



QUICK START GUIDE



Quick Start Guide for CiscoWorks Network Compliance Manager, 1.3

Text Part Number: OL-10194-05

1 Getting Started

CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements. CiscoWorks NCM helps IT staff identify and correct trends that could lead to problems such as network instability and service interruption.

This guide provides information on:

- System Requirements, page 2
- Before Installing CiscoWorks NCM, page 8 on either a Windows, Linux, or Solaris server
- Installing CiscoWorks NCM, page 10
- Installing Nmap, page 14
- CiscoWorks NCM Install Issues, page 15
- Licensing, page 18
- Installing the CiscoWorks NCM License File, page 19
- Logging In, page 20
- Adding a Device Using the New Device Wizard, page 21
- Integrating CiscoWorks NCM with CiscoWorks, page 23
- Exporting CiscoWorks Devices, page 24
- Uninstalling CiscoWorks NCM 1.3, page 26
- Upgrading to Ciscoworks NCM 1.3, page 27
- User Documentation, page 30

- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 30
- Open Source License Acknowledgements, page 31

For complete information on how to use CiscoWorks NCM, see the *User Guide for Network Compliance Manager, 1.3*.



Note All documentation, including this document and any or all of the parts of the CiscoWorks NCM documentation set, *might* be upgraded over time. Therefore, we recommend you access the CiscoWorks NCM documentation set using the Cisco.com URL:
http://www.cisco.com/en/US/products/ps6923/tsd_products_support_series_home.html.
 The Docs tab visible from within CiscoWorks NCM *might* not include links to the latest documents.

2 System Requirements

This section includes the following:

- Protocols and Ports, page 2
- Linux Server Requirements, page 3
- Solaris Server Requirements, page 5
- Windows Server Requirements, page 6
- CiscoWorks NCM and LMS Co-residency Requirements, page 7
- CiscoWorks NCM High Availability System Requirements, page 8

Protocols and Ports

CiscoWorks NCM communicates with devices using a combination of the following protocols and ports as described in Table 1. If you use a given protocol, CiscoWorks NCM requires access to the corresponding port. Specifically, if CiscoWorks NCM communicates with devices protected by firewalls, these ports need to be opened.

Table 1 CiscoWorks NCM Supported Protocols and Corresponding Ports

Protocol/Port	From/To
CiscoWorks NCM Server (running the Mgmt Engine, Syslog, TFTP) and Network Devices	
Telnet (port 23)	From the CiscoWorks NCM server to network devices.
SSH (port 22)	From the CiscoWorks NCM server to network devices.
TFTP (port 69/udp)	From network devices to the CiscoWorks NCM server.
Syslog (port 514/udp)	From network devices to the CiscoWorks NCM server.
SNMP (port 161/udp)	From the CiscoWorks NCM server to network devices.
Oracle (port 1521)	From the CiscoWorks NCM server to an Oracle database. In a Distributed System configuration, the Oracle processes connect to each other on port 1521.
MySQL (port 3306)	From the CiscoWorks NCM server to MySQL database.
SQL Server (port 1433)	From the CiscoWorks NCM server to a SQL Server database. In a Distributed System configuration, the SQL Server databases communicate with each other on port 1433.
CiscoWorks NCM Server and the NMS	
SNMP-trap (port 162/udp)	From the CiscoWorks NCM server to the NMS.
CiscoWorks NCM Server and the AAA Server	
JNDI (port 1099)	From the AAA server to the CiscoWorks NCM server. You can change this by editing the CiscoWorks NCM configuration files.

Table 1 CiscoWorks NCM Supported Protocols and Corresponding Ports (continued)

Protocol/Port	From/To
RMI (port 4444)	From the AAA server to the CiscoWorks NCM server. You can change this by editing the CiscoWorks NCM configuration files.
RMI (port 9901)	When communicating with the CiscoWorks NCM server through a firewall, use a known port for the RMI port by creating a \$NCM/server/ext/jboss/server/default/conf/jnp.properties file with jnp.rmiPort=9901. (\$NCM is the root of the CiscoWorks NCM installtree, typically C:\Rendition.) Port 9901 is required if CiscoWorks NCM is configured to use 9901 as the RMI Port. If CiscoWorks NCM is not configured to use port 9901, the firewall must allow the entire ephemeral port range (>16000). CiscoWorks NCM also uses RMI between CiscoWorks NCM clients and the CiscoWorks NCM Management Engine and between the CiscoWorks NCM Management Engines in separate CiscoWorks NCM Cores. CiscoWorks NCM clients can include: <ul style="list-style-type: none"> • CiscoWorks NCM Syslog Server • CiscoWorks NCM Connectors • AAA Log Reader • Syslog Reader • Customer-written API scripts
CiscoWorks NCM Server and the Software Image Management Server	
HTTPS (port 6099)	From the CiscoWorks NCM server to the Software Image Management server. Contact Customer Support for assistance.
CiscoWorks NCM Server and the NCM Client	
HTTPS (port 443)	From the CiscoWorks NCM client to the CiscoWorks NCM server. You can change this by editing the CiscoWorks NCM configuration files.
Telnet (port 23 for Windows or port 8023 for Solaris and Linux)	From the CiscoWorks NCM client to the CiscoWorks NCM server. You can change this from the Administrative Settings option.
SSH (port 22 for Windows or port 8022 for Solaris and Linux)	From the CiscoWorks NCM client to the CiscoWorks NCM server. You can change this from the Administrative Settings option.

