

CiscoWorks Network Compliance Manager 1.2

Q. What is CiscoWorks Network Compliance Manager (NCM) 1.2?

A. CiscoWorks NCM 1.2 is the third release of a new Web-based network management application in the CiscoWorks product family. It 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.

Q. What enterprise network management problem does CiscoWorks NCM address?

A. Many network managers need comprehensive capabilities to automate the management of device configurations across their entire network from a central location while ensuring compliance with regulatory and business policies, corporate/IT directives, and technology best practices. This problem space is commonly referred to as network configuration and change management (NCCM).

Q. Why is Cisco® releasing an NCCM product?

A. Many enterprise customers have indicated that they require NCCM functions efficiently integrated with the rest of their Cisco configuration management tools. CiscoWorks NCM addresses this requirement today while opening the door for increasingly sophisticated integration.

Q. Who should deploy CiscoWorks NCM?

A. Enterprises and service providers requiring scalable NCCM capabilities that include advanced workflow definition, a robust scripting interface, and the ability to maintain a multivendor network in compliance with regulatory policies, corporate IT methodologies, or technology best practices will find great value in CiscoWorks NCM.

Q. How does CiscoWorks NCM help users meet regulatory compliance goals and enforce internal IT best practices?

A. CiscoWorks NCM helps users meet regulatory compliance goals—such as the Visa Cardholder Information Security Program (CISP), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act of 1999 (GLBA), Sarbanes-Oxley (SOX) Act, and Information Technology Infrastructure Library (ITIL)—in several 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 that 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 for SOX, HIPAA, GLBA, and CISP enabled, providing the detailed metrics required by each of these regulations and providing the network information necessary to prove compliance.

Q. What benefits can I expect from deploying CiscoWorks NCM?

A. Table 1 lists the primary customer benefits of CiscoWorks NCM.

Table 1. CiscoWorks NCM Benefits

Feature	Benefits
Network autodiscovery	Eliminates manual administration of devices
Network diagram	Eases troubleshooting
Configuration and change management	<ul style="list-style-type: none"> • Increases uptime • Eases audit of configuration changes • Improves control of network resources
Audit and compliance management	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 • Ensures consistency of network inventory database using CiscoWorks Device Credential Repository (DCR)—for example, device list and credentials may be imported into CiscoWorks NCM
Software image management	Enables combination of network configuration, change, compliance, and Cisco IOS [®] Software and Cisco Catalyst [™] OS image management
Security management	<ul style="list-style-type: none"> • Enables role-based access control and lock down • Includes centralized access control list (ACL) management
Advanced workflow and approvals	Enables real-time process enforcement
Multivendor support	<ul style="list-style-type: none"> • Supports thousands of device models or versions from Cisco and 35 other vendors • Frequent and easy-to-deploy device driver releases
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.

Q. How does CiscoWorks NCM fit within the Cisco Proactive Automation of Change Execution (PACE) solution?

A. CiscoWorks NCM is at the foundation of the Cisco PACE solution, which combines products and services that accelerate operational success by helping IT organizations to securely automate and control changes and configurations in their networks. The PACE solution helps medium-sized to large enterprises to meet compliance requirements, accelerate growth, help

achieve business continuity, and increase user productivity. For more information, please visit <http://www.cisco.com/go/pace>.

Q. How does CiscoWorks NCM fit within the Cisco network modeling, configuration, and security management product portfolio?

- A.** CiscoWorks NCM is complementary to other Cisco network modeling, configuration, and security management products, such as the Resource Management Essentials (RME) module of CiscoWorks LMS, Cisco Security Manager, and Cisco Configuration Assurance Solution (CAS), with minimal overlap.

Q. How does CiscoWorks RME complement CiscoWorks NCM?

- A.** CiscoWorks NCM provides improved scalability, advanced workflows, and multivendor support that are not available in CiscoWorks RME. When used together, CiscoWorks NCM and RME provide a complete, integrated set of capabilities for discovering network devices and their relationship to one another:
- Visualizing the topology of the network to understand network dynamics
 - Managing change, compliance, and configuration management in a large multivendor network
 - Auditing the current compliance of the network with regulations (SOX, GLBA, Payment Card Industry (PCI)–Visa CISP, Control Objectives for Information and related Technology [COBIT], ITIL, and tailored corporate policies)
 - Automatically applying configuration changes to large groups of devices at scheduled times
 - Deploying new Cisco IOS Software, Cisco Catalyst OS, and Cisco PIX® OS software images with current BootROM version and memory checking
 - Validating configuration changes to a network device before deployment
 - Reporting on regulation-specific reports for compliance with SOX, GLBA, PCI – Visa CISP, COBIT, ITIL, HIPPA, and Committee of Sponsoring Organizations of the Treadway Commission (COSO)
 - Performing real-time detection of changes to device parameters

Q. How does CiscoWorks NCM fit with Cisco Security Manager?

- A.** CiscoWorks NCM helps improve the security of network configurations and control of user access to view, deploy, or change device configurations. Cisco Security Manager is highly optimized for configuration management of security services such as firewalls, VPN devices, and intrusion protection systems (IPSs) on Cisco network devices. As such it offers an enhanced level of efficiency and ease of use when configuring security services on Cisco security devices. The audit and compliance-management features of CiscoWorks NCM greatly complement Cisco Security Manager because security-related configurations are especially important to audit.

