



Release Notes for CiscoWorks Network Compliance Manager, 1.3 SP1

Revised: May, 2008, OL-10194-06

These release notes include important information regarding CiscoWorks Network Compliance Manager (NCM), Release 1.3 SP1.



Note

CiscoWorks NCM 1.3 SP1 may only be installed on any CiscoWorks NCM 1.3 release.

This release is also referred to as CiscoWorks NCM 1.3.1.

CiscoWorks 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.

CiscoWorks NCM includes integration with CiscoWorks—initially launchable from the CiscoWorks home page and interoperability with other CiscoWorks applications such as the LMS bundle through the Common Services Device Credential Repository (DCR).



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.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

This release note contains the following sections:

- [Features in CiscoWorks NCM 1.3 SP1, page 2](#)
- [Features in CiscoWorks NCM 1.3, page 3](#)
- [System Requirements, page 7](#)
- [Important: Read Me First, page 13](#)
- [CiscoWorks NCM 1.3 SP1 Install Issues, page 15](#)
- [Caveats, page 18](#)
- [Known Limitations and Problems, page 28](#)
- [Accessing the CiscoWorks NCM Documentation Set, page 29](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 30](#)
- [Notices, page 30](#)

Features in CiscoWorks NCM 1.3 SP1

CiscoWorks NCM Release 1.3 SP1 contains a number of new features and enhancements.

Service Pack Installer

The CiscoWorks NCM Release 1.3 SP1 Service Pack Installer enables you to easily upgrade from CiscoWorks NCM Release 1.3 to CiscoWorks NCM Release 1.3 SP1.

Enhanced Error Logging

CiscoWorks NCM Release 1.3 SP1 Troubleshooting has been significantly improved. Session log output is more readable, and you can now gather troubleshooting logs specific to a single task.

New Driver Page

The Drivers page displays a list of the installed drivers on your system and the number of drivers currently in use. The Drivers page enables you to determine which CiscoWorks NCM drivers were built in-house or endorsed by Cisco, and as a result are supported by Cisco.

New Export/Import Policy Page

The Export Scripts feature enables you to export command and diagnostic scripts to a file for storage, offline editing, or transferring to another CiscoWorks NCM server.

The Import Script feature enables you to import command and diagnostic scripts created on another CiscoWorks NCM server or edited offline.

Updated New Diagnostics Page

Diagnostics can now be defined as an advanced script without user-defined variables.

LDAP Servers Support

Support for LDAP external authentication was widened from Active Directory to other types of LDAP servers.

Features in CiscoWorks NCM 1.3

CiscoWorks NCM Release 1.3 contains a number of new features and enhancements.

Automated Software Image Management

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

- CiscoWorks NCM queried Cisco.com for the OS versions that are available for the device.
- CiscoWorks NCM presents image choices within the UI.
- You select an image.
- CiscoWorks NCM downloads the software image and automatically populates the requirements for the software image, such as hardware and memory.

CiscoWorks NCM can analyze the Cisco devices, including hardware components and feature sets, and present you with the specific software images that Cisco recommends that you should use with the device, as well as all other valid options.

The Automated Software Image Manager feature requires a valid Cisco.com credential.

End of Sale/End of Life Report Tool

The End of Sale/End of Life Report tool retrieves information about the impacted devices and modules in your network, and the generates an End of Sale/End of Life Report that lists the devices that have reached their End of Sale or End of Life date. You can tell at a glance the status of a device: End of Sale information appears in yellow and End of life information appears in red.

The End of Sale information for a device refers to announcements made in Cisco.com regarding the ending of sales of a device or hardware.

The End of Life information refers to announcements made in Cisco.com regarding the ending of service and support of a device or hardware.

The End of Sale/End of Life Report feature requires a valid Cisco.com credential.

Software Image Synchronization

Software image synchronization ensures that you always have a backup of the OS images running in your network. You can ensure you always have a backup copy of the last “known good” software image. Archiving software images into CiscoWorks NCM from the network is completely automated. In the event you need to Request Material Authorization (RMA) an existing network device, you can use CiscoWorks NCM to deploy the original software image and its configuration files.

