CiscoWorks Network Compliance Manager 1.3

CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior 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.

Product Overview

Enterprises seeking to enable high performance business applications increasingly rely on sophisticated networking infrastructure and the power of new technologies. Network operations and security managers rely on systems that can automate network deployments, handle large and complex topologies, and track and audit how actual network deployments comply with design requirements and best practices. Enterprise networks must comply with regulatory policies, corporate IT methodologies, and technology best practices—independently of scale, networking technologies deployed, and the combination of vendors providing networking equipment.

CiscoWorks NCM helps users meet regulatory compliance goals and enforce internal IT best practices in many ways:

- It tracks all changes to the network—configuration, software, and hardware changes—in real time and captures them in a detailed audit trail.
- It screens all changes against authorized policies immediately to verify whether they comply with regulatory requirements or IT best practices.
- It automatically validates new changes against appropriate policies before they are pushed to the network. If the changes are not compliant, CiscoWorks NCM does not allow them to be deployed.
- It automates the change review process, closing the gap between the approval of a change and the actual configuration change that is pushed to the network.
- It allows managers to enforce the approval of a change through a flexible, integrated approval model, using the exact configuration code that will be pushed to the network. Approvers of a change can review the change in the context of the entire device configuration and the business units it will affect. Event notifications are sent to interested parties, giving network staff immediate visibility into unplanned and unauthorized changes.
- It limits network configuration information to users on a need-to-know basis. CiscoWorks NCM uses highly customizable role-based permissions to control what information a user can view, what actions a user can perform on devices, and which devices a user can gain direct access to.
- It ships with regulatory reports enabled for the Sarbanes-Oxley (SOX) Act, Visa Cardholder Information Security Program (CISP), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act of 1999 (GLBA), Information Technology Infrastructure Library (ITIL), Control Objectives for Information and related Technology (COBIT), and

Committee of Sponsoring Organizations of the Treadway Commission (COSO), and it provides the detailed metrics required by each of these regulations and the network information necessary to prove compliance. Included by default are reports on users, systems, network status, configurations, devices, software vulnerabilities, tasks or jobs, Telnet/Secure Shell (SSH) Protocol sessions, and compliance centers. Reports can be customized to include information such as:

- All Cisco® devices running a given version of Cisco IOS® Software
- All devices using insecure protocols for configuration management
- All devices with a faulty module
- All configuration changes made over a period of time for a set of devices
- All Telnet/SSH sessions initiated by a specific user
- All device changes that result from an approval override
- All access control lists (ACLs) that deny traffic on specific ports

Key Features and Benefits

CiscoWorks NCM 1.3 adds several new features to an already rich feature set seen in the previous versions of NCM. Table 1 lists the key features in CiscoWorks NCM 1.3.

Table 1. CiscoWorks NCM Features and Benefits

Feature	Benefits
Simplified licensing	Simplifies the ordering, licensing, and install processes helping enable customers to get their NCM systems up and running more easily
Enhanced software image management	Facilitates automated software image management with recommendation, validation, synchronization, automatic image download, and automatic rollback on error
End-of-sale and end-of-life reporting and alerting	Provides up-to-date information on devices and modules that have reached end-of-sale/end-of-life status in the network (currently supports Cisco devices only)
Interface provisioning and management	Facilitates speedy and accurate interface management through sophisticated interface search and provisioning capabilities
Policy and compliance manager enhancements	Provides ability to automate compliance on an “as-running” basis as well as the traditional “as-configured” basis
Usability improvements for policy rule creation	Dramatically reduces the need for regular expressions for creating rules
Advanced scripting enhancements	Provides the ability to mask sensitive information when using command scripts
Support for Simple Network Management Protocol version 3 (SNMPv3) and IPv6	Facilitates configuration and change management of the latest secure and cutting edge networks
Search and filtering enhancements	Facilitates searching and filtering on policies, compliance, and interfaces
Device and configuration management enhancements	Provides users a lot more flexibility and ease of use in device configuration
Network autodiscovery	Eliminates manual administration of devices
Network diagram	Eases troubleshooting
Configuration and change management	• Increases uptime • Eases audit of configuration changes • Improves control of network resources
Audit and compliance management	• Includes expansive modeling of regulatory, corporate, IT, and technology policies • Provides visibility into network’s compliance with policies • Identifies critical risks and violations • Prioritizes triage of compliance violations