Linux Server Requirements

The following tables provide the recommended requirements when installing CiscoWorks 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 CiscoWorks 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	One of the following: <ul style="list-style-type: none"> • RedHat Linux AS 3.0, Update 2 • RHAS 3 and RHAS 4 • SUSE Linux Enterprise 9.0 (32 bit)
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	14 GB, Fast SCSI

Table 2 *Requirements for the Application Server on the Linux Platform (continued)*

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: <ul style="list-style-type: none">• Microsoft SQL Server 2000 (SP 2)• Microsoft SQL Server 2005• MySQL Max 3.23 (included with CiscoWorks NCM)• Oracle 9.2• Oracle 10.2.0.2 (32 bit)
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: <ul style="list-style-type: none">• RedHat Linux AS 3.0, Update 2• RHAS 3 and RHAS 4• SUSE Linux Enterprise 9.0 (32 bit)
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 CiscoWorks NCM on a Linux platform, Nmap 3.81 is required for Nmap scanning when running the Tasks > New Task > 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 CiscoWorks 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.gnu.org)
- Star Office (www.sun.com/software/star/staroffice)

Solaris Server Requirements

The following tables provide the recommended requirements when installing CiscoWorks 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 On the Solaris platform, ensure that all standard utilities such as whoami are installed under /usr/ucb.



Note You must stop other network management applications, web servers, databases, and Syslog/TFTP servers running on the same system before installing CiscoWorks 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	One of the following: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• MySQL Max 3.23.55 (included with CiscoWorks NCM)• Oracle 9.2• Oracle 10.2.0.2 Enterprise (32 bit)
CPU	Dual UltraSPARC IIIi+, 1.3+ GHz (SunFire V240)
Memory	2 GB RAM
Swap Space	4 GB Swap

Table 6 Requirements for the Database Server on the Solaris Platform (continued)

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	One of the following: <ul style="list-style-type: none">• 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
Disk	36 GB, Dual Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex



Note When installing CiscoWorks NCM on a Solaris platform, Nmap 3.81 is required for Nmap scanning when running the Tasks > New Task > 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 CiscoWorks 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 (www.sun.com/software/star/staroffice)

Windows Server Requirements

The following tables provide the recommended requirements when installing CiscoWorks 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 CiscoWorks 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)
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Disk	10 GB, Fast SCSI

Table 8 Requirements for the Application Server on the Windows Platform (continued)

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: <ul style="list-style-type: none">• Microsoft SQL Server 2000 (SP 2)• Microsoft SQL Server 2005• MySQL Max 3.23 (included with CiscoWorks NCM)• Oracle 9.2• Oracle 10.2.0.2 (32 bit)
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)
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

CiscoWorks NCM and LMS Co-residency Requirements

The following are the recommended requirements when you are enabling co-residency of CiscoWorks 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 CiscoWorks NCM and LMS co-residency, see the *Usage Notes for CiscoWorks Network Compliance Manager and LMS Co-residency*.

CiscoWorks NCM High Availability System Requirements

The CiscoWorks NCM High Availability Distributed System is a multi master system where the data from each CiscoWorks NCM Core is available to all other CiscoWorks NCM Cores. This collection of CiscoWorks NCM Cores is called a CiscoWorks 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 CiscoWorks NCM Core. Each CiscoWorks NCM Core consists of a CiscoWorks NCM Management Engine, its associated services (Syslog and TFTP), and a single database.

For detailed information on the CiscoWorks NCM High Availability Distributed System, see the appropriated High Availability Distributed System documentation: *High Availability Distributed System on Oracle Configuration Guide for CiscoWorks Network Compliance Manager, 1.3* or *High Availability Distributed System on Microsoft SQL Server Configuration Guide for CiscoWorks Network Compliance Manager, 1.3*.