Interface Provisioning & Management

CiscoWorks NCM interface management capabilities enable you to search for interfaces on devices that match specific criteria. For example, you can now search and identify all interfaces on a device that are configured as “down.” You can also select the specific interfaces and push a change directly to them without requiring any scripting.

Masked Variable Support for Advanced Command Scripts

With CiscoWorks NCM, you can now create sensitive information variables for input within advanced command scripts. The value of the variable is not displayed in the Session Log or when you enter the value. This protects sensitive information, such as passwords, when using command scripts.

Policy Manager and Compliance Enhancements

Until now, CiscoWorks NCM has automated policy compliance on an “as-configured” basis. However, devices can be configured in ways that the installed network interface cards do not support or they could be configured one way, but physically wired another. CiscoWorks NCM adds the ability to automate compliance on an “as-running” basis, as well as the traditional “as-configured” basis. “As-running” policy compliance ensures that not only is the network configured properly, but that it is running as expected.

CiscoWorks NCM introduces the diagnostic policy rule to ensure “as-running” compliance. This capability can be used in conjunction with configuration policy rules to achieve comprehensive network compliance. The ability to set policy on what the “as-running” state is useful in validating that configuration changes have not negatively impacted device operations.

Software Policy Compliance

In CiscoWorks NCM 1.3, Software Compliance is moved under the umbrella of the Policy Manager. You can now create more flexible, powerful software compliance rules to ensure network compliance. Software Compliance, where you could set software levels to be Gold, Silver, and so on is now referred to as Software Levels.

Conditional Logic In Policy Rules

Validating device configuration settings is typically dependent on a number of factors, such as what OS version is running on a device. In CiscoWorks NCM 1.3, you can now use conditional logic to setup policy rules. If, Then, and Else conditional clauses are fully supported. You no longer have to use regular expressions or PERL scripts. You can easily create conditional clauses.

Usability Improvements for Policy Rule Creation

CiscoWorks NCM 1.3 reduces the need for regular expressions when building policy rules. The use of regular expressions is now optional. You can now specify that the lines in a rule must be unique in a given defined section. For example, specific SNMP community strings should be present, but no other SNMP community strings should be defined. There can be no other lines present within this block.

You can also leverage CiscoWorks NCM 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.

Searching Enhancements

You can now search extended device custom data fields in both the Search for Devices and Advanced Search pages. In addition, you can now search for devices using a specific Device Password Rule.

Search for Policies and Search for Compliance

CiscoWorks NCM 1.3 introduces two new search capabilities: Search for Policies and Search for Compliance. Search for Policies enables you to search for existing policies based on name, creation date, CVE number, and more. The Search for Compliance gives you granular searching ability on the compliant state of devices in the network. This enables you to easily create searches and reports that provide information such as:

- Which devices are out of compliance with this specific policy?
- Which devices are out of compliance with this specific rule?
- What policies is this device currently violating?

All standard searching capabilities are included with these new search features, including grouping resulting devices, running tasks against selected devices to remediate, and so on.

Reporting Enhancements

Administrators can now configure CiscoWorks NCM to generate commonly accessible Summary reports. This is only necessary in environments where View Partitions are enabled and Summary reports needs to be accessed by multiple users within one group. CiscoWorks NCM 1.3 also includes a new dashboard report that shows the number of devices in and out of compliance.

Device and Configuration Management Enhancements

CiscoWorks 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 how many Device Password Rules CiscoWorks NCM attempts for each device before failing.
- 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.

New Protocol Support – IPv6 and SNMPv3

CiscoWorks NCM 1.3 has added the IPv6 and SNMPv3 protocols to meet the needs of government, large enterprise, and security conscious customers. With IPv6 support, CiscoWorks NCM is able to manage devices in either a pure IPv6 or dual stack IPv4/IPv6 network. With SNMPv3, CiscoWorks NCM can securely communicate with devices via SNMP.

