The devices exceed the total number of licensed nodes. NCM allows a 20% excess.
License Expired	Your license has expired. NCM will no longer allow logins, but will continue to take scheduled snapshots and record changes.
Module Added	Someone added a module/blade/card to a device.
Module Changed	Someone changed the attributes of a module/blade/card installed in a device.
Module Removed	Someone removed a module/blade/card from a device.
Monitor Error	A server monitor failed to run.
Monitor Okay	A server monitor ran successfully.
Pending Task Deleted	A user deleted a scheduled task before it ran.

Event	Description
Reserved Device Configuration Changed	A user has changed the device configuration on a reserved device.
Scheduled for Deploy Configuration Edited	A user modified a configuration that was scheduled to be deployed.
Scheduled for Deploy Password Modified	A new password was deployed, and there is another Password Deploy task scheduled. This indicates that the new password that was just deployed will be changed again (when the pending Password Deploy task executes).
Scheduled for Deploy Script Modified	Currently not used.
Server Startup	The NCM Management Engine was started.
Session Data Captured	The Proxy saved a connect session to the database.
Software Update Failed	NCM failed to update the OS software on a device.
Software Update Succeeded	NCM successfully updated the OS software on a device.
Software Vulnerability Detected	If you setup a Software Compliance with the Compliance set to “Security Risk,” when NCM snapshots devices and detects an OS version that is tagged as a “Security Risk,” this event is generated.
Summary Reports Generated	A user has generated Summary reports.
Task Completed	A task has completed.
Task Started	A task has started.
Ticket Created	When using the Cisco Remedy AR System Connector (or any of the Cisco Connectors that interact with a 3rd party Ticketing systems), this event indicates that NCM created a ticket in that 3rd party Ticketing system.
User Added	A user has been added.
User Authentication Error	A user entered an incorrect password when logging into NCM.

Event	Description
User Authentication Lockout	A user is locked out due to too many consecutive failed login attempts.
User Deleted	A user has been deleted
User Disabled	A user record was edited and the user's status changes from Enabled to Disabled.
User Enabled	A user record was edited and the user's status changes from Disabled to Enabled.
User Login	A user logged-in to NCM.
User Logout	A user has logged-out of NCM.
User Message	A user created a message by clicking the New Message link.
User Permission Changed	A user's permission has been changed.

Searching for Users

You can use the Search for Users page to search for users by first name, last name, email address, and/or AAA user name. To search for users, on the menu bar under Reports select Search For and click Users. The Search For Users page opens.

When you click the Search button, NCM returns a list of events containing all the specified search criteria on the User Search Results page. Refer to "User Search Results Page" on page 497 for information.

Search For Users Page

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the User Search Results page to show only the selected information.
First Name	Select an operator and enter the user's first name. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal
Last Name	Select an operator and enter the user's last name.
User Name	Select an operator and enter the user's username. You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Email	Select an operator and enter the user's email address.
AAA User Name	Select an operator and enter the user's AAA username.
Comments	Select an operator (contains or does not contain) and then enter the comment text you want to find.

Field	Description/Action
Member of User Group	Select the group of which the user is a member. Options include: • All Users (the default) • Limited Access User • Full Access User • Power User • Administrator • Restricted Users

User Search Results Page

The User Search Results page display the search criteria you selected on the Search for Users page. Refer to "Search For Users Page" on page 495 for information.

Field	Description/Action
Modify this search link	Returns you to the Search For Events page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
User Name	Displays the user's login name.
First Name	Displays the user's first name.
Last Name	Displays the user's last name.
Email	Displays the user's email address.
AAA User Name	Displays the user's AAA username.
Member of User Group	Displays user group to which the user belongs.
Actions	You can select the following actions for each entry in the Tasks Search Results table: • Edit — Open the My Profile page, where you can edit the user's profile. Refer to "My Profile Page Fields" on page 265 for information. • Delete — Enables you to delete the user if you have the proper permissions. Otherwise, the option is greyed out. • Permissions — Opens the My Permissions page, where you can edit the user's permissions. Refer to "My Permissions Page Fields" on page 268 for information. • Config Changes — Opens the Config Search Results, where you can view configuration changes.

Field	Description/Action
Search Criteria	Displays the search criteria used in the search. You can: • Save the search as a user report — Enter the name of the user report, then click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma.

Searching for ACLs

Access Control Lists (ACLs) are part of the configuration on most devices. They filter network traffic by controlling whether routed packets are accepted or blocked at the router's interfaces. In general, an ACL is a collection of statements. Each statement defines a pattern that would be found in an IP packet. ACLs are often used to restrict the contents of routing updates and to provide network security.

NCM retrieves configuration information from devices and extracts the ACL statements from the configuration. NCM then stores the ACLs independent of the configuration. As a result, you can:

- View the current ACLs on a device and compare them against the previous ACLs.
- Add comments to an ACL.
- Modify/create an ACL and deploy it back to the device.

For information on modifying and/or creating an ACL, refer to "Creating ACLs" on page 711.

To search for ACLs, on the menu bar under Reports, select Search For and click ACLs. The Search For ACLs page opens.

Search For ACLs Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the ACL Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device associated with the session. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
ACL ID	Select an operator and enter the ACL's ID. The ACL ID is an number based on the device ACL list, while the ACL Handle is a descriptive name or value assigned by the user. By default, the ACL ID and ACL Handle are the same until the user defines the ACL Handle.
ACL Handle	Select an operator and enter the ACL's Handle. The ACL Handle is a descriptive name or value assigned by the user. By default, the ACL ID and ACL Handle are the same until the user defines the ACL Handle.
Type	Select an operator and enter the type of ACL, for example: "extended." Keep in mind that ACL types are driver dependent.
Configuration	Select an operator, either contains or does not contain, and enter any configuration commands that define the ACL.
Application	Select an operator, either contains or does not contain, and enter the entity that is using the ACL. For example, if an ACL is applied to an interface, the interface is an application of the ACL.

Field	Description/Action
Search Scope	If checked, search results will be limited to those ACLs that are currently configured on all devices. If unchecked, the search results will contain both current and historical ACLs.
Comments	Select an operator, either contains or does not contain, and enter any ACL comments.
Changed by	Select an operator and enter the name of the user that last changed the ACL.
Last Modified	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)

When you click the Search button, NCM returns a list of ACLs containing all the specified search criteria on the ACL Search Results page. Refer to "ACL Search Results Page Fields" on page 502 for information.

ACL Search Results Page Fields

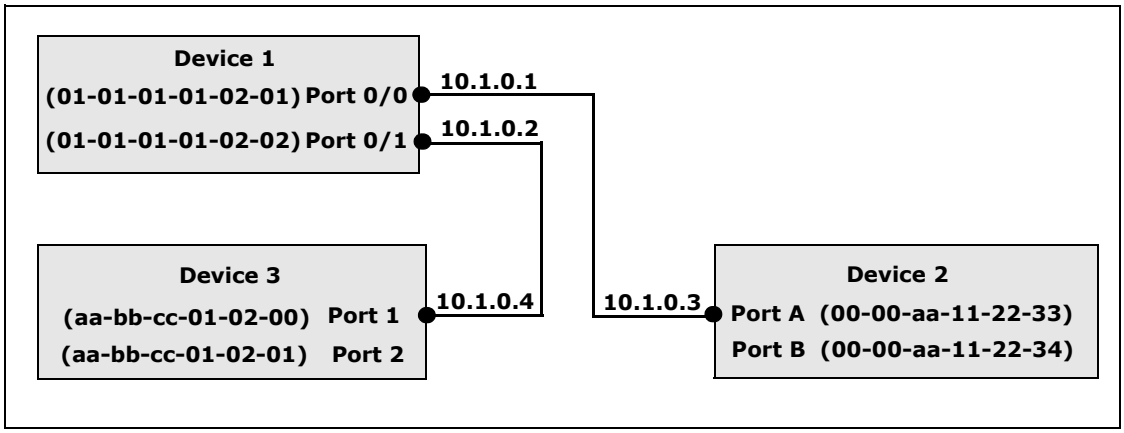
The ALC Search Results page display on the search criteria you selected on the Search for ACLs page. Refer to "Search For ACLs Page Fields" on page 500 for information. The following table describes the available options on the ACLs Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For ACLs page, where you can edit your search criteria and run the search again.
Search Criteria link	Displays the search criteria used in the search. You can: • Save the search as a user report — Enter the name of the user report, then click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform). You have the option of include task result details in the file.
Check Boxes	The check boxes for each ACL enable you to compare two ACLs. Once you have selected the ACLs, select the Actions drop-down menu and click: • Compare — Opens the Compare ACL page, where you can compare any two ACLs. The differences are highlighted for easy reference. You have the option of displaying differences with context, showing full text, or show UNIX-style differences. The adjacent Select drop-down menu enables you to select or deselect all of the ACLs.
Host Name	Displays the host name of the device. If you click the device, the Device Details page, where you can view basic information about the device and its configuration history.
ACL ID	The ACL ID is an number based on the device ACL list, while the ACL Handle is a descriptive name or value assigned by the user. By default, the ACL ID and ACL Handle are the same until the user defines the ACL Handle.

Option	Description/Action
ACL Handle	The ACL Handle is a descriptive name or value assigned by the user. By default, the ACL ID and ACL Handle are the same until the user defines the ACL Handle.
ACL Type	Displays the ACL's type.
Last modified	Displays the date and time the ACL was last modified.
Actions	You can select the following actions for each entry in the ACL Search Results table: • Edit ACL — Opens the Edit ACL page, where you can edit the ACL. Refer to "Deleting ACLs" on page 719 for information. • View ACL — Opens the View ACL page, where you can view the ACL. Refer to "Viewing ACLs" on page 706 for information. • ACL History — Opens ACL Search Results page. Refer to "ACL Search Results Page Fields" on page 502 for information.

Searching for MAC Addresses

MAC addresses are unique addresses that identify ports on a device. MAC addresses are also known as BIAs (Burned-in Addresses), hardware addresses, and physical addresses. NCM gathers information about which MAC addresses are assigned to ports on devices and which MAC addresses are visible from those ports. The following figure illustrates the relationship between MAC addresses, IP addresses, and ports.



To search for MAC Addresses, on the menu bar under Reports, select Search For and click MAC addresses. The Search For MACs page opens. After you enter your search criteria and click the Search button, NCM returns a list of MAC addresses containing all the specified search criteria on the MAC Search Results page. Refer to "MAC Search Results Page Fields" on page 507 for information.

Search For MACs Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the MACs Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device.
Port Name	Select an operator and enter the device port name. The port name is the name of the actual port on the device. For example: Ethernet0/1.
MAC Address	Select an operator and enter a MAC address pattern on which to search.
MAC Address Type	Select one of the following options: • All addresses (the default) • Seen from port — Display only those MAC addresses that are connected to the device/port (i.e., those MAC address types external to the device/port, but visible to it). • Address of port — Display only those MAC addresses that are internal to the device (i.e., the MAC addresses that are assigned to ports on the device). **Note**: The "Limit search to MAC addresses no longer seen" check box enables you to limit the search results to only those MAC addresses that are no longer seen in the latest data capture.

Field	Description/Action
Search Scope	If checked, the search is limited to MAC addresses no longer seen.
VLAN	Select an operator and enter the port's VLAN name. The VLAN name is the name of the VLAN, for example VLAN2 or VLAN3, on which to limit the search.
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)

MAC Search Results Page Fields

The MAC Search Results page displays the search criteria you selected on the Search For MACs page. Refer to "Search For MACs Page Fields" on page 505 for information.

Option	Description/Action
Modify this search link	Returns you to the Search For MACs page, where you can edit your search criteria and run the search again.
View Search Criteria link	Displays the search criteria used in the search. You can: • Save the search as a user report — Enter the name of the user report, then click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform). You have the option of include task result details in the file.
Host Name	Displays the host name of the device that references the MAC address.
Device IP	Displays the MAC address, for example: Address of Port or Seen from Port.
Port Name	Displays the name of the port on the device that references the MAC address.
Type	Displays the type of MAC address, either "seen from port" or "address of port."
VLAN	Displays the name of the VLAN the address belongs to if the type is "Address of Port".
Remote Location	Displays the remote location for the "Seen from Port" MAC addresses. If NCM is able to identify where the MAC address came from, a link to the associated device and port is provided. In the future, this could be the server/interface in SAS to which the address belongs.
First Seen	Displays the date and time the MAC address was first identified.

Option	Description/Action
Last Seen	Displays which MAC address was seen the last time NCM gathered topology data. If not current, this is the date when NCM last saw the MAC address on the network. Keep in mind that there is a filter in the search page to limit the results to those records that are not current. This is a quick way to see if there are any devices that have vanished in some way.
Actions	You can select the following action for each MAC address: • View Details — Opens the MACs Details page, where you can view details on the following information: Device, Device Port, MAC address, Type, First Seen, and Last Updated. • View IP - Opens the IP details page that is cross-referenced with this MAC address. This option is only available on "Seen from Port" records. Cross-referencing means that when NCM gathers data, the IP address and MAC address were indicated as coming from the same source.

Searching for IP Addresses

An IP (Internet Protocol) Address is the unique numerical address of a device. IP addresses are normally expressed in decimal format as a dotted decimal number. However, computers communicate in binary form. The following example shows the same IP address in both dotted decimal number and binary numbers: `216.27.61.137` — `11011000.00011011.00111101.10001001`

To search for IP addresses, on the menu bar under Reports, select Search For and click IP Addresses. The Search For IP Addresses page opens. When you are finished entering search criteria, click the Search button. NCM returns a list of IP addresses containing all the specified search criteria on the IP Address Search Results page.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For IPs Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the IP Addresses Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device associated with the session. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device.

Field	Description/Action
Port Name	Select an operator and enter the device port name. The port name is the name of the actual port on the device. For example: Ethernet0/1.
IP Address	Select an operator and enter a IP address pattern on which to search.
Address Type	Select one of the following options: • All addresses (the default) • Seen from port — Display only those MAC addresses that are connected to the device/port (i.e., those MAC address types external to the device/port, but visible to it). • Address of port — Display only those MAC addresses that are internal to the device (i.e., the MAC addresses that are assigned to ports on the device). **Note**: The "Limit search to IP addresses no longer seen" check box enables you to limit the search results to only those IP addresses that are no longer seen in the latest data capture.
Search Scope	If checked, the search is limited to IP addresses no longer seen.
VLAN	Select an operator and enter the port's VLAN name. The VLAN name is the name of the VLAN, for example VLAN2 or VLAN3, on which to limit the search.
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)

IP Search Results Page Fields

The IP Search Results page displays the search criteria you selected on the Search For IPs page. Refer to "Search For IPs Page Fields" on page 509 for information.

Option	Description/Action
Modify this search link	Returns you to the Search For IP Addresses page, where you can edit your search criteria and run the search again.
View Search Criteria link	Displays the search criteria used in the search. You can: • Save the search as a user report — Enter the name of the user report, then click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform). You have the option of include task result details in the file.
Host Name	Displays the host name of the device that references the IP address.
Port Name	Displays the name of the port on the device that references the IP address.
Address	Displays the IP address, for example: Address of Port or Seen from Port.
Address Type	Displays the type of IP address, either "Seen from Port" or "Address of Port."
VLAN	Displays the name of the VLAN the address belongs to, if the type is "Address of Port".
Remote Location	Displays the remote location for the "Seen from Port" IP addresses. If NCM is able to identify where the IP address came from, a link to the associated device and port is provided. In the future, this could be the server/interface in SAS to which the address belongs.
First Seen	Displays the date and time the IP address was first identified.

Option	Description/Action
Last Seen	Displays which IP address was seen the last time NCM gathered topology data. If not current, this is the date when NCM last saw the IP address on the network. Keep in mind that there is a filter in the search page to limit the results to those records that are not current. This is a quick way to see if there are any devices that have vanished in some way.
Actions	You can select the following action for each MAC address: • View Details — Opens the IP Address Details page, where you can view details on the following information: Device, Device Port, MAC address, Type, First Seen, and Last Updated. • View MAC - Opens the MAC details page that is cross-referenced with this MAC address. This option is only available on "Seen from Port" records. Cross-referencing means that when NCM gathers data, the IP address and MAC address were indicated as coming from the same source.

Searching for VLANs

VLANs (Virtual Local Area Networks) are conglomerations of ports that act as a single destination for packets. VLANs operate at Layer 2 (the Data Link layer). NCM gathers information about what VLANs are defined on a device and what VLAN each port is assigned to.

To search for VLANs, on the menu bar under Reports, select Search For and click VLANs. The Search For VLANs page opens. When you are finished entering search criteria, click the Search button. NCM returns a list of VLANs containing all the specified search criteria on the VLANs Search Results page.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For VLANs Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the VLANs Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device associated with the session. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device.
VLAN	Select an operator and enter the port's VLAN name. The VLAN name is the name of the VLAN, for example VLAN2 or VLAN3, on which to limit the search.

Field	Description/Action
VLAN Description	Select an operator and enter the VLAN's description.
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)

VLAN Search Results Page Fields

The VLAN Search Results page displays the search criteria you selected on the Search For VLANs page. Refer to "Search For VLANs Page Fields" on page 513 for information.

Option	Description/Action
Modify this search link	Returns you to the Search For VLANs page, where you can edit your search criteria and run the search again.
View Search Criteria link	Displays the search criteria used in the search. You can: • Save the search as a user report — Enter the name of the user report, then click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform). You have the option of include task result details in the file.
Host Name	Display the host name of the device with the VLAN.
Port Name	Display the port name of the port on the device that belongs to the VLAN.
VLAN	Displays the name of the VLAN. Clicking the VLAN name opens the Interface Details page.
VLAN Description	Displays a description of the VLAN.
Actions	You can select the following action for each VLAN: • View Details — Opens the Details page, where you can view details about the search with links to the Device and Interface Detail pages.

Searching for Violated Policies

The NCM Policy Manager applies a set of rules, or filters, to each device configuration change that NCM detects. If a change to a device (or group of devices) is non-compliant, the NCM Policy Manager generates an event and triggers a notification rule. As a result, you can correct the non-compliant change, preserving both compliance and network availability. Refer to "Creating a Configuration Policy" on page 384 for detailed information on Policy Management.

The Search For Violated Policies page enables you to search for policies against a specified device or device group that is out of compliance with the policy.

To search for violated policies, on the menu bar under Reports, select Search For and click Polices. The Search For Violated Polices page opens. When you are finished entering search criteria, click the Search button. NCM returns a list of devices containing all the specified search criteria on the Violated Policies Search Results page.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Violated Polices Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Violated Policies Search Results page to show only the selected information.

Field	Description/Action
Host Name	Select an operator and enter the host name of the device associated with the session. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device.
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)

Violated Policies Search Results Page Fields

The Violated Policies Search Results page displays the search criteria you selected on the Search For Violated Policies page. Refer to "Search For Violated Polices Page Fields" on page 516 for information.

Option	Description/Action
Modify this search link	Returns you to the Search For Violated Policies page, where you can edit your search criteria and run the search again.
View Search Criteria link	Displays the search criteria used in the search. You can: • Save the search as a user report — Enter the name of the user report, then click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform). You have the option of include task result details in the file.
Host Name	Display the host name of the device associated with the violated policy.
Device IP Address	Display the IP address of the device associated with the violated policy.
Actions	You can select the following action for each violated policy: • View Details — Opens the Details page, where you can view details about the search with links to the Device Details page.

SingleSearch

To search for device change events, on the menu bar under Reports, click SingleSearch. The SingleSearch Page opens. When you click the Search button, NCM returns a list of events containing all the specified search criteria you specify on this page on the SingleSearch Results page. Refer to "SingleSearch Results Page Fields" on page 521.

SingleSearch Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Events Search Results page to show only the selected information.
Event Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Added By	Select an operator and provide the login name of the person who created the event. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal

Field	Description/Action
Importance	Select one or more Importance level. Options include: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Host Name	Select an operator and enter the host name of the device associated with these events. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator (see above) and enter the IP address of the device associated with these events.
Description	Select an operator (contains or does not contain) and enter the unique text from the event for which you are searching. To show the context lines around the matched line when displaying the event description, check Show and enter the number of lines. Three is the default value.
Device Belongs to	Select an operator (Any of the selected groups, All of the selected groups, or None of the selected groups) and select one or more groups from the scroll-down list.
Site	Select a Site to limit search results to devices in that Site. The Default Site initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Sites. Refer to "Restricted Device Views" on page 166 for information on configuring Sites.)

SingleSearch Results Page Fields

The SingleSearch Search Results page display depends on the search criteria you selected on the Search for Events page. Refer to "SingleSearch Page Fields" on page 519 for information. The following table describes the available options on the SingleSearch Search Results page.

Field	Description/Action
Modify this search link	Returns you to the Search For Events page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	The check boxes for each event enables you to delete events. Once you have selected the events, click the Actions drop-down menu and click: • Delete — Deletes the selected events. The adjacent Select drop-down menu enables you to select or deselect all of the tasks.
Search Criteria	Displays the search criteria used in the search. You can: • Save result devices as a new device group — Enter the name of the new group and click Create Group. • Add result devices to existing device group — Select a group from the drop-down menu and click Add. • Save the search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform).

Advanced Search

The Advanced Search page enables you to:

- Use Boolean expressions (and/or) to filter searches. Keep in mind that you can use parenthesis in the Boolean expressions so as to refine your search.
- Configure searches using one or more search criteria, for example IP address, Domain Name, and Policy Compliance.
- Limit a search by device group.
- Customize the output of the Advanced Search Results page.

To open the Advanced Search page, on the menu bar under Reports, click Advanced Search. When you click the Search button, NCM returns the search criteria you specified.

Advanced Search Page Fields

Field	Description/Action
Search For	Select one of the following options from the drop-down menu: • Devices • Tasks • Configs • Diagnostics • Modules • Sessions • Events • ACLs

Search Criteria
Each time you select a search criterion, it is displayed in the Search Criteria section, where you can then select both a operator, such as Contains, Matches, or Equals, and enter the information on which to search. If you want to delete a defined criterion, click the X next to the search criterion index letter.

Field	Description/Action
Add Criteria	Select one or more search criteria from the drop-down menu, for example: • Host Name • Device IP • Domain Name • Device Status • Policy Compliance
Boolean Expression	
Expression	By default, the defined criteria index letters are displayed with the Boolean 'and' expression. For example, if you defined three search criteria, the expression would look like *A and B and C*. You can edit the Boolean expression as needed. Click the Reset Expression button to reset the expression to the default. (**Note**: The Boolean operator must be entered in lowercase. In addition, the maximum number of criteria is 10.)
Limit search by device group	
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups Note: Use Shift+click to select/deselect multiple device groups. If you do not select a device group, NCM will discard the device group filter when searching.
Customize Output	
Select fields to be included in search results	Select the fields to be included in the Advanced Search Results page. To select multiple fields, click the first field, then Shift+click to select/deselect additional fields.
Sort results by	Select the search criterion from the drop-down menu for which you want to sort the results of the search. You can specify Ascending (the default) or Descending.

Field	Description/Action
Display results in groups of	Enter the number of items you want displayed on the Advanced Search Results page. The default 25.
Show <#> context lines around the matching line when displaying text fields	When displaying text fields on the Advanced Search Results page, enter the number of lines around the matching line to be displayed. The default is 3.

Sample Advanced Search

The following advanced search assumes that you have two data centers under management. One data center is located on the New York and the other in California. The search informs you of all the Cisco devices that do not have the proper timezone set for either of the data centers.

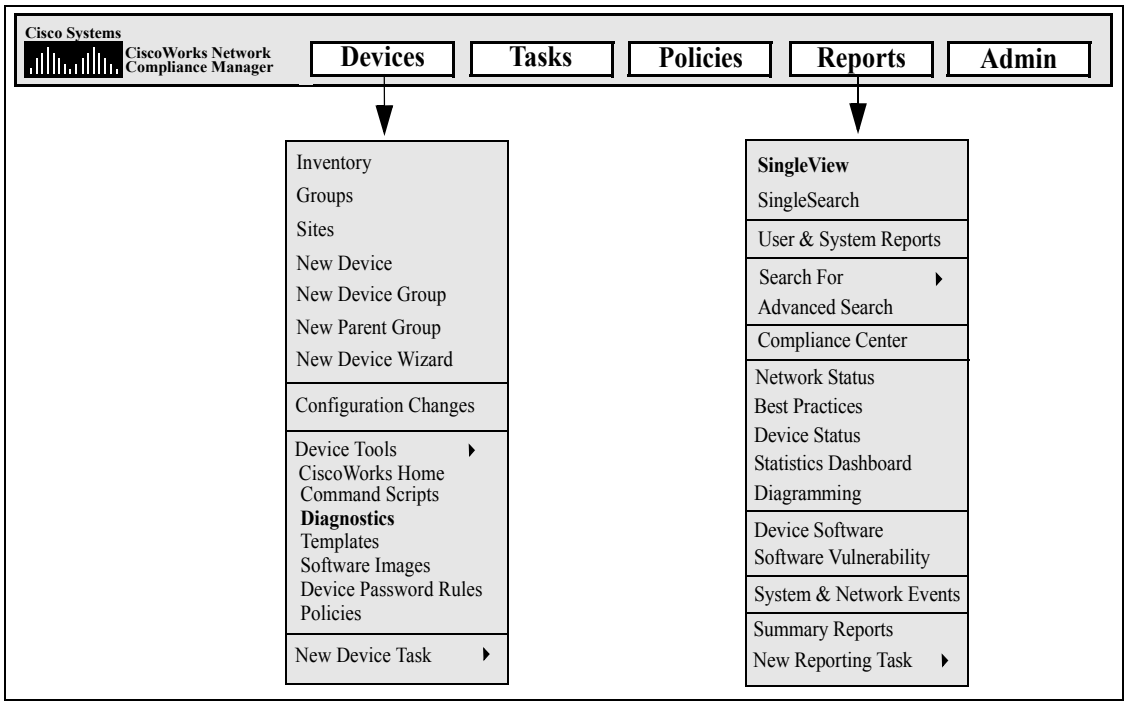
1. Log into NCM.
2. From the main menu bar under Reports, click Advanced Search. The Advanced Search page open.
3. In the Search for field select Devices from the drop-down menu.
4. In the Search Criterias field, select Driver Name from the drop-down menu.
5. Select all Cisco drivers in use by NCM.
6. Select Configuration Text from the Add Criteria drop-down menu.
7. Select does not contain from the drop-down menu and enter: `set timezone PST`.
8. Select Configuration Text again from the Add Criteria drop-down menu.
9. Select does not contain from the drop-down menu and enter: `set timezone PST`.
10. In the Boolean Expression field, modify the default string to read: `A and (B or C)`.
11. Click the Search button.

Chapter 12: Managing Events and Diagnostics

Use the following table to quickly locate information.

Topic	Refer to:
Consolidated View of Events (SingleView)	"Consolidated View of Events (SingleView)" on page 528
Diagnostics	"Diagnostics" on page 532
Adding & Customizing Diagnostics	"Adding & Editing Custom Diagnostics" on page 535

Navigating to SingleView and Diagnostics



Consolidated View of Events (SingleView)

SingleView enables you to track events that indicate changes to either a single device or all of your devices on one page. You can select from a list of event types, including:

- Device Booted
- Device Configuration Change
- Device Diagnostic Changed
- Device Password Change
- Device Software Change
- Module Added
- Module Changed
- Module Removed
- Reserved Device Configuration Changed
- Software Change
- User Message

For a complete list of CiscoWorks Network Compliance Manager (NCM) Events, refer to "Event Descriptions" on page 489.

To view the SingleView page, on the menu bar under Reports, click SingleView. The SingleView page opens.

SingleView Page Fields

Field	Description/Action
View as CSV File link	You are prompted for the location to save the display as a CSV file.
Displayed Change Event Types link	Scrolls down to the Displayed Change Event Types menu, where you can select events to display.
For the:	Displays the time frame for viewing events. Options include: • Past 1, 2, 4, 8, 12, 24, and 48 hours • Past 1 and 2 weeks • Past 1 month • All Events
Current Working Group	Select a device group from the drop-down menu.
Check Boxes	You can use the left-side check boxes to delete events from the NCM database. Once you have selected the events, click the Actions drop-down menu and click Delete. This deletes the selected events from the NCM database. The adjacent Select drop-down menu enables you to select or deselect all of the events.
Event Date	Displays the date/time of the event in the format MMM-dd-yy HH:mm:ss. (The format is configurable by the System Administrator.)
Host Name	Displays the host name or IP address of the device. Clicking the Host Name or IP Address opens the Device Details page, where you can view information about the device and its configuration history.

Field	Description/Action
Summary	Displays the type of event. For a list of NCM Events, refer to "Event Descriptions" on page 489. Clicking the event type link opens the Event Detail page. This page includes: • The date and time the event occurred. • The login name of the person or process that added the event. Clicking the Detail link for diagnostic changes opens the Task Result page where you can view task details. Refer to "Task Information Page Fields" on page 376. • The event type. • A brief description of the event. • A link to detailed information about the device.
Host Name	Displays the host name or IP address of the device. Clicking the Host Name or IP Address opens the Device Details page, where you can view information about the device and its configuration history.
Added By	Displays the login name of the person whose action caused the event to be created.
Actions	The Compare to Previous link appears for the following events: • Device Configuration Change — Opens the Compare Device Configurations page. Refer to "Comparing Device Configurations" on page 209 for information. • Device Diagnostic Changed — Opens the Compare NCM Routing Table page. • Device Password Change — Opens the Compare Device Configurations page. Refer to "Comparing Device Configurations" on page 209 for information.

Field	Description/Action
Displayed Change Event Types	Displays a list of event types from which you can select, including: • Device Booted • Device Configuration Change • Device Diagnostic Changed • Device Password Change • Module Added • Module Changed • Module Removed • Reserved Device Configuration Changed • Software Change • User Message

Diagnostics

In addition to configuration files, NCM gathers other device information, such as routing tables, port statistics, and IP settings. Collectively, these are called Diagnostics. Diagnostics can help you determine the effects of configuration changes and troubleshoot complex issues like routing problems and performance degradations.

By default, NCM captures a basic set of diagnostics from a device each time NCM detects a configuration change on that device. The System Administrator can define additional diagnostic tasks or event rules to capture diagnostics at different times, and can define additional custom diagnostics to capture specific device information that is useful in your environment.

NCM enables you to automatically launch diagnostics as a result of specific events. In addition, environmental diagnostics, such as CPU utilization, can be created and monitored so that automated reactions and responses can take place when certain thresholds are reached. Refer to Chapter 10, "Event Notification Rules" for information on automatically running a diagnostic as a result of a configuration change or other event.

On the menu bar under Devices, select Device Tools and click Diagnostics. The Diagnostics page opens.

Diagnostics Page Fields

Field	Description/Action
New Diagnostic link	Opens the New Diagnostics page, where you can create a new diagnostic. Refer to "New Diagnostic Page Fields" on page 534 for information.
Run Diagnostics link	Opens the Run Diagnostics Task page, where you can run any diagnostic. Refer to "Run Diagnostics Task Page Fields" on page 309 for information.
Check Boxes	You can use the left-side check boxes to delete diagnostics. Once you have selected the diagnostics click the Actions drop-down menu and click Delete. This deletes the selected diagnostics. The adjacent Select drop-down menu enables you to select or deselect all of the diagnostics.

