QUICK START GUIDE

Quick Start Guide for CiscoWorks Network Compliance Manager, 1.2.1

Text Part Number: OL-10194-04

1 Getting Started

CiscoWorks Network Compliance Manager (NCM), Release 1.2.1 provides network configuration and change features, policy-based workflows, compliance reporting capabilities, and APIs. NCM includes integration with CiscoWorks—you can start NCM from the CiscoWorks HomePage window and it works with other CiscoWorks applications such as the LMS bundle through the CommonServices Device Credential Repository (DCR).

This guide provides information on:

For complete information on how to use NCM, see the *User Guide for Network Compliance Manager, 1.2.1*.

Note All documentation, including this document and any or all of the parts of the NCM documentation set, *might* be upgraded over time. Therefore, we recommend you access the NCM documentation set using the Cisco.com URL: http://www.cisco.com/en/US/products/ps6923/tsd_products_support_series_home.html.

In addition, the Docs tab visible from within Network Compliance Manager *might* not include links to the latest documents.

2 System Requirements

This section includes the following:

Protocols and Ports

NCM communicates with devices using a combination of the following protocols and ports as described in Table 1. 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.

Table 1 NCM Supported Protocols and Corresponding Ports

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.

Table 1 NCM Supported Protocols and Corresponding Ports (continued)

Protocol/Port	From/To
RMI (port 4444)	From the AAA server to the NCM server. You can change this by editing the NCM configuration files.
NCM Server and the NCM cIlent	
HTTPS (port 443)	From the NCM client to the NCM server. You can change this by editing the NCM configuration files.
Telnet (port 23 for Windows or port 8023 for Solaris)	From the NCM client to the NCM server. You can change this from the Administrative Settings option.
SSH (port 22 for Windows or port 8022 for Solaris)	From the NCM client to the NCM server. You can change this from the Administrative Settings option.

Linux Server 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 depending on the size of the network.

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.

Table 2 Requirements for the Application Server on the Linux Platform

OS	RedHat Linux AS 3.0, Update 2 SUSE Linux Enterprise 9.0
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	14 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex
Applications	• Adobe Acrobat Reader 4.0 or higher (for viewing documentation) • KDE Desktop Manager • Mozilla Firefox 1.0+

Table 3 Requirements for the Database Server on the Linux Platform

Supported Databases	One of the following: • Microsoft SQL Server 2000 (SP 2) • Microsoft SQL Server 2005 • MySQL Max 3.23.55 (included with NCM) • Oracle 9.2 (32 bit) • Oracle 10.2
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

Table 4 Requirements for the Application and Database on the Same Server on the Linux Platform

OS	One of the following: • RedHat Linux AS 3.0, Update 2 • SUSE Linux Enterprise 9.0
Database	MySQL Max 3.23 (included)
CPU	Dual Processor Intel Xeon or equivalent, 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

Note When installing NCM on a Linux platform, Nmap 3.81 is required for Nmap scanning when running the Detect Network Devices task.

Summary Reports

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 Server 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 depending on the size of the network.

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.

Table 5 Requirements for the Application Server on the Solaris Platform

OS	Solaris 9 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
Applications	• Adobe Acrobat Reader 4.0 or higher (for viewing documentation) • The X Window System, X11 (also known as OpenWindows) • Mozilla Firefox 1.0+

Table 6 Requirements for the Database Server on the Solaris Platform

Supported Databases	One of the following: • Microsoft SQL Server 2000 (SP 2) • Microsoft SQL Server 2005 • MySQL Max 3.23.55 (included with NCM) • Oracle 9 • Oracle 10
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

Table 7 Requirements for the Application and Database on the Same Server on the Solaris Platform

OS	Solaris 9 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

Table 7 Requirements for the Application and Database on the Same Server on the Solaris Platform (continued)

Disk	36 GB, Dual Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Note When installing NCM on a Solaris platform, Nmap 3.81 is required for Nmap scanning when running the Detect Network Devices task.

Summary Reports

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 Linux and can open Excel files:

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

Windows Server 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 depending on the size of the network.

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.

Table 8 Requirements for the Application Server on the Windows Platform

OS	Windows Server 2003 Enterprise Edition (recommended) Windows Server 2003 Standard Edition Windows 2000 Server with SP4 Windows 2000 Advanced Server with SP4
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Disk	10 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex
Applications	• Adobe Acrobat Reader 4.0 or higher (for viewing documentation) • Microsoft Excel 2000 or higher (for viewing Summary Reports) • Microsoft Internet Explorer 5.5 or higher or Mozilla Firefox 1.0 or higher

Table 9 Requirements for the Database Server on the Windows Platform

Supported Databases	One of the following: • Microsoft SQL Server 2000 (SP 2) • Microsoft SQL Server 2005 • MySQL Max 3.23.55 (included with NCM) • Oracle 9.2 (32 bit) • Oracle 10.2
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

Table 10 Requirements for the Application and Database on the Same Server on the Windows Platform

OS	Windows Server 2003 Enterprise Edition (recommended) Windows Server 2003 Standard Edition Windows 2000 Server with SP4 Windows 2000 Advanced Server with SP4
Database	MySQL Max 3.23 (included)
CPU	Dual Processor Intel Xeon or equivalent, 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 are required for Nmap scanning when running the Detect Network Devices task.

NCM and LMS Co-residency Requirements

The following are the recommended requirements when you are enabling co-residency of NCM and CiscoWorks LAN Management Solution (LMS):

- Operating System on the Application Server: Microsoft Windows 2003
- Server Hardware: At least a Xeon (or a Dual Core) Processor with 8 GB of RAM.

For detailed information on NCM and LMS co-residency, see the *Getting Started Guide for Network Compliance Manager and LMS Co-residency.*

NCM High Availability System Requirements

The NCM High Availability Distributed System is a multi master system where the data from each NCM Core is available to all other NCM Cores. This collection of NCM Cores is called an NCM mesh. This configuration helps provides a comprehensive view of your data and allows for redundant data and failover in the event of a problem with the NCM Core. Each NCM Core consists of an NCM Management Engine, its associated services (Syslog and TFTP), and a single database.

Note If you intend to install the NCM High Availability Distributed System, keep in mind that it only supports the Oracle 9.2 database server. If you are running Oracle 10.2 on the Core database server, you cannot upgrade to the NCM High Availability Distributed System.

NCM Gateway Requirements

The Network Compliance Manager Gateway enables a NCM Core to manage servers that are behind one or more NAT devices or firewalls. The NCM Gateway is supported on the following platforms:

- RedHat Linux 3.0 AS
- RedHat Linux 4.0 AS
- SuSE Linux 9.0 ES
- SunOS 5.9
- SunOS 5.10

3 Installing NCM

Make sure you have the requisite equipment and files before installing NCM:

- A Windows, Linux, or Solaris server
- Manageable devices and their CLI passwords and SNMP community strings
- An NCM product license
- The NCM DVD or download URL

Note If you are upgrading from NCM 1.2 to NCM 1.2.1, see the "Upgrading from NCM 1.2 to NCM 1.2.1" section on page 22.

Note We sometimes release patches after the original release of a product. Therefore, you should review the following site on Cisco.com for any updates.

http://www.cisco.com/cgi-bin/tablebuild.pl/cwncm-crypto

Before Installing on a Linux Server

If you are installing NCM on a Linux server, enter the following commands to mount a DVD drive. You must login as root.

Step 1 #> mount /mnt/cdrom

Step 2 #> cd /mnt/cdrom

Step 3 #> cd linux/standard

Step 4 #> ./setup.bin

The Introduction window appears.

Before Installing on a Solaris Server

If you are installing NCM on a Solaris server, do the following:

Step 1 #> mount /mnt/cdrom

Step 2 #> cd /mnt/cdrom

Step 3 #> cd solaris/standard

Step 4 #> ./setup.bin

The Introduction window appears.

Before Installing on a Windows Server

If you are installing NCM on a Windows server, do the following:

Step 1 Insert the NCM DVD into the drive. Click windows/standard/setup.exe.