Enhanced Satellite Mesh Architecture

The Satellite architecture enables you to manage devices that are traditionally difficult to reach due to overlapping IP addressed networks and/or heavily NAT'd environments. CiscoWorks NCM 1.3 has extended the architecture to provide the following new capabilities:

- Software image caching to save time and bandwidth on device OS updates
- Real-time change detection via syslog
- Device management via FTP, TFTP, and SCP

Enhanced Multimaster Mesh Capabilities

CiscoWorks NCM 1.3 contains the following enhancements to the Multimaster Distributed System capabilities:

- Per core maximum concurrent task setting. Each core can now be configured with a max concurrent task setting applicable to that core only. For example, if Core A and B are connected by Multimaster, Core A can have a max concurrent task setting of 200 whereas Core B can have a max concurrent task of 50.
- Continuous real-time change detection via syslog in the event of core failure. You can now configure devices to send syslog messages to multiple cores in a Multimaster mesh without worrying that multiple cores will snapshot the device. CiscoWorks NCM will only snapshot the device once. The benefit of this enhancement is that if one core goes down, you do not need to update the configurations on all devices to issue syslogs to the (temporary) managing core.

Performance Enhancements

CiscoWorks NCM 1.3 includes numerous performance enhancements. You should notice these performance enhancements when:

- Running group tasks, especially group Snapshot tasks
- Performing batch edit operations across hundreds of devices
- Overall task throughput

API and CLI Enhancements

To make Web services integration easier, CiscoWorks NCM 1.3 now includes a WSDL file as a part of its SOAP API. CiscoWorks NCM 1.3 includes the following new API/CLI capabilities:

- Ability to enable and disable user accounts
- Ability to add, edit, and delete Device Password Rules
- Ability to list and show ACLs for a given ACL ID, handle or device ID
- Ability to list and show policies
- Ability to show compliant state for a give device ID
- Ability to list devices compliance state with a given policy
- Compliant state is now an output field in the list device and show device commands (API only)
- Ability to turn off pre and post snapshots when a command script is run

Installation Enhancements

You can now install CiscoWorks NCM updates and CiscoWorks NCM Driver packs using a CLI installer on Linux and Unix systems. X Windows is no longer required for CiscoWorks NCM installs on Linux or Unix.

System Requirements

This section includes the following:

- [Protocols and Ports, page 7](#)
- [Linux Server Requirements, page 8](#)
- [Solaris Server Requirements, page 10](#)
- [Windows Server Requirements, page 12](#)

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.
RMI (port 4444)	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 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:•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

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

Disk	14 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex
Applications	Adobe Acrobat Reader 4.0 or higher (for viewing documentation) KDE Desktop Manager Mozilla Firefox 1.0+

Table 3 Requirements for the Database Server on the Linux Platform

Supported Databases	One of the following: <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 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.gnumeric.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 (included with CiscoWorks NCM) • Oracle 9.2 • Oracle 10.2.0.2 (32 bit)
CPU	Dual UltraSPARC IIIi+, 1.3+ GHz (SunFire V240)
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	22 GB, Single Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

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

OS	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 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 Linux 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
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Disk	10 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex
Applications	Adobe Acrobat Reader 4.0 or higher (for viewing documentation) Microsoft Excel 2000 or higher (for viewing Summary Reports) Microsoft Internet Explorer 5.5 or higher or Mozilla Firefox 1.0 or higher

Table 9 **Requirements for the Database Server on the Windows Platform**

Supported Databases	One of the following: <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
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, refer to the *Usage Notes for CiscoWorks Network Compliance Manager and LMS Co-residency*.

Important: Read Me First

Warning on Installing CiscoWorks NCM and Database Applications on the Same Directory



Warning

If you are installing CiscoWorks NCM and a database application such as MySQL on the same server, Cisco recommends that you do not install them on the same directory. If you have CiscoWorks NCM and a database application already installed on the same directory, contact Technical Support before you install CiscoWorks NCM 1.3 SP1.

Upgrading from the CiscoWorks NCM 1.3 Syslog Reader to the CiscoWorks NCM 1.3 SP1 Syslog Reader

Syslog management enables system administrators to look at Syslogs to troubleshoot performance problems on Syslog supported devices across the network.

When upgrading to the CiscoWorks NCM 1.3 SP1 Syslog Reader:

-
- Step 1** Go to `/usr/local/rendition/syslogreader/probe.rcx`.
1. In the `probe.rcx` file, jot down the values for the `SERVERNAME` and `SOMEPATH/FILE` fields for use in Step 5.
- Document** `<option name=connect/AppServerURL>SERVERNAME:1099</option>`
- Document** `<option name=SyslogReader/LogFile/FileName>SOMEPATH/FILE</option>`
- Step 2** Stop the Syslog Reader. Run `/etc/init.d/truecontrol.syslogreader stop`.
- Step 3** Remove the `/usr/local/rendition` directory.