Field	Description/Action
Name	Displays the name of the diagnostic.
Mode/Device Family	Displays the device access mode in which the diagnostic runs, such as Cisco IOS enable.
Last Modified	Displays the date and time the diagnostic was last modified.
Create By	Displays the name of the last user to modify the diagnostic (when available).
Actions	You can select from the following options: • Edit — Opens the Edit Diagnostic page, where you can edit the diagnostic. Refer to "New Diagnostic Page Fields" on page 534 for information. • Run — Opens the Run Diagnostic Task page, where you can run the diagnostic. Refer to "Run Diagnostics Task Page Fields" on page 309 for information.

New Diagnostic Page Fields

To create a new diagnostic:

1. On the menu bar under Devices, select Device Tools and click Diagnostics. The Diagnostics page opens.
2. Click the New Diagnostic link at the top of the page. The New Diagnostic Page opens. Be sure to click the Save Script button when you are finished.

Field	Description/Action
Diagnostics link	Opens the Diagnostics page, where you can create or run pre-defined diagnostics. Refer to "Diagnostics Page Fields" on page 532 for information.
Name	Enter the name of the diagnostic.
Description	Enter descriptive comments for the diagnostic.
Mode	Select the device access mode, such as Cisco Exec or Nortel Manager.
Driver	Select one of the following options: • All applicable drivers (the default) • Select specific drivers If selecting one or more drivers from the list, you can click one driver or use Shift+click or Ctrl+click to select multiple drivers. (NOTE: Devices that are menu-driven, such as the Baystack 470, cannot be accessed by custom diagnostics.)
Script	Enter the device-specific commands to run. Keep in mind the height and width of the Script box is controlled by settings from the Administrative Settings option. If you use the scripting feature extensively, you may want to adjust these settings so that you can see the script without scrolling. **Note**: Scripts can exist with the same name, but different modes. This is how NCM manages multi-vendor scripts. To run a script, simply select the script name. Each version of the script will load. When you run a script against a device group, NNCM knows the device type and applies the appropriate script.

To view diagnostics for a specific device:

1. On the menu tab under Devices, click Inventory.
2. Click the Host Name or IP Address of the device for which you want diagnostic information.
3. From the View drop-down menu, select Diagnostics and click the diagnostic you want to view. Each option shows a historical list of diagnostics specific to the device.

Adding & Editing Custom Diagnostics

NCM enables you to define custom diagnostics to capture specific information that is useful in your environment. Because each user can run custom diagnostics, any user can analyze network problems, even though they may not have permission to modify the device configuration.

To define a custom diagnostic, you provide one or more commands to run on the device. NCM stores the results of these commands as the diagnostic results. All users have permissions to run diagnostics, therefore it is important that these commands not change the device configuration. Custom diagnostics should perform read-only tasks.

You can use event rules to trigger diagnostics. For example, you could set a rule to run diagnostics whenever a configuration fails to deploy.

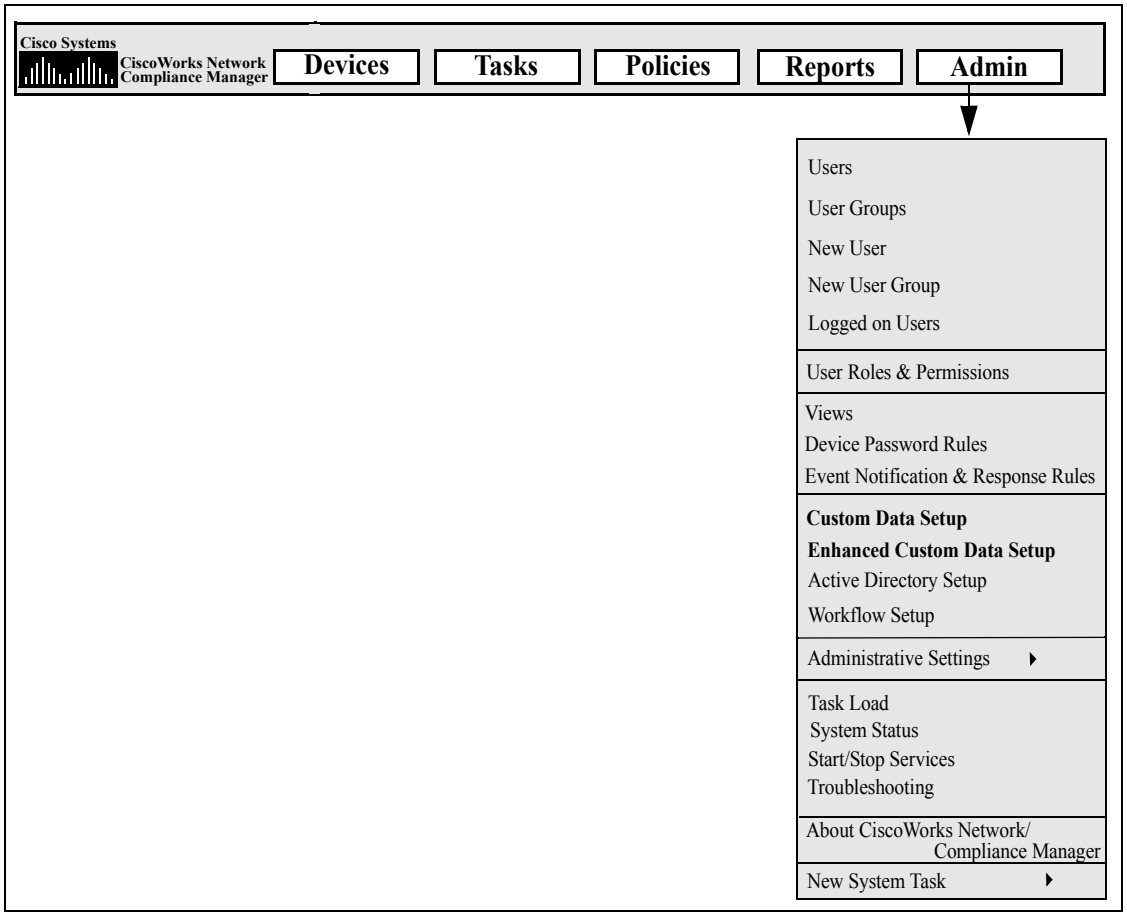
For multi-vendor networks, you can create multiple diagnostics with the same name, but running on different types of devices. Diagnostics with the same name are linked. When you run a group task, NCM automatically runs the correct version of the diagnostic for each device. For example, you could run a group diagnostic to collect data on all your routers in San Francisco, even if the routers are from multiple vendors.

Note: You must periodically purge old data from the NCM database. While it is important to purge all your old data periodically to maintain performance and restore disk space, it is especially important to purge diagnostic and script data. Unlike configurations, which are stored only when they differ from their previous instance, all diagnostic and script data is stored. By default, NCM purges diagnostic data after 45 days. Refer to "Data Pruning Task Page Fields" on page 354 for information.

Chapter 13: Custom Data Setup

Use the following table to quickly locate information.

Navigating to Custom Data Setup



Getting Started

The purpose of custom data fields is to enable you to assign useful data to specific devices, configurations, users, and so on. This gives you added flexibility and enables you to integrate CiscoWorks Network Compliance Manager (NCM) with other applications.

To add custom data, on the menu bar under Admin click Custom Data Setup. The Custom Data Setup page opens. If you have enabled extended custom data fields, refer to "Enhanced Custom Data Setup" on page 544.

Custom Data Setup Page Fields

Field	Description/Action
Custom Data Setup	Select a custom data setup from the drop-down menu. Options include: • Device Configurations & Diagnostics • Devices • Device Blades/Modules • Device Interfaces • Device Groups • Users • Tasks • Telnet/SSH Sessions • Add Custom Device Fields
Check Boxes	You can use the left-side check boxes to enable the field. Consequently, the field appears in the user interface and is available to the integration API.
Device Configuration & Diagnostics	
These fields appear on the Device Configuration Detail page. You can enter or edit the values by clicking the Edit Comments link, which opens the Edit Device Configuration Detail page.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.

Field	Description/Action
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NCM displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Devices

These fields appear on the Device Information page. You can enter or edit the values by clicking the Edit link, which opens the Edit Device page, or by clicking Add from the Devices drop-down menu, which opens the New Device page.

API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NCM displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Device Blades/Modules

These fields appear on the View/Edit Modules pages.

API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.

Field	Description/Action
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NCM displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Device Interfaces

These fields appear on the View/Edit Modules pages.

API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NCM displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Device Groups

These fields appear on the Device List page for the group. You can enter or edit the values by clicking the Edit Group link, which opens the Edit Group page, or by clicking Groups from the Devices drop-down menu, which opens the New Group page.

API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.

Field	Description/Action
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NCM displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Users

These fields appear on the My Profile page. You can enter or edit the values by clicking the Edit link on the User List page, which opens the Edit User page, or by clicking New User on the User List page, which opens the New User page.

API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NCM displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Tasks

These fields appear on Task pages. You cannot enter or edit the values through the user interface, but only through the integration API.

API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.

Field	Description/Action
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NCM displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.
Telnet/SSH Sessions	
These fields appear on the Telnet/SSH Session List page. You cannot enter or edit the values through the user interface, but only through the integration API.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NCM displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Enhanced Custom Data Setup

Custom data fields enable you to assign useful data to specific devices. This gives you added flexibility and enables you to integrate NCM with other applications.

Note: Before you can add enhanced custom fields, you must enable the Enhanced Custom Data application. Refer to "User Interface Page Fields" on page 89 for instructions.

To view the current custom data fields and add data fields to the Device Details and Device Interfaces pages, on the menu bar under Admin click Extended Custom Data Setup. The Enhanced Custom Data Setup page opens.

Enhanced Custom Data Setup Page Fields

Field	Description/Action
Drop-down menu	Select one of the following options from the drop-down menu: • Devices (the default) • Device Interfaces
Add Custom Devices Field link	Clicking the Add Custom Devices Fields link opens the New Custom Data Field page, where you can add custom data fields. These data fields are displayed on the Device Details and Device Interfaces pages. Refer to "New Custom Data Field Page Fields" on page 546 for information. For information on the Device Details and Device Interfaces pages, refer to "View Menu Options" on page 229 and "Device Interfaces Page Fields" on page 234.
Devices / Device Interfaces	
Enabled	Indicates if the custom data field is enabled.
Field Name	Displays the name of the custom data field.
Limit Values To	Displays a list of comma separated values. The list is shown as a drop-down menu when editing the actual data.
Allow HTML	Indicates if users can enter HTML code in this data field. NCM displays the data field as HTML, not text.

Field	Description/Action
Actions	Select one of the following options: • Edit — Opens the Edit Custom Data Field page, where you can edit the current information. Refer to "New Custom Data Field Page Fields" on page 546. • Delete — Enables you to delete Custom Data Fields. Deleting a data field will cause any data associated with that field to be deleted as well.

New Custom Data Field Page Fields

To add custom data fields to the Device Details and Device Interfaces page, on the menu bar under Admin click Enhanced Custom Data Setup. The enhanced Custom Data Setup page opens. Click the Add Custom Devices Field link at the top of the page.

Field	Description/Action
Enabled	If checked, the custom data field is enabled.
Field Name	Enter a data field name.
Limit Values To	Enter a list of comma separated values. The list is shown as a drop-down menu when editing the actual data.
Allow HTML	If checked, users can enter HTML code in this field. NCM displays the field as HTML, not text.

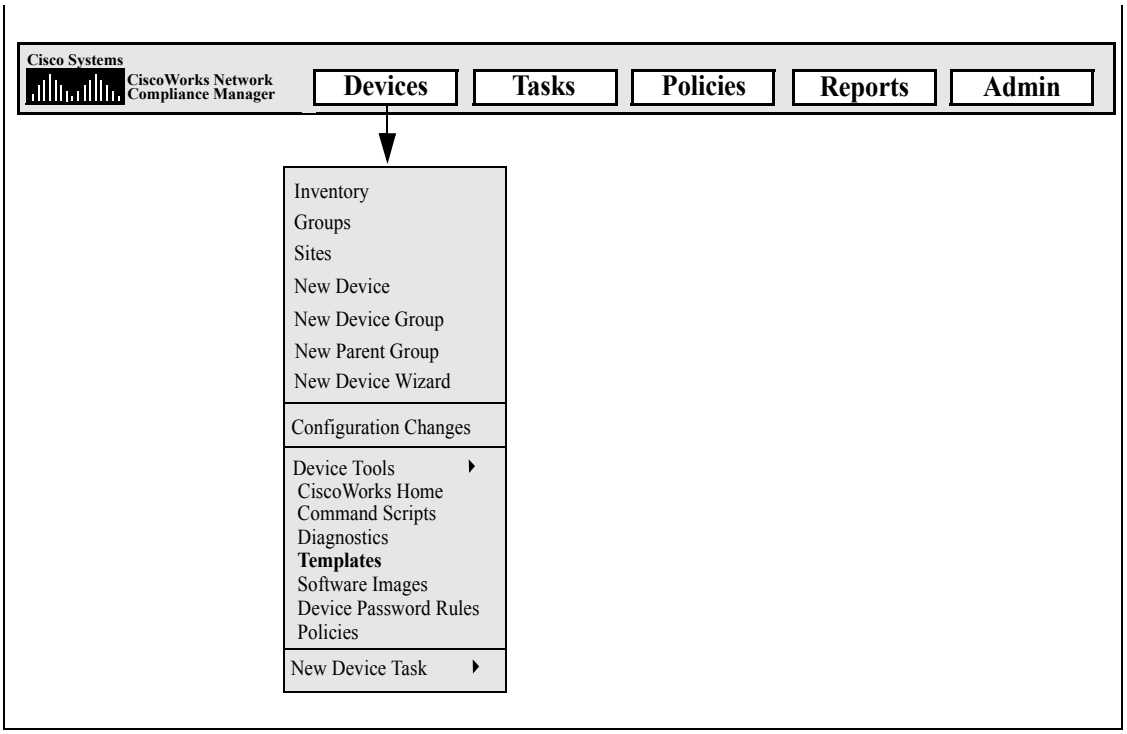
Click the Save button when you are done. The new data field is displayed on the Enhanced Custom Data Setup page.

Chapter 14: Creating Templates

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 548
Viewing Templates	"Viewing Templates" on page 549
Creating New Templates	"Creating New Templates" on page 551

Navigating to Templates



Getting Started

Device configuration templates enable rapid, straightforward deployment of new device configurations. Using templates:

- Engineers can provision new devices or services quickly while conforming to departmental configuration standards.
- Network architects can create friendly GUI prompts with validation parameters so that template users can fill in the blanks to rapidly populate and deploy new configurations.

After you create a template and populate it with configuration commands, you can create a script from the template. When you run the script, it deploys the configuration commands, either as a fragment or an entire configuration, to one or more devices.

Viewing Templates

To view the current templates, on the menu bar under Devices, select Device Tools and click Templates. The Templates page opens. Use this page to view a list of templates sorted by vendor.

Templates Page Fields

Field	Description/Action
New Template link	Opens the New Template page, where you create a new template. Refer to "New Template Page Fields" on page 551 for information.
Check Boxes	You can use the left-side check boxes to delete templates. Once you have selected the templates, click the Actions drop-down menu and click Delete. This deletes the selected templates. The adjacent Select drop-down menu enables you to select or deselect all of the templates.
Vendor	Displays the vendor for the devices to which this template applies. Clicking the vendor link opens the Templates page, where you can view the templates for this vendor. From this page, you can: • Include the template in a script and build a full script from them. • Create a new script.
Name	Displays the name of the template.
Role	Displays the role of the template. The default roles include: • Any • Core • Border • Test
Model	Displays the model of the devices to which this template applies.
Processor/Component	Displays processor of the devices to which this template applies.

Field	Description/Action
Drivers	Displays the drivers assigned to the devices to which this template applies.
Actions	You can select one of the following options: • View Details — Opens the View Template page, where you can view the template as HTML in a separate browser window. Refer to "View Template Page Fields" on page 553 for information. • View Text — Opens a text window, where you can view the template as text in a separate browser window. Refer to "View Template Page Fields" on page 553 for information. • Edit — Opens the Edit Template page, where you can add or edit a template. Refer to "New Template Page Fields" on page 551 for information.

Creating New Templates

To create a new template:

1. On the menu bar under Devices, select Device Tools and click Templates. The Templates page opens.
2. Click the New Template link at the top of the page. The New Template page opens. Be sure to click Save Template when finished.

New Template Page Fields

Field	Description/Action
Templates link	Opens the Templates page, where you can view all of the current templates. Refer to "Templates Page Fields" on page 549 for information.
Name	Enter the name of the template.
Comments	Enter a description of the template. Comments are included in all tables, so include only crucial information.
Role	Select a role for the template. Default roles include: • Any • Core • Border • Test
Model	Enter the model of the devices to which this template applies.
Processor/Component	Enter the processor of the devices to which this template applies.
Mode	Select the device command line interface (CLI) mode in which the template runs. (NOTE: Commands should not change the CLI prompt or mode. Otherwise, the script will stop running at that command and return an error.)

Field	Description/Action
Driver	Select one of the following options: • All applicable drivers (the default) • Select specific drivers — Select the driver assigned to the devices to which this template applies. The list includes only drivers that are compatible with the selected mode.
Template	Enter the configuration commands and comments that populate the template. Each line you enter should represent one complete command for the device. After the command, you should see the device's prompt again. When the template is applied to devices, this configuration will be deployed. Keep in mind that variable names cannot begin with tc_, but can include any combination of uppercase alpha, lowercase alpha, 0 through 9, and underscore characters.

View Template Page Fields

To view a specific template:

1. On the menu bar under Devices, select Device Tools and click Templates. The Templates page opens.
2. Click the View Details option in the Actions column for the template you want to view. The View Template page for that template opens.

Field	Description/Action
Edit Template link	Opens the Edit Template page, where you can create a new template. Refer to "New Template Page Fields" on page 551 for information.

Text Version link	Opens a text window, where you can view the template as text in a separate browser window. The text would look something like the following:
	
	`sflow destination $dest_ip_1$ $dest_udp_port1$`
	`sflow destination $dest_ip_2$ $dest_udp_port2$`

Template link	Opens the Templates page, where you can view a list of templates sorted by vendor. Refer to "Templates Page Fields" on page 549 for information.
Comments	Displays comments entered by the template author or edited later. (NOTE: The Comments box is hidden unless populated.)
Line	Displays the number of each line in the template.
Template Text	Displays the configuration commands and comments that populate the template.
Name	Displays the name of the template.
Model	Displays the model of the devices to which this template applies.

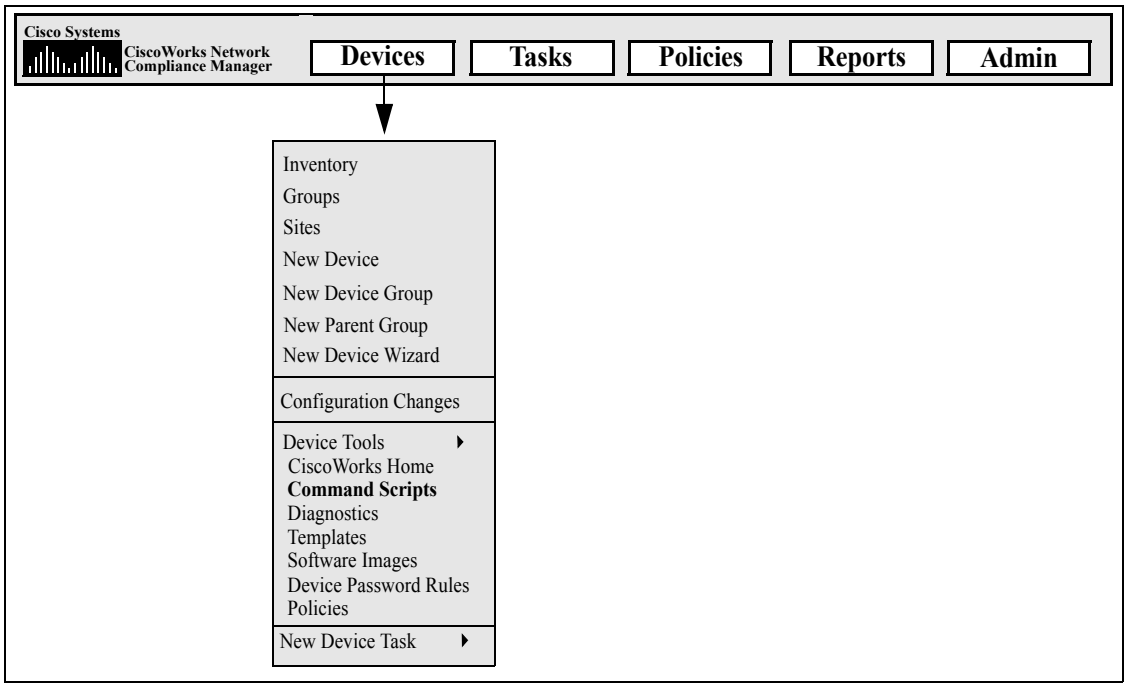
Field	Description/Action
Role	Displays the role of the template. The default roles include: • Any • Core • Border • Test
Processor/Component	Displays the processor of the devices to which this template applies.
Mode	Displays device command line interface (CLI) mode in which the template runs.
Drivers	Displays the drivers assigned to the devices to which this template applies.

Chapter 15: Managing Command Scripts

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 556
Adding & Editing Command Scripts	"Adding Command Scripts" on page 558
Running Command Scripts	"Running Command Scripts" on page 563

Navigating to Command Scripts



Getting Started

You can define command scripts to run a set of commands on one or multiple active devices. Command scripts are particularly useful for batch actions on a group of devices. For example, you could run a script on the Inventory group to update all devices to match standard policies, such as setting the SNMP trap logging host, NTP server, or a corporate login banner.

The Advanced Scripting feature enables you to run custom scripts written in various command line languages, such as Expect and PERL. Advanced scripting enables the extended capability of conditional logic. Because advanced scripts must support a fully functioning Expect engine, external Telnet/SSH clients are called and run in a separate process. Refer to "New Command Script Page Fields" on page 560 for more information on the Advanced Scripting feature.

Note: Language support must be installed to use the Advanced Scripting feature. In addition, you must configure the Administrative Settings to enable it. Support for the Expect language is installed with NCM. Windows environments with PERL scripting capability must install PERL (CPAN).

To view a list of pre-defined and custom command scripts, on the menu bar under Devices select Device Tools and click Command Scripts. The Command Scripts page opens. The page displays a list of command scripts for which you have permissions. Users with full access to command scripts see a selection of pre-defined scripts delivered with CiscoWorks Network Compliance Manager (NCM).

Command Scripts Page Fields

Field	Description/Action
New Command Script link	Opens the New Command Script page, where you can write a new script and pull variables from the script to define prompts. Refer to "New Command Script Page Fields" on page 560 for information.

Field	Description/Action
Run Command Scripts link	Opens the Run Command Script Task page, where you can set up a task to run command scripts. Before saving the task, you can edit variables in the script to create a unique instance of the script. Refer to "Run Command Script Task Page Fields" on page 302 for information.
Script Type	The Script Type drop-down menu enables you to filter the list of scripts to view only scrips of a specific type.
Check Boxes	You can use the left-side check boxes to delete scripts. Once you have selected the scripts, click the Actions drop-down menu and click Delete. This deletes the selected scripts. The adjacent Select drop-down menu enables you to select or deselect all of the scripts.
Name	Displays the name of the script.
Mode / Device Family	Displays the device access mode, such as Cisco Exec or Nortel Manager, in which the script runs. Device Family is used for Advanced Scripting and displays a collection of devices that share a similar configuration CLI command syntax.
Last Modified	Displays the date and time the script was last modified.
Created By	Displays the name of the last user to modify the script. For example, if the script is a script template, this field shows who modified the script for a specific instance.
Actions	You can select one of the following options: • Edit — Opens the Edit Command Script page, where you can modify an existing script. Refer to "New Command Script Page Fields" on page 560 for information. • Run — Opens the Run Command Script Task page, where you can run the command script. Refer to "Run Command Script Task Page Fields" on page 302 for information.

Adding Command Scripts

Command scripts enables you to:

- Run a custom set of commands on one or more devices.
- Run scripts as a scheduled task, and to use event rules to trigger scripts to run. For example, you could set a rule to configure standard settings on a particular device type whenever a device of that type is added.

NCM provides several options for adding scripts. You can:

- Write or copy a script into the New Command Script page, adding variables or defining prompts as needed.
- Create template scripts that enables users to edit variable values before running a script. "Creating a Script from a Template" on page 564 for information.
- Automatically convert a session log to a script. To create a new script from a session log, from the Telnet/SSH Session Log click Convert to Script. The New Command Script page opens with the session commands pre-loaded in the Script box.

NCM supports both simple and advanced scripting.

Simple scripting is mode-based (CLI command language). Keep in mind that simple command scripts do not recognize device CLI errors. Consequently, NCM assumes the device CLI commands executed were successful. A simple command script only fails if it cannot reach the device or it loses connection to the device during the execution of the script.

Advanced scripting is based on any command line scripting language, such as Expect or PERL, including scripts that contain conditional logic (*if*, *while*, and *for* conditions). You can customize instances of a script by including variables. When you run the script, you are prompted for a value for each variable. Refer to the following table for additional details.

Simple Scripts	Advanced Scripts
• No if or loops • Uses device command (Cisco commands like *show conf)* • No error handling • No login required • No NCM device variables	• If and loops permitted • Uses language commands (PERL or Expect commands such as send "show conf\n" or print SOCKET "show conf\n") • Can handle errors • Requires code to login • Can access NCM device variables

You can use scripts to perform the same task on different types of devices by creating multiple scripts with the same name so that all scripts by that name run as a single task. (The devices must be configured as a device group.) When you run the script, you see every instance of the script that applies to any device in the group. For example, you could run a script to change the NTP server on all your routers, even if the routers are from different vendors. When running multiple scripts of the same name, you can edit each instance of the script.

To add a new command script:

1. On the menu bar under Devices, select Device Tools and click Command Scripts. The Command Scripts page opens.
2. Click the New Command Script link at the top of the page. The New Command Script page opens. Be sure to click Save Script when you are finished. When the script is saved successfully, the Command Scripts page opens. The script you added appears in the list and is highlighted. Keep in mind that a script does not run until you schedule it as a task.

Note: Variables beginning with "tc_" are reserved for special use. You cannot define any variables in custom or advanced scripts that begin with this character sequence.

New Command Script Page Fields

Field	Description/Action
Command Scripts link	Opens the Command Scripts page, where you can view the list of command scripts. Refer to "Command Scripts Page Fields" on page 556 for information.
Name	Enter the name of the new script.
Description	Enter a description of the script, such as whether it was created from a template and who created it.
Script Type	Select one of the following options: • General Purpose (the default) • Existing — Select a script from the drop-down menu. • New — Enter a new script type.

Field	Description/Action
Advanced Scripting	If checked, the page is refreshed to provide settings specific to custom scripts written in command line languages such as Expert and PERL. Advanced Scripting specific fields include: • Device Family — A device family is a collection of devices that share a similar configuration CLI command syntax. Select a device family. This restricts the script to run against those devices whose driver is in the selected device family. This feature enables you to assign one name to multiple implementations of a script created for different devices so that they can run as a single task. • Language — Select the scripting language in which the script you are adding is written. You must install language support and configure the language in Administrative Settings/Server/ Advanced Scripting to use this feature. (NOTE: Expect support is installed with NCM, but you must still configure the path.) • Parameters — Enter the authentication parameters for the script. You can include NCM or your own custom variables. (NOTE: Using parameters for authentication is recommended as this strategy reduces the security risk of having passwords written to a file.) • Script — Advanced Scripting commands can contain conditional logic and include pre-defined variables. Variable names can only contain letters, numerals and underscores (_). The required format is the variable name between two dollar signs ($), as illustrated in these examples: $report$, $my_address$, $port_3_ip$. Advanced scripts must include any code required to connect and log in to the device. For example, you can connect to tc_device_ip and log in using $tc_device_password$. • Device variables link — Displays a list of device variables available for use in your advanced custom scripts. These variables always begin with $tc_ and the names are case sensitive. (You can also create your own variables.) • Pull Variables button — Refreshes the page, adding input fields at the bottom of the page for each variable used in the script. Use these fields to define custom prompts for the variables and to limit the values that each prompt will accept. You can select the following options for each variable: - Allow multiple lines in value. - Limit values to (enter values separated with commas).

Field	Description/Action
Mode	Select the device access mode, such as Cisco Exec or Nortel Manager.
Driver	Select one of the following options: • All applicable drivers (the default) • Select specific drivers — If selecting one or more drivers from the list, you can click one driver or use Shift+click or Ctrl+click to select multiple drivers. (NOTE: Devices that are menu-driven, such as the Baystack 470, cannot be accessed by custom scripts.)
Script	Enter the device-specific commands to send to the device, or paste in and edit an existing script. Refer to the help information on the Command Script page regarding how commands must be entered. **Note:** Variable names cannot begin with tc_ (reserved for NCM), but can include any combination of uppercase alpha, lowercase alpha, 0 through 9, and underscore characters.
Pull Variables button	Refreshes the page, adding input fields at the bottom of the page for each variable used in the script. Use these fields to define custom prompts for the variables and to limit the values that each prompt will accept. Sample fields include: • HOSTNAME • ETH_SLOT1 Enter the custom prompt you want the user to respond to when this script runs, and the response values you want this prompt to accept. Values must be separated by commas, so you cannot use values that include commas. If you specify multiple values, when the user sees the prompt, a list of accepted values is provided in the prompt dialog.

Running Command Scripts

Your ability to run and to edit instances of command scripts is restricted by your permissions. Users with Limited permissions and Full or Power users who do not have the Modify Device permission cannot run scripts.

You can set up a script to run once, periodically based on a user-defined interval, or as a recurring task. In addition, you can schedule the task to start at a specific time or as soon as possible. Keep in mind that you can edit the script and supply values for variables before running it.

To run a script from the Command Scripts page:

1. On the menu bar under Devices, select Device Tools and click Command Scripts. The Command Scripts page opens.
2. Select the name of the script you want to run.
3. In the Action column, click Run. The Run Command Script Task page opens. Refer to "Run Command Script Task Page Fields" on page 302 for information.

Note: You can also run a command script from the Tasks menu.