The InstallAnywhere Self Extractor opens and the Introduction window displays.

Installation Procedures

The following steps guide you through the installation process.

Step 1 From the Introduction window, review the NCM database requirements information and click Next.

The System Requirements window appears.

Step 2 Confirm that you have met all system requirements and click Next.

The License Agreement window appears.

Step 3 Review the license agreement, click the I accept the terms of the License Agreement option, and click Next.

The Choose Install Set window appears.

Step 4 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.
- Client and Server using SQL Server 2005—Click this option and then click Next if you already have an SQL Server 2005 running on your network. Go to Step 8.
- Client and Server using MySQL Max—Click this option and then click 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 7.
- Client and Server using Oracle —Click this option and then click Next if you already have an Oracle server running on your network. Go to Step 7.
- Client and Connector—Click this option to install the stand-alone client and the NCM connector. Go to Step 6.

Keep in mind that if you are using an existing database server, you will be prompted for the database server's hostname, port and the username and password to create a new database.

Note When installing SQL Server, set Authentication to mixed mode. Set Collation to SQL_Latin1_General_CP1_CI_AS (the default). In addition, the database must not be case-sensitive and must use local authentication. NCM requires a working SA 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 NCM 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 5 From the Product License folder window, enter the path to the location of the folder that contains the product license files (.lic). Click Choose to browse your system for the location of the folder. If you want to copy the product license files to your NCM install folder at a later time, click Next.

Step 6 From the Choose install folder window, enter the path to the folder where you would like to install NCM or accept the displayed folder and click Next.

Step 7 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. (You will be prompted to accept the Microsoft SQL Server license agreement.)

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. Go to Step 8.

If you want to install Oracle, click the Oracle option and click Next. If you already have an Oracle database installed, click the Use existing Oracle Database option and click Next.

Step 8 From the Previous Admin Settings window, click Yes to use the previous Admin settings.

The Choose Install Folder window appears.

Step 9 Enter the NCM 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.

The Database Settings window appears.

Step 10 Tell NCM where the database software is installed. Either click the 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.

The Configure Email window appears.

Step 11 For event notification, enter the name of the SMTP server and click Next. The default SMTP server is mail.

The Configure ACL Parsing window appears.

Step 12 Check 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 device snapshot. It also increases the amount of data storage required for each snapshot.

The Choose Shortcut Folder window appears.

Step 13 Click Next to accept the default location (in a new Program Group) for the product icons, or choose another location and click Next.

The Pre-Installation Summary window appears.

Step 14 Review the information for accuracy and click Install. Installation could take several minutes.

The Database Admin Login window appears.

Step 15 Enter the hostname, database server port, and the login information for the database administrator, and then click Next. For example:

- Hostname: MySQL1.renditionnetworks.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.

The Configure Database window appears.

Step 16 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 NCM database option and click Next. If you want to use an existing NCM database and upgrade, click the Use existing NCM database option and click Next.

The New Database/Existing Database window appears.

Step 17 Enter the username and password NCM will use to connect to the database, the name of the database to create, and click Next.

If you uncheck the Create NCM user with this username and password check box, you are prompted to enter a username and password for the NCM administrator. If the check box is checked (the default), the username and password you entered for the database is used for the NCM administrator's username and password.

Note For MS-SQL Server databases, you can select the collation type from the drop-down menu. For information on collation, see your MS-SQL Server documentation.

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.

The Confirm Database Settings window appears.

Step 18 Confirm the database information and click Next.

The Configure Admin window appears.

Step 19 Enter the first and last name of the System administrator, his/her email address, and click Next. Setting up the database could take several minutes.

The Install Complete window appears.

Step 20 Be sure to wait at least three minutes before starting NCM. To close the Install Wizard, click Done.

4 NCM Install Issues

You may encounter the following issues when installing NCM 1.2.1. Where possible, workarounds have been provided.

SQL Server 2005 Install: Insufficient Password Length Causes Install to Fail

When installing NCM using a SQL Server 2005 database, you are prompted for the username and password NCM uses to connect to the database. If you enter a password that is not complicated enough for the existing Windows security policy, SQL Server 2005 discards the password and the NCM installation fails. A sample error message is: The password does not meet Windows policy requirements because it is too short.

Workaround: Enter a complex password that includes both lowercase and uppercase letters, several digits, and perhaps a special character. For example: PvyJ319?&

SQL Server 2005 Install: Install Fails Unless a Local SQL Server Admin Account is Used to Connect to the Server

The NCM Installer requires local SQL Server authentication to connect to the database server. It cannot authenticate to an SQL Server 2005 using a Domain account with Local Administrator privileges. You must have a local administrator account on the machine running MS SQL 2005 or the connection to SQL Server will fail, as will the NCM install.

Installer Leaves Database Passwords in Plain Text File After Installation

The NCM installer leaves database passwords in a plain text file after installation.

Workaround: Open the $NCM_HOME/UninstallerData/installvariables.properties file and search for the string: PASSWORD. Set the plain text password to a blank string where present and then save the file. For example, for INPUT_PASSWORD=root, set to INPUT_PASSWORD=.

Using more than One Dollar Sign ($) Character in any Input Causes the Installer to Fail

When installing NCM, ensure that any entered values including password inputs do not contain more than one dollar sign ($) character. The NCM installer treats input text containing an even number of dollar sign ($) characters as an empty variable. As a result, entered values are parsed incorrectly. For example, if your NCM database password is Network, the NCM installer parses 'work' as the password and fails to connect to the database. Note: This issue is not limited to password fields or a specific database.

Workaround: Do not use more than one dollar sign ($) character in any input.

Linux Install: NCM Shuts Down the Syslog Daemon and Renames syslog.conf

When installing NCM on a Linux server, the NCM Installer renames the /etc/syslog.conf file to syslog.conf.rm and stops the Syslog daemon. This might interfere with general log management on the Linux server.

Workaround: After the NCM install is complete, rename the /etc/syslog.conf.rm file to syslog.conf and restart the Syslog daemon.

The Default NCM Return Email Address is Invalid

When NCM is installed, NCM sets the return email address to nobody@localhost. This is an invalid email address on many mail servers and might cause bounced messages to fill up the mail queues. Because NCM is configured by default to send email notifications once installed, it is recommended that you change the return NCM email address to a valid email address immediately after the NCM install is complete. To do this:

1. Log into NCM as an administrator.
2. Navigate Admin > Administrative Settings > Server.
3. Set the SMTP From Address to a valid email address.
4. Click Save.

NCM can not Use Integrated TFTP Server or Syslog Server After Installation

If the /etc/hosts file on a Unix or Linux server is not configured properly prior to installing NCM, the IP address of the TFTP Server and/or Syslog Server used by NCM might not be set correctly.

Workaround: Either enter the NCM hostname and IP address into the /etc/hosts file before you install NCM, or after installing NCM:

1. Navigate Admin > Administrative Settings > Server.
2. Verify that the TFTP Server IP address is set correctly. If not, enter the correct IP address of the TFTP Server used by NCM and click Save. (By default, this is the NCM Server.)

Detect Network Devices Task Reports Errors After Driver Pack Install

When installing NCM on a Solaris or Linux platform, the nmap-os-fingerprints file is in DOS format. Consequently, there is an extra ^M (carriage return) character at the end of each line. As a result, Nmap and NCM report errors.

Workaround: For Solaris, manually run dos2unix on this file.

When installing NCM on Solaris or Linux platform, the version of Nmap distributed with NCM 1.2 (Nmap 3.81) is required for Nmap scanning when running the Detect Network Devices task. (Refer to Chapter 1 in the User Guide Network Compliance Manager 1.2.1 for Nmap installation instructions.)

NCM Might Set Incorrect IP Address when Installed on a Server with Multiple NICs

NCM attempts to determine the IP address of the NCM server to instruct devices to connect back to NCM. On systems with more that one installed NIC, NCM might not be able to determine the correct IP Address.