CiscoWorks NCM Gateway Requirements

The Network Compliance Manager Gateway enables a CiscoWorks NCM Core to manage servers that are behind one or more NAT devices or firewalls. The CiscoWorks 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

Web Browser Requirements


CiscoWorks NCM requires a Web browser. Keep in mind that the Web browser can be installed on a different system other than the CiscoWorks NCM server. CiscoWorks NCM supports the following Web browsers:

- Microsoft Internet Explorer version 5.5 or higher.
- Mozilla Firefox version 1.0 or higher

3 Before Installing CiscoWorks NCM

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

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

 **Note** If you are upgrading from CiscoWorks NCM 1.2 or 1.2.1 to CiscoWorks NCM 1.3, see the “Upgrading to Ciscoworks NCM 1.3” section on page 27.

 **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 CiscoWorks NCM on a Linux server, enter the following commands to mount a DVD drive.

Step 1 Log in as root.

Step 2 Enter:

```
#> mount /mnt/cdrom
#> cd /mnt/cdrom
#> cd linux
#> ./setup.bin
```



Note The GUI installer is no longer supported on Linux.

Before Installing on a Solaris Server

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

Enter the following commands to install CiscoWorks NCM manually. Be sure to change the drive on which you want to install CiscoWorks NCM.

Step 1 At the shell prompt, enter:

```
su root
```

Step 2 When prompted, enter the password.

Step 3 Enter:

```
cd /cdrom/rendition_4_0/solaris
sh setup.bin or ./setup.bin
```

Step 4 Follow the instructions that appear on the screen.



Note The GUI installer is no longer supported on Solaris.

If you log on remotely to run setup, you might see a message such as “*Warning: Cannot convert string...*” As long as you have root access, you can ignore this message and continue.

Keep in mind that the CiscoWorks NCM host system 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.

Before Installing on a Windows Server

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 CiscoWorks NCM manually:

Step 1 On the Windows taskbar, click Start, and then click Run.

Step 2 Enter:

`<drive>:\setup.exe`

where `<drive>` is the letter of your CD-ROM drive.

Step 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 CiscoWorks NCM.

4 Installing CiscoWorks NCM

The procedures for installing CiscoWorks NCM vary depending on the database you are using:

- MySQL Max 3.23 — Refer to MySQL Max 3.23 Installation Procedures, page 10.
- SQL Server 2000 or 2005 — Refer to MS SQL Server 2000 or 2005 Installation Procedures, page 12.
- Oracle 9.2 or 10.2.0.2 — Refer to Oracle 9.2 or 10.2.0.2 Installation Procedures, page 13.



Note Keep in mind that CiscoWorks NCM 1.3 requires that you install the latest Driver Pack after you install CiscoWorks NCM, otherwise you will experience a regression in functionality. After installing CiscoWorks NCM, install the latest Driver Pack. You can obtain the latest driver pack at <http://www.cisco.com/cgi-bin/tablebuild.pl/cwncm-crypto>.

MySQL Max 3.23 Installation Procedures

The following steps guide you through the installation process if you are using MySQL Max 3.23.

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

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 Select the Client and Server using MySQL Max option and click Next.



Note CiscoWorks 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 MySQL Max on a 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 You are prompted as to whether you want to install MySQL Max or use an existing MySQL Max database server. If you want to install MySQL Max, click the MySQL Max option and click Next. Go to Step 7.

If you already have a MySQL Max database installed, click the Use existing MySQL Max option and click Next.

Step 6 The MySQL database must be 3.23.55-MAX, with InnoDB type. Click Next.

Step 7 Enter the location of the license.dat file and click Next.

The Choose Install Folder window appears.

Step 8 Choose a directory that does not contain existing files. The directory path should not contain spaces. Enter the CiscoWorks NCM installation location or accept the default location, c:\NCM and click Next.

The Database Settings window appears.

Step 9 Tell CiscoWorks 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 is only displayed if the MySQL database is installed separately.

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 Pre-Installation Summary window appears.

Step 11 Review the information for accuracy and click Install. Installation could take several minutes.

The Installing CiscoWorks Network Compliance Manager window displays while the installation is in progress.



Note 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.

The Assign Root Password window appears.

Step 12 Assign a non-blank password for the MySQL root user and click Next.

The Database Admin Login window appears.

Step 13 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: root
- Password: password

The Configure Database window appears.

Step 14 Select the Create New Database option is checked and click Next.

The New Database window appears.

Step 15 Enter the username and password CiscoWorks NCM will use to connect to the database, the name of the database to create, and click Next.

The Set NCM Credentials window appears.

Step 16 If an NCM user (administrator) is not created using the database user name and password, you are prompted to enter the username and password. Enter the username and password, confirm the password, and click Next.