Creating a Script from a Template

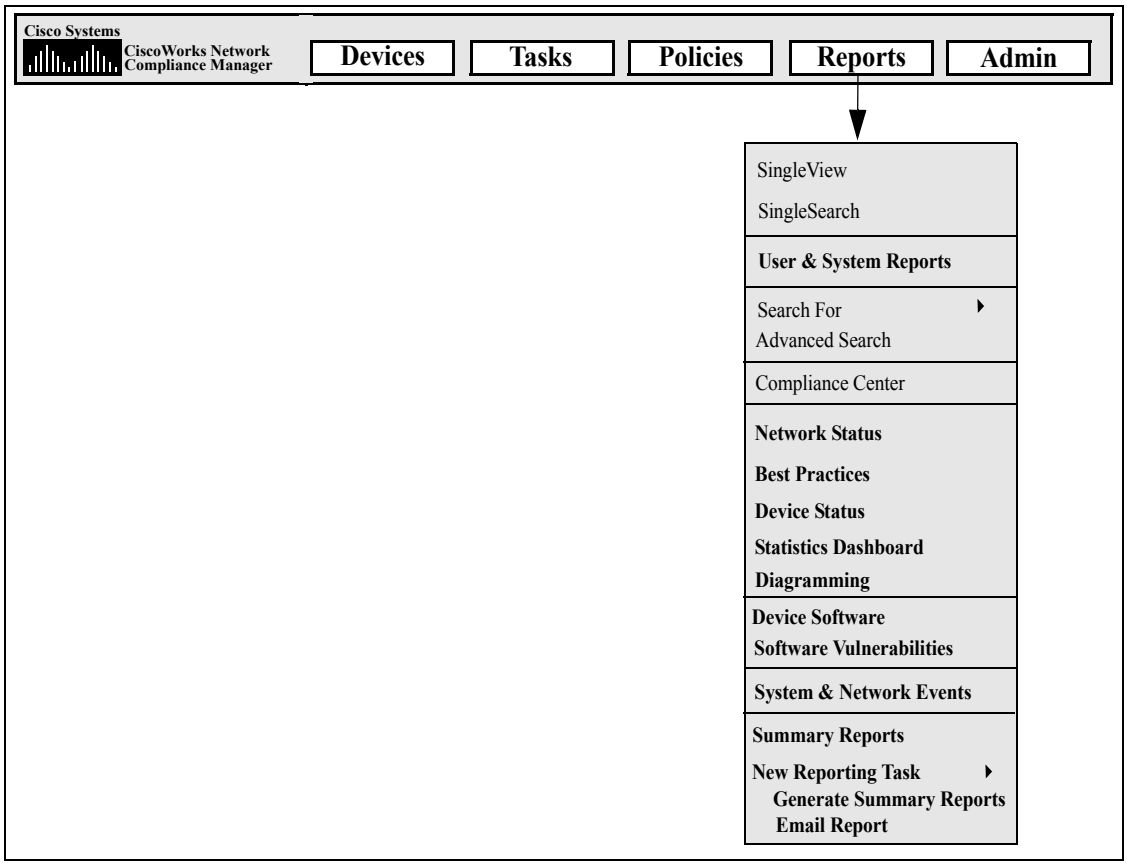
To create a script from a template:

1. On the menu bar under Devices, select Device Tools and click Templates. The Templates page opens. Refer to "Templates Page Fields" on page 549.
2. Click the vendor link. The Templates page for that vendor opens.
3. Select the template to include in your script and click the Actions drop-down menu.
4. Click Update Script.
5. Edit the script, if necessary, and click the Create Script button to create a script that can be deployed to the device. The Save Script from Template page opens.
6. Edit the Name, Description, and any other fields. Keep in mind that variable names cannot begin with "tc_". However, they can include any combination of uppercase alpha, lowercase alpha, 0 through 9, and underscore characters.
7. Click Save Script. The Command Scripts page opens. The new script is highlighted.

Chapter 16: Reports

Use the following table to quickly locate information.

Navigating to Reports



Getting Started

CiscoWorks Network Compliance Manager (NCM) offers both default reports that require no input and ad-hoc reports. Default reports include:

- User and System Reports
- Network Status reports
- Configuration reports
- Device reports
- Software vulnerability reports
- Task/Job reports
- Telnet/SSH User Session Log reports
- Compliance Center reports (refer to Chapter 18)

Ad-hoc reports provide flexibility and control to report on data within NCM. Ad-hoc reports can be manually or automatically generated based on regular expression criteria for one or more fields. Common ad-hoc reports could include:

- All Cisco devices running 12.* versions of IOS
- All devices using insecure protocols for configuration management
- All devices with a faulty module
- All configuration changes made over a period of time for a set of devices
- All Telnet/SSH session logs initiated by a specific user
- All device changes that results because of an approval override
- All ACLs that deny traffic on specific ports

User & System Reports

The User & System reports are the results of searches you defined and saved using the Search capabilities. Only searches for which you defined appear in the list of User reports. You can search for:

- Devices
- Modules
- Configurations
- Diagnostics
- Tasks
- Telnet/SSH Sessions
- Events
- Users
- ACLs
- MAC addresses
- VLANs

For information on performing searches, refer to "Searching for Devices" on page 449.

Each report includes a summary of the criteria used in the search. Your saved searches are not available to anyone but you and the NCM Administrator.

Note: If you have not run and saved any searches, no User reports are available.

System reports on pre-defined queries. They are generated when you select the report. Each report includes a summary of the criteria used in the search. The System reports include:

Configuration	• All changes made in the last 12 hours • All changes made in the last 24 hours • All changes made in the last 48 hours • All changes made in the last week • All changes made in the last month • All changes made by myself in the last 48 hours
Configuration Policy Events	• Policy rule violations in the past 24 hours
Devices	• All devices changed in the last 24 hours • All devices changed in the last week • All devices with access failures • All inactive devices (Note: Rather than deleting inactive devices, you can specify them as inactive so as to retain the configuration history.) • All duplicate IP addresses • All devices without driver assigned • All devices with driver assigned but no configuration stored • All devices with different startup and running configurations
DuplicateIP	• All duplicate IP addresses — This report displays which devices have interfaces that are configured with the same IP address, however it does not remove the IP address that is causing the duplicate detection.

Session	• All sessions created in the last 24 hours • All sessions created in the last 48 hours • All sessions created in the last week • All sessions created by myself in the last 48 hours
Software Compliance	• Device Software Compliance
Task	• All failed, skipped, and duplicate tasks in the last 24 hours • All failed, skipped, and duplicate tasks in the last week
Other	• Best Practices Report • Network Status Report • Device Status Report

To view the User & System reports, on the menu bar under Reports click User & System Reports. The User & System Reports page opens.

User & System Reports Fields

Field	Description/Action
Type	Displays the type of event or report.
Report	Displays the name of the report, for example Device Status, HIPAA Compliance Status, All inactive devices, and so on. Clicking the report opens the report.
Actions	You can select the following actions: • Email Report — Displays the Email Report form where you can create a task to send the output of a report via email. You can specify the recipient. User login is the default. You must save the task to generate the email message. • Modify — For User reports, you can click the Modify option for an event. The Search For Events page opens. • Delete (red X icon) — Permanently deletes the report. • Click the Up or Down arrows to move the report up or down in the list.

Network Status Report

The Network Status Report provides an overview of network configuration, health, and compliance, combined with two independent views of the network:

- Best Practices
- Device Status

The Network Status report delivers proactive reporting capability. By scheduling the report to run as a recurring Email Report task, network administrators and engineers automatically receive up-to-date information that can help eliminate problems before they impact the network. Network Status reports can also provide management with an overview of network operations' effectiveness in resolving policy and software compliance issues and handling configuration changes.

Note: The default configuration for this report is to run against the Inventory device group.

Events are reported based on a three-tiered representation of the risk introduced to the network. The System Administrator sets the threshold for each category and assigns the risk level indicator color to reflect the impact on the network.

- Red — High risk, including policy violations, software compliance violations, and device access failures combined with any other Yellow level event.
- Yellow — Moderate risk, including startup and running configuration mismatches and device access failures.
- Green — Within threshold.

The status of any device group is based on the highest risk condition of any device in the group. The status of the network is based on the highest risk condition of any group in the network.

To view the Network Status report, on the menu bar under Reports, click Network Status. You can run this report on demand using the Run Again button on the report page or schedule the report to run as a task and email it to key network and management staff using the Email Report option. For information on emailing reports, refer to "Emailing Reports" on page 605.

Network Status Report Fields

Field	Description/Action
Best Practices Report link	Opens the Best Practices Report. Refer to "Best Practices Report" on page 576.
Device Status Report link	Opens the Device Status Report. Refer to "Device Status Report" on page 579.
Report Date	Displays the date and time the report was last run.
Device Groups Reported	Displays the number of reported device groups.
Change Device Groups	Displays a list of currently defined device groups. You can run the Network Status report for a single device group or for multiple devices groups. All other parameters are pre-defined. Summary and detail information is provided per category for each device group you specify. Click the Run Again button when finished.
Status	Displays the name of the device group and the number of devices in the group.
Device Status	
Device Status	Displays the status level indicator with percentages of issues found. Status levels include: • Red — High risk • Yellow — Moderate risk • Green — Low risk If you click Device Status, the Device Status report opens. Refer to "Device Status Report" on page 579.
Best Practices Status	

Field	Description/Action
Issue	Displays the five key network issues that NCM tracks, including: • Policy Rule Violations — Devices that do not comply with one or more defined configuration policies. Move the cursor over the information icon for more information. • Software Compliance Violations within 24 hours — Devices that are running non-approved software versions. Move the cursor over the information icon for more information. • Startup vs. Running Configuration Mismatch — Devices with mismatched startup and running configurations. Move the cursor over the information icon for more information. • Device Access Failure — Devices that NCM could not reach. Move the cursor over the information icon for more information. • Configuration Changes within 24 hours — Device configuration changes detected in the past 24 hours. Move the cursor over the information icon for more information. Available action links vary for each issue. For example, for all reported Device Access Failures, you can click the link to view the device details View Task option, where you can identify the tasks that failed. For Startup vs. Running Configuration Mismatches, you can click the link to view the Compare Startup with Running option, which shows both configurations with the differences highlighted. If you click Best Practices Status, the Best Practices report opens. Refer to "Best Practices Report" on page 576.

Network Status Report Details

Field	Description/Action
High Risk (Red) Issues	Displays summary information for any of the five issues that returned a red status. Available action links vary for each issue. For example: • All reported Device Access Failures — Click the link to view the device details View Task option, where you can identify the tasks that failed. • Policy Rule Violations — Click the link to view the Configuration Policy Activity page, where you can view events that show if a device's configuration was not in compliance with the configuration rules contained in one or more configuration policies. The value shown in the Policy Importance column is the highest importance of all configuration rules currently violated by the device. • Startup vs. Running Configuration Mismatches — Click the link to view the Compare Startup with Running option that shows both configurations. All differences are highlighted.

Best Practices Report

Best practices for network management dictate that non-compliance with any of the following issues be carefully monitored:

- Policy Rule Violations within 24 hours
- Software Compliance Violations
- Startup vs. Running Configuration Mismatch
- Device Access Failure
- Configuration Changes within 24 hours

NCM enables you to define the acceptable level of non-conformance with each of these issues. If the threshold is exceeded, a yellow or red warning is shown depending on the level of non-compliance. NCM also displays which devices failed to comply so you can take corrective action.

If all five indicators are green, NCM has evaluated your network and determined your network health is good. If some indicators show yellow, you should target those areas for corrective action. If some indicators are red, the issues flagged could represent a critical risk to network stability and should receive immediate attention.

To view the Best Practices report, on the menu bar under Reports click Best Practices. The Best Practices report opens.

Note: You can also navigate to the Best Practices report from the Network Status report.

Best Practices Report Fields

Field	Description/Action
Network Status Report link	Opens the Network Status report. Refer to "Network Status Report" on page 572.
Device Status Report link	Open the Device Status Report. Refer to "Device Status Report" on page 579.
Report Date	Displays the date and time the report was last run.
Device Groups Reported	Displays the number of reported device groups.
Change Device Groups	Displays a list of currently defined groups. You can run the Best Practices report for a single group or for multiple groups. All other parameters are pre-defined. Summary and detail information is provided per category for each group you specify. Click the Run Again button when finished.
Status	Displays the name of the group and the number of devices in the group. Status levels include: • Red — High risk • Yellow — Moderate risk • Green — Within threshold
Issue	Displays the five key network issues that NCM tracks, including: • Policy Rule Violations within 24 hours — Devices that do not comply with one or more defined configuration polices. Move the cursor over the information icon for more information. • Software Compliance Violations — Devices that are running non-approved software versions. Move the cursor over the information icon for more information. • Startup vs. Running Configuration Mismatch — Devices with mismatch startup and running configurations. Move the cursor over the information icon for more information. • Device Access Failure — Devices that NCM could not reach. Move the cursor over the information icon for more information. • Configuration Changes within 24 hours — Device configuration changes detected in the past 24 hours. Move the cursor over the information icon for more information.

Best Practices Report Details

Field	Description/Action
High Risk (Red) Issues	Displays summary information for any of the five issues that returned a red status. Available action links vary for each issue. For example, for all reported Device Access Failures, you can click the link to view the device details View Task option, where you can identify the tasks that failed. For Startup vs. Running Configuration Mismatches, you can click the link to view the Compare Startup with Running option that shows both configurations. All differences are highlighted.

Device Status Report

The Device Status report lists all of the devices in your network and analyzes them individually for each of the Best Practices issues. Refer to "Network Status Report Fields" on page 573 for information on each of the Best Practices issues.

Each device that does not comply with one or more of the issues is flagged with a yellow or red warning. The report also summarizes the entire network to see how many devices generated yellow or red warnings.

To view the Device Status report, on the menu bar under Reports click Device Status. The Device Status report opens.

Note: You can also navigate to the Device Status report from either the Network Status report or the Best Practices report.

Device Status Report Fields

Field	Description/Action
Network Status Report link	Opens the Network Status report. Refer to "Network Status Report" on page 572.
Best Practices Report link	Opens the Best Practices Report. Refer to "Best Practices Report" on page 576.
Report Date	Displays the date and time the report was last run.
Device Groups Reported	Displays the number of reported device groups.
Change Device Groups	Displays a list of currently defined groups. You can run the Best Practices report for a single group or for multiple groups. All other parameters are pre-defined. Summary and detail information is provided per category for each group you specify. Click the Run Again button when finished.
Status	Displays the name of the group and the number of devices in the group. Status levels include: • Red — High risk • Yellow — Moderate risk • Green — Within threshold

Field	Description/Action
Device Status Report Details	
Moderate Risk (Yellow) and High Risk (Red) Issues	Displays summary information for any of the five issues that returned a yellow or red status. Available action links vary for each issue. For example, for all reported Config Changes within 24 hours, you can click the View Config link to view the configuration information for that decide. For Device Access Failures, you can click the View Device Tasks link, where you can identify the tasks that failed.

Statistics Dashboard

The Statistics Dashboard provides information on the following reports:

- Top 5 Vendors — Refer to "Summary Reports" on page 601 for information.
- Top 5 OS Versions — Refer to "Summary Reports" on page 601 for information.
- Number of Configuration Change - Last 7 Days — Refer to "User & System Reports" on page 568 for information.
- Change History by Time of Day — Refer to "Summary Reports" on page 601 for information.
- Top 10 Most Accessed Devices — Refer to "Summary Reports" on page 601 for information.
- System Status — Refer to "Network Status Report" on page 572 for information.

To view the Statistics Dashboard, on the menu bar under reports, click Statistics Dashboard. The Statistics Dashboard opens.

Diagramming

Diagramming enables you to gather topology data from your network devices. Network diagrams can be viewed in either Visio, static JPEG, or interactive JPEG format and printed. The topology data, including Layer 3 IP addresses and subnets, and Layer 2 details spanning MAC addresses and VLANs, provides a snapshot of the current state of your network.

Keep in mind that Layer 3 data includes IP addresses obtained from the device's configuration file. Layer 2 data is tied to the MAC addresses of the interfaces on each device and data from the MAC tables showing what MAC address the device sees. NCM maps which devices can communicate with each other as a result of being on the same network.

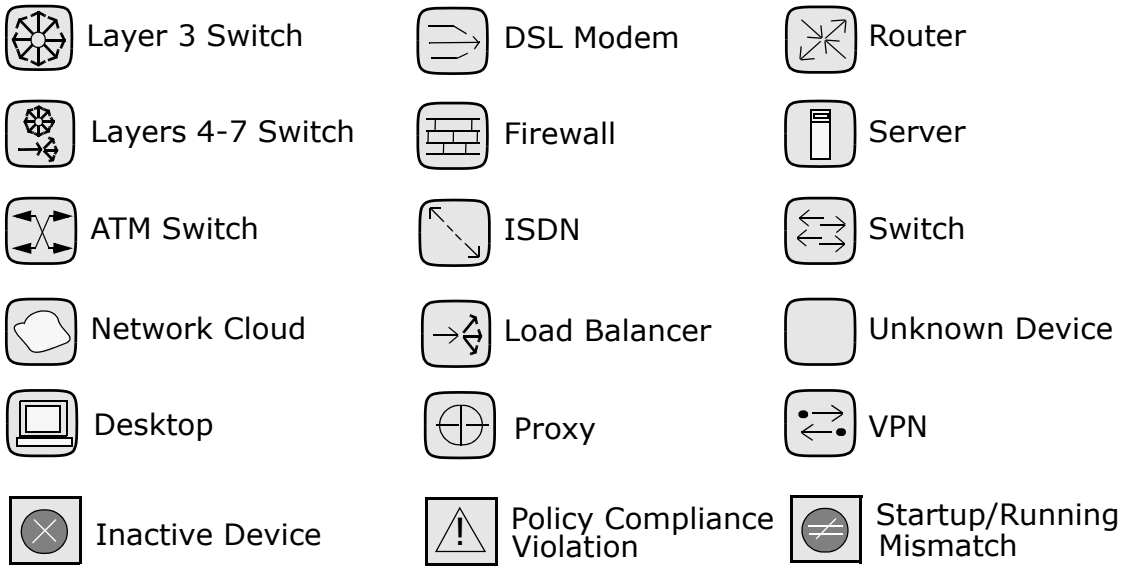
The inferred Layer 1 data is based on heuristics. NCM reduces the number of data link connections between devices and/or servers to make network diagrams more readable. Only connections that can be inferred through transitive connections are reduced.

In the OSI model, each layer is an abstraction designed to hide the layer below. Therefore, the Layer 2 data gathered from devices cannot generate 100% accurate Layer 1 data. In particular, Layer 1 data could be incorrect if any of the following conditions exist:

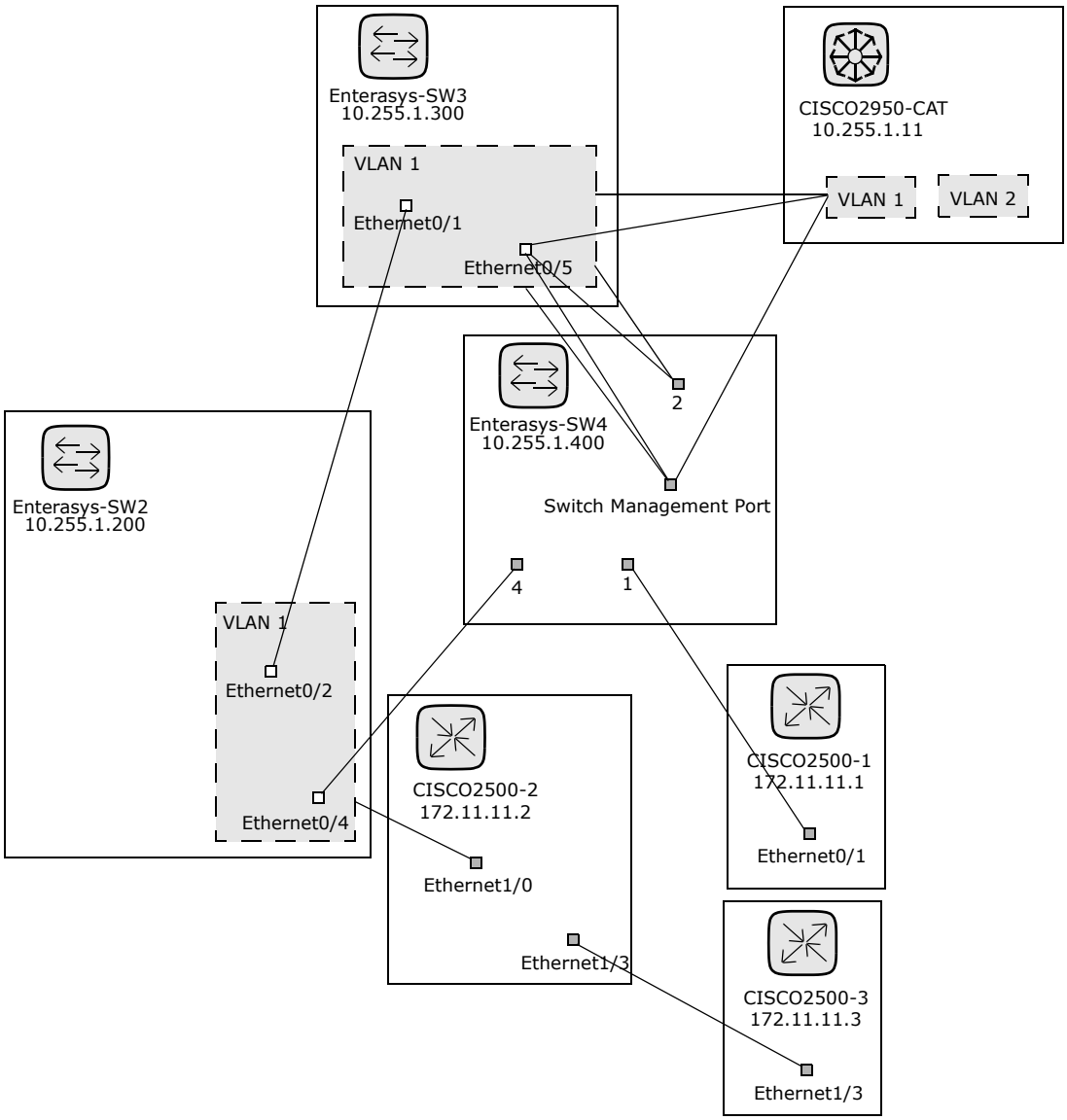
- The device does not return the interface number where MAC addresses are seen.
- There was no traffic between the devices within a few minutes of when NCM gathers the topology data (where MAC addresses are seen).
- There is an unmanaged device between two managed devices.
- There is an unaddressable device, such as a hub, between two managed devices.

The following colors, borders, lines, and icons are used in diagrams.

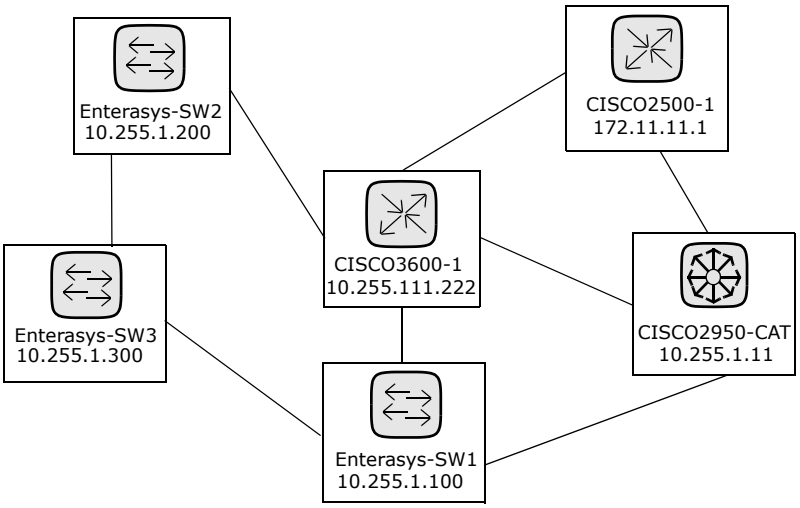
- Red — The device failed its last access, either as a result of a Snapshot task or another task. (**Note**: For VLANs and ports, red indicates that the VLAN is administratively down and gray indicates that the VLAN is up and running.)
- Gray — The device contains no snapshot data.
- White — The device is up and running.
- Device borders — A solid border indicates a device. A dashed border indicates a virtual grouping, where each VLAN in a device is shown as its own device.
- Dashed lines — Depict Layer 3 connections.
- Solid lines — Depict Layer 2 connections.



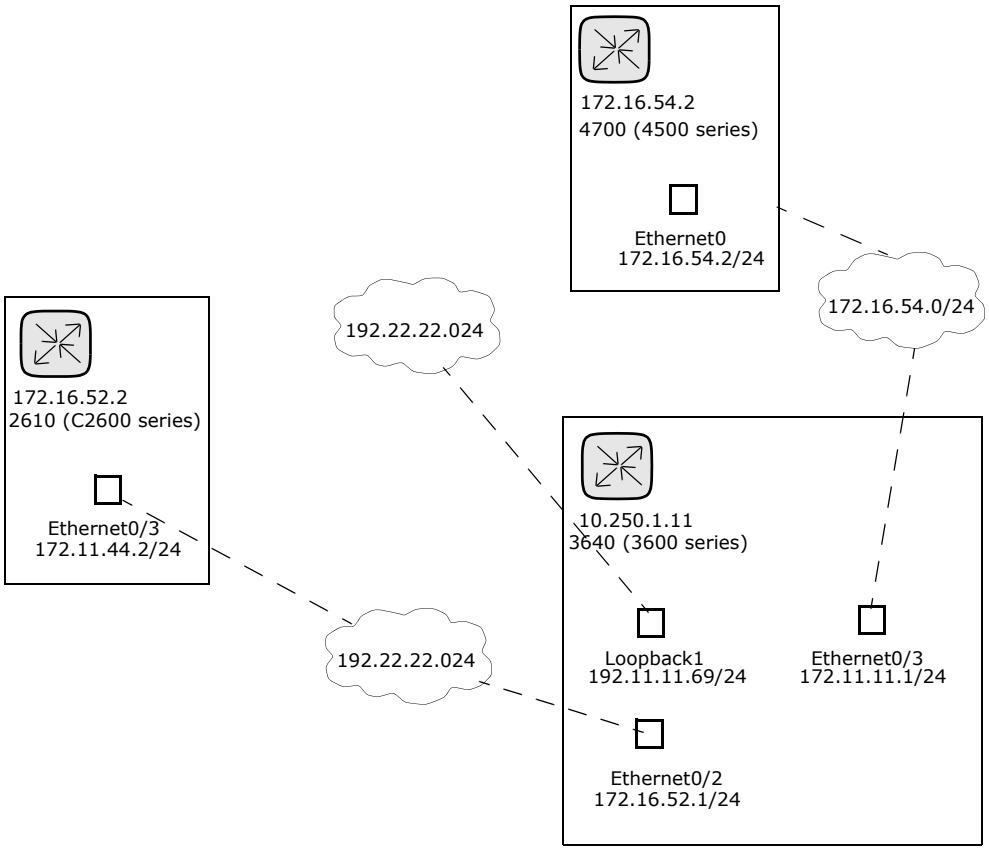
The following figure shows a simple network diagram, including connections between VLANs and ports.


Enterasys-SW3
10.255.1.300
VLAN 1
Ethernet0/1
Ethernet0/5
CISCO2950-CAT
10.255.1.11
VLAN 1
VLAN 2
2
Enterasys-SW4
10.255.1.400
Switch Management Port
4
1
Enterasys-SW2
10.255.1.200
VLAN 1
Ethernet0/2
Ethernet0/4
CISCO2500-2
172.11.11.2
Ethernet1/0
Ethernet1/3
CISCO2500-1
172.11.11.1
Ethernet0/1
CISCO2500-3
172.11.11.3
Ethernet1/3

The following sample figure shows a simple network diagram with collapsed devices.



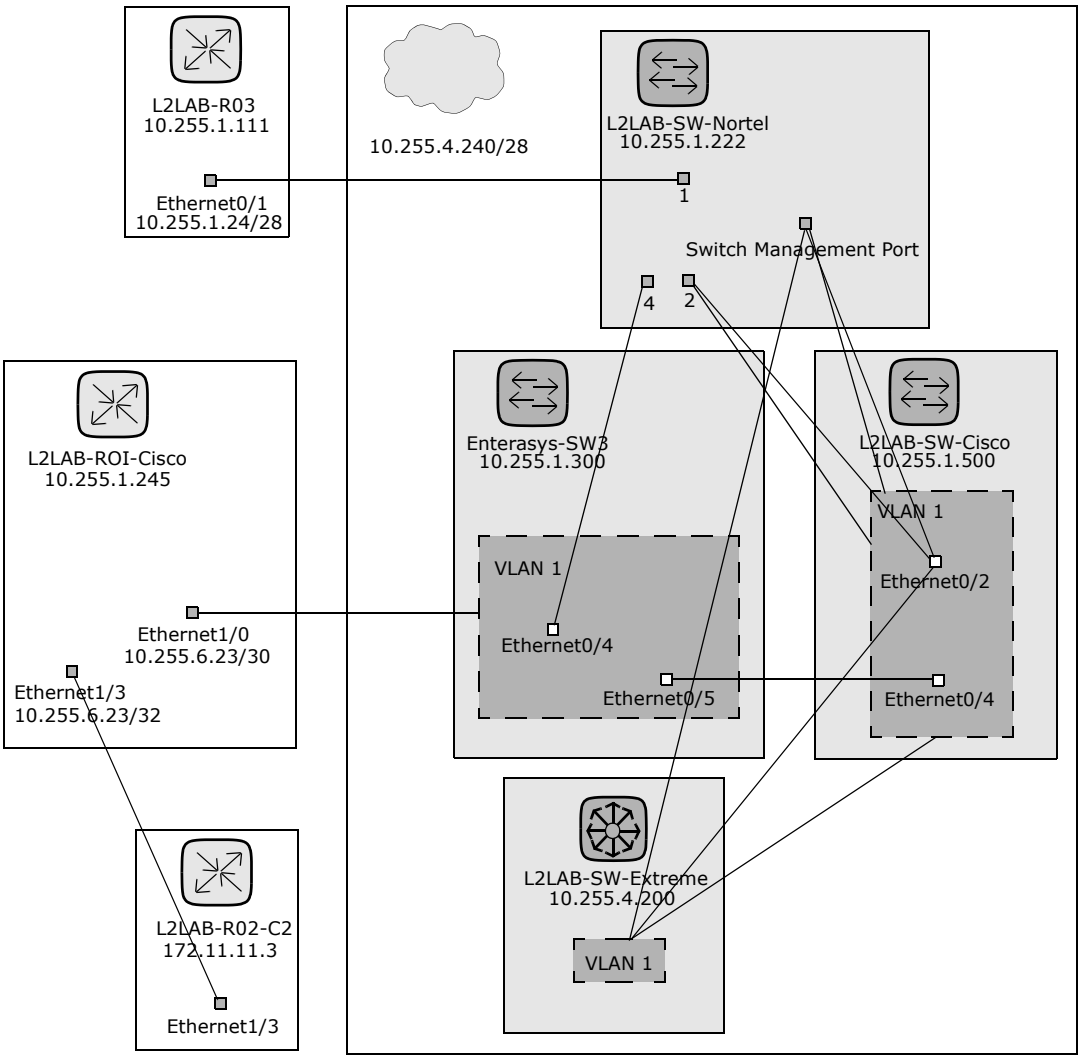
The following sample figure shows a simple network diagram utilizing clouds as a shortcut method to connect devices that share the same subnet. Keep in mind clouds can logically represent gateway objects, such as routers and switches.