NCM Client-only Install does not set NCM Server IP Address

NCM Client-only installs do not set the NCM server IP address correctly. As a result, modules such as Connectors, AAALog Reader, and remote API clients might not be able to connect to the NCM Server.

Workaround: Edit the following file:

<*NCM Install Directory*>/rendition/jre/commandlineclient.rcx and change localhost to the correct NCM server hostname.

Installing the MySQL Service on a Drive other than C:\ Might Cause the MySQL Service not to Start

When installing NCM on a Windows platform using a MySQL database, if you assign a drive other than C:\, the MySQL service does not start. The path remains C:\mysql, even if you use a different path, such as E:\.

Workaround: When installing NCM, after you enter the Database Admin Login password, validate that the following Registry keys have the appropriate path:

Key: My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MySql\ImagePath

ImagePath should be set to the path to the MySQL executable. For example, ImagePath = E:\mysql\bin\mysqld-max-nt.exe

Key: MyComputer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MySql\ImagePath

ImagePath should be set to the path to the MySQL executable. For example, ImagePath = E:\mysql\bin\mysqld-max-nt.exe

If these keys are not set correctly, edit the ImagePath value to the correct path to the MySQL executable. Once this is complete, continue with the NCM installation.

5 Licensing

Network Compliance Manager features software-based product registration and license key activation technologies. The following table provides information about terminology used in the registration process.

Understanding Licensing Terms

Table 11 describes NCM licensing terms.

Table 11 NCM Licensing Terms

Licensing Term	Description
Product Authorization Key (PAK)	The PAK is printed on the software claim certificate included in product packaging. Use the PAK and the LMHOSTID to get your license file from Cisco.com. You can purchase incremental licenses for additional device support. For each incremental license that you purchase, you will receive a PAK, and you must use that PAK to obtain a license file.
License file	When you use the PAK to register your product on the product licensing area of Cisco.com, you will receive a license file. To register, you need to provide both of the following: • The LMHOSTID • The PAK.

Licensing Your Product During Installation

After you install the Network Compliance Manager 1.2.1 product, you should register the product and obtain a license file.

To license your product, you must:

Step 1 From the command line, run the command /<*NCM_ROOT*>/server/ext/wrapper/bin/lmutil lmhostid to generate the LMHOSTID.

Step 2 Register the NCM product with Cisco.com using the LMHOSTID and the PAK.

The PAK is printed on the software claim certificate. Get your license file from:

http://www.cisco.com/go/license

Note You will be asked to log in. You must be a registered user of Cisco.com to log in.

Logging in allows your Cisco user profile information to automatically populate many of the product registration fields. Login is case sensitive.

You might want to request a license without installing NCM. The NCM flexlmhostid is same as the Windows and Linux MAC address or the Solaris system hostid. Run the following commands to get the MAC or host id depending on the platform.

- Windows: ipconfig /all
- Linux: ifconfig -a
- Solaris: hostid

6 Installing the NCM License File

Licenses are issued for specific NCM products including NCM Core, High Availability Distributed Systems, and the Cisco Satellite (or Gateway). This section contains the following:

- Instructions for installing the NCM license file with the NCM software
- Instructions for installing the NCM license file after installing the NCM software
- Information on licensing High Availability Distributed Systems
- Specifics on License error messages

Installing the NCM License with the NCM Software

To install an NCM license file with the NCM software, do the following:

Step 1 Save the .lic file on the server in a separate directory.

Note Make sure there are no spaces in the directory path name.

Step 2 During the NCM install process, the install wizard will prompt for the license file directory.

Step 3 Point the install wizard to the directory where the .lic file is saved.

Installing the NCM License After Installing the NCM Software

To install an NCM license file after installing the NCM software, do the following:

Step 1 Before you proceed, make sure that the NCM software has been installed and configured on the server. Refer to the instructions in the "Installing NCM" section on page 8.

Step 2 Save the .lic license file to the directory where NCM is installed.

Step 3 Restart the NCM server:

- On the Windows platform: Restart the service TrueControl Management Engine
- On Solaris or Linux platforms: enter /etc/init.d/truecontrol restart

Step 4 Open a supported version of a web browser.

Step 5 In the Location or Address field, enter the appropriate URL, to access the NCM server.

Step 6 Log in to the NCM server as system administrator. Be aware that user names and passwords are case-sensitive.

Step 7 From the NCM web page, select the Admin menu.

Step 8 Access About CiscoWorks Network Compliance Manager.

Step 9 Click View License Information.

Step 10 The page should show the updated license status.

Step 11 If the updated license information is NOT visible, copy the information in the .lic file and paste it into the text box. Click the Update License button.

Note When you click the Update License button, a new license file is created with a unique name in the \rendition root directory. 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.

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.

Licensing High Availability Distributed Systems

When installing a High Availability Distributed System, both a High Availability Distrusted System and NCM Core license are required with a license count equal to or greater than your total device inventory. Inactive devices do not count toward this number. Keep in mind that for non- High Availability Distributed Systems, an NCM Core license is required for each NCM Core server in the system.

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

License Error Messages

If an 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 log in 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 file /<NCM_ROOT>/server/log/jboss_wrapper.log might provide helpful troubleshooting information.

For information on NCM license configuration settings and License Monitor messages, see Chapter 2 in the *User Guide for Network Compliance Manager 1.2.1*.

7 Logging In

NCM has a web-based user interface. To run NCM, start a browser (Internet Explorer or Mozilla Firefox) and enter the URL for the NCM server. If you run your browser from the same computer on which you installed the server, use this URL:

https://localhost/

Otherwise, you must know the server's hostname or IP address, for example:

https://192.168.123.210

The NCM login window appears. Enter the Administrator account username and password that you entered in Step 17 of the installation and click Login.

8 Adding a Device Using the New Device Wizard

When running NCM for the first time, you must add devices using the New Device Wizard, which automatically opens.

Enter the host name or IP address of the device you want NCM to manage, along with any comments about the device, and click Next. Enter the device's access username, password, and the read-only and read/write SNMP community strings. Click Finish.

If the device was successfully added to NCM, the New Device Wizard Congratulations window displays. If NCM does not recognize a new device, there are several possible causes. See the following sections.

Device Unresponsive/Bad IP Address

The device could be unresponsive or you could have entered an incorrect IP address. It is also possible that the device is not supported in the current release. See the *Device Driver Reference for Network Compliance Manager 1.2.1* for a list of supported devices. This is recognized by the following message:

```
You have successfully added device x.x.x.x to the system. However, there was a problem discovering the
driver for the device.
Click here for details.
```

Click click here to see the task results, which report the following:

```
Can't open SSH connection to <ip address>
```

or

```
Can't open Telnet connection to <ip address>
```

To correct this, verify that NCM is connected to the device. Use ping, traceroute, or another standard network diagnostic. Then, you can enter the IP address again, if necessary. See the "Editing the Device You Added" section on page 17.

Bad Password

You might have entered the wrong password for the device. If so, you see a variation of the error message for a bad IP address. The task results look like this:

```
Root-CLI – login and password not accepted
```

To correct this, you must first find the correct password for the device. After you have the correct password, you can change the device password by following the Edit Device instructions below.

Detect Network Devices Task

The Detect Network Devices task enables you to locate devices on your network that you want to place under NCM management. After 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, 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. See Chapter 7 of the *User Guide for Network Compliance Manager 1.2*.1 for detailed information on running the Detect Network Devices task.

Keep in mind that when running the Detect Network Devices task, the results show:

- Active Nodes
- Non-active nodes
- Unsupported hosts
- Existing devices

All active devices are added to the system (Inventory) and to their own group. If you select Driver Discovery on the task window, a group snapshot will be performed on that group of active devices.

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

9 Editing the Device You Added

To edit a device’s information, on the menu bar under Devices, click Inventory. The Device List displays. Click the Edit option in the Actions column for the device you are editing. The Edit Device window displays. You can now change the device information, such as the IP address or password.

