CiscoWorks Network Compliance Manager 1.6

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. 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 facilitate 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. NCM helps users meet regulatory compliance goals and enforce internal IT best practices.

Network Lifecycle Automation

NCM automates the complete operational lifecycle of network devices, which includes:

- Discover and track: Includes discovering and cataloging the network, visualizing the Layer 2 and Layer 3 network topology, initial device turn-up, and creating initial snapshots of device configurations
- Change and configure: Includes creating and deploying configuration changes in a structured manner, such as using configuration templates or scripts, peer reviewing and approving proposed changes, and maintaining an archive of previous configurations
- Audit and enforce: Includes defining compliance policies for your network devices, detecting violations in real time, and autoremediating problems
- Maintain and support: Includes providing reports on device inventory, change activity, and compliance

Enforce Policies, Standardize Operations, and Meet Compliance

Bringing networks into compliance with corporate or regulatory standards is a nontrivial, labor-intensive, error-prone, and difficult task. NCM helps you meet compliance standards through a network compliance model that maps device information, including configurations and run-time diagnostics, as well as policies and user roles, into a normalized structure to prevent compliance violations before they occur.

Built-in best practices immediately measure network compliance against industry-accepted best practices. NCM incorporates policies such as the National Security Agency (NSA) router configuration guidelines.

Predefined reports for Information Technology Infrastructure Library (ITIL), the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI) standard, and other regulations offer immediate insight into network compliance. These reports provide the metrics that each of these regulations or processes requires, increasing visibility and saving auditors and network engineers time.

Prevent Network Downtime and Increase Stability

Peer reviews can reduce the number of configuration defects in a network. NCM automates peer reviews, ticketing, and approval processes to reduce the time between approving a configuration change and implementing it on your network.

New Features in NCM 1.6

NCM 1.6 includes the following new features:

- **Task templates:** Task templates allow users to save all desired parameters of an existing or new task into templates that can be used as starting points for executing future NCM tasks.
- **Task “Quick Launch”:** A new task quick launch feature has been introduced to facilitate one-click launches of predefined NCM tasks. A Quick Launch menu section has been included in the “My Workspace” area for easy access to these user-defined one-click tasks.
- **View configuration enhancements:** Large device configurations can span hundreds or even thousands of lines, making it difficult to find the configuration section of interest. NCM now supports the use of expandable/collapsible sections within the configuration for easy viewing of specific areas of the configuration. Configuration sections have a hover over feature to allow you to view details of each section with a simple mouse cursor move over the Section tab. Not all devices support this feature currently. The functionality must be supported on a driver-by-driver basis. Upon initial release, only the most popular Cisco devices are supported.
- **Create device groups from a CSV File:** For bulk device group creation, use a comma-separated value (CSV) file such as an Excel spreadsheet as an input source for device groups. A CSV file is a more efficient means to import device groups into the NCM application than using the UI.
- **Search for device uptime information:** New device search fields including “Uptime” and “Uptime Stored Date” are now available. When you display device reports using the search mechanism, the length of time devices have been up and running is now available. The source of this data is the device boot diagnostic information.
- **Policy to device association improvements:** Determining what policies are applicable to a given device is much easier to determine now. In an enhanced view of a device, you can easily see and edit policies or policy rules from a list that is specifically relevant to the device under review. The policy list in this view is in the context of a specific device, hence it is a natural way of managing policy definitions. In addition, for all policies that are failing for the selected device, a link will be provided to directly review the event details of the policy failure.
- **Custom device data CLI enhancements:** The ability to edit and add multiple custom fields using the command-line interface (CLI) for a given device is now available. Previously, the CLI only allowed one custom field edit at a time. This has been extended so that in one comma-separated list, you can now add multiple custom fields in a single command.
- **Port scan task enhancements:** A new diagnostic task called Port Scan is now available. This task stores port scan information as diagnostic information that can be reviewed and processed in a variety of ways.
- **SFTP/FTP support:** SFTP is a new transfer protocol option supported in NCM 1.6. Edit devices so that they may transfer data through an SFTP or FTP server, as well as the existing mechanisms.
- **Password management enhancements:** Additional NCM access password policy enforcement capability has been added. These optional settings include requirements to change user password on next login, user restriction on password change, user password expiration, and user lock-out. All options are off by default.