A Layer 3 diagram collects all selected devices and connects the devices in the same subnet using the IP address and subnet mask. Multiple devices in a subnet are connected with a cloud. As a result, the cloud represents the subnet.

An expanded Layer 3 diagram starts with a basic Layer 3 diagram. If more than one device is connected to a subnet, the subnet is expanded to locate all the devices that might lie within the subnet. Expanded Layer 3 diagrams include all the interfaces connected to the cloud and traverse to other devices via known Layer 2 connections (discovered from the Topology Gathering diagnostic). The expanded cloud then becomes a container for all devices that participate in the subnet. Keep in mind that as Layer 2 connections are traversed, devices could be added to the diagram that were not originally selected.

The following sample figure shows an expanded Layer 3 network diagram. After the basic Layer 3 diagram is generated, each cloud that has more than one device connected to it is expanded. Keep in mind that NCM walks all of the Layer 2 connections. As a result, the devices in the cloud are grouped within a cloud node.



To view the Diagramming page, on the menu bar under Reports click Diagramming. The Diagramming page opens. When you are done configuring your diagram, click the Generate button.

Diagramming Page Fields

Field	Description/Action
Diagram Type	Select one of the following diagram types from the drop-down menu. A sample diagram indicating the type of diagram is displayed to the right of the drop-down menu. • Layer 1: Ports (Inferred) • Layer 2: Ports • Layer 3: Ports • Layer 3: Ports (Expanded) • Layer 1: Devices (Inferred) • Layer 2: Devices • Layer 3: Devices • Layer 3: Devices (Expanded) **Note**: The inferred Layer 1 data is based on heuristics. NCM reduces the number of data link connections between devices and/or servers to make network diagrams more readable. Only connections that can be inferred through transitive connections are reduced.
Output format	Select one of the following formats for your network diagram: • JPEG (Interactive) — Enables you to display your network diagram in Joint Photographic Experts Group (JPEG) output and select devices in the network diagram. When you select a device, the Device Details page opens for the device. (Refer to "View Menu Options" on page 229.) • JPEG (Static) — Displays your network diagram in Joint Photographic Experts Group (JPEG) format. • Visio — You must have Visio 2003 or higher, including Service Pack 2 or higher, or the Visio Viewer installed on your system for viewing network diagrams in Visio.

Field	Description/Action
Device Selection	Select one of the following options: • Device & Groups — Opens the Device Selector where you can select devices and/or device groups to include in the diagram. For information on how to use the Device Selector, refer to "Device Selector" on page 157 or click the question mark (?) in the upper right-hand corner of the Device Selector. • Route — Enter a starting route device and an end route device. NCM runs an ICMP Test task between the two devices. (Refer to "Run ICMP Test Task Page Fields" on page 296 for information on the ICMP Test task.) This is done as a traceroute, which shows all of the IP addresses that were encountered between the source device and the destination device. • Single Device — Enter a device's host name or IP address and the number of hops to graph between the starting route device and the end route device.
Hierarchy Layer Filter	A hierarchy layer is a device attribute. You can set a device's hierarchy layer when adding or editing a device. (Refer to "Adding Devices" on page 134 for information.) As a result, when configuring a diagram, you can select a hierarchy layer on which to filter. For example, you could diagram your entire network (Inventory) and then filter on "Core" to diagram only your Core devices—devices with a hierarchy layer set to Core. **Note**: The options provided below are default filters. You must assign filtering values to your devices to be able to designate a filter here. Refer to "Editing the appserver.rcx file" on page 592 for information on creating custom filters. Select one or more of the following options from the drop-down menu: • Core • Distribution • Access • Edge
Advanced Options	

Field	Description/Action
Advanced Filter	Select one or more of the following options: • Hide inactive devices — Removes all inactive devices from the network diagram. • Hide devices not connected to any other selected devices — Removes all devices that have no connections to other devices from the network diagram. • Hide VLANs that have no connections — Removes VLANs that are not connected to any ports or other VLANs from the network diagram. • Hide unconnected interfaces/ports — Removes all interfaces and ports that have no connections to other devices from the network diagram. • Hide ports not associated with a device — Removes all Layer 2 ports not associated with a device from the network diagram. (**Note**: NCM collects routing information from each managed device. Often times, devices have routes to devices and ports that are connected to non-managed devices. A device could see a port that is on a NCM managed device, but that device may not support the NCM Topology Data Gathering diagnostic. In this case, NCM cannot make the grouping connection between the port and the device.) • Enter the minimum cloud connections. The default is 2.
Grouping	Select one or both of the following options: • Connect contained subnets to their supernet — Enables you to group subnets together. For example, presume IP address ranges < > in /23 network and IP address ranges <> in /24 network include subnets. The /24 network is contained within the /23 network. It is possible that traffic can flow between the two network. As a result, the /23 network and the /24 network would be shown as connected in the diagram. • Show VLANs as separate devices — Separates a device into multiple representations of the same device (one for each VLAN). VLAN devices are shown with a dashed outline, the same as the VLAN grouping within devices for the other graph types. (**Note**: This option is automatically selected for Expanded L3 diagrams and cannot be disabled.)
Annotations	

Field	Description/Action
Device Annotations	Select the fields you want to appear with each graphed device. Keep in mind that it does not take too many fields for the graph to become overwhelmed with text. Some of the available options include: • Hostname • Primary IP • Fully Qualified Domain Name • Device Description • Site • Model • Serial Number • Last Changed Date
Endpoint Annotations	Select one or more of the following options: • Interface Description • IP Address • Port Name • Port Type • Port Status • MAC Address • Realm
Interconnection Annotations	Select one or more of the following option: • Subnet — Shows the Layer 3 subnet that the connection is showing. This is the same as the Cloud Annotation, just at the edge instead of at the node. • VLAN — Shows the Layer 2 subnet that the connection is showing.
Cloud Annotations	Select the following option: • Subnet — Text is included with a Layer 3 cloud (a shortcut method to connect devices that share the same subnet). • Realm — Text is included with a Layer 3 cloud. (A Realm is a network segment with no overlpaping IP addresses.)

Field	Description/Action
Graph Annotations	Select the following option: • Annotation Titles — Provides a title for each selected annotation. For example: Hostname: L2LAB-SW01-C0000xl
Save diagram as a user report named:	Enter as name for the diagram and click the Save button.
Email diagram to:	Enter an email address and click the Email button.

Once your diagram has been generated, if you selected the JPEG - Interactive option, clicking a device opens the Device Details page for the device. Refer to "Viewing Device Details" on page 225 for information.

Editing the appserver.rcx file

Hierarchy filtering layers are given values in the order of the their appearance. For example, Core is 1, Distribution is 2, and so on. This information is stored in the appserver.rcx file located in the *Product/config* directory. The file looks like the following:

```
<array name="diagramming/hierarchy_layers">
  <value>core</value>
  <value>distribution</value>
  <value>access</value>
  <value>edge</value>
</array>
```

Keep in mind that the numeric values are stored in the database. If you edit the appserver.rcx file, the changes are not reflected in the database. Consequently, you will also need to change the data associated with the device. (Refer to "New Device Page Fields" on page 135 for information.)

Device Software Report

The Device Software report enables you to view the software version and compliance rating currently assigned to each device.

To view the Device Software report, on the menu bar under Reports, click Device Software. The Device Software Report opens.

Device Software Report Fields

Field	Description
Software Vulnerability link	Opens the Software Vulnerability report, where you can view the software version and compliance rating currently assigned to each device, along with any security violation events sorted by importance. Refer to "Software Vulnerability Report Fields" on page 595.
Software Compliance link	Opens the Software Compliance page, where you can edit or delete a compliance. Refer to "Adding a New Compliance" on page 423.
Current Working Group	Select a device group from the drop-down menu. Inventory is the default.
Compliance At or Above	Select a compliance level, for example: • Any Compliance Level • Security Risk • Pre-production • Bronze To set compliance violations, refer to "Reporting Page Fields" on page 100.
Host Name	Displays the hostname of the device. Clicking the hostname opens the Device Details page, where you can view detailed information about the device.
Device IP	Displays the IP address of the device. Devices in red failed the last snapshot attempt. Inactive devices are marked with an icon beside the IP address.
Change Date	Displays when the software was last deployed to the device.

Field	Description
Device Software Version	Displays the detected software version running on the device.
Compliance	Displays the compliance rating of the software, if any.
Importance	Displays the severity of the security vulnerability, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Comments	Provides a detailed description of the vulnerability.
Image Set Name	Displays the name of the last image set deployed to the device.
Changed By	Displays the user name of the person who last deployed the software.
Actions	You can select the following action: • View Software Audit Trail — Opens the Device Software Audit Trail page, where you can view what software is loaded on the device. Refer to "Device Software Audit Trail Page Fields" on page 243 for information.

Software Vulnerability Report

The Software Vulnerability report enables you to view the software version and compliance rating currently assigned to each device, along with any security violation events sorted by importance. By default, no informational events are displayed.

To view the Software Vulnerability report, on the menu bar under Reports, click Software Vulnerabilities. The Software Vulnerabilities report opens.

Software Vulnerability Report Fields

Field	Description
Device Software Report link	Opens the Device Software report, where you can view the software version and compliance rating currently assigned to each device. Refer to "Device Software Report Fields" on page 593.
Software Compliance link	Opens the Software Compliance page, where you can edit or delete a compliance. Refer to "Adding a New Compliance" on page 423.
Current Working Group	Select a device group from the drop-down menu. Inventory is the default.
Importance At or Above	Select an importance level for the severity of the security vulnerability, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Host Name	Displays the hostname of the device. Clicking the hostname opens the Device Details page, where you can view detailed information about the device.

Field	Description
Device IP	Displays the IP address of the device. Clicking the IP address opens the Device Details page, where you can view detailed information about the device.
Change Date	Displays the date and time the software was last deployed to the device.
Device Software Version	Displays the detected software version running on the device.
Compliance	Displays the compliance rating of the software, if any.
Importance	Displays the severity of the security vulnerability, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Comments	Provides a detailed description of the vulnerability.
Actions	You can select the following action: • View Software Audit Trail — Opens the Device Software Audit Trail page, where you can view what software is loaded on the device. Refer to "Device Software Audit Trail Page Fields" on page 243 for information.

System & Network Events Report

The System & Network Events report enables you to track events that indicate changes to either a single device or all of your devices. For a complete list of events, refer to "Event Descriptions" on page 489.

To view the System & Network Events report, on the menu bar under Reports click System & Network Events. The System & Network Events report opens.

System & Network Events Report Fields

Field	Description/Action
New Message link	Opens the New Message page, where you can post a message to all users referring to this device. You also have the option of tracking the event with SingleView.
For the:	Displays the time frame for viewing events. Options include: • Past 1, 2, 4, 8, 12, 24, and 48 hours • Past 1 and 2 weeks • Past 1 month • All Events
Current Working Group	Select a device group from the drop-down menu.
Check Boxes	You can use the left-side check boxes to delete events from the NCM database. Once you have selected the events, click the Actions drop-down menu and click Delete. This deletes the selected events from the NCM database. The adjacent Select drop-down menu enables you to select or deselect all of the events.
Event Date	Displays the date/time of the event in the format MMM-dd-yy HH:mm:ss. (The format is configurable by the System Administrator.)
Host Name	Displays the host name or IP address of the device. Clicking the Host Name or IP Address opens the Device Details page, where you can view information about the device and its configuration history.

Field	Description/Action
Summary	Displays the type of event. For a list of Events, refer to "Event Descriptions" on page 489. Clicking the event type link opens the Event Detail page. This page includes: • The date and time the event occurred. • The login name of the person or process that added the event. Clicking the Detail link for diagnostic changes opens the Task Result page where you can view task details. Refer to "Task Information Page Fields" on page 376. • The event type. • A brief description of the event. • A link to detailed information about the device.
Added By	Displays the login name of the person whose action caused the event to be created.

Software Vulnerabilities Event Details Report

The software vulnerabilities event details report enables you to view details about software vulnerability, including advisory information and possible solutions.

To view the Software Vulnerabilities Event details:

1. On the menu bar, select Search For and click Events. The Search For Events page opens.
2. Select the Software Vulnerability Detected event summary and click the Search button. The Event Search Results page opens.

Field	Description/Action
Check Boxes	You can use the left-side check boxes to delete events from the NCM database. Once you have selected the events, click the Actions drop-down menu and click Delete. This deletes the selected events from the NCM database. The adjacent Select drop-down menu enables you to select or deselect all of the events.
Date	Displays the date/time of the event in the format MMM-dd-yy HH:mm:ss. (The format is configurable by the System Administrator.)
Summary	Displays Software Vulnerability Detected. If you click the link, the Event Detail page opens, where you can view information on the security vulnerability, including: • Date • Added by • Summary • Description, including the name, Importance, and CVE (Common Vulnerabilities and Exposures) • Actions — Provides links to NCM reports and external links to advisory and solution information. • Device
Host Name	Displays the host name or IP address of the device. Clicking the Host Name or IP Address opens the Device Details page, where you can view information about the device and its configuration history.

Field	Description/Action
Added by	Displays the username of the person who added the event.

Summary Reports

Summary reports provide an overview of configuration activity on your network. They can help you analyze trends and identify problem areas that require particular attention. You can easily provide these reports to upper management to help communicate what your team does and the value it contributes to the organization. Because the data is presented in a standard Microsoft Excel spreadsheet, it is easy to sort and filter information and cut & paste it into other applications.

By default, NCM is configured to update Summary reports on a weekly basis. Each time they are updated, the prior Summary reports file is backed up, so you can maintain an archive of these reports for historical analysis or to provide an audit trail. Reports are stored by default in *.\<install directory>\addins*.

To update the Summary reports manually:

1. On the menu bar under Tasks, click New Tasks and select Generate Summary Reports. The New Task - Generate Summary Reports page opens.
2. Make sure Start As Soon As Possible is selected.
3. Click Save Task.

The task updates the Summary reports, showing you the status of the task on the Task Information page. When the status is Succeeded, you can open the latest Summary reports.

Note: The Summary reports are available in Microsoft Excel. Excel macros are used to calculate the report data. Depending on your browser and Excel security settings, you may be prompted to enable macros when you open the Summary reports.

To open the Summary reports, on the menu bar under Reports click Summary Reports. If Summary Reports does not appear on the drop-down menu, the System Administrator should check your Administrative setting.

To navigate to specific Summary reports, you can either click the contents links on the top-level Summary report and use the Home link to return to the top-level Summary report, or use the tabs at the bottom of each report. If you do not see all the tabs at the bottom, try maximizing the window or click and drag the column adjustor to the right.

Summary Reports Descriptions

Report	Reported Information
Summary	Displays an overview of the rate of recent change activity, the most active users, and the network profile. Reports include: • Top 5 Vendors — Displays the number of devices per the top five vendors. • Top 5 OS Versions — Displays the top five OS versions that are in use. • Number of Configuration Change - Last 7 Days — Displays the average number of configuration changes per day for the past 7 days. • Change History by Time of Day — Displays when configuration changes were made. • Top 10 Most Accessed Devices — Displays the top 10 most accessed devices during the reporting period.
Change Frequency	Displays an overview of changes made in your network. The report provides the average number of changes per week over the past 30 days, broken down by users and device groups. This helps you identify top performers, as well as network areas showing a disproportionate rate of change.
Changes Per Day	Displays the number of configuration changes per day for the past two weeks. The report includes both a bar chart and table with the same data. The vertical axis shows the number of changes. The horizontal axis shows each day in the two week period.

Report	Reported Information
Statistical Charts	Displays configuration changes over the past week. The Change Detection Methods pie chart shows you how changes were detected, including: • Syslog • Telnet/SSH • Proxy • Regular or manual polling • AAA • Configuration or script deployment The Change History by Time of Day bar chart shows you at what time NCM detected changes. You can use these charts to monitor your changes. You can also set a policy to have network engineers make changes using the Telnet/SSH Proxy, Command Scripts, or Configuration Edit & Deploy.
Configuration Changes	Displays the following for the past week: • Change detection, including the trigger and number of changes. • Change history by time of day. • Device configuration changes, including the Host Name, IP Address, the date and time of the last change, and the User Name from Proxy, AAA, Syslog, and so on.
Device Status	Displays the inactive devices tracked by NCM. • The Top 10 Most Accessed Devices — Displays which devices took the most configuration snapshots of in the past week. Typically, these are the devices engineers are logging into or changing most often. • Device Password Changes — Displays a record of all devices whose passwords were changed in the past week. • Devices With Access Failures — Displays which devices NCM could not access, either because the device was unavailable or its password information was incorrect. This list serves as a checklist to ensure NCM is managing devices successfully.

Report	Reported Information
Device Inventory	Displays all devices tracked by NCM, including: • Host Name (from the Device Information page) • IP Address (from the Device Information page) • Asset Tag (from the Device Information page) • Location (from the configuration file) • Vendor (from the configuration file) • Model (from the configuration file) • Operating System Version (from the configuration file) • Serial Number (from the configuration file) • Device Description (from the Device Information page) • Last Snapshot Result (from tasks) • Last Modified Configuration (from tasks)
Operating System (OS) Inventory	Displays all the device OS versions running in your network, and lists how many devices are running each version. This report helps you to: • Ensure compliance with corporate standards for accepted OS versions. • Test or evaluate proposed changes to your architecture or services. • Save time when applying a vendor's security alert or patch to specific OS versions.

Report	Reported Information
System Status	Displays the activity and health of the NCM system. The report lists devices that do not have a device driver assigned and cannot be managed. It also provides summary information about recent system activity and the number of records in the NCM database. • System Status — For devices and groups, the report displays the total number of configurations, devices, device groups, unmanaged devices, and authentication rules. For users, the report displays the total number of users and AAA users without NCM accounts. The report also displays the number of custom reports. • System Activity — For tasks and messages, the report displays the total number of successful tasks, failed tasks, and system events. For the integrated Telnet/SSH client, the report displays the total number of Telnet and SSH sessions recorded. • Devices with No Driver — Displays the Host Name and IP Address of devices without drivers.
Policy Compliance	Displays the number of policies that are and are not in compliance. The Host Name, IP Address, and the last configuration change information is displayed. The report includes both a simple pie chart with numeric totals and three tables with detailed data, including: • Configuration Policies in Compliance • Configuration Policies not in Compliance • Configuration Polices (including that name of the configuration policy and the number of associated rules).

Emailing Reports

You can email reports. On the menu bar under Reports, select New Reporting Tasks and click Email Report. The Email Report Task page opens. Refer to "Email Report Task Page Fields" on page 348 for information.

Chapter 17: Using SecurID

Use the following table to quickly locate information.

Getting Started

The RSA SecurID® solution is designed to protect your organization by helping to ensure that only authorized users are granted access to networked resources. In general, SecurID is a two part authentication scheme, requiring a password/PIN, along with a physical hardware component. The hardware component changes its passcode every 60 seconds. Some device makers incorporate this authentication system into their routers/switches. Please refer to your SecurID documentation for detailed information on how SecurID works.

Note: When NCM is configured to use SecurID for external authentication, Single Sign-on functionality will not be enabled when connecting to the NCM proxy. You will need to authenticate again using your SecurID credentials because SecurID passcodes cannot be reused.

NCM supports SecurID for highly secure, two-factor authentication for:

- Authenticating users logging into NCM
- Accessing network devices through NCM

The following table describes SecurID device access support.

Accessing NCM	Connection Method	SecurID Support
Web User Interface	HTTP	Yes
SSH/Telnet Proxy	SSH Telnet	No Yes
API	RMI	No

Note: When using SecurID software tokens for device access, the ACEServer administrator must ensure that the software tokens are not in “New Pin” mode. Otherwise, access to the device will fail. If you are using SSH as a connection method, disable the SSH key authentication on the SSH client before connecting.

Installation Prerequisites

For user authentication into NCM, make sure:

- You have purchased hardware or software tokens from RSA.
- The ACEServer 5.2 is running and accessible from the NCM server.
- You have created a user on the ACEserver.
- On the ACEServer, the host where NCM is running is added as an Agent Host.
- In the Agent Host settings, the Agent type is “UNIX Agent.”
- You created users on the ACEServer.
- You assigned software tokens to the ACEServer users.
- You enabled users to connect from Agent Hosts.

For NCM to access devices, make sure:

- NCM is running on a Windows server.
- The RSA software token software is installed.
- The ACEServer 5.2 is running and accessible from the devices.
- You have obtained software tokens from RSA.
- You have imported the SecurID tokens to the NCM server using the RSA Software Token application.
- You have assigned a software token to the user.
- You have added licenses to the ACEServer.
- You have created a user on the ACEServer.
- You have assigned a software token to the user.
- You have enabled the user to connect to the devices.
- You have set the PIN for the token.
- In NCM, you added a user corresponding to the SecurID user.
- You selected if you are using unique per user tokens or a pool of tokens.
- You assigned a token pool username if using a token pool.
- You assigned the token to the user.

- You added a password rule (or a device specific password) with the Device Access variable User SecurID set to either “Exec” or “Enable”.

Note: If you are using SecurID on a Linux or Solaris system, only authentication into NCM is supported.

Accessing Network Devices

Using NCM to connect to devices using SecurID is only supported on Windows systems. For access from NCM to devices, you will need to download software token software and licenses from RSA. Hardware token licenses, such as FOBS and pinpads, cannot be used.

You can download the software token software from RSA's Website. Be sure to install the software on the same Windows system on which NCM is installed. You will also need to import the software token licenses to this Windows system through the normal SecurID mechanisms.

Note: The ACEServer and the server running NCM need to be time synchronized. Evidently, software tokens are sensitive to time differences. If the two servers are more than a minute out of sync, the generated passcodes will fail. You can use NTP on both servers to keep the clocks accurate.

NCM monitors access to devices when using SecurID to ensure that a given tokencode is not used twice. This means that activities in NCM might be slower when using SecurID device access. To address this, NCM provides the ability to load multiple software token seeds into the system. You can use one of the following token management modes:

- Per user — Each NCM user has one or more corresponding software token seeds. In this mode, each device access uses only the seed(s) corresponding to the user that initiated the task or Telnet proxy connection. It is recommended that all users in the system have valid software tokens assigned.
  - On the Home page under My Workplace, click My Settings. The My Workspace page opens.

- Click the My Profile tab. The My Profile page opens. Refer to "My Profile Page Fields" on page 265 for information on the My Profile page fields.

Note: Refer to "Adding SecurID Software Tokens" on page 613 for information on adding and/or updating SecurID tokens.

- Pool — A pool of general use software token seeds are provided to NCM and used as efficiently as possible for maximum performance.
  - On the menu bar under Admin, select Administrative Settings and click Configuration Mgmt. The Configuration Management page opens.
  - Click the Device Access tab. The Device Access page opens, where you can configure SecurID device access. Refer to "Device Access Page Fields" on page 69 for information.

Once software seeds have been loaded into NCM, you can designate specific devices or sets of devices for management via RSA SecurID authentication. To enable SecurID access to a specific device:

1. On the menu bar under Devices, click Inventory. A list of all managed devices opens.
2. Click the device for which you want to enable SecurID access. The Device Details page opens.
3. In the Action column, click Edit. The Edit Device page opens. Refer to "New Device Page Fields" on page 135 for information.
4. Scroll down and click the Show Device Access Settings (device-specific settings) link.
5. Select UseSecurID from the Setting drop-down menu and enter ether *exec* or *enable* for the Value. If you want to use SecurID in Exec Mode, enter *exec*. Using *exec* enables Exec Mode, typically the first mode you are in when logging into a device. If you want to use SecurID in both Exec Mode and Enable Mode, enter *enable*.
6. Click the Save Device button.

When a device (or group of devices) is configured for SecurID access and software seeds have been entered, NCM automatically generates the correct time-limited tokencode each time it needs to access the device.

You can also setup a network password rule on devices for management via RSA SecurID authentication. Refer to "Device Password Rule Page Fields" on page 147 for information. Then follow Steps 4, 5, and 6 above.

Adding SecurID Software Tokens

To add SecurID software tokens:

1. Using the RSA Software Token application, import the tokens to the server where NCM is running.
2. On the NCM Home page under My Workspace/My Settings, click the My Profile tab. The My Profile page opens.
3. Under the SecurID section at the bottom of the page, click the Manage Software Token licenses link. The View SecurID Tokens page opens, where you can view, add, and/or update software token licenses associated with your user login. These licenses are used to login into devices if the devices are configured to require SecurID credentials.
4. Click the Add Token link. The New SecurID Tokens page opens. You can add a single software token or a pool of general use software tokens per user.

Note: You can also navigate to the Manage Software Token licences link by clicking the Users option under Administration and then clicking the Edit option for that user.

New SecurID Tokens Page

Field	Description/Action
SecurID User	Enter the username assigned to the token on the ACEServer.
Software Token Serial Number	Enter the serial number of the token (zero padded).
PIN	If a PIN is configured for the token when issued from the ACE/Server, enter it here. (**Note**: If the PIN is updated, it must also be updated here.)
Confirm PIN	Re-enter the PIN for confirmation.
Password	If a password is configured for the token when issued from the ACE/Server instead of a PIN, enter it here.

Be sure to click Save when you are done.

Logging In Using SecurID

You can designate RSA SecurID as the external authentication mechanism. Refer to "User Authentication Page Fields" on page 109 for information.

Note: You must install the *sdconf.rec* file from the RSA SecurID ACE server onto the NCM server (e.g., *C:\WINDOWS\SYSTEM32\sdconf.rec)*. This file provides the necessary connection information for NCM to access SecurID. Upon completing the install, it is necessary to restart the NCM Management Engine. Refer to "Starting and Stopping Services" on page 127 for information on restarting the NCM Management Engine.

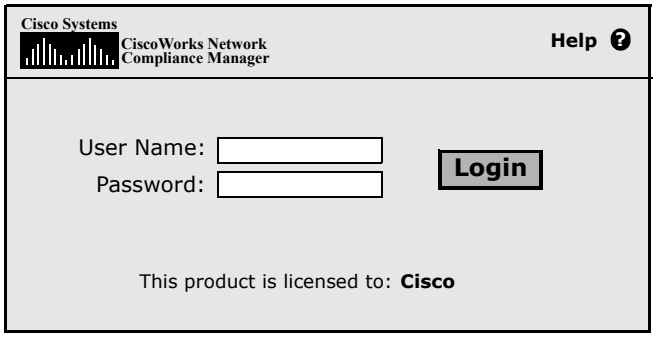
There are two methods for logging into NCM via SecurID if the token is in New Pin mode:

- Using a SecurID system PIN
- Using a new SecurID PIN

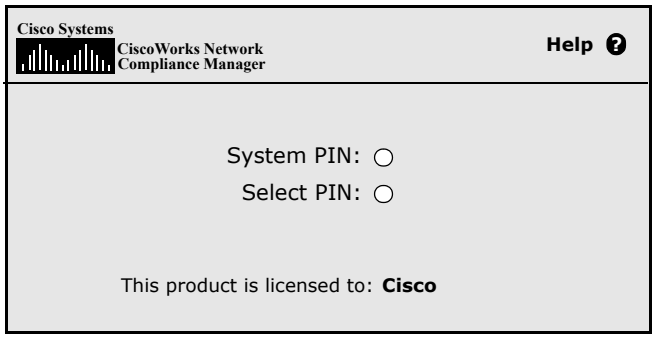
In all cases, RSA's login procedures require users to re-authenticate with the new PIN.

At the NCM login prompt (as shown below):

1. Enter your NCM username.
2. Enter your passcode in the Password field.
3. Click Login.



If your SecurID system is configured to prompt you to use either a System PIN or a new PIN, the following page opens.



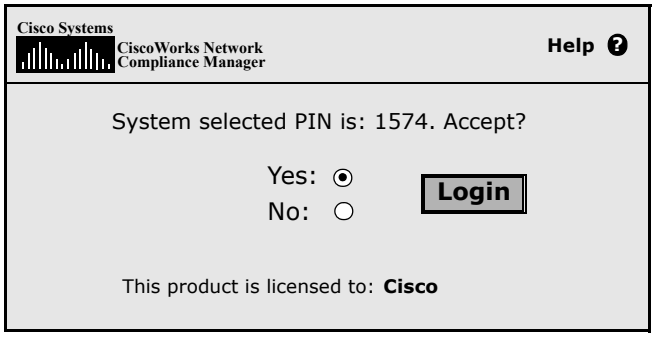
If you click System PIN, refer to "Login Method One: Using a System PIN" on page 616. If you click Select PIN, refer to "Login Method Two: Using a New PIN" on page 617.

Note: If your SecurID system is not configured to prompt you for either a System PIN or a new PIN, refer to either Login Method One or Login Method Two depending on your SecurID system configuration.

Login Method One: Using a System PIN

At the login page:

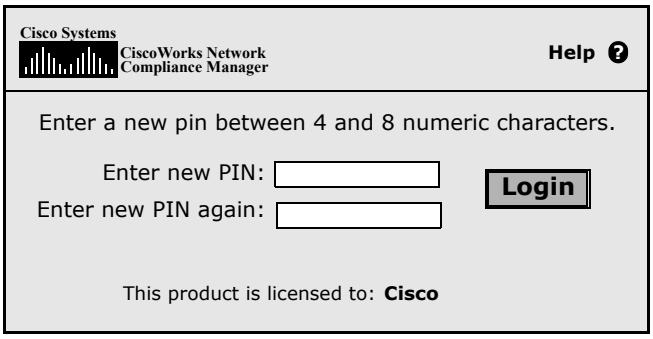
1. Click System PIN, as shown on page 460. After you have attained a System PIN from SecurID, click Yes, as shown below.
2. Click Login.
3. You are prompted you to wait and use the next tokencode to login.



Login Method Two: Using a New PIN

At the login page:

1. Click Select PIN, as shown on page 402.
2. Enter the new PIN twice, as shown below.
3. Click Login. The PIN is checked for adherence to the PIN parameters.



SecurID Troubleshooting

I. If you cannot login to NCM using SecurID, contact your RSA Administrator.

II. If you are using SecurID for device access, it is recommended that you turn off the Syslog User Identification option for change detection, or you could receive Snapshot Task Failed messages.

1. On the menu bar under Admin, select click Administrative Settings and click Configuration Mgmt. The Configuration Mgmt page opens.
2. At the Change User Identification section — Syslog User Identification, uncheck the "Identify who made a configuration change from the syslog message text, if possible." check box.
3. At the Change User Identification section — Auto-Create Users from Syslog, uncheck the "Create new users in NCM when the change author identified from syslog does not already exist (Auto-Create Users must be enabled)." check box.
4. Click the Save button.

III. If external authentication fails, NCM attempts to fall-back to the local user credentials in the following cases:

- When the external authentication service is down or inaccessible.
- For static user accounts that have never successfully logged in via an external authentication method.
- For the built-in Admin user account.