10 Taking a Snapshot of a Device’s Current Configuration

NCM is configured by default to take periodic device snapshots. In other words, to periodically poll all active devices in the NCM database and store all current configurations that have changed since the last snapshot. You can also request an immediate snapshot.

To take a snapshot, on the menu bar under Tasks, select New Task and click Take Snapshot. In the New Task – Take Snapshot window, enter the device name or IP address, any Task or Scheduling options you want, and click Save Task. The Task Information window displays, where you can view task status.

11 Reviewing Task Results

NCM can perform many tasks, such as discovering a device's identity (brand and model) and taking a device snapshot (retrieving the current configuration). To view task results, on the menu bar under Tasks, click Recent Tasks. On the Recent Tasks window, successful tasks have the status Succeeded. If a task has failed, click the Detail option for information.

12 Reviewing Device Configuration

From the Recent Tasks window, you can view a device's current configuration. Click the device's hostname or IP address whose configuration you want to see, in this case the device you just added. The Device Details window displays. From the View drop-down menu, click Current Configuration. The device configuration information is displayed.

13 Integrating NCM with CiscoWorks

You can configure NCM so that you can start the application from either the CiscoWorks Home Page or from the NCM Device Tool menu. You can also configure CiscoWorks so that you can start NCM from the CiscoWorks LMS sever.

To set up the cross-starting of NCM and CiscoWorks LMS, you must do the following:

- From the NCM server, register the CiscoWorks LMS server so that it can be recognized by NCM.
- From the CiscoWorks server, register the NCM Client and Connector so that NCM can be recognized by CiscoWorks.

For information on these procedures, see the following sections. For detailed information on NCM and LMS co-residency on the Windows platform, see the Getting Started Guide for Network Compliance Manager and LMS Co-residency.

Registering the CiscoWorks LMS Server with NCM

To register the CiscoWorks LMS server with NCM, do the following:

Step 1 From the NCM server, choose Admin->Administrative Settings->Server.

Step 2 In the field titled CiscoWorks Server URL enter http://<ciscoworks server name>:1741/.

Step 3 Click Save.

To start the CiscoWorks Home Page from NCM, choose Devices->Device Tools->CiscoWorks Home.

To start CiscoView for a device from NCM, do the following:

Step 1 Click on Devices->Inventory.

Step 2 Select the device that is of interest from the list of devices.

Step 3 Click on View->CiscoView.

To start CiscoWorks Device Center for a device from NCM, do the following:

Step 1 Click on Devices->Inventory.

Step 2 Select the device that is of interest from the list of devices.

Step 3 Click on View->CiscoWorks Device Center.

Registering the NCM Server with CiscoWorks LMS

To register the NCM server with the CiscoWorks LMS server, do the following:

Step 1 Start the appropriate version (Windows or Solaris) of the NCM installer. See the "Installing NCM" section on page 8 for instructions.

Step 2 From the Choose Install Set window, click Client and Connector to install the stand-alone client and the NCM connector. Click Next.

Step 3 When prompted Do you want to install NCM connector, make sure that the option I want to install NCM connector is checked and click Next.

Step 4 When prompted for the NMSroot, specify the root directory of the LMS NMS system.

Step 5 When prompted, specify a location where you want the NCM Client and Connector to be installed.

Wait for the installer to complete.

Step 6 When prompted for the Hostname, enter the name of the NCM server.

This will automatically register the NCM server's links on the CiscoWorks Home Page. Wait for the installer to complete.

Step 7 Complete the installation.

To start NCM from the CiscoWorks homepage, log into the CiscoWorks desktop and start NCM.

14 Exporting CiscoWorks Devices

After NCM is integrated to work with CiscoWorks, you can export CiscoWorks and LMS devices into a CSV formatted file to transfer information on these devices to NCM. You can using either the LMS GUI or you can run a script on the Solaris or Windows platforms. See the following sections.

Exporting LMS Devices Using the LMS GUI

To export devices and credentials from CiscoWorks LMS to CSV, you can use the LMS GUI. To export DCR devices from LMS server, do the following:

Step 1 Go to the CiscoWorks Homepage.

Step 2 Choose Common Services->Device and Credentials and select Device Management.

Step 3 Click Export on the bottom of Device Management window.

Step 4 Select all or required devices from the device selector.

Step 5 Provide the output file name where you needed to be exported.

Step 6 Click OK.

Step 7 You can find the selected devices exported to the specified CSV file.

Exporting LMS Devices Using a Script

You can export devices and credentials from CiscoWorks LMS to CSV using a script. All of the necessary import/export scripts are located in the directory specified during the installation of the Client and Connector. Execute all commands from the CiscoWorks LMS system.

To export devices and credentials from CiscoWorks LMS, use one of the following scripts. The script must be executed on the CiscoWorks LMS server.

The path for the scripts is:

<*CWNCM_HOME*>/client/

where <*CWNCM_HOME*> is the name of the folder where you installed NCM Client and Connector. When running the exporting script, you will be prompted for a password. Enter the password of the admin_user.

From a Solaris platform, enter the following:

dcr_export.sh <*path_to_dcr_csv_file*> <*admin_user*>

From a Windows platform, enter:

dcr_export.bat <*path_to_dcr_csv_file*> <*admin_user*>

Where:

<*path_to_dcr_csv_file*> is the path/file to store the created export file.

<*admin user*> is the CiscoWorks login name

Importing Devices to the NCM Server

The next step in integrating NCM with CiscoWorks is to import CiscoWorks and LMS devices to the NCM server. To do this, you can run a script on the Solaris or Windows platforms. The path for the scripts is:

<*CWNCM_HOME*>/client/

where <*CWNCM_HOME*> is the name of the folder where you installed NCM. When running the script, you will be prompted for a password. Enter the password of the admin_user.

Before you can import devices and authentication credentials to the NCM server, you must first copy the export file <*path_to_dcr_csv_file*> you created in the previous section. See the following sections.

Note Multiple imports of the same devices will generate error messages. These error messages can be ignored. Appropriate authentication changes will be imported successfully. The user can export the device list currently in CiscoWorks and import that device list into NCM.

Several informational options must be set for the CiscoWorks Connector to function properly. They are specified in the following file on the NCM Server:

RENDITION_HOME/jre/commandlineclient.rcx

A sample set of options for this file is shown below. You will need change the user and password entries to match the administrative user account you established during the Client or Server installation.

```
<!-- com.rendition.connect.DistributedComponent options -->
<option name="tcHost">CWNCM_HOST_NAME_OR_IP</option>
<option name="tcPort">1099</option>
<option name="user">admin</option>
<option name="password">admin_password</option>
<option name="passwordEncrypted">true</option>
```

The admin_password needs to be encrypted using the ConnectorTool utility. Do the following:

Step 1 Change to the client directory under RENDITION_HOME($RENDITION_HOME/client).

Step 2 Run the following command:

/rendition/jre/bin/java -cp truecontrol-client.jar com.rendition.tools.ConnectorTool -encrypt xxxxxxx

The following example on a Windows platform shows how to encrypt the rendition password:

```
c:/rendition/jre/bin/java -cp truecontrol-client.jar com.rendition.tools.Connecto rTool -encrypt
rendition
```

The string rendition is encrypted in single quotation marks. For example, 'K2IGjPQjw6/k3 tKNW9KFLg=='

Step 3 Copy the encrypted password without the quotation marks to the commandline.rcx file.

Note If you change the password or if a different user tries to import DCR devices into NCM, you might need to change the Connect, tcHost, tcPort, user, and password values to match those that you established during the Client or Server installation.

Solaris Platform

To import devices and authentication credentials to the NCM server, enter:

cwncm_import.sh <*path_to_dcr_csv_file*>

Windows Platform

To import devices and authentication credentials to the NCM server, enter:

cwncm_import.bat <*path_to_dcr_csv_file*>

The cwncm_import.bat file requires an argument that includes a path to the exported DCR information from CiscoWorks to be imported into NCM. Typically, a Windows path would be similar to \rendition\client\devices.csv. However in the current version, the path must be a full path specified in UNIX format, for example: /rendition/client/devices.csv.