The Confirm Database Settings window appears.

Step 17 Confirm the database information and click Next.

The Configure Admin window appears.

Step 18 Enter the CiscoWorks NCM System Administrator's information and click Next.

The Install Complete window appears.

Step 19 Review the information regarding the installation and click Done.

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

MS SQL Server 2000 or 2005 Installation Procedures

The following steps guide you through the installation process if you are using SQL Server 2003 or 2005.

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

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 Select the Client and Server using MS SQL Server option and click Next.



Note CiscoWorks 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 MS SQL Server on a 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 Installation of MS SQL Server requires the Microsoft SQL Server 2005 JDBC Driver. Review the Microsoft Software License terms. Select the I accept the terms of the License Agreement option and click Next.

Step 6 Enter the location of the license.dat file and click Next.

The Choose Install Folder window appears.

Step 7 Choose a directory that does not contain existing files. The directory path should not contain spaces. Enter the CiscoWorks NCM installation location or accept the default location, c:\NCM and click Next.

The Database Settings window appears.

Step 8 Tell CiscoWorks 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 9 For event notification, enter the name of the SMTP server and click Next. The default SMTP server is mail.

The Pre-Installation Summary window appears.

Step 10 Review the information for accuracy and click Install. Installation could take several minutes.

The Installing CiscoWorks Network Compliance Manager window displays while the installation is in progress.

The Database Admin Login window appears.

Step 11 Enter the hostname, database server port, and the login information for the database administrator, and then click Next. For example:

- Hostname: 10.255.00.00
- Port: 1433
- Username: sa
- Password: password

The Configure Database window appears.

Step 12 Select the Create New Database option is checked and click Next.

The New Database window appears.

- Step 13** Enter the username and password CiscoWorks NCM will use to connect to the database, the name of the database to create, and click Next.
The Set NCM Credentials window appears.
- Step 14** If an NCM user is not created using the database user name and password, you are prompted to enter the username and password. Enter the username and password, confirm the password, and click Next.
The Confirm Database Settings window appears.
- Step 15** Confirm the database information and click Next.
The Configure Admin window appears.
- Step 16** Enter the CiscoWorks NCM System Administrator's information and click Next.
The Install Complete window appears.
- Step 17** Review the information regarding the installation and click Done.
- Step 18** Be sure to wait at least three minutes before starting CiscoWorks NCM. To close the Installation Wizard, click Done.
-

Oracle 9.2 or 10.2.0.2 Installation Procedures

The following steps guide you through the installation process if you are using Oracle 9.2 or 10.2.0.2.

If you plan to use Oracle as your database, you must create the Oracle database before installing CiscoWorks NCM. Refer to your Oracle documentation for information on creating and configuring an Oracle database. Keep in mind that during the CiscoWorks NCM installation, you are 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 CiscoWorks NCM database requirements information and click Next. 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.
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** Select the Client and Server using MS SQL Server option and click Next.



Note CiscoWorks 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 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** Enter the location of the license.dat file and click Next.
The Choose Install Folder window appears.
- Step 6** Choose a directory that does not contain existing files. The directory path should not contain spaces. Enter the CiscoWorks NCM installation location or accept the default location, c:\NCM and click Next.
The Database Settings window appears.
- Step 7** Tell CiscoWorks 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 8 For event notification, enter the name of the SMTP server and click Next. The default SMTP server is mail. The Pre-Installation Summary window appears.

Step 9 Review the information for accuracy and click Install. Installation could take several minutes. The Installing CiscoWorks Network Compliance Manager window displays while the installation is in progress.



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

The Database Admin Login window appears.

Step 10 Enter the hostname, database server port, and the login information for the database administrator, and then click Next. (The user must have the following privileges: CREATE SEQUENCE, CREATE SESSION, CREATE TABLE, CREATE ANY PROCEDURE, and SELECT ANY DICTIONARY. For example:

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

The Configure Database window appears.

Step 11 Choose the A clean database for use by CiscoWorks Network Compliance Manager option and click Next.

The Configure Database window appears.

Step 12 Choose Yes to create a NCM system user with the supplied database username and password and click Next. If you choose No and click Next, go to step Step 14.

The Set NCM Credentials window appears.

Step 13 Enter the username and password, confirm the password, and click Next.

The Configure Admin window appears.

Step 14 Enter the CiscoWorks NCM System Administrator's information and click Next.

The Install Complete window appears.

Step 15 Review the information regarding the installation and click Done.

Step 16 Be sure to wait at least three minutes before starting CiscoWorks NCM. To close the Installation Wizard, click Done.

5 Installing Nmap

The procedures for installing Nmap vary depending on the platform. Refer to the following section that is appropriate to your platform.