IV. The Node Secret file is used to authenticate communication between the RSA ACE/Agent client and RSA ACE/Server. If you see the following type of message in the ACE/Server log file, you must update the Node Secret file for the NCM server.

```
07/12/2006 22:00:19U ----/core15.cisco.com       ---->/
07/12/2006 18:00:19L Node verification failed      ncmrsa.rduncm.cisco.com
```

To create a Node Secret:

1. Click Agent Host --> Add (or Edit) Agent Host.
2. Click Create Node Secret.
3. In the Password box, enter a password and then enter it again in the Confirm Password box.
4. If you want to save the Node Secret file under the default name and directory, click OK. The Node Secret file is created in the default directory using the default name *nodesecret.rec*. The default directory is *ACEPROG* until you specify a different directory, in which case the directory you specify becomes the default directory until you restart the Database Administration application. If you want to save the file under a different name, click Browse. In the Node Secret Filename Specification dialog box, change the name and directory, and then click Save.

   Note: If a Node Secret file with the same name exists in the specified directory, click Yes to overwrite it or click No to return to the Node Secret Filename Specification dialog box. When you click Yes, the Node Secret file is created using the name and directory you specify.

   In the Add (or Edit) Agent Host dialog box, the Create Node Secret File button is unavailable. Node Secret Created is selected.
5. Click OK.
6. Copy the new Node Secret file and the Load Node Secret utility to the Agent host. The Load Node Secret utility loads the new Node Secret file into the Agent host. RSA Security provides four platform-specific versions (Windows, Solaris, HP-UX, and IBM AIX) of the utility (agent_nsload) on the RSA Authentication Manager CD.
7. On the Agent host, run the Load Node Secret utility. On the command line prompt, enter: `agent_nsload -f path -p password` (where `path` is the directory location and name of the Node Secret file and `password` is the password used to protect the Node Secret file.)

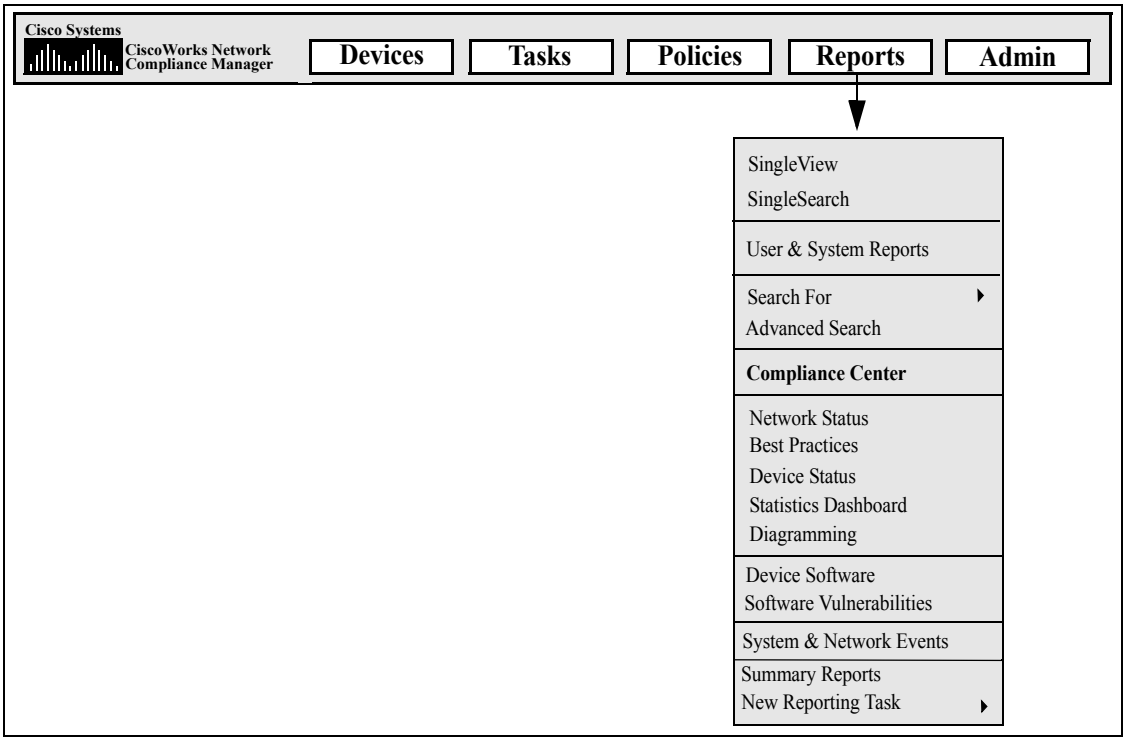
   Note: If your ACE/Server is on a different platform than your NCM server, the *agent_nsload* executable might not be compatible. In this case, please contact RSA to get the correct binary. In addition, you might have to reboot the NCM server so that RSA dlls can locate the new Node Secret file.

Chapter 18: Compliance Center

Use the following table to quickly locate information.

Note: Cisco Compliance Center is based on Cisco's understanding of the regulations and standards presented. Cisco is not an auditor or legal authority, and you should consult your corporate auditor or legal representative for guidance.

Navigating to Compliance Center



Getting Started

The Compliance Center is NCM's portal for accessing reports and information that help determine the current compliance status of your network infrastructure with respect to Sarbanes-Oxley (Section 404) and supporting internal control frameworks.

The Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as Sarbanes-Oxley, is designed to improve the accuracy and reliability of corporate disclosures to investors. Sarbanes-Oxley generally applies to all U.S. companies registered with or required to file reports with the SEC (Securities and Exchange Commission). The regulation requires the CEO and CFO of reporting companies to certify their companies' SEC reports.

A key provision of Sarbanes-Oxley is Section 404, which specifically addresses internal control over financial reporting. Section 404 requires that reporting companies include an internal controls report and assessment as part of their financial reporting. Sarbanes-Oxley (Section 404) provides no specific control requirements for IT-related compliance efforts, so organizations must select an internal control framework, such as COSO, COBIT, ITIL, or Visa CISP and enforce and report against that framework. For detailed information regarding managing Sarbanes-Oxley (Section 404) compliance using NCM, refer to the online information presented on the Compliance Center Home page.

To access the Compliance Center Home page, on the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.

Compliance Center Home Page

Options	Description/Action
Sarbanes-Oxley (Section 404)	Opens the Sarbanes-Oxley (Section 404) Compliance Status overview information.
COBIT Compliance Status link	Opens the COBIT Compliance Status report. Refer to "COBIT Compliance Status Reports" on page 625 for information.
COSO Compliance Status link	Opens the COSO Compliance Status report. Refer to "COSO Compliance Status Reports" on page 639 for information.
ITIL Compliance Status link	Opens the ITIL Compliance Status report. Refer to "ITIL Compliance Status Reports" on page 644 for information.
GLBA Compliance Status link	Opens the GLBA Compliance Status report. Refer to "GLBA Compliance Status Reports" on page 650 for information.
HIPAA Compliance Status link	Opens the HIPAA Compliance Status report. Refer to "HIPAA Compliance Status Reports" on page 655 for information.
Visa CISP (PCI Data Security Standard) Compliance Status link	Opens the PCI Data Security Standard (Visa CISP) report. Refer to "Visa CISP (PCI Data Security Standard) Compliance Status Reports" on page 667 for information.

COBIT Compliance Status Reports

COBIT (Control Objectives for Information and related Technology) is an internal control framework that helps meet the needs of management by bridging the gaps among business risks, control needs, and technical issues, while balancing risk versus return over IT and its processes.

NCM enhances the implementation of four domains for effective internal control system as defined by COBIT:

- Monitoring — NCM monitors processes, assesses internal control adequacy, secures independent assurance, and provides for independent audit.
- Delivery & Support — NCM helps to manage service levels, third-party services, and performance and capacity, ensure continuous service system security, identify and allocate costs, educate and train users, assist and advise customers, and manage configurations, data, facilities, and operations.
- Planning & Organization — NCM helps to define a strategic IT plan, determine technological direction, manage the IT investment and human resources, communicate management aims and directions, and ensure compliance with external requirements.
- Acquisition & Implementation — NCM helps to identify automated solutions, acquire and maintain technology infrastructure, develop and maintain procedures, install and accredit systems, and manage changes.

For detailed information on COBIT and how NCM enhances the implementation of COBIT, click the “More information about COBIT and achieving compliance using CiscoWork Network Compliance Manager” link on the COBIT Status Compliance page.

To view the COBIT Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the COBIT Compliance Status link. The COBIT Compliance Status page opens.

COBIT Compliance Status Page Fields

Fields	Description/Action
MONITORING	
M1 Monitor the processes	Displays the number of: • Devices with different startup and running configurations. Clicking the Device List link opens Device Search Results report. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Inactive devices. Clicking the Inactive Devices link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information. • ACLs. Clicking the All ACLs link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information. • ACLs in use. Clicking the ACLs In Use link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information. • ACL changes in the last 7 days. Clicking the ACL Changes link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page. Refer to "Searching for Events" on page 485 for information.

Fields	Description/Action
M2 Assess internal control adequacy	Displays the number of: • Workflow rules in place. Clicking the Workflow Setup link opens the Workflow Wizard. Refer to "Workflow Wizard" on page 688 for information. • Configuration polices in place. Clicking the Configuration Polices link opens the Polices page. Refer to "Policies Page Fields" on page 385 for information. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page. Refer to "Searching for Events" on page 485 for information. • ACLs with comments. Clicking the ACLs With Comments link opens the ACLs Search Results page. Refer to "Commenting ACLs and Creating ACL Handles" on page 716 for information.
M3 Obtain independent assurance	Displays the number of: • Monitors showing an "okay" status. Clicking the System Status link opens the System Status report. Refer to "System Status Page Fields" on page 120 for information. • Devices in software compliance. Clicking the Device Software Report link opens the Software Compliance Search Results page. Refer to "Device Software Report Fields" on page 593 for information. • Configuration policy non-compliance events in the last 24 hours. Clicking the Configuration Policy Events (24 hours) link opens the Configure Policy Activity page. Refer to "Configuration Policy Activity Page Fields" on page 398 for information. • Configuration policy non-compliance events in the last 7 days. Clicking the Configuration Policy Events (7 days) link opens the Configure Policy Activity page. Refer to "Configuration Policy Activity Page Fields" on page 398 for information. • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information.

Fields	Description/Action
M4 Provide for independent audit	Displays the number of: • Accessible User reports. Clicking the User & System Reports link opens the User & System Reports page. Refer to "User & System Reports" on page 568 for information. • Accessible System reports. Clicking the User & System Reports link opens the User & System reports. Refer to "User & System Reports" on page 568 for information.
DELIVERY & SUPPORT	
DS1 Define and manage service levels	Displays the number of: • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information. • Average changes per day (last 7 Days). Clicking the Summary Reports link opens the Summary reports. Refer to "Summary Reports Descriptions" on page 602 for information. • Average changes per day (last 30 Days). Clicking the Summary Reports link opens the Summary reports. Refer to "Summary Reports Descriptions" on page 602 for information.
D22 Manage third-party services	Displays the number of: • Devices with access failures. Clicking the Inaccessible Devices link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information. • Devices that have different startup and running configurations. Clicking the Devices List link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information. • Inactive devices. Clicking the Inactive Devices link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information.
DS3 Manage performance and capacity	Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information.

Fields	Description/Action
DS4 Ensure continuous service	Displays the number of: • Diagnostics run in the last 24 hours. Clicking the Diagnostics (24 hours) link opens the Diagnostic Search Results page. Refer to "Diagnostics" on page 532 for information. • Diagnostics run in the last 7 days. Clicking the Diagnostics (7 days) link opens the Diagnostic Search Results page. Refer to "Diagnostics" on page 532 for information.
DS5 Ensure systems security	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Users assigned Administrator access permissions. Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Device Password Rules in place. Clicking the Device Password Rules link opens the Device Password Rules List page. • ACLs. Clicking the All ACLs link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information. • ACLs in use. Clicking the ACLs In Use link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information. • ACL changes in the last 7 days. Clicking the ACL Changes link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information.
DS6 Identify and allocate costs	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Inventory page. Refer to "Adding Devices" on page 134 for information. • Modules in inventory. Clicking the Module link opens the Module Search Results page. Refer to "Device Blades/Modules Page Fields" on page 240 for information.

Fields	Description/Action
DS7 Educate and train users	Provides links to the following documentation: • *User Guide for Network Compliance Manager 1.2* • *Device Driver Reference* • *Release Notes*
DS8 Assist and advice customers	Provides links to the following: • Download driver update packages • View latest Release Notes • View license Information • Create a Technical Support ticket • Email Customer Support • Request new driver support
DS9 Manage the configuration	Displays the number of: • Configuration changes detected in the last 7 days. Clicking the Configuration Changes link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information. • Stored active device configurations. Clicking the Active Configurations link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information. • Changes pending approval. Clicking the Changes Pending Approval link opens the Changes Pending Search Results page. Refer to "Searching for Events" on page 485 for information. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page. Refer to "Searching for Events" on page 485 for information. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page. Refer to "Searching for Events" on page 485 for information.

Fields	Description/Action
DS10 Manage problems and incidents	Displays the number of: • Configuration Changes detected in the last 24 hours. Clicking the Dashboard link opens the Home page. Refer to "My Homepage Fields" on page 270 for information. • NCM events that occurred in the last 24 hours. Clicking the Dashboard link opens the Home page. Refer to "My Homepage Fields" on page 270 for information.
DS11 Manage data	Displays the number of stored active device configurations. Click the Active Configuration link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information.
DS12 Manage facilities	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Device Details page. Refer to "Viewing Devices" on page 217 for information. • Modules in inventory. Clicking the Modules link opens the Module Search Results page. Refer to "Device Blades/Modules Page Fields" on page 240 for information.

Fields	Description/Action
DS13 Manage operations	Displays the number of: • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Software deployments scheduled for the next 24 hours. Clicking the Pending Deployments (24 hours) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Software deployments scheduled for the next 7 days. Clicking the Pending Deployments (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Changes pending approval. Clicking the Changes Pending Approval link opens the Changes Pending Search Results page. Refer to "Searching for Events" on page 485 for information.
PLANNING & ORGANIZATION	
PO1 Define a strategic IP plan	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Device Details page. Refer to "Viewing Devices" on page 217 for information. • Modules in inventory. Clicking the Modules link opens the Module Search Results page. Refer to "Device Blades/Modules Page Fields" on page 240 for information. • Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information.

Fields	Description/Action
PO2 Define the information architecture	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Inventory page. Refer to "Adding Devices" on page 134 for information. • Modules in inventory. Clicking the Modules link opens the Module Search Results page. Refer to "Device Blades/Modules Page Fields" on page 240 for information. • Active stored configurations. Clicking the Active Configurations link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information.
PO3 Determine the technological direction	Displays the number of devices in inventory from the total number of vendors. Clicking the Device List by Vendors link opens the Inventory page. Refer to "Adding Devices" on page 134 for information.
PO4 Define the IT organization and relationships	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Users assigned Administrator access permissions Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Device Password Rules in place Clicking the Device Password Rules link opens the Device Password Rules List page.
PO5 Manage the IT investment	Displays the number of: • Monitors showing an "okay" status. Clicking the System Status link opens the System Status report. Refer to "System Status Page Fields" on page 120 for information. • Devices in inventory. Clicking the Device List link opens the Inventory page. Refer to "Adding Devices" on page 134 for information. • Modules in inventory. Clicking the Modules link opens the Module Search Results page. Refer to "Device Blades/Modules Page Fields" on page 240 for information.

Fields	Description/Action
PO6 Communicate management aims and directions	Displays the number of: • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information. • Active configurations policies. Clicking the Configurations Policies link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information.
PO7 Manage human resources	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Users assigned Administrator access permissions. Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Device Password Rules in place. Clicking the Device Password Rules link opens the Device Password Rules List page.
PO8 Ensure compliance with external requirements	Displays the number of active configurations policies. Clicking the Configurations Policies link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information. Clicking the Compliance Center link opens the Compliance Center Home page. Refer to "Compliance Center Home Page" on page 624 for information.
PO9 Assess risks	Displays the number of: • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information. • Devices with access failures. Clicking the Inaccessible Devices link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information. • Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information.

Fields	Description/Action
PO10 Manage projects	Displays the number of: • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Software deployments scheduled for the next 24 hours. Clicking the Pending Deployments (24 hours) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Software deployments scheduled for the next 7 days. Clicking the Pending Deployments (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information.
PO11 Manage quality	Displays the number of: • Monitors showing an "okay" status. Clicking the System Status link opens the System Status report. Refer to "Server Monitoring Page Fields" on page 117 for information. • Devices in software compliance. Clicking the Device Software Report link opens the Software Compliance Search Results page. Refer to "Device Software Report Fields" on page 593 for information. • Configuration policy non-compliance events in the last 24 hours. Clicking the Configuration Policy Events (24 hours) link opens the Configure Policy Activity page. Refer to "Configuration Policy Activity Page Fields" on page 398 for information. • Configuration policy non-compliance events in the last seven days. Clicking the Configuration Policy Events (7 days) link opens the Configure Policy Activity page. Refer to "Configuration Policy Activity Page Fields" on page 398 for information. • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information.

Fields	Description/Action
ACQUISTION & IMPLEMENTATION	
AI1 Identify automated solutions	Provides the following default links: • System task to prune database runs weekly. Clicking the Pending Tasks link opens the Pending Tasks page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • System task to gather module inventory data runs weekly. Clicking the Pending Tasks link opens the Scheduled Tasks page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • System task to update Summary Reports runs daily. Clicking the Pending Tasks link opens the Scheduled Tasks page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • System task to poll for device configuration changes runs daily. Clicking the Pending Tasks link opens the Scheduled Tasks page. Refer to "Viewing Scheduled Tasks" on page 369 for information.
AI2 Acquire and maintain application software	This is not applicable.
AI3 Acquire and maintain technology infrastructure	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Inventory page. Refer to "Device Configuration Detail Page Fields" on page 206 for information. • Modules in inventory. Clicking the Modules link opens the Module Search Results page. Refer to "Device Blades/Modules Page Fields" on page 240 for information. • Stored active device configurations. Clicking the Active Configurations link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information.

Fields	Description/Action
AI4 Develop and maintain procedures	Displays the number of: • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information. • Active configurations policies. Clicking the Configurations Policies link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information.
AI5 Install and accredit systems	Displays the number of: • Monitors showing an "okay" status. Clicking the System Status link opens the System Status report. Refer to "System Status Page Fields" on page 120 for information. • Devices in software compliance. Clicking the Device Software Report link opens the Software Compliance Search Results page. Refer to "Device Software Report Fields" on page 593 for information. • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information.

Fields	Description/Action
AI6 Manage changes	Displays the number of: • Telnet/SSH Proxy sessions in the last 7 days. Clicking the Sessions link opens the Session Search Results page. Refer to "Session Search Results Page Fields" on page 483 for information. • Device change tasks scheduled in the last 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Changes pending approval. Clicking the Changes Pending Approval link opens Changes Pending Search Results page. Refer to "Searching for Events" on page 485 for information. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page. Refer to "Searching for Events" on page 485 for information. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page. Refer to "Searching for Events" on page 485 for information.

COSO Compliance Status Reports

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a landmark report on internal control. *Internal Control—Integrated Framework*, which is often referred to as "COSO", provides a basis for establishing internal control systems and determining their effectiveness.

NCM provides five essential components for an effective internal control system:

- Control Environment — Establishes the foundation for the internal control system by providing fundamental discipline and structure.
- Risk Assessment — Includes identification and analysis by management of relevant risks to achieving objectives.
- Control Activities — Ensures management objectives are achieved and risk mitigation strategies are carried out.
- Information and Communication — Supports all control components by communicating control responsibilities to employees, and by providing information in a form and timeframe that enables employees to carry out their duties.
- Monitoring — Includes the external oversight of internal controls by management or other parties outside the process.

For detailed information on COSO, click the "More information about COSO and achieving compliance using CiscoWorks Network Compliance Manager" link.

To view the COSO Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the COSO Compliance Status link. The COSO Compliance Status page opens.

COSO Compliance Status Page Fields

Fields	Description/Action
Control Environment	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Users assigned Administrator access permissions Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Device Password Rules in place. Clicking the Device Password Rules link opens the Device Password Rules List page. • Configuration polices in place. Clicking the Configuration Polices link opens the Polices page. Refer to "Policies Page Fields" on page 385 for information. • Workflow rules in place. Clicking the Workflow Setup link opens the Workflow Wizard. Refer to "Workflow Wizard" on page 688 for information. • ACLs. Clicking the All ACLs link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information. • ACLs in use. Clicking the ACLs In Use link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information.
Risk Assessment	Displays the number of: • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information. • Devices with access failures. Clicking the Inaccessible Devices link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information. • Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information.

Fields	Description/Action
Control Activities	Displays the number of: • Telnet/SSH Proxy sessions in the last 7 days. Clicking the Sessions link opens the Session Search Results page. Refer to "Session Search Results Page Fields" on page 483 for information. • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Software deployments scheduled for the next 24 hours. Clicking the Pending Deployments (24 hours) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Software deployments scheduled for the next 7 days. Clicking the Pending Deployments (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Changes pending approval. Clicking the Changes Pending Approval link opens Changes Pending Search Results page. Refer to "Searching for Events" on page 485 for information.

Fields	Description/Action
Information and Communication	Displays the number of: • Configuration changes detected in the last 24 hours. Clicking the Dashboard link opens the Home page. Refer to "My Homepage Fields" on page 270 for information. • NCM events that occurred in the last 24 hours. Clicking the Dashboard link opens the Home page. Refer to "My Homepage Fields" on page 270 for information. • Average number of changes per day (last 7 days). Clicking the Summary Reports link opens the Summary reports. Refer to "Summary Reports Descriptions" on page 602 for information. • Average number of changes per day (last 30 days). Clicking the Summary Reports link opens the Summary reports. Refer to "Summary Reports Descriptions" on page 602 for information. • ACLs with comments. Clicking the ACLs With Comments link opens the ACLs Search Results page. Refer to "Commenting ACLs and Creating ACL Handles" on page 716 for information.

Fields	Description/Action
Monitoring	Displays the number of: • Monitors showing an "okay" status. Clicking the System Status link opens the System Status report. Refer to "System Status Page Fields" on page 120 for information. • Devices in software compliance. Clicking the Device Software Report link opens the Software Compliance Search Results page. Refer to "Device Software Report Fields" on page 593 for information. • Configuration policy non-compliance events in the last 24 hours. Clicking the Configuration Policy Events (24 hours) link opens the Configure Policy Activity page. Refer to "Configuration Policy Activity Page Fields" on page 398 for information. • Configuration policy non-compliance events in the last 7 days. Clicking the Configuration Policy Events (7 days) link opens the Configure Policy Activity page. Refer to "Configuration Policy Activity Page Fields" on page 398 for information. • Devices that have different startup and running configurations. Clicking the Devices List link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information. • Inactive devices. Clicking the Inactive Devices link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page. Refer to "Searching for Events" on page 485 for information. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page. Refer to "Searching for Events" on page 485 for information. • ACL changes in the last 7 days. Clicking the ACL Changes link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information.

ITIL Compliance Status Reports

ITIL (IT Infrastructure Library) was developed for the British government by the CCTA (now the OGC: Office of Government Commerce), and has been rapidly adopted across the world as the standard for best practice in the provision of IT services. Three major areas of ITIL include:

- Service Support — Enables IT services to be effectively provided.
- Service Delivery — Enables the management of IT services.
- Security Management — Enables the protection of data and infrastructures.

For detailed information on ITIL, click the "More information about ITIL and achieving compliance using CiscoWorks Network Compliance Manager" link.

To view the ITIL Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the ITIL Compliance Status link. The ITIL Compliance Status page opens.

ITIL Compliance Status Page Fields

Fields	Description/Action
Configuration Management	
service support process	Displays the number of: • Configuration changes detected in the last 7 days. Clicking the Configuration Changes link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information. • Stored device configurations. Clicking the Active Configurations link opens the Config Search Results page. Refer to "Device Configuration Detail Page Fields" on page 206 for information.
Incident Management	

Fields	Description/Action
Service support process	Displays the number of: • Configuration changes detected in the last 24 hours. Clicking the Dashboard link opens the Home page. Refer to "My Homepage Fields" on page 270 for information. • NCM events that occurred in the last 24 hours. Clicking the Dashboard link opens the Home page. Refer to "My Homepage Fields" on page 270 for information.
Problem Management	
Service support process	Displays the number of: • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information. • Devices with access failures. Clicking the Inaccessible Devices link opens the Device Search Results page. Refer to "Viewing Devices" on page 217 for information.
Change Management	

Fields	Description/Action
service support process	Displays the number of: • Telnet/SSH Proxy sessions in the last 7 days. Clicking the Sessions link opens the Session Search Results page. Refer to "Session Search Results Page Fields" on page 483 for information. • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Changes pending approval. Clicking the Changes Pending Approval link opens Changes Pending Search Results page. Refer to "Searching for Events" on page 485 for information. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page. Refer to "Searching for Events" on page 485 for information. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page. Refer to "Searching for Events" on page 485 for information. • Configuration polices in place. Clicking the Configuration Polices link opens the Policies page. Refer to "Policies Page Fields" on page 385 for information. • Workflow rules in place. Clicking the Workflow Setup page opens the Workflow Wizard. Refer to "Workflow Wizard" on page 688 for information.
Service Desk	

Fields	Description/Action
service support function	Displays the number of: • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information.
Release Management	
service support process	Displays the number of: • Software deployments scheduled for the next 24 hours. Clicking the Pending Deployments (24 hours) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Software deployments scheduled for the next 7 days. Clicking the Pending Deployments (7 days) link opens the Task Search Results page. Refer to "Viewing Scheduled Tasks" on page 369 for information. • Devices in software compliance. Clicking the Device Software Report link opens the Software Compliance Search Results page. Refer to "Device Software Report Fields" on page 593 for information.
Service Level Management	
service delivery process	Displays the number of: • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. Refer to "Network Status Report Fields" on page 573 for information. • Average changes per day (last 7 Days). Clicking the Summary Reports link opens the Summary reports. Refer to "Summary Reports Descriptions" on page 602 for information. • Average changes per day (last 30 Days). Clicking the Summary Reports link opens the Summary reports. Refer to "Summary Reports Descriptions" on page 602 for information.

Fields	Description/Action
Capacity Management	
Service delivery process	Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page. Refer to "Inventory Page Fields" on page 217 for information.
Continuity Management	
Service delivery process	Displays the number of: • Diagnostics run in the last 24 hours. Clicking the Diagnostics (24 hours) link opens the Diagnostic Search Results page. Refer to "Diagnostics" on page 532 for information. • Diagnostics run in the last 7 days. Clicking the Diagnostics (7 days) link opens the Diagnostic Search Results page. Refer to "Diagnostics" on page 532 for information.
Availability Management	
Service delivery process	Displays the number of: • Configuration policy non-compliance events in the last 24 hours. Clicking the Configuration Policy Events (24 hours) link opens the Configure Policy Activity page. Refer to "Configuration Policy Activity Page Fields" on page 398 for information. • Configuration policy non-compliance events in the last seven days. Clicking the Configuration Policy Events (7 days) link opens the Configure Policy Activity page. Refer to "Configuration Policy Activity Page Fields" on page 398 for information.
IT Financial Management	

Fields	Description/Action
Service delivery process	Displays the number of: • Monitors showing an "okay" status. Clicking the System Status link opens the System Status report. Refer to "System Status Page Fields" on page 120 for information. • Devices in inventory. Clicking the Device List link opens the Inventory page. Refer to "Adding Devices" on page 134 for information. • Modules in inventory. Clicking the Module link opens the Module Search Results page. Refer to "Device Blades/Modules Page Fields" on page 240 for information.
Security Management	
Service delivery process	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Users assigned Administrator access permissions. Clicking the User List link opens the User Search Results page. Refer to "All Users Page Fields" on page 252 for information. • Device password rules in place. Clicking the Device Password Rules link opens the Device Password Rules List page. • ACLs. Clicking the All ACLs link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information. • ACLs in use. Clicking the ACLs In Use link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information. • ACL changes in the last 7 days. Clicking the ACL Changes link opens the ACLs Search Results page. Refer to "Viewing ACLs" on page 706 for information. • ACLs with comments. Clicking the ACLs With Comments link opens the ACLs Search Results page. Refer to "Commenting ACLs and Creating ACL Handles" on page 716 for information.

GLBA Compliance Status Reports

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal privacy requirements:

- Pretexting provisions
- Financial Privacy Rule
- Safeguards Rule

The Safeguards Rule requires all financial institutions to design, implement, and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions, such as credit reporting agencies that receive customer information from other financial institutions.

For detailed information on GLBA, click the "More information about GLBA and achieving compliance using CiscoWorks Network Compliance Manager" link.

To view the GLBA Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the GLBA Compliance Status link. The GLBA Compliance Status page opens.

GLBA Compliance Status Page Fields

Fields	Description/Action
Interagency Guideline Section	
II.A. Information Security Program	Displays the number of: • Devices in inventory. Refer to "Viewing Devices" on page 217 for information. • Modules in inventory. Refer to "Viewing Device Details" on page 225 for information. • Stored device configurations. Refer to "Viewing Device Details" on page 225 for information.
II.B. Objectives	Displays the number of: • Users restricted to specific groups of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned Administrator permissions. Refer to "All Users Page Fields" on page 252 for information. • Failed user login attempts in the past seven days. Refer to "Event Descriptions" on page 489 for information. • Changes pending approval. Refer to "What Are Tasks?" on page 278. • Approved changes in the last seven days. Refer to "What Are Tasks?" on page 278 for information. • Unapproved changes in the past seven days. Refer to "What Are Tasks?" on page 278 for information. • ACLs identified. Refer to "Viewing ACLs" on page 706 for information. • ACLs in use. Refer to "Viewing ACLs" on page 706 for information. • ACL changes in the past seven days. Refer to "Viewing ACLs" on page 706 for information. • ACLs with comments. Refer to "Viewing ACLs" on page 706 for information.
III.A. Involve the Board of Directors	Displays the number of: • Available user reports. Refer to "User & System Reports" on page 568 for information.

Fields	Description/Action
	• Available System reports. Refer to "User & System Reports" on page 568 for information.
III.B. Assess Risk	Displays the number of: • Configuration management "Best Practices" green status. Refer to "Network Status Report Fields" on page 573 for information. • Devices in software compliance. Refer to "Adding a New Compliance" on page 423 for information. • Monitors with an "Okay" status. Refer to "Network Status Report" on page 572 for information. • Devices with access failures. Refer to "Viewing Devices" on page 217. • Devices with port availability of less than 10%. Refer to "Viewing Devices" on page 217. • Devices with different startup and running configurations. Refer to "Viewing Device Configuration Changes" on page 203 for information.
III.C.1. Manage and Control Risk (Policies & Procedures)	Displays the number of: • Workflow rules in place. Refer to "Workflow Wizard" on page 688 for information. • Configuration policies in place. Refer to "Device Configurations Page Fields" on page 204 for information. • Device password rules in place.
III.C.2. Manage and Control Risk (Training)	You can access the following Cisco documentation: • *User Guide for Network Compliance Manager 1.2* • *Device Driver Reference* • *Release Notes*

Fields	Description/Action
III.C.3. Manage and Control Risk (Testing)	Displays the number of: • Configuration policy non-compliance events in the past 24 hours. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Configuration policy non-compliance events in the past seven days. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Devices not in software compliance. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Diagnostics run in the past 24 hours. Refer to "Diagnostics" on page 532 for information. • Diagnostics run in the past seven days. Refer to "Diagnostics" on page 532 for information.
III.D. Oversee Service Provider Arrangements	Displays the number of: • Stored configurations. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Devices with different startup and running configurations. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Non-active devices. Refer to "Viewing Devices" on page 217 for information. • Devices with access failures. Refer to "Viewing Devices" on page 217 for information.
III.E. Adjust the Program	Displays the number of: • Users added in the last month. Refer to "All Users Page Fields" on page 252 for information. • Devices added in the last month. Refer to "Viewing Device Details" on page 225 for information. • Device groups added in the last month. Refer to "Viewing Device Groups" on page 220 for information. • Configuration stored in the last month. Refer to "Viewing Device Configuration Changes" on page 203 for information.