- Step 4** Follow the install instructions in the Solaris SyslogReader **ReadMe.txt** file. Be sure to include the correct values from the **probe.rcx** file.
-

Important File is not Restored After CiscoWorks NCM Upgrade

To ensure that no settings or files are lost during an upgrade, backup the entire CiscoWorks NCM directory to a safe location before starting the upgrade. For example, if you installed CiscoWorks NCM in c:\CWNCM, backup the entire directory to a safe location.

The current CiscoWorks NCM upgrade process does not restore the *<CWNCM Install Dir>\jre\reporting.rcx* file.

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

Installing the Latest Driver Pack (for new installs only)

CiscoWorks NCM1.3 SP1 requires that you install the latest CiscoWorks NCM Incremental Driver Update (IDU) after you install CiscoWorks NCM, otherwise you will experience a regression in functionality. Before installing CiscoWorks NCM1.3 SP1, go to <http://www.cisco.com/cgi-bin/tablebuild.pl/cwncm-crypto> and download the latest CiscoWorks NCM IDU. After installing CiscoWorks NCM, install the latest CiscoWorks NCM IDU.

Advanced Encryption Standard (AES) Encryption

If you have installed a previous version of CiscoWorks NCM with Advanced Encryption Standard (AES) encryption enabled and upgrade to CiscoWorks NCM 1.3 SP1, all AES encrypted data is not propagated or used after restarting the CiscoWorks NCM server. To solve this issue:

- Step 1** Stop the CiscoWorks NCM Management Engine.

- Step 2** Change the following lines in the **cwncm/jre/appserver.rcx** file:

From:

```
<option name="CRYPTO/ALGORITHM">AES</option>
<option name="CRYPTO/ALGORITHM/KeySize">256</option>
```

To:

```
<option name="CRYPTO/ALGORITHM">AES</option>
<option name="CRYPTO/ALGORITHM/KeySize">128</option>
```

- Step 3** Log in to the database.

- Step 4** Change the **Crypto Key**. For Oracle, enter:

```
update RN_CRYPTO_KEY set ModeType = 4
```

- Step 5** Restart the CiscoWorks NCM Management Engine.
-

Using Gateways

When upgrading to CiscoWorks NCM 1.3 SP1 where Gateways are used, after the upgrade you must run the **Deploy Remote Agent** task to re-install the upgraded Satellite agent on all of the remote Gateways. Refer to the *CiscoWorks NCM Satellite User's Guide* for information on configuring the CiscoWorks NCM Satellite functionality.

Using the New Export/Import Policy Feature

The Export Scripts feature enables you to export command and diagnostic scripts to a file for storage, offline editing, or transferring to another CiscoWorks NCM server.

The Import Script feature enables you to import command and diagnostic scripts created on another CiscoWorks NCM server or edited offline.

To use the Export Scripts feature, do the following:

-
- Step 1** From CiscoWorks NCM navigate **Devices > Device Tools > Export Scripts**.
 - Step 2** Select the scripts to export.
 - Step 3** Click **Export**.
 - Step 4** Click **Save**.
 - Step 5** Specify the file where the scripts are to be exported. For example, /my_scripts.
 - Step 6** Click **Save**.
-

To use the Import Scripts feature, do the following:

-
- Step 1** Copy the export file to the <CWNCM_Install_Dir>\server\ext\jboss\rendition_imports folder where CWNCM_Install_Dir is the install location of CiscoWorks NCM.
 - Step 2** Change the file's extension to **.imp**.
 - Step 3** Navigate **Admin > Start/stop services** and click **Reload Content**.
-

CiscoWorks NCM 1.3 SP1 Install Issues

You might encounter the following issues when installing CiscoWorks NCM 1.3 SP1. Where possible, workarounds have been provided.