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 CiscoWorks 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)

To install Nmap on a Solaris platform, do the following:

-
- Step 1** Navigate to `/CWNCM_HOME/server/ext/nmap`.
- Step 2** Unzip and add the packages using the following commands:
- ```
gunzip <filename>
pkgadd -d <filename>
```
- For example:
- ```
cd /<CWNCM_install_path>/CWNCM/server/ext/nmapgunzip nmap-3.81-sol9-sparc-local.gzpkgadd -d
nmap-3.81-sol9-sparc-local
```
- Step 3** Create a link to the nmap executable in the `CWNCM_HOME/server/ext/nmap` directory:
- ```
cd /<CWNCM_install_path>/CWNCM/server/ext/nmap
ln -s /usr/local/bin/nmap nmap
```
- 

## Installing Nmap on Linux

To install Nmap on a Linux platform, do the following:

- 
- Step 1** Navigate to `/CWNCM/server/ext/nmap`.
- Step 2** Install the RPM package using the following command:
- ```
rpm -i <rpm file>
```
- For example:
- ```
cd /CWNCM/server/ext/nmap
rpm -i nmap-3.81-1.i386.rpm
```
- Step 3** Create a link to the nmap executable in the `CWNCM/server/ext/nmap` directory:
- ```
cd /CWNCM/server/ext/nmap
ln -s /usr/bin/nmap nmap
```
-

6 CiscoWorks NCM Install Issues

You may encounter the following issues when installing CiscoWorks NCM 1.3. Where possible, workarounds have been provided.

No Support for .pkg File Extensions

Note that CiscoWorks NCM Release 1.3 Software Upgrade Recommendation does not support images with the .pkg file extension.

Limitations with SNMPv3 Configurations

Devices configured with SNMPv3 parameters will not be discovered in Tasks > New Task > Detect Network Devices.

Workaround: Configure SNMPv2 parameters on devices to discover them using Tasks > New Task > Detect Network Devices.

Using the CLI Installer on Solaris and Linux Platforms

When installing CiscoWorks NCM using the CLI Installer on a Solaris platform, do not enter back and press Enter at any of the password prompts. Your input will be masked for all fields.

When installing CiscoWorks NCM using the CLI Installer on a Solaris platform, do not press Backspace at any password prompt. Your password will be exposed in the CLI.

When installing the CiscoWorks NCM client-only on a Solaris or Linux platform, do not use the CLI Installer. You must use the following command to install the CiscoWorks NCM client-only:

```
setup.bin -i gui
```



Note

For this command to run successfully, the X-Windows client library must be installed on the Solaris or Linux host.

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

When installing CiscoWorks NCM using a SQL Server 2005 database, you are prompted for the username and password CiscoWorks 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 CiscoWorks 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 CiscoWorks 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 CiscoWorks NCM install.

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

When installing CiscoWorks NCM, ensure that any entered values including password inputs do not contain more than one dollar sign (\$) character. The CiscoWorks 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 CiscoWorks NCM database password is \$Net\$work, the CiscoWorks 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: CiscoWorks NCM Shuts Down the Syslog Daemon and Renames syslog.conf

When installing CiscoWorks NCM on a Linux server, the CiscoWorks 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 CiscoWorks NCM install is complete, rename the /etc/syslog.conf.rm file to syslog.conf and restart the Syslog daemon.

The Default CiscoWorks NCM Return Email Address is Invalid

When CiscoWorks NCM is installed, CiscoWorks 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 CiscoWorks NCM is configured by default to send email notifications once installed, it is recommended that you change the return CiscoWorks NCM email address to a valid email address immediately after the CiscoWorks NCM install is complete. To do this:

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

CiscoWorks 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 CiscoWorks NCM, the IP address of the TFTP Server and/or Syslog Server used by CiscoWorks NCM might not be set correctly.

Workaround: Either enter the CiscoWorks NCM hostname and IP address into the /etc/hosts file before you install CiscoWorks NCM, or after installing CiscoWorks 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 CiscoWorks NCM and click Save. (By default, this is the CiscoWorks NCM Server.)

Detect Network Devices Task Reports Errors After Driver Pack Install

When installing CiscoWorks 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 CiscoWorks NCM report errors.

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

When installing CiscoWorks NCM on Solaris or Linux platform, the version of Nmap distributed with CiscoWorks NCM 1.3 (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, 1.3* for Nmap installation instructions.)

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

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

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

When installing CiscoWorks 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 CiscoWorks 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 CiscoWorks NCM installation.

7 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 CiscoWorks NCM licensing terms.

Table 11 CiscoWorks 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: <ul style="list-style-type: none">• The LMHOSTID• The PAK.