Integration with CiscoWorks applications	• Includes cross-launch capabilities between CiscoWorks NCM and other CiscoWorks applications such as CiscoWorks LAN Management Solution (LMS), Home Page, Device Center, and CiscoView • Allows user to run scripts to register with CiscoWorks servers • Helps ensure consistency of network inventory database using CiscoWorks Device Credential Repository (DCR)—for example, device list and credentials may be imported into CiscoWorks NCM
Security management	• Facilitates role-based access control and lock down • Includes centralized ACL management
Advanced workflow and approvals	• Facilitates real-time process enforcement
Multivendor support	• Supports thousands of device models or versions from Cisco and 35 other vendors • Frequent and easy-to-deploy device driver releases
Connectors with third-party software	Includes connectors with HP OpenView NNM, Remedy AR, Smarts InCharge, HP Service Desk, and CA Unicenter
Alert Center	Subscription service that complements the NCM software offering. CiscoWorks NCM Alert Center content, such as security compliance policies in NCM format and product extensions, is uploaded into CiscoWorks NCM Alert Center and is hosted at a Cisco.com URL for subscribers to download into CiscoWorks NCM.

Policy and Compliance Management Enahancements

In the previous versions of NCM, policy compliance could be automated on an “as-configured” basis. In this mode NCM validates the running configuration on the device. This is an important first step, since your network will not run properly if it’s not configured correctly. However, even when every network element is configured correctly, problems still occur.

NCM 1.3 provides a new dimension of policy compliance with the ability to automate compliance on an “as-running” basis, as well as the traditional “as-configured” basis. “As-running” policy compliance helps ensure not only that the network is configured properly but that it is running as expected on an ongoing basis.

Software Image Management

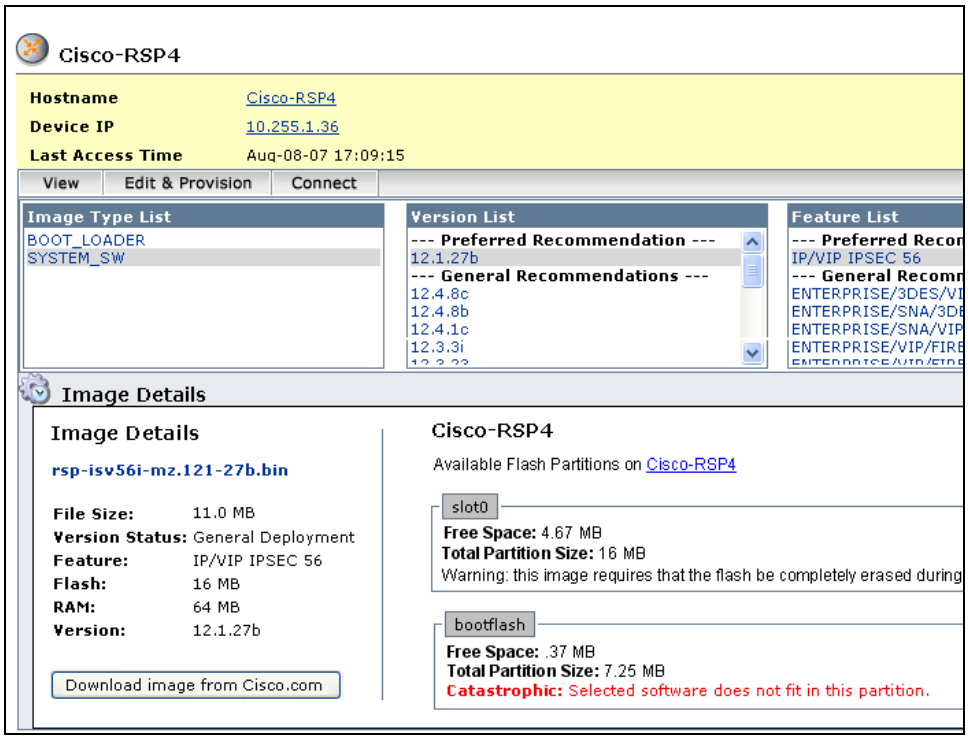
The Automated Software Image Manager dynamically downloads device images from Cisco.com into NCM. The Automated Software Image Manager utilizes custom integration with Cisco.com to dynamically download software images into NCM for deployment. NCM uses the following steps:

- NCM will query Cisco.com for the OS versions that are available for the device to run.
- NCM will present image choices within the user interface to the user.
- Users then select an image from the user interface.
- NCM then downloads the software image and automatically populates the requirements for the software image, such as hardware and memory.