Using the CLI Installer on Solaris and Linux Platforms

When installing CiscoWorks NCM 1.3 SP1 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 1.3 SP1 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 1.3 SP1 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 1.3 SP1 client-only using the CiscoWorks NCM 1.3 SP1 Install Wizard:

Linux Platform: **Linux_ServicePack_4534-043008_Setup.bin**
Solaris Platform: **Solaris_ServicePack_4534-043008_Setup.bin**



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: Inadequate password length causes install to fail

When installing CiscoWorks NCM 1.3 SP1 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 fails unless a local SQL Server admin account is used to connect to server

The CiscoWorks NCM 1.3 SP1 Installer requires local SQL Server authentication to connect to the database server.

It cannot authenticate to SQL Server 2005 using a Domain account with Local Administrator privileges. You must have a local administrator account on the machine running MS SQL 2005 or the connection to SQL Server will fail, as will the CiscoWorks NCM install.

Using more than one dollar sign (\$) character in any input, including password inputs, causes the installer to fail

When installing CiscoWorks NCM 1.3 SP1, ensure that any entered values 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 empty variables. As a result, entered values are parsed incorrectly. For example, if your CiscoWorks NCM database password is \$N\$CM, the CiscoWorks NCM installer parses 'NC' as the password and fails to connect to the database. (Note: This issue is not limited to a specific database or just password fields.)

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

During Linux install, CiscoWorks NCM shuts down the Syslog daemon and renames syslog.conf

When installing CiscoWorks NCM 1.3 SP1 on Linux, the CiscoWorks NCM Installer renames the `/etc/syslog.conf` file to `syslog.conf.rm` and stops the Syslog daemon. This could interfere with general log management on the Linux server.

Workaround: After the CiscoWorks NCM 1.3 SP1 install is complete, rename the `/etc/syslog.conf.rm` file to `syslog.conf` and restart the Syslog daemon.

The default CiscoWorks NCM 1.3 SP1 return email address is invalid

When CiscoWorks NCM 1.3 SP1 is installed, CiscoWorks NCM sets the return email address to **nobody@localhost**. This is an invalid email address on many present mail servers and can 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 you change the return CiscoWorks NCM email address to a valid email address immediately after the CiscoWorks NCM install is complete.

To do this:

-
- Step 1** Log into CiscoWorks NCM as an administrator.
 - Step 2** Navigate **Admin > Administrative Settings > Server**.
 - Step 3** Under the **Servers** section, set the **SMTP From Address** to a valid email address.
 - Step 4** Click **Save**.
-

CiscoWorks NCM 1.3 SP1 cannot use Integrated TFTP Server or Syslog Server post installation

If the **/etc/hosts** file on a Unix or Linux server is not configured properly prior to installing CiscoWorks NCM 1.3 SP1, 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 1.3 SP1, or after installing CiscoWorks NCM 1.3 SP1 do the following:

-
- Step 1** Navigate **Admin > Administrative Settings > Server**.
 - Step 2** On the **Administrative Settings > Server** page, under the **Servers** section, 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.)
-

Installing CiscoWorks NCM 1.3 SP1 on Solaris or Linux

When installing CiscoWorks NCM 1.3 SP1 on a Solaris or Linux platform, the version of Nmap distributed with CiscoWorks NCM (Nmap 3.81) is required for Nmap scanning when running the Detect Network Devices task. (Refer to Chapter 1 in the *CiscoWorks NCM User's Guide* for Nmap installation instructions.)

CiscoWorks NCM could 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:\ could 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 might 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.

CLI Installer

Any CLI commands sent while the CiscoWorks NCM install/upgrade is uninstalling are not executed until the uninstall finishes. As a result, your system could appear to hang. Do not issue CLI commands until the uninstall is complete.

Caveats

Please read the following regarding usability issues before using CiscoWorks NCM 1.3 SP1.

Uninstalling CiscoWorks NCM does not remove the registry setting

After doing an uninstall of CiscoWorks NCM on a Windows platform, the registry key is not removed until you reboot the system. Until you reboot, you will be unable to install the CiscoWorks NCM HP NNM connector.

Changing a Device's Site

If you edit a device and change the Site, when you click **Save Device**, you could receive the following error message: **Device with IP address Default Site: x.x.x.x already exists in group MySite**. Clicking **Save Device** again saves the device with the new Site.