Licensing Your Product During Installation

After you install the Network Compliance Manager 1.3 product, you should register the product and obtain a license file. To license your product, you must do the following:

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 CiscoWorks 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 CiscoWorks 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`

8 Installing the CiscoWorks NCM License File

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

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

Installing the CiscoWorks NCM License with the CiscoWorks NCM Software

To install a CiscoWorks NCM license file with the CiscoWorks 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 CiscoWorks 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 CiscoWorks NCM License After Installing the CiscoWorks NCM Software

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

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

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

Step 3 Restart the CiscoWorks 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 CiscoWorks NCM server.

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

Step 7 From the CiscoWorks 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 \CWNCM 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 CiscoWorks 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 CiscoWorks NCM.

Licensing High Availability Distributed Systems

When installing a High Availability Distributed System, both a High Availability Distrusted System and CiscoWorks 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, a CiscoWorks NCM Core license is required for each CiscoWorks NCM Core server in the system.

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

License Error Messages

If a CiscoWorks 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 CiscoWorks NCM. The login screen displays a License Error message. Keep in mind that CiscoWorks NCM records when the license server starts and how many license files are found. If you encounter license errors, the CiscoWorks NCM log file `<NCM_ROOT>/server/log/jboss_wrapper.log` might provide helpful troubleshooting information.

For information on CiscoWorks NCM license configuration settings and License Monitor messages, see Chapter 2 in the *User Guide for Network Compliance Manager, 1.3*.

9 Logging In

CiscoWorks NCM has a web-based user interface. To run CiscoWorks NCM, start a browser (Internet Explorer or Mozilla Firefox) and enter the URL for the CiscoWorks 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 CiscoWorks NCM login window appears. Enter the Administrator account username and password that you entered during installation and click Login.

10 Adding a Device Using the New Device Wizard

When running CiscoWorks 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 CiscoWorks 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 CiscoWorks NCM, the New Device Wizard Congratulations window displays. If CiscoWorks NCM does not recognize a new device, there are several possible causes. See the following sections.

Configuring Devices

For device-specific configuration information, refer to the *CiscoWorks NCM 1.3 Device Driver Reference*.

- By default, when you add a device CiscoWorks 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 CiscoWorks NCM to configure Syslog messaging automatically, manually configure all devices to forward syslog change notifications to the CiscoWorks NCM Syslog server.
- If you use a Syslog relay, configure the relay to forward all Syslog notifications to CiscoWorks NCM.
- If you use TACACS+ or RADIUS, it is recommended that you set up a new username and password to enable CiscoWorks 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 Network Compliance Manager* for issues that might affect your devices or overall network.

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, 1.3* 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 CiscoWorks 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 22.

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 CiscoWorks NCM management. After you provide a range of IP addresses, CiscoWorks NCM scans your network looking for devices. Newly discovered devices are automatically added, along with the appropriate device drivers. In addition, CiscoWorks 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, 1.3* 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.

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.

Taking a Snapshot of a Device's Current Configuration

CiscoWorks NCM is configured by default to take periodic device snapshots. In other words, to periodically poll all active devices in the CiscoWorks 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.

Reviewing Task Results

CiscoWorks 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.

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.

11 Integrating CiscoWorks NCM with CiscoWorks

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

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

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

For information on these procedures, see the following sections. For detailed information on CiscoWorks 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 CiscoWorks NCM

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

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

Step 2 Depending on your platform, do the following:

- On a Windows platform, set the environment system Variable PATH to *<LMS path>\bin* followed by the other PATH values. For example, C:\Progra~\CSCOPx\bin;<other existing PATH variables>.

To set the environment variable, navigate My Computer > Go to Properties. Select Advanced , then select the Environment Variables button on the lower part of the display box.

Go to System Variables section. Edit PATH to add C:\Progra~\CSCOPx\bin; as the first value. Click OK and then continue with the following steps.

- On a Linux and Solaris platform, set the PATH variable to have *<LMS_install_path>/bin/* as the first value, followed by the existing values.

Step 3 In the field titled CiscoWorks Server URL enter http://<cisoworks server name>:1741/.

Step 4 Click Save.

Step 5 After making these changes, start installing the CiscoWorks NCM client.