NCM can then analyze the Cisco devices, including hardware components and feature sets, and present the user with the specific software images that Cisco recommends.

Figure 1 shows a sample device software image recommendation page.

Figure 1. A Sample Device Software Image Recommendation Page



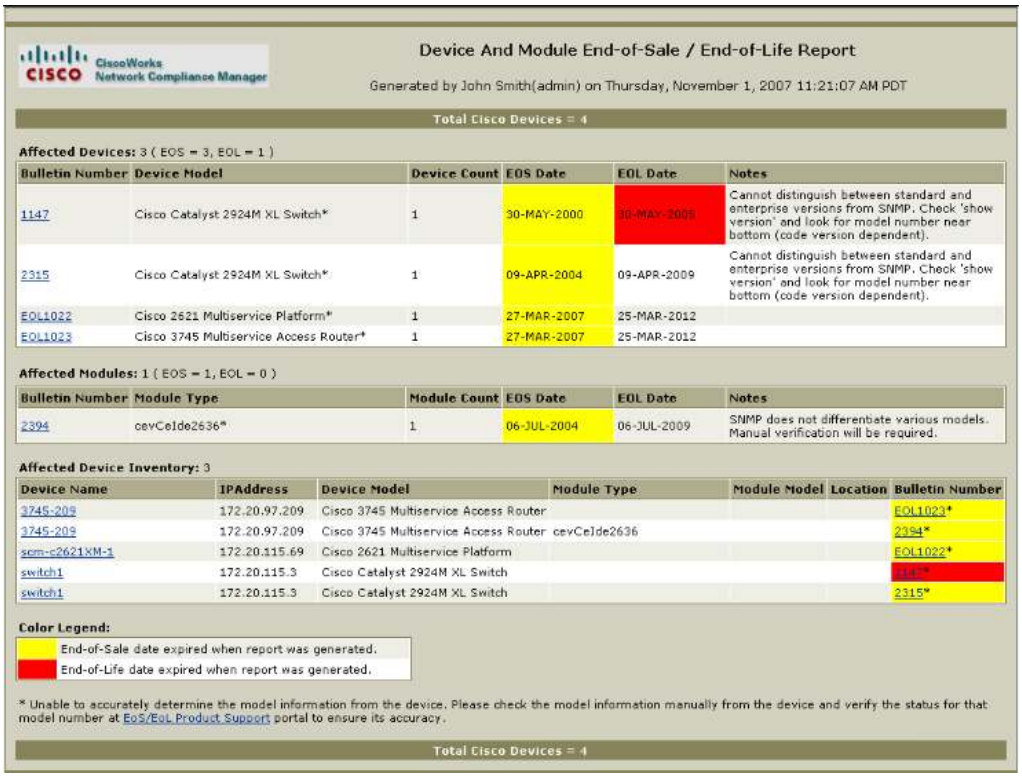
Software image synchronization helps ensure that you always have a backup of the OS images running in your network.

End-of-Sale and End-of-Life Reporting and Alerting

NCM 1.3 helps enable customers to maintain their Cisco network devices up to date with the end-of-sale/end-of-life reports and alerts. Customers can create a schedule in NCM to e-mail them the latest end-of-sale/end-of-life report of their Cisco network devices periodically. This report will clearly mark our the devices and modules that have reached end-of-sale and end-of-life status and will provide links to each of the end-of-sale/end-of-life annoucements on Cisco.com.

Figure 2 shows a screen shot of the end-of-sale/end-of-life report.