15 Uninstalling NCM 1.2 .1

To uninstall NCM 1.2.1 from the Windows platform perform the following:

Step 1 Click Start > Programs > CWNCM > Uninstall CiscoWorks Network Compliance Manager.

The Uninstall_CiscoWorks_Network_Compliance_Manager screen displays.

Step 2 Click Uninstall.

Step 3 When the uninstall program is complete, the Uninstall Complete page displays.

You should restart your system to complete the uninstall procedure. If you want to restart your system immediately, click Done. If you want to restart your system later, select No, I will restart my system myself and then click the Done button.

Keep in mind that not all files and folders are removed during the uninstall process. These files will be removed when you restart your system.

To uninstall NCM 1.2.1 from the Solaris or Linux platform:

Step 1 Log on from the console as root.

Step 2 Change directory to ./<Install Directory>/UninstallerData.

Step 3 Enter ./Uninstall__CiscoWorks_Network_Compliance_Manager.

16 More Basic Tasks

This section suggests some typical tasks you are likely to take when setting up NCM for the first time, including:

- Importing and discovering devices using a CSV file
- Adding users, user groups (or connecting to an external authentication server), and roles/permissions
- Setting up device rules
- Adding device groups
- Segmenting devices
- Configuring syslog messages
- Reviewing the default tasks and entering your own recurring tasks

For information on running tasks, see the *User Guide for Network Compliance Manager 1.2.1*.

17 Upgrading from NCM 1.2 to NCM 1.2.1

When upgrading from NCM 1.2 to NCM 1.2.1, you must do the following:

1. Stop the NCM Management Engine. See the "Stopping the NCM Management Engine" section on page 26.
2. Backup the NCM database. See the "Backing Up and Restoring the NCM Database" section on page 26.
3. Uninstall NCM. See the "Uninstalling NCM 1.2" section on page 29.
4. Install NCM 1.2.1. See the "Installing NCM 1.2.1" section on page 29.

Important: Read Me First

Before you begin to upgrade to NCM 1.2.1, be aware of the following.

Critical Settings and Important Files that are not Restored after NCM Upgrade

To ensure none of the following settings or files are lost during an upgrade, backup the entire NCM directory to a safe location before starting the upgrade. For example, if you installed NCM in c:\programs\NCM, backup the entire directory to a safe location. Then, follow the instructions below to recover lost settings and files.

The current NCM upgrade process does not restore the following settings and files:

- The license key that allows you to login to NCM.
- Active Directory certificates that allow NCM to authenticate to the Active Directory server.
- Memory customizations to increase the amount of memory the JVM uses:
  <*NCM Install Directory*>\server\ext\wrapper\conf\jboss_wrapper.conf
- Any customizations to the wrapper.conf configurations:
  <*NCM Install Directory*>\server\ext\wrapper\conf\
- Any customizations to the NCM Application configuration, such as Max DB Connections:
  <*NCM Install Directory*>\server\ext\jboss\server\default\deploy\truecontrol-service.xml
- Any modified Summary reports:

<*NCM Install Directory*>\client\Reports.xls

<*NCM Install Directory*>\config\reporting.rcx

- Any customized or standard drivers that have been changed outside of the monthly NCM Driver Pack release.
- Any customizations to the logging configuration:

  <*NCM Install Directory*>\server\ext\jboss\server\default\conf\log4j.xml

Note Many of the above items are advanced settings and are not customized in most NCM deployments.

Recovering Lost Settings

Once the NCM upgrade is complete, do the following to restore critical settings and important files. For these instructions, it is implied that you backed up the NCM Directory to <*NCM Backup Directory*> and the current NCM install location is <*NCM Install Directory*>.

Step 1 Copy the license.dat file from the <*NCM Backup Directory*> to the <*NCM Install Directory*>.

Step 2 If you are using Active Directory to authenticate users into NCM, copy the following files from the <*NCM Backup Directory*> to the <NCM Install Directory>.

a. <*NCM Backup Directory*>\server\ext\jboss\server\default\conf\truecontrol.keystore to <*NCM Install Directory*>\server\ext\jboss\server\default\conf\truecontrol.keystore

b. <*NCM Backup Directory*>\jre\lib\security\cacerts to <NCM Install Directory> \jre\lib\security\cacerts

Step 3 If you have made modifications to the jboss_wrapper.conf file to increase the amount of memory the JVM uses, manually update the settings from the backed up version of jboss_wrapper.conf. For memory settings, open <*NCM Backup Directory*>\server\ext\wrapper\conf\jboss_wrapper.conf in notepad. Take the integer value for the following parameters and set the same values in the <*NCM Install Directory*>\server\ext\wrapper\conf\jboss_wrapper.conf file.

wrapper.java.initmemory=<*INTEGER VALUE*>

wrapper.java.maxmemory=<*INTEGER VALUE*>

Note The following items are advanced settings. As a result, they are not typically customized in NCM deployments. Do not make changes to these files unless it is absolutely required.

Step 4 If you have made modifications to any of the wrapper.conf configurations (typically done to change how large log files can grow and how often they roll over), manually update the settings from the backed up version of wrapper.conf to the new installed version of the file. The backed up versions of these files are located here: <*NCM Backup Directory*>\server\ext\wrapper\conf*_wrapper.conf

Step 5 If you have made any customizations to the NCM application configuration, such as changing the Max DB Connections, manually update the customized settings from the backed up version of the file to the new installed version of the file. The backed up versions are located here:

<*NCM Backup Directory*>\server\ext\jboss\server\default\deploy\truecontrol-service.xml

Step 6 If you have made any customizations to the NCM Summary Reports template or specification, such as adding additional report tabs, manually update the customized settings from the backed up version of the files to the new installed version of the file. The backed up files are located here:

<*NCM Backup Directory*>\client\Reports.xls and <NCM Install Directory>\config\reporting.rcx

Step 7 If you have made any customizations to NCM drivers or received a driver before it was available in a monthly NCM Driver Pack release, after you have installed the latest NCM Driver Pack, validate which drivers have been updated and if your customizations conflict with the newer updates. If not, migrate the customizations into the new driver.

Step 8 If you have made any customizations to the application server logging configuration, manually update the customized settings from the backed up version of the file to the new installed version of the file. The backed up version is located here:

<*NCM Backup Directory*>\server\ext\jboss\server\default\conf\log4j.xml

Once you have made these changes, stop and restart the NCM Service.

Installing the Latest Driver Pack

NCM 1.2.1 requires that you install the latest NCM Driver Pack after you install NCM, otherwise you will experience a regression in functionality. Do the following to ensure that you have latest NCM Driver Pack:

Step 1 Before installing NCM, go to http://www.cisco.com/cgi-bin/tablebuild.pl/cwncm-crypto.

Note You will be asked to log in. You must be a registered Cisco.com user to log in.

Step 2 Download the latest NCM Driver Pack along with the *Incremental Device Update for CiscoWorks Network Compliance Manager.*

Step 3 After installing NCM, install the latest NCM Driver Update (IDU) for your specific platform following the instructions in the *Incremental Device Update for CiscoWorks Network Compliance Manager.*

NCM Upgrade Issues

You may encounter the following issues when upgrading NCM. Where possible, workarounds have been provided.

NCM Upgrade Leaves Database Passwords in Plain Text File

The NCM upgrade leaves database passwords in a plain text file after an upgrade.

Workaround: Open the $NCM_HOME/UninstallerData/installvariables.properties file and search for the string: PASSWORD. Set the plain text password to a blank string where present and then save the file. For example, for INPUT_PASSWORD=root, set to INPUT_PASSWORD=.

Upgrade on Linux: NCM Shuts Down the Syslog Daemon and Renames syslog.conf

When upgrading NCM on Linux, the NCM Installer renames the /etc/syslog.conf file to syslog.conf.rm and stops the Syslog daemon. This could interfere with general log management on the Linux server.