Fields	Description/Action
III.F. Report to the Board	Displays: • The number of Configuration management "Best Practices" green status. Refer to "Network Status Report Fields" on page 573 for information. • System Status report. Refer to "Network Status Report Fields" on page 573 for information. • Summary reports. Refer to "Summary Reports Descriptions" on page 602 for information. • Network Compliance. Refer to "Compliance Center Home Page" on page 624 for information.
III.G. Implement the Standards	This requirement is outside the scope of NCM.

HIPAA Compliance Status Reports

HIPAA is the Health Insurance Portability & Accountability Act of 1996. The final HIPAA Security Rule was published on February 20, 2003. Under the final rule, covered entities include the Department of Health and Human Services (HHS) Medicare Program, other federal agencies operating health plans or providing health care, state Medicaid agencies, private health plans, health care providers, and health care clearinghouses that process, transmit, and/or store protected health information (PHI) in electronic form.

For detailed information on HIPAA, click the "More information about HIPAA and achieving compliance using CiscoWorks Network Compliance Manager" link.

To view the HIPAA Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the HIPAA Compliance Status link. The HIPAA Compliance Status page opens.

HIPAA Compliance Status Page Fields

Fields	Description/Action
Security Standards: General Rules	
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.	Displays the number of: • Stored device configurations. Refer to "Device Configuration Detail Page Fields" on page 206 for information. • Devices with access failures. Refer to "Inventory Page Fields" on page 217 for information. • Devices with port availability of less than 10%. Refer to "Inventory Page Fields" on page 217 for information.

Fields	Description/Action
(2) Protect against any reasonably-anticipated threats or hazards to the security or integrity of such information.	Displays the number of: • Failed user login attempts in the past seven days. Refer to "Event Descriptions" on page 489 for information. • ACLs identified. Refer to "Viewing ACLs" on page 706 for information. • ACLs in use. Refer to "Viewing ACLs" on page 706 for information. • ACL changes in the past seven days. Refer to "Viewing ACLs" on page 706 for information. • ACLs with comments. Refer to "Commenting ACLs and Creating ACL Handles" on page 716 for information.
(3) Protect against any anticipated uses or disclosures that are not permitted or required under subpart E of this part.	Displays the number of: • Users restricted to specific sets of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned Administrator access permissions. Refer to "All Users Page Fields" on page 252 for information.
(4) Ensure compliance with this subpart by its workforce.	You can open the CiscoWorks Network Compliance Center HIPAA Compliance Status report.

Administration Safeguards

Fields	Description/Action
A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Displays the number of: • Configuration management "Best Practices" green status. Refer to "Network Status Report Fields" on page 573 for information. • Devices in software compliance. Refer to "Device Software Report Fields" on page 593 for information. • Monitors with an "Okay" status. Refer to "System Status Page Fields" on page 120 for information. • Devices with access failures. Refer to "Inventory Page Fields" on page 217 for information. • Devices with port availability of less than 10%. Refer to "Inventory Page Fields" on page 217 for information. • Software vulnerabilities detected. Refer to "Inventory Page Fields" on page 217 for information. • Devices with different startup and running configurations. Refer to "Viewing Device Configuration Changes" on page 203 for information.
(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	Displays the number of: • Workflow rules in place. Refer to "Workflow Wizard" on page 688 for information. • Active configuration policies. Refer to "Device Configuration Detail Page Fields" on page 206 for information. • Device Password Rules in place.
(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	This requirement is outside the scope of NCM.

Fields	Description/Action
(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Displays the number of: • User login attempts in the past seven days. Refer to "Event Descriptions" on page 489 for information. • Users added in the past seven days. Refer to "All Users Page Fields" on page 252 for information. • Users deleted in the past seven days. Refer to "All Users Page Fields" on page 252 for information. • User permissions changed in the past seven days. Refer to "Editing User Preferences and Profiles" on page 264 for information. • Configuration policies changed in the past seven days. Refer to "Policies Page Fields" on page 385 for information. • Configuration policies added in the past seven days. Refer to "Policies Page Fields" on page 385 for information.
Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	This requirement is outside the scope of NCM.
Workforce Security	
(A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Displays the number of: • Users restricted to specific group of devices. Refer to "All Users Page Fields" on page 252 for information. • Approved changes in the last 7 days. Refer to "Searching for Events" on page 485 for information. • Unapproved changes in the last 7 days. Refer to "Searching for Events" on page 485 for information.

Fields	Description/Action
(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Displays the number of users assigned Administrator Access permissions. Refer to "All Users Page Fields" on page 252 for information.
(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Displays the number of users deleted in the past seven days. Refer to "All Users Page Fields" on page 252 for information.
Information Access Management	
(A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Displays the number of: • Users restricted to specific groups of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned restricted (non-Admin) access permissions. Refer to "All Users Page Fields" on page 252 for information.
(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Displays the number of: • Users restricted to specific groups of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned restricted (non-Admin) access permissions. Refer to "All Users Page Fields" on page 252 for information.
(C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Displays the number of: • User accounts enabled in NCM. Refer to "All Users Page Fields" on page 252 for information. • User accounts disabled in NCM. Refer to "All Users Page Fields" on page 252 for information.

Fields	Description/Action
Security Awareness and Training	
(A) Security reminders (Addressable). Periodic security updates.	Displays the number of: • User accounts enabled in NCM. Refer to "All Users Page Fields" on page 252 for information. • User accounts disabled in NCM. Refer to "All Users Page Fields" on page 252 for information.
(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	This requirement is outside the scope of NCM.
(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	Displays the number of: • User login attempts in the past seven days. Refer to "Event Descriptions" on page 489 for information. • Failed user login attempts in the past seven days. Refer to "Event Descriptions" on page 489 for information.
(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	Displays the number of NCM password changes in the past seven days. Refer to "Deploy Passwords Task Page Fields" on page 284 for information.
Security Incident Procedures	
Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Displays the number of: • User login attempts in the past seven days. Refer to "Event Descriptions" on page 489 for information. • Failed user login attempts in the past seven days. Refer to "Event Descriptions" on page 489 for information. • Configuration changes detected in the past seven days. Refer to "Device Configuration Detail Page Fields" on page 206 for information.

Fields	Description/Action
Contingency Plan	
(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	NCM does not create or maintain electronic protected health information.
(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.	NCM is a high-availability (HA) system that can be implemented to support automatic failure detection and automatic (or manual) failover with no data loss.
(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	NCM is a high-availability (HA) system that can be implemented to support automatic failure detection and automatic (or manual) failover with no data loss.
(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.	NCM supports periodic testing of automatic failure detection and automatic (or manual) failover.
(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.	NCM's robust reporting capabilities provide the foundation to assess NCM's relative criticality with respect to other contingency plan components.
Evaluation	

Fields	Description/Action
Perform a periodic technical and nontechnical evaluation.	Displays the number of: • Users restricted to specific group of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned Administrator Access permissions. Refer to "All Users Page Fields" on page 252 for information. • Workflow rules in place. Clicking the Workflow Setup page opens the Workflow Wizard. Refer to "Workflow Wizard" on page 688 for information. • Configuration policies in place. Refer to "Policies Page Fields" on page 385 for information. • Device password rules in place.
Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	This requirement is outside the scope of NCM.
Physical Safeguards	
(i) Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	This requirement is outside the scope of NCM.
(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	This requirement is outside the scope of NCM.

Fields	Description/Action
(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Displays the number of: • User login attempts in the past seven days. Refer to "Event Descriptions" on page 489 for information. • Failed user login attempts in the past seven days. Refer to "Event Descriptions" on page 489 for information. • Users restricted to specific groups of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned restricted (non-Admin) access permissions. Refer to "All Users Page Fields" on page 252 for information.
(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	This requirement is outside the scope of NCM.
Workstation Use	
Implement policies and procedures that specify the proper functions to be performed.	This requirement is outside the scope of NCM.
Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	This requirement is outside the scope of NCM.
Device and Media Controls	
(i) Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	This requirement is outside the scope of NCM.

Fields	Description/Action
(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	This requirement is outside the scope of NCM.
(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	This requirement is outside the scope of NCM.
(iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	This requirement is outside the scope of NCM.
Technical Safeguards	
(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.	Displays the number of: • User accounts enabled in NCM. Refer to "All Users Page Fields" on page 252 for information. • User accounts disabled in NCM. Refer to "All Users Page Fields" on page 252 for information.
(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	NCM is a high-availability (HA) system that can be implemented to support automatic failure detection and automatic (or manual) failover with no data loss.
(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Web user sessions terminated after 18000 seconds of inactivity.
(iv) Encryption and decrypting (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.	This requirement is outside the scope of NCM.
Audit Controls	

Fields	Description/Action
Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	This requirement is outside the scope of NCM.
Standard Integrity	
Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	This requirement is outside the scope of NCM.
Person or Entity Authentication	
Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	This requirement is outside the scope of NCM.
Transmission Security	
(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	This requirement is outside the scope of NCM.
(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	This requirement is outside the scope of NCM.
Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements.	This requirement is outside the scope of NCM.
Documentation	

Fields	Description/Action
(i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	This requirement is outside the scope of NCM.
(ii) Availability (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	This requirement is outside the scope of NCM.
(iii) Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	This requirement is outside the scope of NCM.

Visa CISP (PCI Data Security Standard) Compliance Status Reports

In an effort to combat data theft and maintain consumer confidence, all of the major credit card issuers have formulated detailed security programs, including:

- Visa USA Cardholder Information Security Program (CISP)
- MasterCard Site Data Protection (SDP) program
- Discover Information Security and Compliance (DISC) program
- American Express Data Security Operating Policy (DSOP)

In late 2004, Visa and MasterCard aligned their programs under a single standard: the Payment Card Industry (PCI) Data Security Standard. Fundamental security best practices focused on protecting cardholder data comprise the 12 PCI requirements. Penalties for failure to comply with the requirements or to rectify a security issue are severe: possible restrictions on the merchant or permanent prohibition of the merchant's participation in Visa programs, and a fine of up to $500,000 per incident.

For detailed information on Visa CISP, click the "More information about the PCI Data Security Standard (Visa CISP) and achieving compliance using CiscoWorks Network Compliance Manager" link.

To view the Visa CISP Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the Visa CISP Compliance Status link. The Visa CISP Compliance Status page opens.

Visa CISP (PCI Data Security Standard) Compliance Status Page Fields

Fields	Description/Action
Build and Maintain a Secure Network	
1.1: Establish firewall configuration standards that include: • A formal process for approving and testing all connections and changes to the firewall configuration. • A current network diagram with all connections to cardholder data. • Requirements for a firewall at each Internet connection and between any DMZ and the Intranet. • Description of groups, roles, and responsibilities for logical management of network components. • Documented list of services/ports necessary for business. • Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN. • Justification and documentation for any risky protocols. • Periodic review of firewall/router rule sets. • Configuration standards for routers.	Displays the number of: • Deployed devices (routers/firewalls). Refer to "Viewing Device Details" on page 225 for information. • Stored device (routers/firewalls) configurations. Refer to "Viewing Device Details" on page 225 for information. • Firewall configurations changes in the last 7 days. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Configuration policies in place. Refer to "Policies Page Fields" on page 385 for information. • Violations of NSA Router Security Best Practices policy in last 7 days. Refer to "Network Status Report Fields" on page 573 for information. • Approved firewall changes in the last 7 days. Refer to "Viewing Device Details" on page 225 for information. • Unapproved firewall changes in the last 7 days. Refer to "Viewing Device Details" on page 225 for information.

Fields	Description/Action
1.2: Build a firewall configuration that denies all traffic from "untrusted" networks/hosts, except for: • Web protocols - HTTP (port 80) and Secure Sockets Layer (SSL) (typically port 443). • System administration protocols. • Other protocols required by the business.	Displays the number of: • Firewalls in configuration policy non-compliance. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Firewall configuration non-compliance events in the last 7 days. Refer to "Viewing Device Configuration Changes" on page 203 for information.

Fields	Description/Action
1.3: Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including: • Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters). • Restricting inbound and outbound Internet traffic to ports 80 and 443. • Not allowing internal addresses to pass from the Internet into the DMZ (egress filters). • Placing the database in an internal network zone. • Restricting outbound traffic to that which is necessary for the payment card environment. • Securing and synchronizing router configuration files. • Denying all other inbound and outbound traffic not specifically allowed. • Installation of perimeter firewalls between any wireless networks and the payment card environment. • Installation of personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet.	Displays the number of: • Firewalls in configuration policy non-compliance. Refer to Refer to "Viewing Device Configuration Changes" on page 203 for information. • Firewall configuration non-compliance events in the last 7 days. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Deployed firewalls. Refer to "Viewing Device Details" on page 225 for information.

Fields	Description/Action
1.4: Prohibit direct public access between external networks and any system component that stores cardholder information, including: • Implement a DMZ to filter and screen all traffic, to prohibit direct routes for inbound and outbound Internet traffic. • Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	Displays the number of: • Firewalls in configuration policy non-compliance. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Firewall configuration non-compliance events in the last 7 days. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Deployed firewalls. Refer to "Viewing Device Details" on page 225 for information.
1.5: Implement Internet Protocol (IP) masquerading to prevent internal addresses from being translated and revealed on the Internet.	Displays the number of: • Firewalls in configuration policy non-compliance. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Firewall configuration non-compliance events in the last 7 days. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Deployed firewalls. Refer to "Viewing Device Details" on page 225 for information.
2.1: Always change the vendor-supplied defaults before you install a system on the network. For wireless environments, change wireless vendor defaults.	Displays the number of: • Device password rules in place. • Password changes in the last 7 days. Refer to "Deploy Passwords Task Page Fields" on page 284 for information. • Device password change failures in the last 7 days. Refer to "Deploy Passwords Task Page Fields" on page 284 for information.

Fields	Description/Action
2.2: Develop configuration standards for all system components, including: • Implement only one primary function per server. • Disable all unnecessary and insecure services and protocols. • Configure system security parameters to prevent misuse. • Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, and file systems.	Displays the number of: • Devices in configuration policy non-compliance. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Configuration policy non-compliance events in the last 7 days. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Configuration policies in place. Refer to "Policies Page Fields" on page 385 for information. • Configuration policy rules added in the last 7 days. Refer to "Policies Page Fields" on page 385 for information. • Configuration policy rules changed in the last 7 days. Refer to "Policies Page Fields" on page 385 for information.
2.3: Encrypt all non-console administrative access.	Displays the number of devices configured to use SSH or SCP. Refer to "Viewing Device Details" on page 225 for information.
Protect Cardholder Data	
4.1: Use strong cryptography and encryption techniques. For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit.	Displays the number of: • Devices in configuration policy non-compliance. Refer to "Viewing Device Configuration Changes" on page 203 for information • Configuration policy non-compliance events in the last 7 days. Refer to "Viewing Device Configuration Changes" on page 203 for information • Violations of NSA Router Security Best Practices policy in last 7 days. Refer to "Network Status Report Fields" on page 573 for information. • Configuration policies in place. Refer to "Policies Page Fields" on page 385 for information.
4.2: Never send cardholder information via unencrypted e-mail.	This requirement is outside the scope of NCM.
Maintain a Vulnerability Management Program	

Fields	Description/Action
6.1: Ensure that all system components and software have the latest vendor-supplied security patches and install relevant security patches within one month of release.	Displays the number of: • Successful software updates in the last 7 days. Refer to "Device Software Report Fields" on page 593 for information. • Failed software updates in the last 7 days. Refer to "Device Software Report Fields" on page 593 for information.
6.2: Establish a process to identify newly discovered security vulnerabilities.	Displays the number of: • Devices not in software compliance. Refer to "Software Compliance Page Fields" on page 406 for information. • Software vulnerabilities detected in the last 7 days. Refer to "Software Vulnerability Report Fields" on page 595 for information.
6.3: Develop software applications based on industry best practices and include information security throughout the software development life cycle, including: • Testing of all security patches and system and software configuration changes before deployment. • Separate development/test and production environments. • Production data (real credit card numbers) are not used for testing or development. • Removal of test data and accounts before production systems become active. • Review of custom code prior to release to production or customers, to identify any potential coding vulnerability.	NCM provides the ability to test policies against configuration data entered into the system prior to deployment to identify policy non-compliance.

Fields	Description/Action
6.4: Follow change control procedures for all system and software configuration changes, including: • Documentation of impact • Management sign-off by appropriate parties • Testing that verifies operational functionality • Back-out procedures	Displays the number of: • Users restricted to specific sets of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned administrator access permissions. Refer to "All Users Page Fields" on page 252 for information. • Workflow rules in place. Refer to "Workflow Wizard" on page 688 for information. • Approved changes in the last 7 days. Refer to "Searching for Events" on page 485 for information. • Unapproved changes in the last 7 days. Refer to "Searching for Events" on page 485 for information. • Stored device configurations. Refer to "Viewing Device Details" on page 225 for information. • Stored device configurations in the last 7 days. Refer to "Viewing Device Details" on page 225 for information.
6.5: Develop web software and applications based on secure coding guidelines, including: • Invalidated input • Broken access control • Broken authentication/session management • Cross-site scripting (XSS) attacks • Buffer overflows • Injection flaws • Improper error handling • Insecure storage • Denial of service • Insecure configuration management	Cisco uses industry-accepted software design principles and coding practices, and its internal engineering policies emphasize writing secure, high-quality code. Cisco monitors various security bulletin boards and alerts, subscribes to mailing lists, and conducts period security reviews of its code to ensure that any vulnerabilities are identified and addressed.

Fields	Description/Action
Implement Strong Access Control Measures	
7.1: Limit access to computing resources and cardholder information to only those individuals whose job requires such access.	Displays the number of: • User login attempts in the last 7 days. Refer to "All Users Page Fields" on page 252 for information. • Users added in the last 7 days. Refer to "All Users Page Fields" on page 252 for information. • Users deleted in the last 7 days. Refer to "All Users Page Fields" on page 252 for information. • User permissions changed in the last 7 days. Refer to "All Users Page Fields" on page 252 for information.
7.2: Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Displays the number of: • Users restricted to specific sets of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned administrator access permissions. Refer to "All Users Page Fields" on page 252 for information.
8.1: Identify all users with a unique username before allowing them to access system components or cardholder data.	Displays the number of: • User accounts enabled in NCM. Refer to "All Users Page Fields" on page 252 for information. • User accounts disabled in NCM. Refer to "All Users Page Fields" on page 252 for information.
8.2 Employ at least one of the methods below, in addition to unique identification, to authenticate all users: • Password • Token devices • Biometrics	Displays the number of: • Password changes in the last 7 days. Refer to "Deploy Passwords Task Page Fields" on page 284 for information. • External authentication is enabled via Active Directory. Refer to "User Authentication Page Fields" on page 109 for information.
8.3: Implement 2-factor authentication for remote access to the network by employees, administrators, and third parties.	Displays the number of external authentication is enabled via Active Directory. Refer to "User Authentication Page Fields" on page 109 for information.

Fields	Description/Action
8.4: Encrypt all passwords during transmission and storage, on all system components.	NCM passwords are masked when keyed in at login and encrypted on disk and during transmission.

Fields	Description/Action
8.5: Ensure proper user authentication and password management for non-consumer users and administrators, including: • Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects. • Verify user identity before performing password resets. • Set first-time passwords to a unique value per user and change immediately after first use. • Remove inactive user accounts at least every 90 days. • Enable accounts used by vendors for remote maintenance only during the time needed. • Distribute password procedures and policies to all users who have access to cardholder information. • Do not use group, shared, or generic accounts/passwords. • Change user passwords at least every 90 days. • Require a minimum password length of at least seven characters. • Use passwords containing both numeric and alphabetic characters. • Limit repeated access attempts by locking out the user ID after not more than six attempts. • Set the lockout duration to thirty minutes or until administrator enables the user ID. • Authenticate all access to any database containing cardholder information.	Displays the number of: • User login attempts in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Failed user login attempts in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Password changes in the last 7 days. Refer to "Deploy Passwords Task Page Fields" on page 284 for information. • User accounts enabled in NCM. Refer to "All Users Page Fields" on page 252 for information. • User accounts disabled in NCM. Refer to "All Users Page Fields" on page 252 for information.

Fields	Description/Action
Regularly Monitor and Test Networks	
10.1: Establish a process for linking all access to system components.	Displays the number of: • User accounts enabled in NCM. Refer to "All Users Page Fields" on page 252 for information. • User accounts disabled in NCM. Refer to "All Users Page Fields" on page 252 for information.
10.2: Implement automated audit trails to reconstruct the following events: • All individual user accesses to cardholder data. • All actions taken by any individual with root or administrative privileges. • Access to all audit trails. • Invalid logical access attempts. • Use of identification and authentication mechanisms. • Initialization of the audit logs. • Creation and deletion of system-level objects.	Displays the number of: • Audit logging of user actions is disabled. Refer to "Server Page Fields" on page 80 for information. • Failed user login attempts in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • External authentication is not enabled. Refer to "User Authentication Page Fields" on page 109 for information. • Users added in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Users deleted in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Devices added in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Devices deleted in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Device configuration changes in the last 7 days. Refer to "Viewing Device Details" on page 225 for information.

Fields	Description/Action
10.3: Record at least the following audit trail entries for each event: • User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected data, system component, or resource	Displays the number of: • User login attempts in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Failed user login attempts in the last 7 days. Refer to "Event Descriptions" on page 489 for information.
10.4: Synchronize all critical system clocks and times.	Displays the number of devices configured with NTP. Refer to "Viewing Device Details" on page 225 for information.
10.5: Secure audit trails so they cannot be altered, including: • Limit viewing of audit trails to those with a job-related need. • Protect audit trail files from unauthorized modifications. • Promptly back-up audit trail files to a centralized log server or media that is difficult to alter. • Copy logs for wireless networks onto a log server on the internal LAN. • Use file integrity monitoring/change detection software on logs to ensure that existing log data cannot be changed without generating alerts.	Displays the number of: • Users can delete sessions. Refer to "All Users Page Fields" on page 252 for information. • Users can delete system events. Refer to "All Users Page Fields" on page 252 for information.
10.6: Review logs for all system components at least daily.	Displays the number of Log files saved for 30 days. Refer to "Server Page Fields" on page 80 for information.

Fields	Description/Action
10.7: Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations.	Displays the number of saved (refer to "Server Page Fields" on page 80 for information): • Configurations • Diagnostics: • Events • Tasks • Sessions • Log files
11.1: Test security controls, limitations, network connections, and restrictions.	Displays the number of: • All ACLs. Refer to "Viewing ACLs" on page 706 for information. • ACLs in use. Refer to "Viewing ACLs" on page 706 for information. • ACL changes in the last 7 days. Refer to "Viewing ACLs" on page 706 for information.
11.2: Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.	This requirement is outside the scope of NCM.
11.3: Perform penetration testing on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification.	Displays the number of: • Devices in configuration policy non-compliance. Refer to "Configuration Policy Activity Page Fields" on page 398 for information. • Configuration policy non-compliance events in the last 7 days. Refer to "Configuration Policy Activity Page Fields" on page 398 for information. • Devices not in software compliance. Refer to "Device Software Report Fields" on page 593 for information. • Software vulnerabilities detected in the last 7 days. Refer to "Software Vulnerability Report Fields" on page 595 for information. • Event Notification & Response Rules in place. Refer to "Event Notification & Response Rules Page Fields" on page 435 for information.

Fields	Description/Action
11.4: Use network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	NCM can centrally and securely manage devices with IDS (intrusion detection system) and IPS (intrusion prevention system) modules.
11.5: Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files, and perform critical file comparisons at least daily (or more frequently if the process can be automated).	Displays the number of: • Device configuration changes in the last 7 days. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Configuration policy non-compliance events in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Devices in configuration policy non-compliance. Refer to "Event Descriptions" on page 489 for information. • Successful software updates in the last 7 days. Refer to "Device Software Report Fields" on page 593 for information. • Failed software updates in the last 7 days. Refer to "Device Software Report Fields" on page 593 for information. • Software vulnerabilities detected in the last 7 days. Refer to "Software Vulnerability Report Fields" on page 595 for information. • Devices not in software compliance. Refer to "Device Software Report Fields" on page 593 for information.

Maintain an Information Security Policy

Fields	Description/Action
12.2: Develop daily operational security procedures.	Displays the number of: • Users restricted to specific sets of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned administrator access permissions. Refer to "All Users Page Fields" on page 252 for information. • Users added in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Users deleted in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • User permissions changed in the last 7 days. Refer to "All Users Page Fields" on page 252 for information. • Saved configurations, saved diagnostics, saved tasks, saved sessions, and saved Log files. Refer to "Server Page Fields" on page 80 for information.

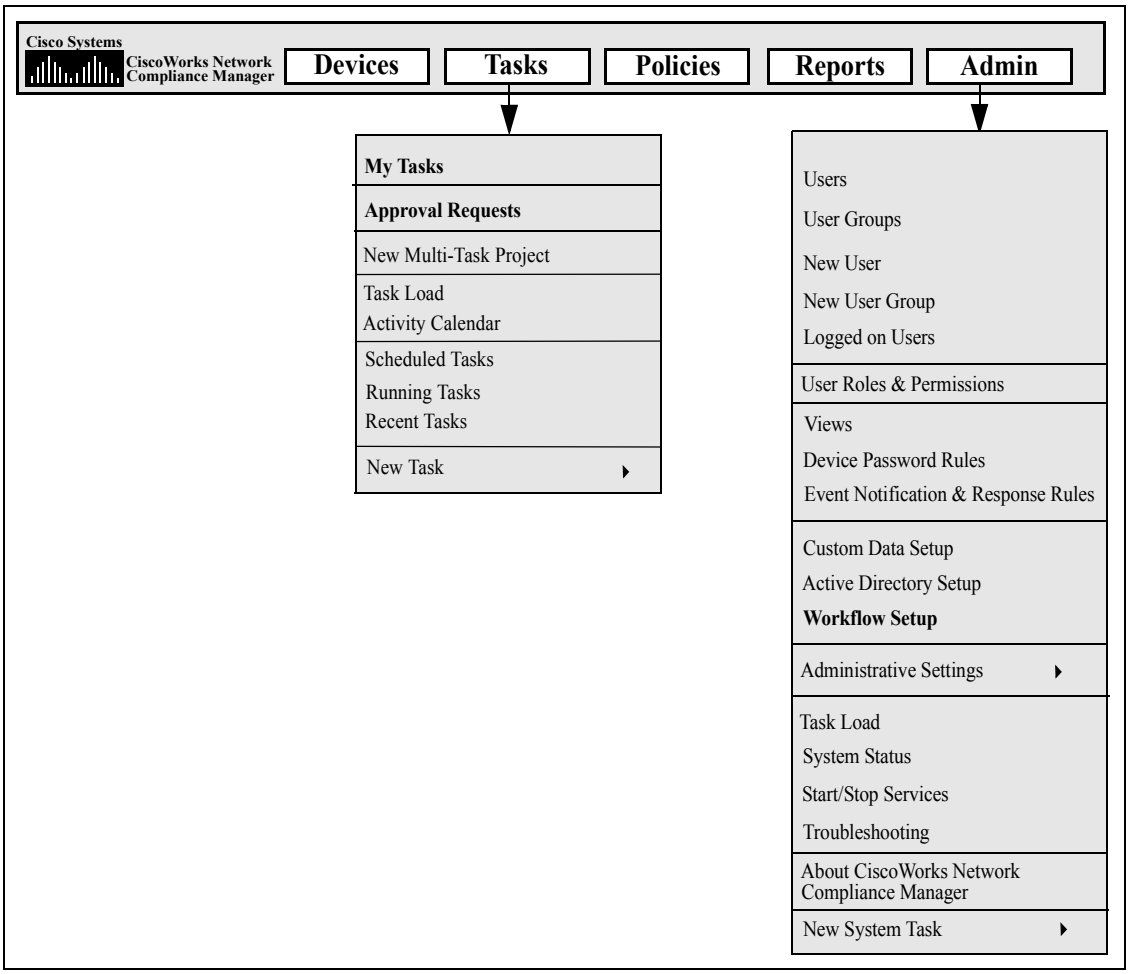
Fields	Description/Action
12.5: Assign to an individual or team the following information security management responsibilities: • Establish, document, and distribute security policies and procedures. • Monitor and analyze security alerts and information, and distribute to appropriate personnel. • Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. • Administer user accounts, including additions, deletions, and modifications. • Monitor and control all access to data.	Displays the number of: • Configuration policies in place. Refer to "Policies Page Fields" on page 385 for information. • Event Notification & Response Rules in place. Refer to "Event Notification & Response Rules Page Fields" on page 435 for information. • Monitors that have an "Okay" status. Refer to "System Status Page Fields" on page 120 for information. • Configuration management best practices in green status. Refer to "Network Status Report Fields" on page 573 for information. • User accounts enabled in NCM. Refer to "All Users Page Fields" on page 252 for information. • User accounts disabled in NCM. Refer to "All Users Page Fields" on page 252 for information. • Users restricted to specific sets of devices. Refer to "All Users Page Fields" on page 252 for information. • Users assigned administrator access permissions. Refer to "All Users Page Fields" on page 252 for information. • Users added in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Users deleted in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • User permissions changed in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • User login attempts in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Failed user login attempts in the last 7 days. Refer to "Event Descriptions" on page 489 for information.

Fields	Description/Action
12.9: Implement an incident response plan, including: • Create an incident response plan to be used in the event of system compromise. • Test the plan at least annually. • Designate specific personnel to be available on a 24/7 basis to respond to alerts. • Provide appropriate training to staff with security breach response responsibilities. • Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems. • Have a process to modify and evolve the incident response plans.	Displays the number of: • Device configuration changes in the last 7 days. Refer to "Viewing Device Configuration Changes" on page 203 for information. • Configuration policy non-compliance events in the last 7 days. Refer to "Event Descriptions" on page 489 for information. • Successful software updates in the last 7 days. Refer to "Device Software Report Fields" on page 593 for information. • Failed software updates in the last 7 days. Refer to "Device Software Report Fields" on page 593 for information. • Software vulnerabilities detected in the last 7 days. Refer to "Software Vulnerability Report Fields" on page 595 for information.

Chapter 19: Creating Workflows

Use the following table to quickly locate information.

Navigating to Workflow



Getting Started

The CiscoWorks Network Compliance Manager (NCM) Workflow Integration & Routing Engine (WIRE) manages the process of network configuration, making sure that network changes are made according to predefined policies, completed in the correct sequence, and approved by the appropriate people.