Figure 2. Device and Module End-of-Sale/End-of-Life Report



CiscoWorks Network Compliance Manager

Device And Module End-of-Sale / End-of-Life Report

Generated by John Smith(admin) on Thursday, November 1, 2007 11:21:07 AM PDT

Total Cisco Devices = 4

Affected Devices: 3 (EOS = 3, EOL = 1)

Bulletin Number	Device Model	Device Count	EOS Date	EOL Date	Notes
1147	Cisco Catalyst 2924M XL Switch*	1	30-MAY-2000	30-MAY-2005	Cannot distinguish between standard and enterprise versions from SNMP. Check 'show version' and look for model number near bottom (code version dependent).
2315	Cisco Catalyst 2924M XL Switch*	1	09-APR-2004	09-APR-2009	Cannot distinguish between standard and enterprise versions from SNMP. Check 'show version' and look for model number near bottom (code version dependent).
EOL1022	Cisco 2621 Multiservice Platform*	1	27-MAR-2007	25-MAR-2012	
EOL1023	Cisco 3745 Multiservice Access Router*	1	27-MAR-2007	25-MAR-2012	

Affected Modules: 1 (EOS = 1, EOL = 0)

Bulletin Number	Module Type	Module Count	EOS Date	EOL Date	Notes
2394	cevCe1de2636*	1	06-JUL-2004	06-JUL-2009	SNMP does not differentiate various models. Manual verification will be required.

Affected Device Inventory: 3

Device Name	IPAddress	Device Model	Module Type	Module Model	Location	Bulletin Number
3745-209	172.20.97.209	Cisco 3745 Multiservice Access Router				EOL1023*
3745-209	172.20.97.209	Cisco 3745 Multiservice Access Router	cevCe1de2636			2394*
scm-c2621XM-1	172.20.115.69	Cisco 2621 Multiservice Platform				EOL1022*
switch1	172.20.115.3	Cisco Catalyst 2924M XL Switch				1147*
switch1	172.20.115.3	Cisco Catalyst 2924M XL Switch				2315*

Color Legend:

End-of-Sale date expired when report was generated.

End-of-Life date expired when report was generated.

* Unable to accurately determine the model information from the device. Please check the model information manually from the device and verify the status for that model number at EoS/EoL Product Support portal to ensure its accuracy.

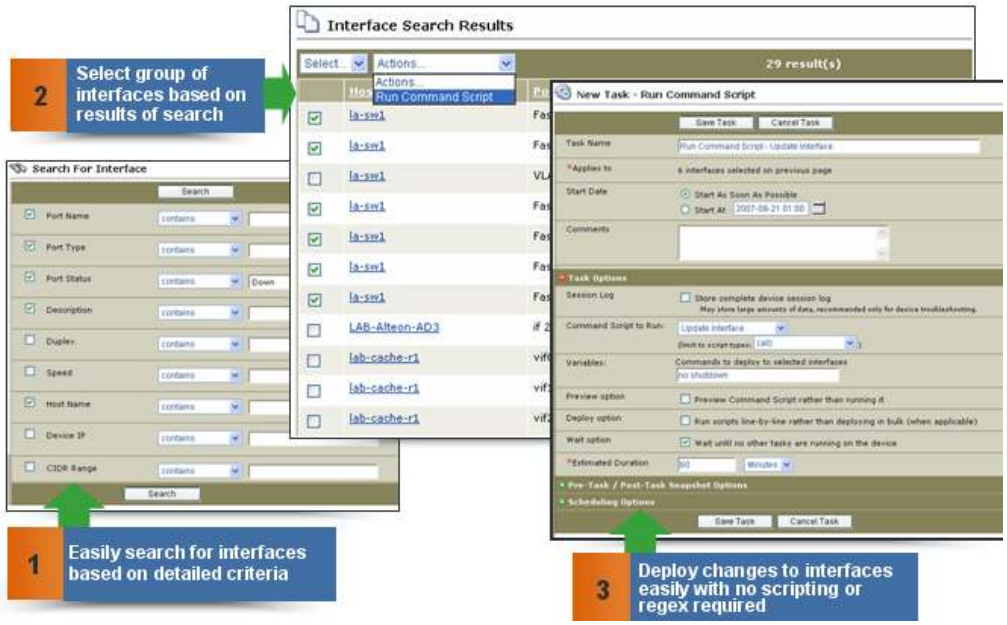
Total Cisco Devices = 4

Interface Provisioning and Management

The new interface management capability helps enable you to search for interfaces on devices that match specific criteria and display a list of interfaces matching those criteria. You can then select the specific interfaces and push a change directly to them without requiring any scripting.

Figure 3 illustrates the automated interface management.