- **Extended maximum number of models associated with software image set:** Software images used to have a limit on the number of device models that could be associated with the image. This limitation is now lifted and a virtually unlimited number of models may be associated with a single software image.
- **Native 64-bit support:** NCM 1.6 supports native 64-bit in Solaris, Windows, and Red Hat Linux. This platform support dramatically extends performance as the full 64-bit memory architecture is now utilized. For Windows environments, a fresh install is required on Windows 2008 to fully utilize the 64-bit architecture. Upgrades of legacy installs on Windows 2003, even on a 64-bit OS, will run in 32-bit emulation mode. For Solaris (Solaris 10) and Linux (Red Hat 5 Enterprise), upgrades are available to move to full 64-bit environments.
- **Windows Server 2008 support:** NCM 1.6 is supported on Windows Server 2008. Take advantage of the new flexibility, capabilities, and security of Windows Server 2008, as well as 64-bit on Windows, while maintaining interoperability with the NCM 1.6 product in 64-bit mode.
- **Oracle 11g support:** Oracle 11g is now supported as an interoperable database with NCM. Take advantage of the new flexibility and capabilities of Oracle 11g while maintaining interoperability with the NCM product.
- **Microsoft SQL Server 2008 support:** Microsoft SQL Server 2008 is now supported as an interoperable database with NCM. Take advantage of the new flexibility and capabilities of Microsoft SQL Server 2008 while maintaining interoperability with the NCM product.
- **NNMi integration enhancements:** Integration improvements between NCM and Network Node Manager have been extended into NCM 1.6.
- **Satellite support on Red Hat 5:** Satellites are supported on the Red Hat Enterprise Linux 5 server.

Table 1 provides a summary of the key CiscoWorks NCM features, along with a description of each feature and its benefits.

Table 1. CiscoWorks NCM Features and Descriptions

Feature	Description/Benefit
Network lifecycle management	NCM delivers a complete management and automation solution to support the full lifecycle of your network.
Process-powered automation	Using integrated, single-source software, automate IT workflows for otherwise manual processes, accomplished primarily through complex scripting.
Real-time configuration and asset tracking	In real time, detect configuration and asset information changes made across a multivendor device network, regardless of how each change is made.
Compliance control	Perform rapid troubleshooting and manage network compliance by comparing devices to well-defined, best-practice standards. Control noncompliance with automatic remediation of devices that violate standards. Speed internal and external audit processes with predefined network compliance reports for ITIL, SOX, HIPAA, PCI DSS, and more. Validate device operating states in real time to stay in compliance.
Diagramming and visualization, including Layer 2 and Layer 3 modeling	Generate a graphical representation of your network. Identify which devices are inactive or out of compliance. Use filters to immediately view isolated specific network segments. Capture a snapshot of the current state of the network, including topology and virtual LAN (VLAN) information. Identify the hosts connected to specific switches or interfaces by MAC address.
Automated software image management	Update device images and feature sets quickly, reliably, and easily.
Real-time audit trail	In real time, store a complete audit trail of configuration changes (hardware and software) made to network devices, including critical change information.
Role-based access control	Configure granular, customizable user roles to control permissions on device views, device actions, and system actions. Support common authentication systems, such as TACACS+, RADIUS, SecurID, Active Directory, and Lightweight Directory Access Protocol (LDAP).
Template-based device provisioning	Automate routine configuration tasks for updates, such as password or community string changes. Reduce the time needed to build automation scripts and increase accuracy with autogenerated scripts derived from device sessions.
Automated software synchronization and image management	Create a repository, and synchronize all device software images across your enterprise network. Use image management to automatically identify, download, and install the recommended software image for your network devices.
Automation engine	Create complex automation flows, integrating internal and third-party systems. Make use of more than 200 system triggers to drive automation.