Workaround: After the NCM upgrade is complete, rename the /etc/syslog.conf.rm file to syslog.conf and restart the Syslog daemon.

Upgrade on Windows: NCM Upgrade Program Requests an Unnecessary Server Reboot

When upgrading to a new NCM version, after the uninstall portion of the upgrade is complete, you are prompted to reboot the server. A server reboot is not required. It is recommended that you skip this step.

Upgrade Could Take a Long Time, Depending on the Size of Your NCM Database

Depending on the size of your NCM database, a NCM upgrade could take a long time. With a very large NCM database, updating the schema could take hours. Make sure you schedule enough time to perform the NCM upgrade. If you are concerned that the NCM upgrade has hung or is not responding, contact Support before cancelling the installer.

SQL Server 2005: Upgrade Fails Unless a Local SQL Server Administrator Account is Used to Connect to the Server

The NCM upgrade requires local SQL Server authentication to connect to the database server. It cannot authenticate to SQL Server 2005 using a Domain account with Local Administrator privileges. You must have a local administrator account on the machine running MS SQL 2005 or the connection to SQL Server will fail, as will the upgrade.

Installing the MySQL Service on a Drive other than C:\ Might Cause the MySQL Service not to Start

When installing NCM on a Windows platform using a MySQL database, if you assign a drive other than C:\, the MySQL service does not start. The path remains C:\mysql, even if you use a different path, such as E:\.

Workaround: When installing NCM, after you enter the Database Admin Login password, validate that the following Registry keys have the appropriate path:

Key: My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MySql\ImagePath

ImagePath should be set to the path to the MySQL executable. For example, ImagePath = E:\mysql\bin\mysqld-max-nt.exe

Key: MyComputer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MySql\ImagePath

ImagePath should be set to the path to the MySQL executable. For example, ImagePath = E:\mysql\bin\mysqld-max-nt.exe

If these keys are not set correctly, edit the ImagePath value to the correct path to the MySQL executable. Once this is complete, continue with the NCM installation.

Administrative Settings - User Authentication Page Crypto Key Exception

It is possible that after upgrading to NCM 1.2.1, you will not be able to access any of the menu items under Administrative Settings. This is due to a corrupted encryption option in the site_options.rcx file.

Workaround:

1. Go to the $NCM_HOME/jre directory.
2. Backup the current site_options.rcx file.
3. Open the site_options.rcx file and locate all encrypted text options by searching for EncryptedText.
4. Remove the value for all encrypted text options if it is not empty. In the following example, you would delete the information between </*comment*> and </*option*>.

   Before:

   <*option name*="authentication/tacacs/secret"><*title*>TACACS+ or RADIUS Secret</*title*><*section*>TACACS+ / RADIUS Authentication</*section*><*size*>30</*size*><type>EncryptedText</*type*><*comment*>Shared secret for the CiscoWorks Network Compliance Manager host configured on the TACACS+ or RADIUS server.</*comment*>encrypted:sQAHLgjGjdGIbvNB18NEoQ==</*option*>

   After:

   <*option name*="authentication/tacacs/secret"><*title*>TACACS+ or RADIUS Secret</*title*><*section*>TACACS+ / RADIUS Authentication</*section*><*size*>30</*size*><*type*>EncryptedText</*type*><*comment*>Shared secret for the CiscoWorks Network Compliance Manager host configured on the TACACS+ or RADIUS server.</*comment*></*option*>
5. Save the file.
6. Log in to NCM.
7. On the menu bar under navigate Admin > Administrative Settings > User Authentication.
8. Scroll down to the TACACS+ / RADIUS Authentication section.
9. For the TACACS+ or RADIUS Secret option, enter the shared secret for the NCM host configured on the TACACS+ or RADIUS server.
10. Scroll down to the “Opsware Server Automation System Authentication” section.
11. For the Twist Password option, enter the SAS password to use when locating connected servers.
12. Click Save.
13. Click the Device Access tab.

14. Scroll down to the Bastion Host Settings section.
15. For the Default Bastion Host Password option, enter the password of the Bastion Host to use for Telnet and/or SSH access.
16. Click Save.

Stopping the NCM Management Engine

To stop the NCM Management Engine (also referred to as the NCM server), on the menu bar under Admin, click Start/Stop Services. Under Management Engine, click Stop.

Note If you do not know the name of the existing NCM database, before shutting down NCM do the following.

Step 1 Under Admin on the menu bar, click System Status. The System Status page displays.

Step 2 In the Monitor Name column, locate DatabaseMonitor.

Step 3 Click the View Details option in the Actions column. The database information is displayed.

Backing Up and Restoring the NCM Database

Although your data should be safe during the upgrade process, be sure that you have backed up all of the data in the database. For information on backing up your device software images and NCM files, see the "Device Software Image and NCM Files Backup" section on page 28.

Note When you enter a database name to identify the NCM database, it must be in the identical case as the database name in the database application. For example, if you created your NCM database as NCMdb, be sure to enter NCMdb when backing up and restoring the database.

SQL Server Backup and Restore Instructions

To back up SQL Server databases do the following

Step 1 Start Enterprise Manager.

Step 2 Connect to the MSSQL database server and navigate to your database.

Step 3 Right-click and select All Tasks > Backup Database.

Step 4 Under Destination, if there are any entries, highlight them and click Remove.

Step 5 Under Destination, click Add.

Step 6 Open the file browser.

Step 7 Under File name, enter a filename for your backup. Be sure to provide a new filename or you will overwrite any existing backups.

Step 8 Click OK three times to start the backup procedure. Depending on the size of your database, this could take several minutes.

To restore SQL Server databases do the following:

Step 1 Make a backup of the database you are about to restore (see above).

Step 2 Start Enterprise Manager.

Step 3 Connect to the SQL Server database server and navigate to your database.

Step 4 Right-click and select All Tasks > Restore Database.

Step 5 Click Restore: From Device.

Step 6 Click Select Devices.

Step 7 Click Add.

Step 8 Open the file browser under File name and select the filename you want to restore.

Step 9 Click OK three times.

Step 10 Click the Options tab.

Step 11 Select Force restore over existing database.

Step 12 Click OK. The database should be restored.

If you receive an error message, such as Database is in use, you need to either close the connection to that database (stop your JBoss server), or go to the Options tab and change the names of the physical files listed to a different name. If you are not using the sa login to connect to the database, you might need to change the database login.

To do this, start Query Analyzer from Enterprise Manager. In the database you just restored, execute the following command:

```
SQL command "sp_change_users_login 'auto_fix' 'username'
```

Where: *username* is the username that your JBoss is using to communicate to the SQL server.

MySQL Backup and Restore Instructions

To back up MySQL databases used by NCM do the following:

Step 1 From the command line prompt in the mysql\bin folder, enter the following command:

```
mysqldump -h<databaseserver> -u<username> -p<password> -r <YourFileName>.sql <DatabaseName> Example:
mysqldump -hNCMDBServer -utc -ptc -rNCM_ Backup_04_30_04.sql NCM
```

Step 2 Copy (or move) the file to a backup location.

Step 3 Stop the MySQL service by clicking My Computer > Control Panel > Administrative Tools > Services.

Step 4 Locate the mysql\data folder. It should contain a large ibdata file. For a standard install, this file is located in c:\mysql\data. Copy that entire data folder to a backup location.

Step 5 Restart the MySQL service. Note that both of these operations can take ten minutes or more for large databases.

To restore MySQL databases used by NCM, there are two methods. To restore using the copied files restores all MySQL databases that were on the server at the time of the backup, not just the NCM database. This method should only be used if NCM is the only application using the database server.

Step 1 Make a backup of the MySQL database (see above).

Step 2 Stop the MySQL service by clicking My Computer > Control Panel > Administrative Tools > Services.

Step 3 Copy all of the files that were backed up from the mysql\data directory originally back into the mysql\data directory.

Step 4 Restart the MySQL service.