By controlling who does what to the network and why, device configurations can be accomplished accurately and in accordance with the objectives of your organization. Because Workflow manages the sequencing of tasks, the gaining of approvals, and the auditing of results, out-of-policy changes and inadvertent configuration errors are far less likely to occur.

The following terms are used in this chapter.

- Task — Tasks are the primary mechanism by which NCM interacts with your network. Tasks are specific actions you can either schedule or run immediately. Completed tasks provide the result of NCM activities. Workflow tasks include all tasks, for example:
  - Deploy Passwords
  - Reload Device
  - Task Snapshot
  - Run Command Script
  - Synchronize Startup and Running Configurations
  - Update Device Software
  - Run Diagnostics

  For a complete list of tasks, refer to "What Are Tasks?" on page 278.
- Project — A project is an ordered sequence of tasks. From NCM's point of view, a project is just another type of task with sub-tasks that are sequentially run (instead of in parallel).
- Originator — An individual who submits a task.
- Approver — An individual or a group of individuals who can approve a task and confirm that the task complies with all internal policies.
- FYI Recipients — An individuals or a group of individuals who receive notification based on actions taken by the originator or the approver.

- Approved — The approval status of a task that has been approved for execution.
- Not Approved — The approval status of a task that has been rejected. A rejected task either does not have enough data or has incorrect data that could lead to negative consequences on the network. A rejected task cannot be recycled.
- Suspended — The approval status of a task that is temporarily (or permanently) on hold.
- Override — An action performed by the Originator of a task for use in emergencies when the approval process needs to be overridden. This function is only available if enabled in the Administrative Settings.

Note: You may want to enable all Power users to create tasks that do not require approval. Refer to "Workflow Wizard" on page 688 for information on creating rules. For example, you can create a rule, "All Power Users do not need approval," before a "All Users need approval by Admin" rule to enable Power users to bypass approval.

Workflow Wizard

The Workflow Wizard enables you to easily setup a Workflow for tasks. To open the Workflow Wizard, on the menu bar under Admin click Workflow Setup. The Workflow Wizard opens.

Step	Description/Action
Welcome Page	The Welcome page provides a brief introduction to the Workflow Wizard. Click Next to continue.
Step 1: Enable Workflow	You are asked if you want to enable Workflow and require approval for some or all tasks. Click Yes and then click Next to continue. If you click No and then click Next, the Setup Complete page opens, where you can return to Workflow Wizard home page.
Step 2: Enable Workflow - Cont'd.	The Enable Workflow - Cont'd page provides an overview of the information you must provide when creating a Workflow. Click Next to continue.

Step	Description/Action
Step 3: Manage Approval Rules	Enter the name of the new Workflow Approval Rule and click Next to continue. You also have the option of modifying or deleting existing Workflow Approval Rules. All existing Workflow Approval Rules are displayed at the bottom of the page. (**Note**: NCM is shipped with one default Workflow Approval Rule: *All users approved by Administrator*.)
Step 4: Originator Setup	The Originator Setup page enables you to designate the users that will trigger this rule when they create a task. When you are done adding users, click Next to continue.
Step 5: Task Setup	The Task Setup page enables you to designate which tasks need approval. When you are done adding tasks, click Next to continue.
Step 6: Device Group Setup	The Device Group Setup page enables you to define Workflow Approval Rules based on device groups. This enables you to configure Workflow Approval Rules on device usage, device type, and so on. When you are done adding device groups, click Next. Keep in mind that at task creation time, the Workflow Approval Rule only applies if: • The task is against a single device and the Workflow Approval Rule's device group contains the device. • The task is against a device group and the Workflow Approval Rule's device group has a non-empty intersection with the task's device group.
Step 7: Approver Setup	The Approver Setup page enables you to designate who can approve a task and confirm that the task complies with all internal policies, or if no approval is required. Keep in mind that a task originator cannot review his/her own tasks. When you are done adding users, click Next to continue.
Step 8: FYI Recipient Setup	The FYI Recipient Setup page enables you to designate who receives notification based on actions taken by the Workflow Approval Rule originator or approver. When you are done adding users, click Save. Keep in mind that originators and approvers need not be added as recipients. Refer to "Email Notification" on page 701 for detailed information on email notification.

Step	Description/Action
Setup Complete	After you have successfully added a Workflow Approval Rule, the "Successfully created new rule <rule name>" message is displayed at the top of the page. You can now create a new Workflow Approval Rule for other users (originators) or modify/delete existing approval rules by clicking the Manage Approval Rules link. You can click the My Tasks option from the Tasks drop-down menu to view a summary of originator and approver actions. Refer to "My Tasks" on page 691 for information.

My Tasks

The My Tasks page shows tasks originated by the currently logged in user, including the task approval status, if applicable, and if the task has not yet run.

To view the My Tasks page, on the menu bar under Tasks click My Tasks. The My Tasks page opens.

My Tasks Page Fields

Field	Description/Action
My Drafts link	If applicable, opens the My Drafts page.
Approval Requests link	If the task requires approval, opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. By default, the page shows tasks that have not completed, including tasks that are: • Not approved • Waiting Approval • Waiting to run Refer to "Approval Requests" on page 695 for information.
Scheduled Tasks link	Opens the Scheduled Tasks page, where you can view scheduled tasks that are in the queue, but have not yet run. Refer to "Scheduled Tasks Page Fields" on page 369 for information.
Running Tasks link	Opens the Running Tasks page, where you can view all running tasks. Refer to "Running Tasks Page Fields" on page 371 for information.
Recent Tasks link	Opens the Recent Tasks page, where you can view all recent tasks. Refer to "Recent Tasks Page Fields" on page 373 for information.

Field	Description/Action
Show Tasks Check Boxes	If the task requires approval, you can select the following display options: • Approved • Not Approved • Waiting Approval • Overridden • Draft • No Approval Required
Check Boxes	You can use the left-side check boxes to delete tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Schedule Date	Displays the date and time the task was created.
Task Name	Displays the task name. Clicking a task opens the Task Information page. Refer to "What Are Tasks?" on page 278 for information on Tasks.
Approved By Date	If applicable, displays the date and time the task must be approved. If a task is not approved by its approval date, its status is set to "Not Approved." (**Note**: Approval options are only displayed if the task is part of a Workflow Approval Rule.)
Approval Status	If applicable, displays the task's approval status. Approval status is only displayed if the task is part of a Workflow Approval Rule. Approval statuses include: • Awaiting Approval • Approved • Not Approved • Overridden • No Approval Required

Field	Description/Action
Task Status	Displays the status of the task. Statuses include: • Warning — A group task containing some failed sub-tasks, but not all tasks failed. • Draft — NCM will not run the task, nor is the task sent out for approval, when in Draft status. • Duplicate — The task was not started because an identical task is already running. • Failed — The task failed. • Paused — Someone paused the task. It will not run when its scheduled time arrives. • Pending — The task is queued and waiting for its scheduled time. • Running — The task has started, but has not yet finished. • Skipped — The task was skipped due to errors, for example incorrect permissions, unmanaged devices, and so on. • Succeeded — The task succeeded. • Waiting — Although the scheduled time has arrived, the task is waiting because the "Max Concurrent Tasks" limit has been reached.
Task Type	Displays the task type, for example: • Deploy Password • Deploy Config • Discover Driver • Reload Device • Take Snapshot • Synchronize Startup and Running Configurations For a complete list of tasks, refer to "What Are Tasks?" on page 278. (**Note**: Multi-Task Project tasks may or may not be displayed on the My Tasks results page. It depends on whether the Multi-Task Project task includes at least one of the task types listed above as a sub-task.)

Field	Description/Action
Actions	You can select one of the following options: • Edit — Opens the Edit Task page for that task. • Delete — Enables you to delete the task. • Pause — Pauses the task so it does not run at its scheduled time. (NOTE: You can select Resume if you want to resume the task.) • Run Now — Runs the task as soon as possible. If the maximum number of concurrent tasks has not been reached, the task runs immediately.
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

Approval Requests

The Approval Requests page enables you to view tasks needing approval by the currently logged in user. By default, the page shows tasks that have not yet completed where the approval status is either Approved, Waiting Approval or Not Approved.

Note: To view completed tasks, on the menu bar under Reports, select Search For and click Tasks. Refer to "Search For Tasks Page Fields" on page 472 for information.

To view the Approval Requests page, on the menu bar under Tasks, click Approval Requests. The Approval Requests page opens.

Approval Requests Page Fields

Field	Description/Action
My Tasks	Opens the My Tasks page, where you can view the status of each task. Refer to "My Tasks Page Fields" on page 691 for information.
Scheduled Tasks link	Opens the Scheduled Tasks page, where you can view scheduled tasks that are in the queue, but have not yet run. Refer to "Scheduled Tasks Page Fields" on page 369 for information.
Running Tasks link	Opens the Running Tasks page, where you can view all running tasks. Refer to "Running Tasks Page Fields" on page 371 for information.
Recent Tasks link	Opens the Recent Tasks page, where you can view all recent tasks. Refer to "Recent Tasks Page Fields" on page 373 for information.
Show Tasks	If checked, tasks with the following approval status are displayed: • Approved • Not Approved • Waiting Approval

Field	Description/Action
Task Name	Displays the task name. To approve a task, click the Task name. The Task Information page opens. Refer to "Task Information Page Fields" on page 698 for information.
Approve By	Displays the date and time the task must be approved. If a task is not approved by its approval date, its status is set to "Not Approved." (NOTE: Tasks that have run are removed from the Approval Request page. Tasks past their approval date are marked Not Approved and will remain on the Approval Request page until the data pruner deletes them. Refer to "Data Pruning Task Page Fields" on page 354 for information on data pruning.)
Approval Status	Displays the task's approval status. Approval statuses include: • Waiting Approval • Not Approved
Priority	Displays the task's priority.
Date	Displays the date and time the task was created.

Field	Description/Action
Status	Displays the status of the task. Statuses include: • Warning — A group task containing some failed tasks, but not all tasks failed. • Draft — NCM will not run the task, nor is the task sent out for approval, when in Draft status. • Duplicate — The task was not started because an identical task is already running. • Failed — The task failed. • Paused — Someone paused the task. It will not run when its scheduled time arrives. • Pending — The task is queued and waiting for its scheduled time. • Running — The task has started, but has not yet finished. • Skipped — The task was skipped due to errors, for example incorrect permissions, unmanaged devices, and so on. • Succeeded — The task succeeded. • Waiting — Although the scheduled time has arrived, the task is waiting because the "Max Concurrent Tasks" limit has been reached.
Scheduled By	Displays the name of the person who scheduled the task.

Approving Tasks

If you have been designated to approve a task:

1. On the menu bar under Tasks, click Approval Requests. The Approval Requests page opens. Refer to "Approval Requests Page Fields" on page 695.
2. Click the task name to view approval options. The Task Information page opens.
3. Click the Approve button.

Task Information Page Fields

The Task Information page includes detailed information on tasks, including:

- Task status
- Originator
- Devices affected
- Duration
- Approval information
- Result details

The Task information page also provides links to more detailed information in the event of a warning or failure. Keep in mind that a task can be successfully completed but still contain errors. For example, you could successfully deploy to a running configuration but have invalid commands within the configuration.

To open the Task Information page:

1. Select a device from the Inventory page. The Device Details page opens.
2. From the View drop-down menu, click Device Tasks. The Device Tasks page opens.
3. Click the Detail option in the Actions column for the task on which you want detailed information. The Task Information page opens.

Field	Description/Action
Edit Task link	Opens the task page so that you can edit the task. This link is only displayed for pending tasks.
Run Again link	Opens the task page so that you can re-run the task. This link is only displayed for completed tasks.
Return to List link	Opens the My Tasks page. Refer to "My Tasks Page Fields" on page 365.
General Information	
Task Name	Displays the task name.
Task Status	Displays the task status, including: • Draft • Duplicate • Failed • Paused • Pending • Requested (Note: Requested means the task is waiting for Approval. Refer to "Approving Tasks" on page 698.) • Running • Skipped • Succeeded • Synchronous (Note: NCM typically runs tasks by creating a thread and letting the task run asynchronously in the background. The CLI and API enable synchronous tasks where they are run in the current thread and the command blocks until the command completes.) • Waiting • Warning **Note**: Multi-task projects will continue processing when a warning is encountered. The warning status is shown in the parent task.
Comments	Displays any comments about the task.

Field	Description/Action
Originator	Displays the username or process that scheduled the task.
Create Date	Displays the date and time the task was created.
Devices Affected	Displays the host name and/or IP address of the affected device.
Schedule Date	Displays the date and time the task was scheduled to run.
Start Date	Displays the task's start date.
Complete Date	Displays the task's complete date.
Duration	Displays the task's duration.
Repeat Type	Displays the repeat type, for example: non-recurring.
Approval Information	
Approver(s)	Displays a list of task approvers.
Approval Status	Displays the task approval status.
Priority	Displays the task priority.
Approved By	Displays the date and time the task must be approved.
New Comments	Enter additional comments about the task.
Approve Button	Click the Approve button to approve the task.
View Task Details link	Clicking the View Tasks link opens the Diagnostics History page.
Additional Information	
Result Details	Displays the diagnostics that were automatically run (depending on the device type), for example: • Diagnostic "CWNCM Module Status" completed • Diagnostic "CWNCM Routing Table" completed • Diagnostic "CWNCM OSPF Neighbors" completed
Task History	
Task History Information	Displays task history information, such as when the task was run, the repeat type, and status.

Email Notification

Task approvers receive email notification based on actions taken by the Workflow Rule originator. The Workflow Wizard's FYI Recipient Setup page can be used to notify users other than approvers of the task. Refer to "Workflow Wizard" on page 688.

A sample email notification is shown below.

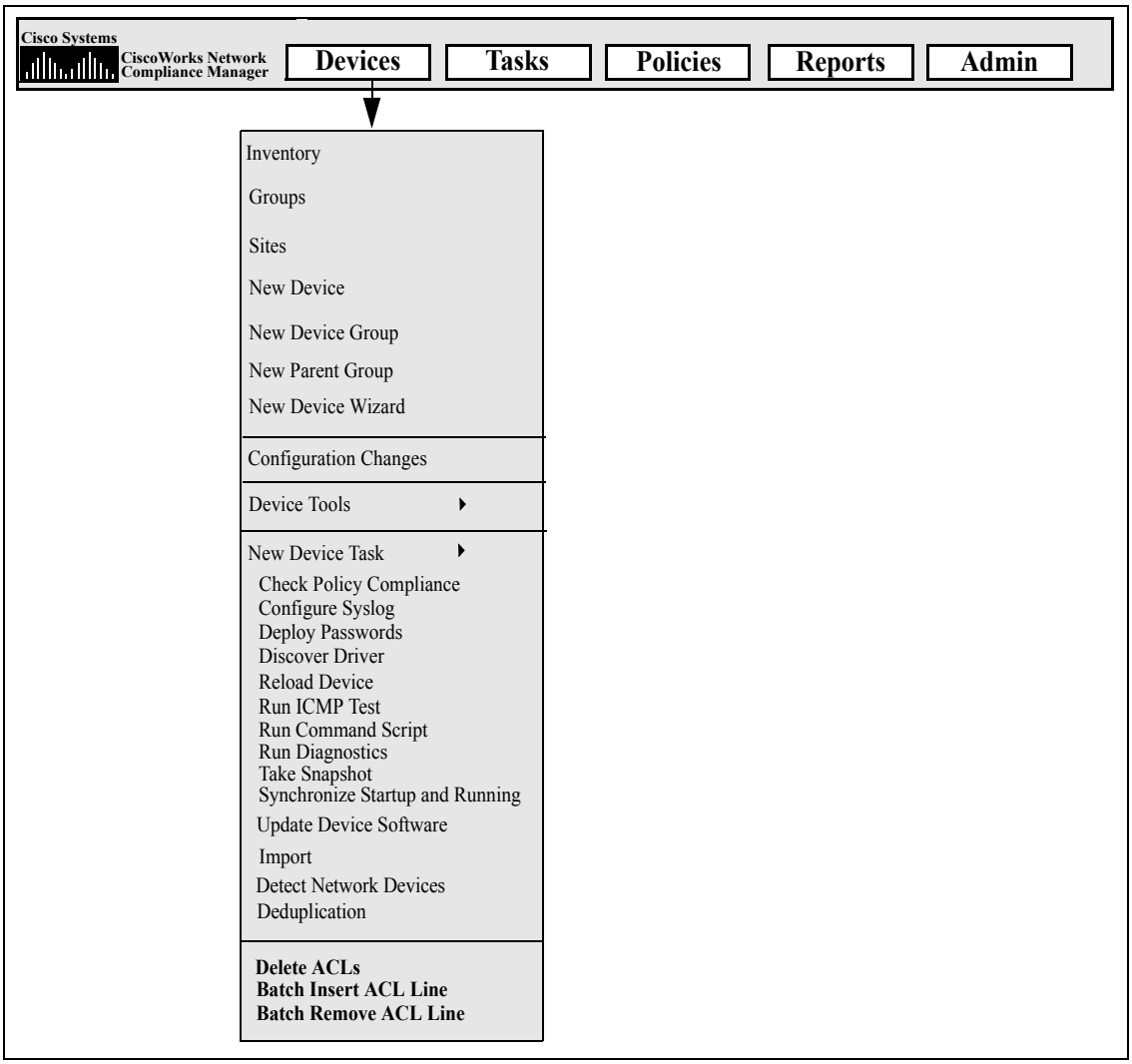
```
From: Cisco on jbrennan1
Sent: Thursday, January 20, 2006 2:00 PM
To: Tad Martin
Subject: Request for Approval
_____________________________________________________

Liza has requested the Snapshot task for your approval
on or before 2005-11-06 00:00:00:0

Task Name: Snapshot
Description: Taking a snapshot of Lab2
Priority: High
Approval required on or before: 2005-11-06 00:00:00:0
Originator: Liza
Devices Affected: 172.22.123.26
Task Frequency: Repeat once
Task Start Date: 2005-11-06 15:00:00.0

You may approve, reject, or request clarification by
accessing CiscoWorks Network Compliance Manager at
http://liza/task.view.htm/taskID=10023
```

Clicking the link at the bottom of the email opens the Approval Requests page where you can approve or not approve a task. Refer to "Approval Requests Page Fields" on page 695.

Chapter 20: Working With ACLs

Use the following table to quickly locate information.

Navigating to ACLs



Getting Started

Access Control Lists (ACLs) are used by many organizations to control the flow of IP traffic. This is done mostly for increased security, but can also be used to increase performance by preventing the operation of bandwidth intensive systems, such as streaming audio or video, from public Web sites.

In general, the definition of an ACL is a collection of configuration statements. These statements define addresses and/or patterns to accept or deny. CiscoWorks Network Compliance Manager (NCM) retrieves configuration information from devices and extracts the ACL statements from the configuration. NCM then stores the ACLs independent of the configuration.

The NCM ACL Manager provides a quick way to:

- View ACLs on devices
- Maintain a history of ACLs
- Comment on ACLs and maintain those comments in the configuration

The ACL Manager also provides a quick way to use existing ACL configurations to create ACL templates.

This chapter includes instructions on how to enable (and disable) ACLs parsing for a device or group of devices.

- For information on turning on ACL parsing for a single device, refer to "Configuration Mgmt Page Fields" on page 58.
- For information on turning on ACL parsing for a group of devices, refer to "Batch Edit Device Page Fields" on page 191.
- For information on searching for ACLs, refer to "Searching for ACLs" on page 499.

Note: ACL information is not available until after the first stored or checkpoint snapshot is taken of the device after ACL parsing is enabled.

Viewing ACLs

To view ACLs on a device:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens. (**Note**: When adding devices that support ACLs, make sure that the Enable Parse ACLs check box is checked.) Once the devices are discovered, and a checkpoint snapshot is taken, you are able to view a device's ACLs. (Refer to "Adding Devices" on page 134 for more information on adding devices.)
3. From the View drop-down menu, select Device Detail and then click ACLs. The Device ACLs page opens. Refer to "Device ACLs Page Fields" on page 706.
4. On the Device ACLs page, click the View ACL option for any ACL listed. The View ACL page opens. Refer to "View ACL Page Fields" on page 708.

Device ACLs Page Fields

Field	Description/Action
Hostname	Displays the device's host name. Clicking the device's host name opens the Device Details page, where you can view information about this device.
Device IP	Displays the device's IP address. Clicking the device's IP address opens the Device Details page, where you can view information about this device.
Last Access Time	Displays the date and time the device was last accessed.
Last Snapshot Result	Displays the last snapshot result, for example "Configuration Change Detected."

Field	Description/Action
Check Boxes	You can use the left-side check boxes to compare two ACLs and delete ACLs. Once you have selected the ACLs, click the Actions drop-down menu and click either: • Compare — Opens the Compare Script page, where you can compare the two selected ACLs side by side. The differences are highlighted in different colors to make them easy to view. • Delete — Deletes the checked ACLs. The adjacent Select drop-down menu enables you to select or deselect all of the device configurations.
ACL ID	Displays the ACL ID. The ACL ID refers to how the device identifies the ACL in its configuration. Keep in mind that while many devices use an integer index as the ACL ID, not all do. As a result, ACL IDs are stored as strings.
Handle	Displays the ACL handle. The ACL Handle is the ACL name you defined. By default, the ACL Handle is the same as the ACL ID. If you do not supply a specific ACL Handle, the driver uses the ACL ID. (Note: This field is used to sort ACLs by default.)
Type	Displays the ACL type, as defined by the device.
Last Modified Date	Displays the date and time the ACL was last modified.
Actions	You can select the following actions: • Edit ACL — Opens the Edit ACL page, where you can edit the ACL. Refer to "Running Command Scripts" on page 710 for information. • View ACL — Opens the View ACL page, where you can view the ACL. Refer to refer to "View ACL Page Fields" on page 708 for information. • ACL History — Opens the ACL History page. Keep in mind that you can use the ACL history to facilitate restoring an ACL to a prior configuration. To do this, you would view the historical ACL and then click the Edit ACL action link.

View ACL Page Fields

To open the View ACL page:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens. (Note: When adding devices that support ACLs, make sure that the Enabled Parse ACLs check box is checked.) Once the devices are discovered, and an initial snapshot is taken, you are able to view a device' ACLs.
3. From the View drop-down menu, select Device Detail and then click ACLs. The Device ACLs page opens.
4. On the Device ACLs page, click the View ACLs option for any ACL listed. The View ACL page opens.

Field	Description/Action
Device	Display the host name and IP address of the device. Clicking the device's IP address opens the Device Details page, where you can view information about this device.
ID	Displays the ACL ID. The ACL ID refers to how the device identifies the ACL in its configuration.
Handle	Displays the ACL handle. The ACL Handle is the ACL name you defined.
Type	Displays the ACL type.
Last Modified Date	Displays the date and time the ACL was last modified.
Last Modified User	Displays the user who last modified the ACL. Keep in mind that the last modified user can be "N/A" to indicate that NCM does not know which user is responsible for this particular version of the ACL. If a user is shown, a link to the ACL Details page is provided, showing all activity NCM knows about that occurred prior to retrieving this version of the ACL. Because the user is only NCM' best guess, it is possible that other activity represents the actual cause for the ACL change.

Field	Description/Action
ACL Script	Displays the configuration scripting that defines the ACL. The ACL script represents the configuration lines necessary to define the ACL. You can select the following options: • New ACL — Opens the Run Command Script Task page, enabling you to use the existing ACL as a template. (Refer to "Creating ACLs" on page 711.) • Edit ACL — Opens the Run Command Script Task page, enabling you to edit the ACL. (Refer to "Running Command Scripts" on page 710.) • New ACL Template — Opens the New Command Script page, enabling you to save the existing ACL as a template. (Refer to "Creating ACL Templates" on page 717.) • Edit ACL Template — Opens the New Command Script page, enabling you to create a template that edits the current ACL. (Refer to "Creating ACL Templates" on page 717.)
ACL Application	If the ACL is applied, the ACL application is displayed. ACL applications include a list of configuration commands that define where the ACL is used. Keep in mind that some ACL types do not have any separate application scripting. These ACLs will not show any application script. You can select the following options: • Apply ACL — Opens the New Command Script page, enabling you to (re) apply the ACL. (Refer to "Creating ACLs" on page 711.) • Apply ACL Template — Opens the New Command Script page, creating an ACL application template. (Refer to "Creating ACL Templates" on page 717.)
Comments	Displays any comments about the ACL. You can select the following options: • Edit Comments — Opens the Edit ACL Page. • History — Opens the ACL History page. • View Related Config — Opens the Device Configuration page. (Refer to "Device Configuration Detail Page Fields" on page 206.)

Running Command Scripts

The Run Command Script task enables you to run command scripts. Refer to "Run Command Script Task Page Fields" on page 302 for information. Keep in mind that on the Run Command Script Task page, the following Task Options are shown:

- Command Script to Run — Indicates that you are running an ACL Edit Script from a specific ACL on the device. The ACL is identified both by its ID and Handle (in parentheses).
- Limit to script types — The script type is automatically set to "ACL Edit Script."
- Mode — Displays the device access mode, such as Cisco IOS configuration.
- Script — Displays the device-specific commands to run. The script to run is automatically populated, providing a copy of the existing ACL configuration. Keep in mind that if you are editing an ACL with applications, you will be provided with copies of the ACL application scripting, both before the ACL configuration scripting (to undo applications, if necessary) and after the ACL configuration scripting (to reapply the ACL). In many cases (such as IOS), to make an ACL configuration exactly match what you specify in a script, you will need to remove that ACL first, then put it back. (**Note**: The height and width of the Script box is controlled by settings in the Administrative Settings page, User Interface tab. If you use the scripting feature extensively, you may want to adjust these settings so that you can see the script without scrolling.)

Creating ACLs

To create a new ACL using an existing ACL as a template:

1. On the menu bar under Devices, click Inventory.
2. Select the device whose ACL parsing you want to enable. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. Click the Edit ACL option. The Run Command Script page opens. Refer to "Creating ACLs" on page 711.

The following fields in the Run Command Script Task page are automatically populated:

- Command Script to Run — Displays the type of script (Apply ACL) and the source ACL.
- Limit to script types — Displays the type of script (ACL Edit Script).
- Mode — Displays the correct script mode for applying an ACL on the device.
- Script — Displays a copy of the existing ACL application scripting. Be sure to check this thoroughly and make any necessary changes.

Note: You should not run ACL scripts line-by-line. ACL scripts can result in lost connectivity when run line-by-line.

If you add an ACL to a device using the same ACL ID that already exists, you are actually editing the existing ACL on that device.

Changing ACL Applications

To change ACL applications:

1. On the menu bar under Devices, click Inventory.
2. Select the device whose ACL parsing you want to enable. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. Click the View ACL option. The View ACL page opens. (Refer to "View ACL Page Fields" on page 708.)
5. Click the Apply ACL option. The Run Command Script page opens. (Refer to "Creating ACLs" on page 711.)

The following fields in the Run Command Script Task page are automatically populated:

- Command Script to Run — Displays the type of script (Apply ACL) and the source ACL.
- Limit to script types — Displays the type of script (ACL Application Script).
- Mode — Displays the correct script mode for applying an ACL on the device.
- Script — Displays the copy of the existing ACL application scripting.

Note: You should not run ACL scripts line-by-line. ACL scripts can result in lost connectivity when run line-by-line.

Batch Inserting ACL Lines

You can batch deploy ACL lines. NCM automatically adds the necessary lines to the appropriate ACL on single or multiple devices, based on ACL ID or ACL Handle. The following steps are specific to Cisco IOS devices only.

To batch insert a line into an ACL(s)

1. On the menu bar under Devices, select New Device Task and click Batch Insert ACL Line. The New Task - Run Command Script page opens. (Refer to "Creating ACLs" on page 711.)
2. You can select a device or group of devices on which to run the task. Upon selecting device or group, the page will update.
3. Command Script to Run — Choose either:

   a) Cisco IOS Insert Line into ACL by ACL ID

      - Id of ACL to insert line into — Enter the ACL ID that you want to add a line to. If you selected a group of devices, this adds a line to each device that contains an ACL that matches this ACL ID.
      - ACL line to insert — Enter the ACL line exactly as you would on the device.
      - Location to add line — Choose where to add the line. Options include first, last, and next-to-last.
      - Update Scripts — Click when you have completed the above variables.
      - Parameters — Optional parameters.
      - Script — This is the actual script that updates the ACL. The option to edit this script before execution makes this feature very flexible.

   b) Cisco IOS Insert Line into ACL by Handle

      - ACL Handle — Enter the ACL Handle that you want to add a line to. If you selected a group of devices, this will add a line to each device that contains an ACL that matches this ACL Handle.
      - ACL line to insert (without 'access-list {id}') — Enter the ACL line that you want to insert without any "access-list ACLID." The script will place this if necessary.

- Location to add line — Choose where to add this line. Options include first, last, and next-to-last.
- Update Scripts — Click when you have completed the above variables.
- Parameters — Optional parameters.
- Script — This is the actual script that will update the ACL. The option to edit this script before execution makes this feature very flexible.

Batch Deleting ACL Lines

You can batch remove ACL lines. NCM automatically removes the necessary lines to the appropriate ACL on single or multiple devices, based on the ACL ID or ACL Handle. The following steps are specific to Cisco IOS devices only.

To batch delete a line into an ACL(s)

1. On the menu bar under Devices, select New Device Task and click Batch Remove ACL Line. The New Task - Run Command Script page opens. (Refer to "Creating ACLs" on page 711".)
2. You can select a device or group of devices on which to run the task. Upon selecting a device or group, the page will update.
3. Command Script to Run — Choose either:
   a) Cisco IOS Remove Line from ACL by ACL ID
      - Id of ACL to delete line from — Enter the ACL ID that you want to remove a line from. If you have selected a group of devices, this will remove a line from each device ACL that matches this ACL ID.
      - ACL line to delete — Enter the ACL line exactly as it appears on the device. Keep in mind that some ACL lines have multiple space characters, for example: `access-list 139` and `deny ip host 192.168.139.2 any` contains three spaces between "deny" and "ip."
      - Update Scripts — Click when you have completed the above variables.
      - Parameters — Optional parameters.

- Script — This is the actual script that will update the ACL. The option to edit this script before execution makes this feature very flexible.

b) Cisco IOS Remove Line from ACL by Handle

- ACL Handle — Enter the ACL Handle that you want to delete a line from. If you selected a group of devices, this will delete a line from each device that contains an ACL that matches this ACL Handle.
- ACL line to delete (without 'access-list {id}') — Enter the ACL line that you want to delete without any "access-list ACLID." The script will place this if necessary.
- Update Scripts — Click this when you have completed the above variables.
- Parameters — Optional parameters.
- Script — This is the actual script that will update the ACL. The option to edit this script before execution makes this feature very flexible.

Commenting ACLs and Creating ACL Handles

NCM integrates an in-line commenting feature with ACL comments. This allows the comments for an ACL to be included in the configuration and for changes in the configuration comments to get included and reapplied to the ACL.

On devices that support in-line commenting, the ACLNAME: text following the double-comment character sequence that identifies a NCM in-line comment indicates the ACL Handle. On devices that do not support in-line commenting, the ability to move ACL comments to and from the configuration is not available. However, ACL comments and handles will continue to be maintained within the ACL.