Feature	Description/Benefit
Workflow and approvals	Enforce change processes in real time. Model complex approval processes with flexible rules. Force approvals for changes, including changes made by a direct command-line interface session. Combine multiple tasks into a project workflow to determine whether the system should proceed to the next step.
High availability and satellite deployments	Implement high availability and disaster-recovery solutions with the high availability and satellite deployments. Administrators can effectively manage geographically dispersed networks without a single point of failure. Satellites help deal with devices located behind a firewall or handle overlapping IP address situations.
Horizontal scalability	The horizontal scalability feature offers you added flexibility in how you can grow capacity while controlling software and hardware costs.
Browser-based GUI	NCM uses a browser-based GUI and as such does not require any dedicated client software. The GUI is highly intuitive and responsive, so you can accomplish tasks quickly and efficiently.

Table 2 lists the minimum server and technical requirements for NCM. Refer to the CiscoWorks NCM 1.6 Installation Guide for detailed requirements at http://www.cisco.com/go/cwncm.

Table 2. NCM Server Requirements and Technical Specifications

Component	Requirement
Server operating system	One of the following: ● Microsoft Windows Server 2008 R2 (64-bit) ● Microsoft Windows Server 2003 with Service Pack 2 (32-bit) ● Oracle Solaris 10 SPARC (64-bit) ● Red Hat Enterprise Linux 4 (32-bit) ● Red Hat Enterprise Linux 5 (64-bit) ● SuSE Enterprise Linux Server 10 (64-bit)
Database	One of the following: ● Oracle 10g (10.2.0.2 and 10.2.0.4) Standard Edition and Enterprise Edition (64-bit is supported. If running in a distributed system environment you will need Enterprise Edition) ● Oracle 11g (11.1.0.7.0) Standard Edition and Enterprise Edition (64-bit is supported. If running in a distributed system environment you will need Enterprise Edition) ● Microsoft SQL Server 2005 and 2008 Standard and Enterprise Edition (64-bit is supported) ● MySQL 5.0.58 (included with NCM)
Application server hardware requirements	Memory: 4 GB RAM Swap space: 4 GB Disk: 40 GB, Fast SCSI Network: 100 Mbps Fast Ethernet, full duplex
Database server	Memory: 4 GB RAM Swap space: 4 GB Disk: 60 to 100 GB, Single Channel RAID, Fast SCSI Network: 100 Mbps Fast Ethernet, full duplex
Virtual environments (optional)	● VMware ESX 3.5 or 4.0 or ● Solaris 10 LDOM

For more information on NCM 1.6 hardware and software requirements, refer to the CiscoWorks Network Compliance Manager 1.6 Installation and Upgrade Guide at http://www.cisco.com/go/cwncm.

NCM Alert Center

CiscoWorks NCM Alert Center is an optional subscription service that provides your NCM application with the latest set of the compliance policies based on device-vendor announced security vulnerabilities. As new security vulnerabilities are found, Alert Center will deliver these vulnerabilities to the NCM server in the form of actionable compliance policies to allow you to quickly identify all vulnerable devices on your network and rapidly remediate them before hackers can compromise their security.

NCM Collaboration Portal

An NCM collaboration portal is available for the NCM user community at https://ncm.itorigin.net. This portal provides a wealth of information about NCM such as detailed training material, archived Videos on Demand (VODs), discussion forums, NCM virtual machines, and other useful information.

Evaluation and Ordering Information

NCM 1.6 can be ordered through regular sales channels. NCM 1.6 is also available for evaluation at http://www.cisco.com/go/nmsevals.

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 NCM, please visit http://www.cisco.com/go/cwncm, contact your local account representative, or send an email to ask-ncm-pm@cisco.com. For more information about PACE, please visit http://www.cisco.com/go/pace.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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 C78-621895-00 10/10