To restore MySQL databases using the .sql backup file:

Step 1 Make a backup of the MySQL database (see above).

Step 2 Edit the .sql file. Add the following line to the top of the file:

```
SET FOREIGN_KEY_CHECKS=0;
```

Note If you are restoring to a different database name, the foreign key constraints inside the dump file reference <Database_Name>.RN_DEVICE (DeviceID), including the database name. If you restore this to a different database name, in effect you are referencing the database <Database_Name> for your FK checks. This is a known defect in mysqldump and how it interacts with the InnoDB table types. The solution is to remove the <Database_Name>.

Step 3 Navigate to the mysql\bin directory and enter the following command to get to the mysql command interface: mysql -h<*hostname*> -u<*username*> -p<*password*>

Step 4 Enter the following commands in the mysql command interface. (Note that mysql needs forward slashes '/' in path names.)

```
drop database <DatabaseName>;
create database <DatabaseName>;
use <DatabaseName>;
source <BackupFileName>.sql;
grant all privileges on <DatabaseName>.* TO <username> identified by '<password>';
```

Where: *username* is the username that NCM uses to connect to the database and *password* is the user's password.

Oracle Backup and Restore Instructions

Please see your Oracle DBA for information on backing up and restoring the databases.

Device Software Image and NCM Files Backup

In an enterprise environment, system administrators are usually required to periodically backup crucial software applications. NCM's server state is maintained in several configuration files.

The ConfigMonitor feature automatically backs up copies of the original .rcx files after the first system startup, and will periodically back up copies of modified .rcx files. In general, the .rcx files are copied to InstallDirectory\server\ext\jboss\server\default\log\rcx*.rcx_BAK and *.rcx_ORIG, where *InstallDirectory* is c:\rendition by default.

Cisco recommends that you use a commercial backup/restore utility to back up and restore the entire hard disk of the server that hosts. This minimizes risks of missed, corrupted, or misplaced files.

During an upgrade, the NCM Setup program automatically backs up user files, such as the Summary reports and NCM scripts, to the following directories:

For Windows:

- \winnt\temp\rendition\addins
- \winnt\temp\rendition\images
- \winnt\temp\rendition\log
- \winnt\temp\rendition\scripts

For Solaris:

- /var/Rendition/addins
- /var/Rendition/images
- /var/Rendition/log
- /var/Rendition/scripts

The installer restores all user files automatically, except log files. If you want to keep appending to saved log files, copy them to \InstallDirectory\server\log.

After upgrading to NCM 1.2.1:

- Device software images from the backup directory are copied to InstallDirectory\server\images.

- Summary reports from the backup directory are copied to InstallDirectory\addins.
- The site_options.rcx file from the backup directory is copied to InstallDirectory\jre, if you selected the use the previous administrative settings option during installation.

During an upgrade, if you move the installation from C:\rendition to C:\NCM, the repository will not work despite the fact the software images were successfully moved from C:\rendition\server\images to C:\NCM\server\images. The database still points to C:\rendition\server\images. If this happens, you will have to create the repository as outlined below.

1. Delete all existing images sets names from the NCM database.
2. Re-download the software images from the vendor.
3. Re-enter all the images to the NCM database, including their compatibility information.

It is recommended that you call Cisco Technical Support for assistance.

Uninstalling NCM 1.2

To uninstall NCM 1.2 from the Windows platform perform the following:

Step 1 Click Start > Programs > CWNCM > Uninstall CiscoWorks Network Compliance Manager.

The Uninstall_CiscoWorks_Network_Compliance_Manager screen displays.

Step 2 Click Uninstall.

Step 3 When the uninstall program is complete, the Uninstall Complete page displays.

You should restart your system to complete the uninstall procedure. If you want to restart your system immediately, click Done. If you want to restart your system later, select No, I will restart my system myself and then click the Done button.

Keep in mind that not all files and folders are removed during the uninstall process. These files will be removed when you restart your system.

To uninstall NCM 1.2 from the Solaris or Linux platform:

Step 1 Log on from the console as root.

Step 2 Change directory to ./<Install Directory>/UninstallerData.

Step 3 Enter ./Uninstall__CiscoWorks_Network_Compliance_Manager.

Installing NCM 1.2.1

To install NCM 1.2.1, see one of the following sections:

- “Installing NCM 1.2.1 Using MySQL” section on page 30
- “Installing NCM 1.2.1 Using SQL Server 2000” section on page 31
- “Installing NCM 1.2.1 Using Oracle Enterprise 9.2.0.1” section on page 33

Keep in mind the following:

- Manually Saving Summary Reports

  After NCM 1.2 is uninstalled, the last generated Summary reports are not saved to the Install directory from the backup location. You need to save this file manually to the Install directory.

- Uninstalling Services

  Although you uninstalled NCM 1.2, occasionally some services are not uninstalled. If needed, enter the following commands (in a command window) to manually uninstall services:

  – InstallDirectory\server\ext\wrapper\bin>UninstallJBossWrapper-NT.bat

- InstallDirectory\server\ext\wrapper\bin>UninstallTFTPWrapper-NT.bat
- InstallDirectory\server\ext\wrapper\bin>UninstallSyslogWrapper-NT.bat

- NCM Database Username and Password

  If the NCM database username and password specified during the install are also used for the NCM login and password, do not use any special characters in the NCM database username and passwords.

Installing NCM 1.2.1 Using MySQL

To install NCM 1.2.1 using MySQL, do the following:

Step 1 From the Introduction window, review the NCM database requirements information. Keep in mind that if you choose to use an existing database, you need to know the database server's hostname and port, as well as the username and password. Click Next.

The System Requirements window appears.

Step 2 Confirm that you have met all system requirements and click Next.

The License Agreement window appears.

Step 3 Review the license agreement, click the I accept the terms of the License Agreement option, and click Next.

Step 4 Indicate the location of the license.dat file in the /license directory on the root of the NCM product DVD.

The Choose Install Set window appears.

Step 5 Select Client and Server using MySQL Max and click Next.

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 NCM 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 6 Click the Use existing MySQL Max option and click Next.

Step 7 Confirm that you are running the proper version of MySQL on the Important: MySQL Version Wizard page. If the version is correct, click Next. If the version is not correct, click Previous and click the Install MySQL Max option.

Step 8 From the Previous Admin Settings window, click Next to use the previous Admin settings.

The Choose Install Folder window appears.

Step 9 Choose a directory that does not contain existing files. The default location is c:\Rendition. Click Next.

The Database Settings window appears.

Step 10 Tell NCM where the database software is installed. Either click the The database software is installed on this computer option or The database software is installed on another computer option and click Next.

The Configure Email window appears.

Step 11 For event notification, enter the name of the SMTP server and click Next. The default SMTP server is mail.

The Configure ACL Parsing window appears.

Step 12 Check 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 device snapshot. It also increases the amount of data storage required for each snapshot.

The Choose Shortcut Folder window appears.

Step 13 Click Next to accept the default location (in a new Program Group) for the product icons, or choose another location and click Next.

The Pre-Installation Summary window appears.

Step 14 Review the information for accuracy and click Install. Installation could take several minutes.

If you are installing a new version of MySQL, the MySQL Servers and Client 3.23.55 setup program will automatically run. Simply accept the default setting to install MySQL.

a. Confirm that the MySQL database engine is installed on the Database Installation Install Wizard page. Review the information and click Next.

b. Enter a non-blank password for the MySQL root user on the Assign Root Password Install Wizard page and click Next.

c. Enter a username and password that NCM will use to connect to the MySQL database, and the name of the MySQL database that you want NCM to use. If you do not want to create a NCM user with that username and password, uncheck the checkbox for that option on the Assign Root Password Install Wizard page.

d. Confirm the database information and click Next on the Confirm Database Setting Install Wizard page.

e. Enter the first and last name of the database administrator, his/her email address, and click Next. Setting up the database could take several minutes.

The Database Admin Login window appears.