Figure 3. Automated Interface Management



Usability Improvements for Policy Rule Creation

NCM 1.3 dramatically reduces the need for regular expressions during policy rule creation. The use of regular expressions is now optional. In addition, you can now easily specify that the lines in a rule must be unique in a given defined section. For example, these SNMP community strings should be present, but no other community strings should be defined. There can be no other lines present within this block.

NCM also lets you make use of its internal data model elements within rules, including standard and extended device custom data fields. For example, you can create a single rule that validates that all devices have their hostname formatted to company standards or validates the contents of a custom data field.

Additional policy management enhancements include the ability to test inactive policies against devices in the system.

Device and Configuration Management Enhancements

NCM 1.3 includes many enhancements to the device and configuration management features, including:

- Device groups on the Device Groups page are now expandable and collapsible. The page will retain the expanded/collapsed state for each user.
- The ability to configure the number of device password rules NCM attempts for each device before failing. If your devices are set to lock a user out after three failed attempts, you can use this enhancement to set NCM to make only two access attempts to prevent NCM from locking itself out.
- The ability to dynamically group devices based on which device password rule they are currently using.
- The ability to view which device password rule a device is using on the device home page.
- The ability to save a device configuration to a text file with one click.
- Improved diagramming and dependency mapping algorithms with additional Layer 2 connection data, such as VLAN and trunking, to more accurately determine Layer 1 and 2 connections.

CiscoWorks Integration

As a CiscoWorks application, CiscoWorks NCM integrates with the extensive features and capabilities of other CiscoWorks products. It also provides cross-launch of various features across CiscoWorks NCM and other CiscoWorks applications such as the CiscoWorks LAN Management Solution bundle.

Integration features include:

- Import of detailed device credential data from CiscoWorks DCR, providing data consistency between the two CiscoWorks products
- Launching CiscoWorks NCM from CiscoWorks Homepage, providing a centralized dashboard for network operations tasks
- Accessing other CiscoWorks applications from CiscoWorks NCM menus, including CiscoWorks Device Center and CiscoView
- Same-server coexistence: CiscoWorks NCM software, CiscoWorks NCM database (Oracle or MySQL), and CiscoWorks LMS can be configured to run on the same host. CiscoWorks

NCM and LMS can share the TFTP server, and LMS can receive all syslog messages forwarded by NCM.

High Availability Deployment Options

CiscoWorks NCM is designed for fairly large network deployments of up to tens of thousands of managed nodes, thanks to robust features such as data redundancy and high availability. For network managers concerned about high availability due to the critical nature of network compliance, configuration, and change management, CiscoWorks NCM can be deployed in (optional) high availability server configurations. The high availability and satellite deployment options provide a robust deployment architecture:

- High availability facilitates visibility and control across the entire globally distributed network environment, automatically replicating information to multiple locations and dramatically reducing time to recover by enabling immediate re-creation of the environment in a new location. It also allows IT organizations to extend best practices and knowledge across multiple locations and help achieve operational consistency across the enterprise.
- Satellite facilitates central management of network devices in remote locations across Network Address Translation (NAT) boundaries.

Device Support

CiscoWorks NCM supports an extensive range of Cisco equipment plus devices from 35 other vendors. Categories include routers, switches, firewalls, wireless access points, VPN devices, network accelerators, network load balancers, and other appliances that serve dedicated functions such as terminal and proxy servers. CiscoWorks NCM can be easily upgraded to support new devices as they become available or to meet market demand.

Alert Center

CiscoWorks NCM Alert Center is a subscription service that complements the Cisco NCM software offering. Alert Center content, such as security compliance policies in NCM format and product extensions, is uploaded into CiscoWorks NCM Alert Center biweekly and is hosted at a Cisco.com URL for subscribers to download into CiscoWorks NCM.

Licensing

CiscoWorks NCM 1.3 is licensed on the basis of the number of nodes to be managed and whether the high availability and satellite features are enabled.

Customers must purchase the following,

- Software for the core server (mandatory)
- Software for the high availability features (if required)
- Note: No license is required to install the above core and high availability software. In addition to the above software, customers must purchase the following as appropriate:
  - Appropriate core node count increment license (mandatory)
  - Appropriate high availability node count increment license (if required)
  - Licenses for satellite features based on number of satellites (if required)
  - Software licenses for the connectors with third-party software (if required)

A managed node is a management IP address and the configuration details for the system accessed by the management IP address. In most cases, a single device is equivalent to a single node. In more complex cases, such as a Cisco Catalyst® Switch in hybrid mode, where the device is running as two separate configurations, each configuration is counted as a managed node. This is because in hybrid mode the switch has two management IP addresses and two configuration files. For licensing purposes, unmanaged nodes are not counted toward the licensed total node count. See the ordering guide for more details.