Q. How does CiscoWorks NCM work with Cisco CAS?

- A.** CiscoWorks NCM provides the ability to deploy configurations across the enterprise network and is well suited to serve as an up-to-date configuration data source for modeling and impact analysis purposes. Cisco CAS automatically performs network-level consistency checks that identify misconfigurations, policy violations, inefficiencies, security gaps, and resiliency problems. Cisco CAS analyzes and validates network-level consistency by executing rules that audit the entire network, checking security vulnerabilities, IP addressing, route maps and attributes (such as QoS), regulatory compliance, and a wide variety of switching and routing

protocols. Cisco CAS allows for scheduled or event-based automated data import on configuration changes from CiscoWorks NCM and then automatically generates a model of the network for high-performance analysis.

Q. Can CiscoWorks NCM use device inventory data stored in CiscoWorks DCR?

A. Yes. CiscoWorks NCM can automatically discover the devices available in the enterprise network. Additionally, device inventory can be imported into CiscoWorks NCM from CiscoWorks DCR, helping ensure consistency between the two CiscoWorks products.

Q. Can CiscoWorks NCM be launched from within another CiscoWorks application?

A. Yes. CiscoWorks NCM can be launched from CiscoWorks Home Page.

Q. Conversely, can CiscoWorks applications be accessed through CiscoWorks NCM?

A. Yes. For example, CiscoWorks Home Page, CiscoWorks Device Center, and CiscoView can be viewed by clicking in the appropriate CiscoWorks NCM menus.

Q. My network is large and will soon exceed a thousand nodes to be managed. How can I help ensure that my CiscoWorks NCM deployment is highly available?

A. CiscoWorks NCM is designed for fairly large-scale network deployments (up to tens of thousands of managed nodes) thanks to robust features such as data redundancy and high availability. For customers concerned about high availability due to the critical nature of NCCM, CiscoWorks NCM can be deployed in (optional) high-availability server configurations.

Q. What high-availability deployment options are supported in CiscoWorks NCM?

A. High Availability and Satellite deployment options provide a robust deployment architecture:

- High Availability enables visibility and control across the entire globally distributed network environment, automatically replicating information about the environment to multiple locations and dramatically reducing time to recover from failure 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 enables central management of network devices in remote locations and enables failover due to network instability across Network Address Translation (NAT) boundaries.

Q. Which types of network devices are supported by CiscoWorks NCM?

A. 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.

Q. How is CiscoWorks NCM licensed?

A. The software 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 a software license for the core server, software licenses for the High Availability and Satellite features (if required), software licenses for the connectors with third-party software (if required), and the appropriate core and high-availability node count increments for the desired count of managed nodes..

Q. What is considered a managed node for licensing purposes?

- A.** 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.

Q. For licensing purposes, are unmanaged nodes counted toward my licensed total node count?

- A.** No. Nodes that are unmanaged in CiscoWorks NCM are not counted toward the total licensed node count. For example, if your license is for 5000 nodes and you have 5100 nodes in CiscoWorks NCM but 100 nodes are unmanaged, you do not exceed your license limit.

Q. What server operating systems does CiscoWorks NCM support?

- A.** CiscoWorks NCM is available on the following platforms:
- Microsoft Windows Server 2000 or 2003 Enterprise Edition
 - Linux RedHat ES/AS 3UP2/4
 - SUSE Linux Enterprise Server 9
 - Sun Solaris 9
 - Sun Solaris 10

Q. What database management systems does CiscoWorks NCM support?

- A.** CiscoWorks NCM supports the following database management systems:
- Microsoft SQL Server 2000
 - Microsoft SQL Server 2005
 - Oracle 9i
 - Oracle 10g
 - MySQL 3.23

Q. Should CiscoWorks NCM be installed on its own dedicated server?

- A.** In CiscoWorks NCM 1.0, users were restricted to installing NCM on a dedicated server to avoid port access conflict for HTTP, HTTPS, Telnet, syslog, and other functions. This restriction has been removed since CiscoWorks NCM 1.1. Users can now install NCM and LMS on the same server (Windows version only).

Q. How do I prepare my network for the deployment of CiscoWorks NCM?

- A.** CiscoWorks NCM communicates with devices using a combination of protocols and ports. Please refer to the CiscoWorks NCM installation checklist in the Get Started Guide for detailed information on preparing your network for CiscoWorks NCM deployment.

Q. What kind of administrator reports can I generate from CiscoWorks NCM?

- A.** CiscoWorks NCM offers both default reports that require no input and customizable reports. Default reports include:
- User and system reports
 - Network status reports
 - Configuration reports

- Device reports
- Software vulnerability reports
- Task/job reports
- Telnet/Secure Shell (SSH) Protocol user session log reports
- Compliance Center reports (SOX, Visa CISP, HIPAA, GLBA, ITIL, COBIT, COSO, and more)

Customized reports may include information such as:

- All Cisco devices running a specific 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 session logs initiated by a specific user
- All device changes that result from an approval override
- All ACLs that deny traffic on specific ports

Q. What is CiscoWorks NCM Alert Center?

- A.** CiscoWorks NCM Alert Center is a subscription service that complements the CiscoWorks 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.

For More Information

For more information about CiscoWorks Network Compliance Manager, visit

<http://www.cisco.com/go/cwncm> or contact your local account representative or 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, 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.

©2007 Cisco Systems, Inc. All rights reserved. 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 Registrar, 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 logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The 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. (0701R)