Step 15 Enter the Hostname, Database Server Port, and the login information for the database administrator, and then click Next. For example:

- Hostname: MySQL1.cisco.com
- Port: 3306
- Username: admin
- Password: password

The Configure Database window appears.

Step 16 Click the Use existing NCM database option and click Next.

The Existing Database window appears.

Step 17 Enter the username and password NCM will use to connect to the database, the name of the database to create, and click Next.

If you uncheck the Create NCM user with this username and password check box, you are prompted to enter a username and password for the NCM administrator. If the check box is checked (the default), the username and password you entered for the database is used for the NCM administrator's username and password.

The Confirm Database Settings window appears.

Step 18 Confirm the database information and click Next.

The Configure Admin window appears.

Step 19 Enter the NCM administrator's information and click Next. Setting up the database could take several minutes.

The Install Complete window appears.

Step 20 Review the information regarding the installation. Be sure to wait at least three minutes before starting NCM. To close the Install Wizard, click Done.

Installing NCM 1.2.1 Using SQL Server 2000

To install NCM 1.2.1 using SQL Server 2000, do the following:

Step 1 From the Introduction window, review the NCM database requirements information. Keep in mind that if you choose to use an existing database, you need to know the database server's hostname and port, as well as the username and password. Click Next.

The System Requirements window appears.

Step 2 Confirm that you have met all system requirements and click Next.

The License Agreement window appears.

Step 3 Review the license agreement, click the I accept the terms of the License Agreement option, and click Next.

Step 4 Indicate the location of the license.dat file in the /license directory on the root of the NCM product DVD.

The Choose Install Set window appears.

Step 5 Select Client and Server using SQL Server 2000 and click Next.

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 NCM 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 6 When prompted, accept the Microsoft SQL Server 2005 JDBC Driver. Review the terms of the license agreement, click I accept the terms of the License Agreement and click Next.

Step 7 From the Previous Admin Settings window, click Next to use the previous Admin settings.

The Choose Install Folder window appears.

Step 8 Enter the NCM installation location or accept the default location, c:\Rendition by clicking Next.

The Database Settings window appears.

Step 9 Tell NCM where the database software is installed. Either click the The database software is installed on this computer option or The database software is installed on another computer option and click Next.

Note If you migrated from another database to SQL Server 2000, and this is a new installation, you will be prompted to download the JDBC driver from Sun Microsystems' website. Follow the directions on the Download JDBC Driver page.

The Configure Email window appears.

Step 10 For event notification, enter the name of the SMTP server and click Next. The default SMTP server is mail.

The Configure ACL Parsing window appears.

Step 11 Check 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 device snapshot. It also increases the amount of data storage required for each snapshot.

The Choose Shortcut Folder window appears.

Step 12 Click Next to accept the default location (in a new Program Group) for the product icons, or choose another location and click Next.

The Pre-Installation Summary window appears.

Step 13 Review the information for accuracy and click Install. Installation could take several minutes.

The Database Admin Login window appears.

Step 14 Enter the Hostname, Database Server Port, and the login information for the database administrator, and then click Next. For example:

- Hostname: QA-MSSQL
- Port: 1433
- Username: admin
- Password: password

The Configure Database window appears.

Step 15 Click the Use existing NCM database option and click Next.

The Existing Database window appears.

Step 16 Enter the username and password NCM will use to connect to the database, the name of the database to create, and click Next.

If you uncheck the Create NCM user with this username and password check box, you are prompted to enter a username and password for the NCM administrator. If the check box is checked (the default), the username and password you entered for the database is used for the NCM administrator's username and password.

The Confirm Database Settings window appears.

Step 17 Confirm the database information and click Next.

The Configure Admin window appears.

Step 18 Enter the NCM Administrator's information and click Next. Setting up the database could take several minutes.

The Install Complete window appears.

Step 19 Review the information regarding the installation. Be sure to wait at least three minutes before starting NCM. To close the Install Wizard, click Done.

Installing NCM 1.2.1 Using Oracle Enterprise 9.2.0.1

To install NCM 1.2.1 using Oracle Enterprise 9.2.0.1, do the following:

Note If you plan to use Oracle as your back-end database, you must create the Oracle database before installing NCM. Please see your Oracle documentation for information on creating and configuring an Oracle database. 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 1 From the Introduction window, review the NCM database requirements information. Keep in mind that if you choose to use an existing database, you need to know the database server's hostname and port, as well as the username and password. Click Next.

The System Requirements window appears.

Step 2 Confirm that you have met all system requirements and click Next.

The License Agreement window appears.

Step 3 Review the license agreement, click the I accept the terms of the License Agreement option, and click Next.

Step 4 Indicate the location of the license.dat file in the /license directory on the root of the NCM product DVD.

The Choose Install Set window appears.

Step 5 Select Client and Server using Oracle and click Next.

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 NCM 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 6 From the Previous Admin Settings window, click Next to use the previous Admin settings.

The Choose Install Folder window appears.

Step 7 Enter the NCM installation location or accept the default location, c:\Rendition by clicking Next.

The Database Settings window appears.

Step 8 Tell NCM where the database software is installed. Either click the The database software is installed on this computer option or the The database software is installed on another computer option and click Next.

The Configure Email window appears.

Step 9 For event notification, enter the name of the SMTP server and click Next. The default SMTP server is mail.

The Configure ACL Parsing window appears.

Step 10 Check 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 device snapshot. It also increases the amount of data storage required for each snapshot.

The Choose Shortcut Folder window appears.

Step 11 Click Next to accept the default location (in a new Program Group) for the product icons, or choose another location and click Next.

The Pre-Installation Summary window appears.

Step 12 Review the information for accuracy and click Install. Installation could take several minutes.

Note NCM does not automatically build an Oracle database. Please see your Oracle DBA for assistance.

The Database Admin Login window appears.

Step 13 Enter the Hostname, Port, Database Name, and the login information for the database administrator, and then click Next. For example:

- Hostname: QA-ORACLE
- Port: 1521
- Username: admin
- Password: password

The Configure Database window appears.

Step 14 Click the Use existing NCM database option and click Next.

Step 15 When prompted if you have already run the upgrade script, click Next (No).

The Confirm Database Settings window appears.

Step 16 Confirm the database information and click Next.

The Configure Admin window appears.

Step 17 Enter the username and password NCM will use to connect to the database, the name of the database to create, and and click Next. Setting up the database could take several minutes.

The Install Complete window appears.

Step 18 Review the information regarding the installation. Be sure to wait at least three minutes before starting NCM. To close the Install Wizard, click Done.

18 User Documentation

To open any of the NCM documentation, on the menu bar click Docs. The Network Compliance Manager Documentation window displays. Click the name of the document you want to view. NCM also provides context-sensitive Help that you can access via the Help icon at the top of each page.

The documents for NCM include:

- *Documentation Guide for Network Compliance Manager 1.2*—Provides information on the complete NCM documentation suite and contains information for obtaining documents from Cisco.com.
- *Release Notes for Network Compliance Manager 1.2.1*—Includes information on the latest NCM features, known anomalies, workarounds, and fixes.
- *User Guide for Network Compliance Manager 1.2.1*—Includes information on how to use each NCM feature.
- *Device Driver Reference for Network Compliance Manager*—Includes device-specific information for configuring devices to work with CWNCM. This guide includes the NCM features supported by each device.
- *Configuration Guide for NCM and LMS Co-residency, 1.2*—Includes information on enabling NCM and LMS co-residency on the Windows platform.
- API Reference Guides—Includes instructions for using the application programming interfaces PERL, Java, and SOAP.

Note All documentation, including this document and any or all of the parts of the NCM documentation set, *might* be upgraded over time. Therefore, we recommend you access the NCM documentation set using the Cisco.com URL: http://www.cisco.com/en/US/products/ps6923/tsd_products_support_series_home.html.

In addition, the Docs tab visible from within Network Compliance Manager *might* not include links to the latest documents.

19 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

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 800 020 0791
Fax: 31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in the USA on recycled paper containing 10% postconsumer waste.

OL-10194-04