Installation

CiscoWorks NCM 1.3 can be installed on a dedicated server or on a server with CiscoWorks LMS. Please refer to the recommended configurations given in Tables 2 through 7 for detailed information on preparing your network for CiscoWorks NCM deployment. For a large number of managed nodes, it is recommended to install CiscoWorks NCM on a dedicated server.

Table 2. Recommended Configuration, Dual Windows Server

Application Server	
OS	Windows Server 2003 Enterprise Edition
CPU	Intel Xeon, 3.0+ GHz
Memory	2 GB RAM
Disk space	10 GB – Fast SCSI
Network	100 Mbps Fast Ethernet full duplex
Database Server	
Supported databases	• Oracle 9.2.0.1 or 10.2.0.2 • Microsoft SQL Server 2000 (SP2) or SQL 2005 (SP2) • MySQL Max 3.23 (included)
CPU	Intel Xeon, 3.0+ GHz
Memory	2 GB RAM
Disk space	18 GB – Single Channel RAID/Fast SCSI
Network	100 Mbps Fast Ethernet full duplex

Table 3. Recommended Configuration, Single Windows Server

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

Table 4. Recommended Configuration, Dual Solaris Server

Application Server	
OS	Solaris 9 or 10
CPU	Dual UltraSPARCIIIi+, 1.3+ GHz (SunFire V240)
Memory	4 GB RAM
Swap space	8 GB Swap

Disk space	14 GB – Fast SCSI
Network	100 Mbps Fast Ethernet full duplex
Database Server	
Supported databases	• Oracle 9.2.0.1 or 10.2.0.2 • MySQL Max 3.23 (included) • Microsoft SQL Server 2000 (SP2) or SQL 2005 (SP2)
CPU	Dual UltraSPARC IIIi+, 1.3+ GHz (SunFire V240)
Memory	2 GB RAM
Swap space	4 GB Swap
Disk space	22 GB – Single Channel RAID/Fast SCSI
Network	100 Mbps Fast Ethernet full duplex

Table 5. Recommended Configuration, Single Solaris Server

Application and Database Server	
OS	Solaris 9 or 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 space	36 GB – Dual Channel RAID/Fast SCSI
Network	100 Mbps Fast Ethernet full duplex

Table 6. Recommended Configuration, Dual Linux Server

Application Server	
OS	RedHat Linux AS 4.0 or Suse Linux Enterprise Server 9
CPU	Intel Xeon, 3.0+ GHz
Memory	2 GB RAM
Swap space	4 GB Swap
Disk space	14 GB – Fast SCSI
Network	100 Mbps Fast Ethernet full duplex
Database Server	
Supported databases	Oracle 9.2.0.1 or 10.2.0.2 MySQL Max 3.23 (included) Microsoft SQL Server 2000 (SP2) or SQL 2005 (SP2)
CPU	Intel Xeon, 3.0+ GHz
Memory	2 GB RAM
Swap space	4 GB Swap
Disk space	22 GB – Single Channel RAID/Fast SCSI
Network	100 Mbps Fast Ethernet full duplex

Table 7. Recommended Configuration, Single Linux Server

Application and Database Server	
OS	RedHat Linux AS 4.0 or Suse Linux Enterprise Server 9
Database	MySQL Max 3.23 (included)

CPU	Dual Processor Intel Xeon, 3.0+ GHz
Memory	4 GB RAM
Swap space	8 GB Swap
Disk space	36 GB – Dual Channel RAID/Fast SCSI
Network	100 Mbps Fast Ethernet full duplex

Ordering Information

Please see the CiscoWorks NCM product bulletin for ordering information at http://www.cisco.com/go/cwncm.

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about CiscoWorks Network Compliance Manager, visit http://www.cisco.com/go/cwncm, contact your local account representative, or send an e-mail to ask-ncm-pm@cisco.com

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 (USA) Pte. Ltd.
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 USA C78-442919-00 11/07