To enter comments:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. Click the View ACL option. The View ACL page opens. Refer to "View ACL Page Fields" on page 708.
5. Click the Edit Comments option. The Edit ACL page opens.
6. Enter comments in the Comments field.
7. Edit the ACL Handle.
8. Click Save.

For devices that support NCM in-line commenting, changing the comments in the configuration will be reflected in the ACL comments.

Creating ACL Templates

In addition to directly creating scripts based on existing ACLs, you can use ACLs to form the basis for ACL command script templates. ACL templates can also be created for editing and applying ACLs.

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. Click the View ACL option in the Actions column. The View ACL page opens.
5. Click the New ACL Template link under the ACL Script. The New Command Script page opens. Refer to "New Command Script Page Fields" on page 560. The following fields in the New Command Script page are automatically populated:
   - Script Type — Displays the ACL script template type being created, including: ACL Creation Script, Edit ACL Script, or Apply ACL Script.
   - Mode — displays the correct script mode to run the ACL script on the device.
   - Script — Displays a copy of the existing ACL application scripting.

   Note: You can use the reserved variable "$tc_aclid_for_handle$" in your script when you need an ACL ID. When you run the script, you are prompted for the ACL handle. When the script is actually run on the device, each instance of this variable in the script will be replaced by the ACL ID on the device whose handle matches what you provided.

6. Enter a name for your new ACL creation script.
7. Edit the script. Refer to "Running Command Scripts" on page 710 for information.
8. Be sure to click Save Script when you are finished. When the script is saved successfully, the Script Search Results (Command Scripts) page opens. The script you added appears in the list and is highlighted. Keep in mind that a script does not run until you schedule it as a task.
9. Select the Run action.

10. Specify the Hostname or IP address of one a device that is capable of running the script.
11. Enter the ACL ID.
12. Save the task. When the task is complete, the new ACL is displayed on the View ACL Page. Refer to "View ACL Page Fields" on page 708.

Editing ACLs

To edit an ACL:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. Click the Edit ACL option for the ACL you want to edit. The Run Command Script page opens. Refer to "Creating ACLs" on page 711 for information.

When you click the Edit ACL link, the following fields in the Run Command Script task are automatically populated:

- Command Script to Run — Displays the type of script (Edit ACL) and the source ACL.
- Limit to script types — Displays the type of script (Edit ACL Script).
- Mode — Displays the correct script mode for editing an ACL on the device.
- Script — Displays the device-specific commands to run. Be sure to check this thoroughly and make any necessary changes.

Note: You should not run ACL scripts line-by-line. ACL scripts can result in lost connectivity when run line-by-line.

Deleting ACLs

When deleting ACLs for a single device, the ACLs on that device are listed. When deleting ACLs for a group of devices, all ACL handles on all devices in the group are listed, and the deletion of ACLs is by handle, not by ACL ID.

To delete ACLs:

1. On the Device ACLs page, select the ACLs you want to delete. Refer to "Device ACLs Page Fields" on page 706.
2. From the Options menu, click Delete. The Delete ACLs Task page opens. Refer to "Delete ACLs Task Page" on page 720. (You can also use the Delete ACLs option from the Edit & Provision drop-down menu.)

When you delete an ACL from a device configuration, the ACL no longer appears in the list of managed ACLs. Although the history of the ACL is still searchable using the Search For ACL option, the ACL history is not displayed when viewing device specific ACLs. There is no tracking of deleted ACLs from a device specific interface. To rollback the configuration of a deleted ACL, search for that ACL and then re-deploy it.

Keep in mind that ACLs that have no applications are deleted. However, ACLs with applications are not deleted. By default, NCM will not delete ACLs if they have an application script. An option is provided that forces the deletion of ACLs even if they have applications. If this is checked, all ACLs selected will be deleted.

Note: NCM does not guarantee that it will locate all applications of an ACL in the device's configuration. It is possible that an ACL has no application script, but is actually in use somewhere on the device. In such cases, the Delete ACLs task will attempt to delete the ACL (since it knows of no applications), resulting in unexpected device behavior.

Delete ACLs Task Page

The Delete ACLs task enables you to delete ACLs. When you are finished click Save Task.

Field	Description/Action
Task Name	Displays Delete ACLs. You can enter a different task name if applicable.
Applies to	You can select the following options: • Device — Enter the host name or IP address of the device (the default). • Group — Select a group or groups from the list. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file.
Start Date	You can select the following options: • Start As Soon As Possible — If selected, the default, the multiple task job will start as soon as possible. • Start At — If selected, you can click the calendar icon to open the calendar where you can select the date and time to start the multiple task job.
Comments	Add any comments about the multiple task job.
Task Options	
Session Log	Check the “Store complete device session log” box to store a debugging log. This is useful when debugging a failed snapshot, however large amounts of data can be stored.

Field	Description/Action
ACLs to delete	You can select the following options: • Show ACLs without applications — Displays only ACLs without known applications (the default). • Show all ACLs — If selected, all ACLs, including the ACL IDs, with handles in parentheses, are displayed. You can select any number of ACLs from the list. (Note: If you are running this task against a group of devices, the list contains all ACL handles found on all devices in the group. There is no option to filter the list by ACLs without applications.)
Delete ACLs even with applications check box	If checked, selected ACLs are deleted even if they have known applications.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options

Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Server page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Server Page Fields" on page 80 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Field	Description/Action
Pre-Task / Post-Task Snapshot Options Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 58 for information.)	
Pre-Task Snapshot	Select one of the following options: • None (the default) • As part of task
Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NCM Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NCM will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times

Field	Description/Action
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Chapter 21: Troubleshooting

Use the following table to quickly locate information.

Topic	Refer to:
Driver Discovery Failed	"Driver Discovery Failed" on page 726
Device Snapshot Failed	"Device Snapshot Failed" on page 727
No Real-Time Change Detection via Syslog	"No Real-Time Change Detection Via Syslog" on page 728
Automation Tasks	"Automation Tasks" on page 729

For information on sending Troubleshooting information to Cisco, refer to "Send Troubleshooting Page Fields" on page 23.

Driver Discovery Failed

If you cannot discover a driver for a device:

1. Make sure that the device you are trying to discover is a supported device model and OS version. Refer to the *Device Driver Reference for Network Compliance Manager* for a list of the currently supported devices. If the device is not supported, contact Customer Support. If the device is supported, go to Step 2.
2. Telnet and/or SSH to the device from the NCM server. An easy way to verify that CiscoWorks Network Compliance Manager (NCM) can Telnet or SSH to a device is to click the Telnet or SSH link for the device on the Device List page. Refer to "Inventory Page Fields" on page 217 for information. NCM automatically attempts to login to the device. If you cannot login to the device, this could be caused by incorrect access lists on the device, incorrect password information, or network connectivity issues. Contact Customer Support. If you can Telnet and/or SSH to the device, but the Discover Driver task still fails, go to Step 3.
3. Check to see if you have read-only SNMP enabled on the device. If read-only SNMP is enabled, using this OID, try to contact to the device via read-only SNMP from the NCM server. Make sure you use the community string you configured for the device within NCM. If you do not want to enable read-only SNMP, you can manually select the driver from the driver drop-down list when you add or edit devices. Refer to "Editing Device Configuration Data" on page 208 for information. Once you have enabled read-only SNMP, login to NCM, select the device you are trying to add, and click Edit Device. Update the device with the correct read-only SNMP community string and click Discover Driver. If the Discover driver task still fails, go to Step 4.
4. Login to NCM. On the menu bar, select Admin and click Troubleshooting. In the list box, select dataconnection, deviceaccess, and devicedata. Set the level to Trace (most message). Click Submit. Click the device you are attempting to discover and then click Discover Driver. Once the Discover Driver task fails, on the menu bar select Admin and click Troubleshooting. Click Send Troubleshooting Information. In the comments section, specify what is failing and the device model and OS version. Refer to "Send Troubleshooting Page Fields" on page 23 for information.

Device Snapshot Failed

If a device snapshot failed:

1. Make sure the device you are trying to snapshot is a supported device model and OS version for NCM. Refer to the *Device Driver Reference for Network Compliance Manager* for a list of the currently supported devices. If the device is not supported, contact Customer Support. If the device is supported, go to Step 2.
2. Make sure that there is a device driver assigned to the device. On the Device List page, click the problem device. Refer to "View Menu Options" on page 229 for information. Scroll down to the Driver Name field and check if it has a value. If there is no driver, contact Customer Support. If there is a driver, click the Discover Driver link. If the Snapshot task still fails, go to Step 3.
3. Telnet and/or SSH to the device from the NCM server. An easy way to verify that NCM can Telnet or SSH to a device is to click the Telnet or SSH link for the device on the Device List page. Refer to "Inventory Page Fields" on page 217 for information. If you cannot login to the device, this could be caused by incorrect access lists on the device, incorrect password information, or network connectivity issues. Contact Customer Support. If you can Telnet and/or SSH to the device, but the Discover driver task fails, go to Step 4.
4. Check to see if you have read-only SNMP enabled on the device. If read-only SNMP is enabled on the device, using this OID, try to contact the device via read-only SNMP from the NCM server. Make sure you use the community string you configured for the device within NCM. If you do not want to enable read-only SNMP, you can manually select the driver from the driver drop-down list when you add or edit devices. Refer to "Editing Device Configuration Data" on page 208 for information. Once you have enabled read-only SNMP, login to NCM, select the device you are trying to add, and click Edit Device. Update the device with the correct read-only SNMP community string and click Snapshot. If the Snapshot task still fails, call Customer Support.

No Real-Time Change Detection Via Syslog

If there is no real-time change detection via Syslog:

1. Make sure that the device you are trying to snapshot is a supported device model and OS Version for NCM. Refer to the *Device Driver Reference for Network Compliance Manager* for a list of the currently supported devices. If the device is not supported, contact Customer Support. If the device is supported, go to Step 2.
2. Make sure the Syslog settings are configured correctly so that Syslog messages are reaching the NCM server. Initiate an event that will trigger a Syslog change message to be sent to NCM.
3. Make sure that the device/OS combination supports real-time change detection via Syslog. Refer to the *Device Driver Reference for Network Compliance Manager* for device configuration information. If possible, verify on the vendor's website that Syslog notification of change is available in this device and OS. If the device does not support real-time change detection via Syslog, go to Step 4.
4. There is another method by which NCM provides real-time change detection: AAA logging. Check to see if you have AAA change detection enabled. Refer to "Configuration Mgmt Page Fields" on page 58 for information. If you are using AAA, make sure that the device supports real-time change detection via AAA.

Automation Tasks

The difficult part of any automation task is not the automation itself, but trying to determine the cause of failure if an automation task fails. NCM provides detailed troubleshooting capabilities to help you quickly identify reasons for failure and resolve them.

NCM provides a detailed device session log from any device task. As a result, you can see what NCM is sending to the device and how the device is responding.

1. Log into NCM.
2. On the main menu bar under Devices and select New Device Task and click Run Command Script. The New Task - Command Script page opens.
3. In the Applies to field, enter a device hostname or IP address on which you are allowed to make configuration changes.
4. Under Task Options — Session Log, check the “Store complete device session log” box.
5. Under Task Options — Command Script to Run, select the command script you want to run from the drop down menu.
6. Specify the mode to run in. For example, if this is an IOS device, select Cisco IOS Configuration.
7. Enter the commands you want to send to the device.
8. Click the Save Task button.

As the task runs, you will see the output of the NCM <-> device interaction. You should be able to determine:

- What NCM sent to the device.
- What NCM expected to receive from the device.
- What NCM actually received from the device.

Appendix A: Command Line Reference

There are several ways to run the Command Line Interface (CLI).

1. At the top of any page, click Connect under the left-hand Search tab. This runs the Telnet/SSH Proxy. When you see the prompt, you can enter CLI commands. You can also connect to devices on your network. Enter exit and close the window when you are finished.

   If you use the Telnet/SSH Proxy to connect directly to devices, you remain in the Telnet/SSH Proxy when you exit the device. Unless you enter exit again, you can enter CLI commands and connect to other devices.

2. Click Start → Programs → CWNCM → CWNCM Client.

3. Click Start → Run and enter cmd. A command line window opens. At the prompt, enter:

   `c:\rendition\client\runclient`

   where `c:\rendition` is assumed to be where you installed NCM. If you installed the software in a different folder, use that folder name. If prompted, enter your user name and password. You should now be logged in and see the CLI prompt.

Note: The CLI is case-sensitive. Enter all commands and options in lowercase.

CLI Help is available online using the following commands:

- At the CLI prompt, enter: `help`. You should see a list of nearly all the CLI commands in alphabetical order. For example, to see Help for the Import command, enter: import. (Note: There is no Help text for the help or the exit/quit commands.)
- At the CLI prompt, enter: `help del group`. The command help <command name> returns detailed information on that command, including the name, a synopsis, a description, and examples.
- When you are finished with the command line, enter: exit. Depending on the type of session you started, you may need to enter exit again and manually close the window.

Note: You can also enter the help command and just the first word of a command to return a list of all the commands that begin with the same first word.

The type conventions used in the CLI Help text have specific meanings. The following table lists the conventions and their meanings.

Convention	Meaning
>	A single right angle bracket indicates the command prompt where you enter your commands.
-	A dash precedes a command option.
< >	Angle brackets surround variable text that you must fill in, such as an IP address. Do not include the angle brackets.
[ ]	Square brackets delineate one or more optional elements.
|	A vertical pipe separates arguments within brackets. Include only one argument.

CLI Commands

The following table lists the CLI commands (also called scripting interface commands). Asynchronous commands only return if the task was scheduled successfully. You must look at the task status to see if the commands completed successfully.

Note: For information on using CLI commands with the Java or Perl APIs, refer to the either the *Java API Reference Guide* or the *Perl API Reference Guide* available from the Docs option.

Command	Asynchronous
activate device	No
add advanced script	No
add authentication	No
add command script	No
add device	No
add device to group	No
add diagnostic	No
add event	No
add group	No
add group to parent group	No
add ip	No
add parent group	No
add system message	No
add user	No
annotate access	No
annotate config	No

Command	Asynchronous
configure syslog	No
connect [in Proxy Interface only]	No
deactivate device	No
del access	No
del authentication	No
del device	No
del device data	No
del device from group	No
del drivers	No
del event	No
del group	No
del group from parent group	No
del ip	No
del script	No
del session	No
del system message	No
del task	No
del user	No
deploy config	Yes
diff config	No
discover driver	Yes
discover drivers	Yes
exit	No
get snapshot	No

Command	Asynchronous
help	No
import	No
list access	No
list access all	No
list basicip	No
list config	No
list config all	No
list config id	No
list device	No
list device family	No
list device group	No
list device id	No
list device model	No
list device software	No
list device type	No
list device data	No
list deviceinfo	No
list diagnostic	No
list drivers	No
list event	No
list groups	No
list icmp	No
list int	No
list ip	No

Command	Asynchronous
list ip all	No
list module	No
list ospfneighbor	No
list partition	No
list port	No
list routing	No
list script	No
list script id	No
list script mode	No
list session	No
list site	No
list system message	No
list task	No
list task all	No
list topology	No
list topology ip	No
list topology mac	No
list user	No
list view	No
list vlan	No
list vlan ports	No
mod advance script	No
mod authentication	No
mod command script	No

Command	Asynchronous
mod device	No
mod diagnostic	No
mod group	No
mod ip	No
mod module	No
mod port	No
mod task	No
mod unmanaged device	No
mod user	No
passwd	Yes
pause polling	No
ping	Yes
quit	No
Reload drivers	No
reload server options	No
replication start	No
replication status	No
replication stop	No
replication sync	No
resume polling	No
run command script	No
run diagnostic	Yes
run script	Yes
show access	No

Command	Asynchronous
show advacned script	No
show basicip	No
show config	No
show device	No
show device config	No
show device latest diff	No
show deviceinfo	No
show diagnostic	No
show event	No
show group	No
show icmp	No
show int	No
show ip	No
show latest access	No
show module	No
show ospfneighbor	No
Show Permission	No
show polling status	No
show port	No
show routing	No
show script	No
show session	No
show session commands	No
show snapshot	No

Command	Asynchronous
show system message	No
show task	No
show topology	No
show user	No
show version	No
ssh [in Proxy Interface only]	No
synchronize	Yes
telnet [in Proxy Interface only]	No
test config	No
test software	No
test view	No
traceroute	Yes
version	No

Appendix B: Command Permissions

Users must be explicitly granted the corresponding command permission for each action they want to perform, such as viewing a Web page or executing a command. A set of command permissions creates a command permission role. You can then apply the role to a user group to set the command permissions for that given user group. Refer to "New User Role Page Fields" on page 263 for more information.

Note: CiscoWorks Network Compliance Manager (NCM) includes four types of permissions, including Command permissions, Modify Device permissions, Script permissions, and View Device permissions. Some Command permissions require one or more of the other permissions. Refer to "Command Permission Definitions" on page 744 for information.

Granting Command Permissions

To grant Command permissions:

1. On the menu bar under Admin, click User Roles & Permissions. The User Roles & Permissions page opens.
2. Click the New User Role link at the top of the page. The New User Role page opens. Refer to "Adding User Roles" on page 261 for information.

List of Commands

Activate/Deactivate Device
Add Device
Add Device Group
Add Device To Group
Add Event
Add SNMP Trap Config
Admin Settings
Annotate Device Configuration
Authorize Concurrent Telnet/SSH Sessions
Batch Edit Device
Change Device Password
Check Configuration Policy Compliance
Configure Syslog
Data Pruning
Deduplication
Delete Access
Delete Device
Delete Device Configuration
Delete Driver
Delete Session
Delete Software Compliance
Delete Software Image
Delete System Event
Delete Task
Deploy Software
Detect Network Devices
Discover Device Driver
Edit ACL
Edit ACL Comments
Edit Config [Changed By] User
Edit Device
Edit Inactive Device
Edit Task
Edit User
Email Report
External Authentication Setup
Generate Summary Reports
Import Devices and Passwords
Manage License
Manage Software Compliance
Manage Software Image
Manage System Report
Manage Template
Manage User
Manage User Group
Manage User Role
Modify Device Configuration
Modify SecurID
Multi-Task Project
Override Workflow Approvals
Reload Device Task
Resolve FQDNs
Run Command Script
Run Diagnostic
Run External Application
Run ICMP Test
Schedule Recurring Task
Schedule Non-Recurring Task
Synchronize Recurring Task
Take Snapshot
Telnet/SSH Client
Troubleshooting
Update Device Comments
Update Device Ticket
Workflow Setup
View ACL
View Command Script
View Configuration Policy Event
View Deployed Software
View Configuration Policy
View Device Configuration
View Device Diagnostic
View Device Information
View Diagnostic Script
View Driver
View Event Rule
View Full Device Configuration

(*continued on next page*)

List SysOIDs
Manage ACL
Manage Command Script
Manage Configuration Policy
Manage Device Password Rule
Manage Diagnostic Script
Manage Event Rule
Manage IP Address
View Script & Diagnostic Result
View SecurID
View Session
View Software Image Archive
View Task
View Template
View User Information
View Workflow Setup

Command Permission Definitions

Command Permission	Description
Activate/Deactivate Device	Enables you to activate or deactivate devices.
Add Device	Enables you to add devices to the NCM system. This permission includes adding devices via the Add Device Wizard.
Add Device Group	Enables you to create device groups. To create a public device group, you must also be granted the Administer Device Groups permission.
Add Device To Group	Enables you to add devices to a device group. Devices must already exist in the NCM database.
Add Event	Enables you to use the New Message option from the Edit & Provision menu.
Add SNMP Trap Config	Enables you to configure SNMP traps and run the “add SNMP trap config” CLI command (which in turn adds to the config option “snmp/traps/global”).
Admin Settings	Enables you to change Admin settings. Keep in mind that there are some Admin settings that require additional permissions, such as Workflow Setup and External Authentication Setup.
Administer Device Groups	Enables you to manage device groups, including adding, modifying, and removing parent and public groups.
Annotate Device Configuration	Enables you to annotate device configurations.
Authorize Concurrent Telnet/ SSH Sessions	Enables you to override the prevention of multiple proxy connections to a device.
Batch Edit Device	Enables you to modify multiple devices during a batch edit.
Change Device Password	Enables you to schedule a task to change a single device’s password. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.

Command Permission	Description
Change Device Password (Group)	Enables you to schedule a task to change passwords for a device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.
Check Configuration Policy Compliance	Enables you to run the Check Configuration Policy Compliance task. The Check Policy Compliance task enables you to determine if devices are in compliance with either configuration policies or software compliance policies.
Clear Device Reservation	Enables you to clear device reservation conflicts that appear on the Activity Calendar.
Configure Syslog	Enables you to schedule a task to configure a device's Syslog settings. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Configure Syslog (Group)	Enables you to schedule a task to configure a group of devices' Syslog settings. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.
Data Pruning Task	Enables you to schedule the Data Pruning task for a single device. Data pruning removes obsolete files, diagnostics, events, and tasks.
Data Pruning Task (Group)	Enables you to schedule the Data Pruning task for a group of devices. Data pruning removes obsolete files, diagnostics, events, and tasks.
Deduplication	Enables you to remove or deactivate a single device, such that the device's interfaces only occur once within the NCM database.
Deduplication (Group)	Enables you to remove or deactivate a group of devices, such that the devices' interfaces only occur once within the NCM database.
Delete Access	Enables you to delete a device's access log.
Delete Device	Enables you to permanently delete a device from the NCM database.

Command Permission	Description
Delete Device Configuration	Enables you to remove device configurations.
Delete Device Group	Enables you to delete device groups.
Delete Driver	Enables you to delete device drivers.
Delete Event Rule	Enables you to delete Event Notification & Response rules.
Delete Session	Enables you to delete Telnet/SSH session records.
Delete Software Compliance	Enables you to delete software compliance records.
Delete Software Image	Enables you to delete software images from the NCM software repository.
Delete System Event	Enables you to delete system events.
Delete Task	Enables you to delete tasks.
Deploy Software	Enables you to schedule a task that deploys device software to a single device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Deploy Software (Group)	Enables you to schedule a task that deploys device software to a device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.
Detect Network Devices	Enables you to scan IP addresses and automatically add unknown devices to the NCM database.
Detect Network Devices (Group)	Enables you to scan IP addresses and automatically add unknown device groups to the NCM database.
Discover Device Driver	Enables you to discover a device's driver. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Discover Device Driver (Group)	Enables you to discover a group of devices' driver. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.

Command Permission	Description
Edit ACL	Enables you to edit ACL scripts.
Edit ACL Comments	Enables you to edit ACL comments.
Edit Config [Changed By] User	Enables you to reset the [changed by] user for a device configuration. It is recommended that this permission be set to Admin user only.
Edit Device	Enables you to change devices group membership, access device settings and other attributes. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Edit Device Group	Enables you to edit device groups, including adding devices to and removing devices from the device group.
Edit Inactive Device	Enables you to edit the Comments field for inactive devices.
Edit Task	Enables you to edit scheduled tasks.
Edit User	Enables you to edit user profiles. By default, users can only edit their own user profiles.
Email Report	Enables you to schedule tasks that run various reports and send email to specified recipients.
External Authentication Setup	Enables you to setup external authentication, such as ActiveDirectory, TACACS+, SecurID, and RADIUS.
Generate Summary Reports	Enables you to schedule tasks that generate Summary reports for a single device.
Generate Summary Reports (Group)	Enables you to schedule tasks that generate Summary reports for a group of devices.
Import Devices & Passwords	Enables you to import devices and device authentication information.
List SysOIDs	Enables you to list sysOIDs of supported devices.
Manage ACL	Enables you to manage device ACLs, including deleting ACLs.
Manage Command Script	Enables you to create, modify, and delete command scripts.

Command Permission	Description
Manage Configuration Policy	Enables you to create, edit, and delete configuration policies.
Manage Device Password Rule	Enables you to create, edit, and delete device password rules.
Manage Diagnostic Script	Enables you to create, edit, and delete diagnostic scripts.
Manage Event Rule	Enables you to create, edit, and delete Event Notification & Response rules.
Manage IP Address	Enables you to add, edit, and delete device IP addresses.
Manage License	Enables you to view and update NCM license information.
Manage Software Compliance	Enables you to add and/or edit software compliance information.
Manage Software Image	Enables you to add, edit, and delete software images.
Manage System Report	Enables you to change the order of the System and User reports and delete System reports.
Manage Template	Enables you to create, edit, and delete script templates.
Manage User	Enables you to create, edit, and delete NCM users.
Manage User Group	Enables you to create, edit, and delete user groups. Because user permissions are managed through this interface, this permission should be granted with care.
Manage User Role	Enables you to add, edit, and delete user roles.
Modify Device Configuration	Enables you to schedule a task that deploys an edited configuration to a device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Modify SecurID	Enables you to modify SecurID token Information.
Multi-Task Project	Enables you to modify a multi-task project.
Override Workflow Approvals	Enables you to run a task without going through the Workflow approval process.

Command Permission	Description
Reload Device Task	Enables you to reload (reboot) a device via a reload script provided in the driver. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Resolve FQDNs	Enables you to schedule the Resolve FQDN task that resolves a device's fully qualified domain name.
Resolve FQDNs (Group)	Enables you to schedule the Resolve FQDN task that resolves a device group's fully qualified domain name.
Run Command Script	Enables you to schedule the Run Command Script task that executes a script on a specified device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed. It also requires the Script permission for the selected script.
Run Command Script (Group)	Enables you to schedule the Run Command Script task that executes a script on a specified device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed. It also requires the Script permission for the selected script.
Run Diagnostic Script	Enables you to schedule the Run Diagnostic task that executes a diagnostic script on specified device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Run Diagnostic Script (Group)	Enables you to schedule the Run Diagnostic task that executes a diagnostic script on specified device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.
Run External Application	Enables you run a user-defined external application. This permission should be granted with care.
Run ICMP Test	Enables you to schedule the Run ICMP Test task that executes a ICMP test on a device.
Run ICMP Test (Group)	Enables you to schedule the Run ICMP Test task that executes a ICMP test on a device group.

Command Permission	Description
Synchronize Startup & Running	Enables you to schedule the Synchronize Startup & Running task that brings the startup & running configuration in sync for a targeted device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Synchronize Startup & Running (Group)	Enables you to schedule the Synchronize Startup & Running task that brings the startup & running configuration in sync for a targeted device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission of the device group on which the command is executed.
Take Snapshot	Enables you to schedule the Take Snapshot task that takes a device's configuration snapshot.
Take Snapshot (Group)	Enables you to schedule the Take Snapshot task that takes a device group's configuration snapshot.
Telnet/SSH Client	Enables you to access a device using Telnet or SSH via the NCM proxy service.
Troubleshooting	Enables you to access the Troubleshooting page, send troubleshooting information via email, and change the NCM server's logging level.
Update Device Comments	Enables you to change a device's comments.
Update Device Ticket	Enables you to configure NCM to communicate with third-party ticketing systems, such as Remedy.
View ACL	Enables you to view ACL scripts.
View Command Script	Enables you to view Command scripts.
View Configuration Policy & Compliance	Enables you to view configuration policy and compliance information.
View Configuration Policy Event	Enables you to view configuration policy event details. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission of the device for which the command is executed.
View Deployed Software	Enables you to view deployed software, as opposed to the software archive.

Command Permission	Description
View Device Configuration	Enables you to view device configurations. Keep in mind that sensitive information, such as passwords and community strings, are masked.
View Device Diagnostic	Enables you to view device diagnostics.
View Device Information	Enables you to view all information related to device, except the device configuration.
View Diagnostic Script	Enables you to view diagnostic script details.
View Driver	Enables you to view driver details.
View Event Rule	Enables you to view the event rules list.
View Full Device Configuration	Enables you to view unmasked device configurations. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission of the device for which the command is executed upon.
View Script & Diagnostic Result	Enables you to view the result details of a command script or diagnostic task.
View SecurID	Enables you to view SecurID token Information.
View Session	Enables you to view Telnet/SSH session command and response history.
View Software Image Archive	Enables you to view software images stored in the NCM archive.
View Task	Enables you to view task details.
View Template	Enables you to view script template details.
View User Information	Enables you to view user information.
Workflow Setup	Enables you to configure Workflow approval rules.

Appendix C: Sample Scripts

This appendix contains sample scripts.

Sample PERL Script #1

This PERL script sets all FastEthernet interfaces to full duplex on Cisco 2600s and 7200s.

```
#
# Sample Script to set all FastEthernet interfaces
# to full duplex on Cisco 2600s and 7200s
#
use Socket;

$iaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaddr);
socket(DEV, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
connect(DEV, $sin) || die "Can't connect to $tc_device_hostname$: $!\n";

sendln("");
sendln("$tc_device_password$");
sendln("en");
sendln("$tc_device_enable_password$");
sendln("conf t");

for $name (split(" ","$tc_device_port_name_list$")) {
  if ($name =~ /FastEthernet/)
      sendln("interface $name");
      sendln("duplex full");
      sendln("exit");
   }
}
sendln("exit");
sendln("exit");
sendln("");
close(DEV);
exit;
```

(continued on next page)

```
sub sendln {
  my ($line) = @_;
  $line .= "\n";
  syswrite(DEV,$line,length($line));
  while (<DEV>) {
   print;
   die "Failed to execute command\n"
     if (/\% (Unknown|Unrecognized|Invalid|.*uthorization failed)/);
   last if (/name:/ ||
           /word:/ ||
           />/ ||
           /\#/);
   }
}
```

Sample PERL Script #2

This PERL script sets all interfaces to no IP-directed broadcast.

```
#
# Sample Script to set all interfaces
# to no ip directed broadcast
#
use Socket;

$iaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaddr);
socket(DEV, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
connect(DEV, $sin) || die "Can't connect to $tc_device_hostname$: $!\n";

sendln("");
sendln("$tc_device_password$");
sendln("en");
sendln("$tc_device_enable_password$");
sendln("conf t");

for $name (split(" ","$tc_device_port_name_list$")) {
   sendln("interface $name");
   sendln("no ip directed-broadcast");
   sendln("exit");
}
sendln("exit");
sendln("exit");
sendln("");
close(DEV);
exit;

sub sendln {
  my ($line) = @_;
  $line .= "\n";
  syswrite(DEV,$line,length($line));
  while (<DEV>) {
    print;
    die "Failed to execute command\n"
      if (/\% (Unknown|Unrecognized|Invalid|.*uthorization failed)/);
    last if (/name:/ ||
            /word:/ ||
           />/ ||
          /\#/);
```

Sample Expect Script

This Expect script modifies the banner to contain a given string only if the banner does not already contain the string.

```
#
# Sample Script to set the banner only if
# it is not already set correctly
#
spawn telnet $tc_device_ip$
set banner "****Unauthorized Access Prohibited****"
expect {
   $banner {
      puts "\nBanner is already set correctly\n"
      exit 0
   } "word:"
}
send "$tc_device_password$\r"
expect ">"
send "en\r"
expect "word:"
send "$tc_device_enable_password$\r"
expect "\#"
send "config t\r"
expect "\#"
send "banner motd /$banner/\r"
expect "\#"
send "exit"
```

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W