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

To start CiscoView for a device from CiscoWorks 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 CiscoWorks 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 CiscoWorks NCM Server with CiscoWorks LMS

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

-
- Step 1** Start the appropriate version (Windows or Solaris) of the CiscoWorks NCM installer. See the “Before Installing CiscoWorks 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 CiscoWorks 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 CiscoWorks 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 CiscoWorks NCM server.
This will automatically register the CiscoWorks NCM server’s links on the CiscoWorks Home Page. Wait for the installer to complete.
 - Step 7** Complete the installation.
-

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

12 Exporting CiscoWorks Devices

After CiscoWorks 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 CiscoWorks NCM. You can use either the LMS GUI or you can run a script on the Solaris or Windows platforms. CiscoWorks LMS does not support the Linux platform. 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 CiscoWorks 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 CiscoWorks NCM Server

The next step in integrating CiscoWorks NCM with CiscoWorks is to import CiscoWorks and LMS devices to the CiscoWorks 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 CiscoWorks NCM. When running the script, you will be prompted for a password. Enter the password of the *admin_user*.



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 CiscoWorks NCM.

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

```
<NCM_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 *CWNCM_HOME* (*\$CWNCM_HOME/client*).

Step 2 Run the following command:

```
/cwncm/jre/bin/java -cp truecontrol-client.jar com.rendition.tools.ConnectorTool -encrypt xxxxxxxx
```

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

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

The string cwncm 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 CiscoWorks 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 CiscoWorks NCM server, enter:

```
cwncm_import.sh <path_to_dcr_csv_file>
```

Windows Platform

To import devices and authentication credentials to the CiscoWorks 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 CiscoWorks 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.

13 Uninstalling CiscoWorks NCM 1.3

To uninstall CiscoWorks NCM 1.3 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.

When the uninstall starts, it backs up CiscoWorks NCM log files to a temporary folder before it deletes any files. This task might take up to several minutes depending on the size of the log files. Be sure to review the Uninstall window periodically to check the progress of the uninstall.

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

Step 4 Be sure to manually delete any remaining files and subfolders in the CiscoWorks NCM folder.

To uninstall CiscoWorks NCM 1.3 from the Solaris or Linux platform:

Step 1 Log on from the console as root.

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

Step 3 Enter *./Uninstall_CiscoWorks_Network_Compliance_Manager*.

Step 4 Be sure to manually delete any remaining files and subfolders in the CiscoWorks NCM folder.

1.4 Upgrading to CiscoWorks NCM 1.3

When upgrading from CiscoWorks NCM 1.2 or CiscoWorks NCM 1.2.1 to CiscoWorks NCM 1.3, you must do the following:

1. Stop CiscoWorks NCM Services. See the “Stopping CiscoWorks NCM Services” section on page 27.
2. Backup the CiscoWorks NCM database. See the “Backing Up the CiscoWorks NCM Database” section on page 27.
3. Uninstall CiscoWorks NCM. See the “Uninstalling CiscoWorks NCM 1.2” section on page 29.
4. Install CiscoWorks NCM 1.3. See the “Installing CiscoWorks NCM 1.3” section on page 29.

Stopping CiscoWorks NCM Services

When upgrading to CiscoWorks NCM 1.3, you must first stop the CiscoWorks NCM Services. These services include the CiscoWorks NCM Management Engine (also referred to as the CiscoWorks NCM server), CiscoWorks NCM Syslog server, and CiscoWorks NCM TFTP server.

To stop the CiscoWorks NCM Services on a Windows platform, do the following:

-
- Step 1** Navigate Start > Programs > Administration Tools > **Services**.
 - Step 2** Under TrueControl Management Engine, click Stop.
 - Step 3** Under Start > Programs > CWNCM > FTP Server , click Stop.
 - Step 4** Under TrueControl Syslog Server , click Stop.
-

To stop the CiscoWorks NCM Services on a Linux or Solaris platform, do the following:

-
- Step 1** Login in as root and enter:
`/etc/init.d/truecontrol stop`
 - Step 2** If you do not know the name of the existing CiscoWorks NCM database, before shutting down CiscoWorks NCM do the following.
 - a. Under Admin on the menu bar, click System Status. The System Status page displays.
 - b. In the Monitor Name column, locate DatabaseMonitor.
 - c. Click the View Details option in the Actions column. The database information is displayed.
-

Backing Up the CiscoWorks 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 CiscoWorks NCM files, see the “Device Software Image and CiscoWorks NCM Files Backup” section on page 28.



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

SQL Server Backup 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.
-

MySQL Backup and Restore Instructions

To back up MySQL databases used by CiscoWorks 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.
-

Oracle Backup Instructions

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

Device Software Image and CiscoWorks NCM Files Backup

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

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.

Before running the CiscoWorks NCM upgrade, create a full copy of your CiscoWorks NCM folder. During an upgrade, the CiscoWorks NCM Setup program automatically backs up user files, such as the Summary reports and CiscoWorks NCM scripts, to the following directories:

For Windows:

- \WINNT\Temp\Rendition
- or
- \WINDOWS\Temp\Rendition

For Solaris and Linux:

- /var/Rendition/

After upgrading to CiscoWorks NCM 1.3, the installer automatically restores the following files:

- 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.
- The SecurID token file.
- The Gateway encryption key.
- The SSL public key certificate.
- The *license.dat* file is restored if you do not have a new license file.

The following files are backed up but not restored during the CiscoWorks NCM upgrade:

- Log files in the *<InstallDirectory>\server\log* folder. If you want to keep appending to saved log files, copy them to *<InstallDirectory>\server\log*.
- All *.rcx* files in the *<InstallDirectory>\jre* folder. The *site_options.rcx* and adjustable *_options.rcx* files will be restored if you selected the use the previous administrative settings option during installation.
- *<InstallDirectory>\server\ext\jboss\server\default\conf\log4j.xml*.
- Wrapper config files in *<InstallDirectory>\server\ext\wrapper\conf*.

Uninstalling CiscoWorks NCM 1.2

To uninstall CiscoWorks NCM 1.2 or 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.

When the uninstall starts, it backs up CiscoWorks NCM log files to a temporary folder before it deletes any files. This task might take up to several minutes depending on the size of the log files. Be sure to review the Uninstall window periodically to check the progress of the uninstall.

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

Step 4 Be sure to manually delete any remaining files and subfolders in the CiscoWorks NCM folder.

To uninstall CiscoWorks NCM 1.2 or 1.2.1 from the Solaris or Linux platform:

Step 1 Log on from the console as root.

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

Step 3 Enter *./Uninstall__CiscoWorks_Network_Compliance_Manager*.

Step 4 Be sure to manually delete any remaining files and subfolders in the CiscoWorks NCM folder.

Installing CiscoWorks NCM 1.3

To install CiscoWorks NCM 1.3, see one of the following sections:

- “MySQL Max 3.23 Installation Procedures” section on page 10
- “MS SQL Server 2000 or 2005 Installation Procedures” section on page 12
- “Oracle 9.2 or 10.2.0.2 Installation Procedures” section on page 13

15 User Documentation

The CiscoWorks NCM documentation set for Release 1.3 includes:

- *Documentation Guide for Network Compliance Manager, 1.3*—Provides information on the complete CiscoWorks NCM documentation suite and contains information for obtaining documents from Cisco.com.
- *Release Notes for CiscoWorks Network Compliance Manager, 1.3*—Contains information about this specific CiscoWorks NCM release (for example, new and changed information and known problems in CiscoWorks NCM 1.3).
- *User Guide for Network Compliance Manager, 1.3*—Contains information on using CiscoWorks NCM including configuring CiscoWorks NCM, adding devices and device groups, managing device configurations, managing users, scheduling tasks, and managing policy assurance.
- *Device Driver Reference for Network Compliance Manager, 1.3*—Contains a list of devices supported by CiscoWorks NCM and includes specific information on each device.
- *Incremental Device Update for CiscoWorks Network Compliance Manager*—Contains information on device updates including information on installing device drivers.
- *Usage Notes for CiscoWorks Network Compliance Manager and LMS Co-residency*—Explains how to install CiscoWorks NCM software and enable co-residency with CiscoWorks LAN Management Solution (LMS).
- *Usage Notes for the CiscoWorks NCM 1.3 End of Sale/End of Life Report Tool*—Describes how to use the CiscoWorks NCM 1.3 End of Sale/End of Life Report Tool.

For High Availability and Satellite deployment options, the CiscoWorks NCM documentation set includes:

- *High Availability Distributed System on Oracle Configuration Guide for Network Compliance Manager, 1.3*
- *High Availability Distributed System on Microsoft SQL Server Configuration Guide for Network Compliance Manager, 1.3*
- *Installation and Upgrade Guide for Network Compliance Manager Gateway*

The CiscoWorks NCM documentation set also includes the following API Reference Guides:

- *Java API Reference for Network Compliance Manager, 1.3*
- *PERL API Reference for Network Compliance Manager, 1.3*
- *SOAP API Reference for Network Compliance Manager, 1.3*

In addition, the CiscoWorks NCM documentation set includes User Guides for connectors that are supported by CiscoWorks NCM.

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

You can access the entire CiscoWorks Network Compliance Manager documentation set from the following Cisco.com URL:

http://www.cisco.com/en/US/products/ps6923/tsd_products_support_series_home.html

From here you can navigate to any documentation for CiscoWorks NCM 1.3 you need.

16 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>

17 Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

© 1998-1999 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].



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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registr: Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems log Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, IQ Expertise, the iQ logo, iQ N Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, T Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company (0609R)

© 2007 Cisco Systems, Inc. All rights reserved.

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

OL-10194-05