Advanced ACL Scripts

Selecting **Update Script** when specifying an advanced ACL script can lock-in values. As a result, running (or re-running) the script could result in variables not being updated properly.

Workaround: Avoid using **Update Script** with advanced ACL scripts.

Use of Dollar Signs (\$) in Scripts

If generating a script from a Telnet/SSH session log, the script will fail or perform in unexpected ways if the session contains dollar signs (\$) in the executed commands.

Template Scripts

When using template scripts (i.e., Batch insert line into ACL by handle), selecting the **Run Again** option will rerun the same script. Attempting to change fields will not change the script that is run.

Twist Authentication Server

To change the Hostname or IP address of the Twist Authentication server, you must restart the CiscoWorks NCM Management Engine. Otherwise, CiscoWorks NCM will continue to attempt to use the previous Twist Authentication server.

Auto-remediation Scripts

Because policy rules have more than one condition, variables include the prefix of **tc_policy_manager_custom_**, followed by an index letter of condition and index number of matches in the condition, for example: **\$tc_policy_manager_custom_b_0\$**.

OS Analysis Task

When using CiscoWorks NCM in an environment with overlapping IP addresses, the OS Analysis task is not supported for devices behind remote Realm gateways. OS Analysis tasks run on devices in the locally reachable network. This could result in an image recommendation being incorrect for devices behind the gateway. Keep in mind that CiscoWorks NCM will report OS recommendations for a device in the default Realm instead of a remote Realm if they share an IP address.

Device Tasks Ignores User-defined *enforce_save* Device Variable

Device tasks that modify a device's configuration, such as the **Deploy Password** or **Deploy Configuration** tasks ignore the setting for the *enforce_save* device access setting. As a result, the current configuration is always saved to startup (via a mechanism such as **write memory**).

Workaround: The **DeviceInteraction/EnforceConfigurationSave/ConfiguringModels** configuration option in **appserver.rcx** can be set to false. This has the effect of disabling the save from running to startup configuration for all device tasks that reconfigure the device.

Email Report Task

When scheduling an Email Report task, if you select a report other than Summary Reports in the **Reports to run** field, the task is reported as failed. However, the report is successfully emailed to the recipient. Please disregard the error message.

Potential for Task Failure When Using Reserved CiscoWorks NCM Characters in Device Prompts

There are eleven characters with special meanings to CiscoWorks NCM:

- Opening square bracket ([)
- Opening round bracket and the closing round bracket (()).
- Backslash (\)
- Caret (^)
- Dollar sign (\$)
- Period or dot (.)
- Vertical bar or pipe symbol (|)
- Question mark (?)
- Asterisk or star (*)
- Plus sign (+)

If you use these characters in a device prompt, there is the possibility that null pointer exception errors could occur during tasks execution. As a result, the task will fail. These characters should not be used when naming devices that interact with CiscoWorks NCM.

Oracle Database Errors Cause Failed Tasks and Other Issues

Due to a bug in the JDBC Oracle driver, it is possible for the driver to cause database errors, causing tasks to fail and other issues. The information you will see in the error message is **OALL8 is in an inconsistent state**.

Workaround: Restart your server if the problem persists.

ACLs with the Same Name, but Different Case in CiscoWorks NCM, is not Recommended

CiscoWorks NCM supports case-sensitivity in ACL names. As a result, you can have two ACLs with the same name, but different case. If you delete one of those ACLs, however, all ACLs with the same name are deleted, regardless of the case. Cisco does not recommend multiple ACLs with the same name, but differing case in CiscoWorks NCM.

Downloading Software Images from Cisco.com

You can download software images from Cisco.com for devices that are not currently in your CiscoWorks NCM system. However, to be able to successfully deploy the software image, you may need to modify the driver and/or model information.

Workaround:

1. From the **Devices** menu, select **Device Tools** and click **Software Images**. The Software Images page opens.
2. In the **Action** column, click **Edit** for the software image you want modify. The Edit Software Image page opens.
3. In the **Image Set Requirements** field, modify the driver and/or model information to be compatible with the device in CiscoWorks NCM.
4. Click **Save Software**.

Multimaster Distributed System: Importing Devices

If you import two devices with identical IP addresses into two separate CiscoWorks NCM Cores at approximately the same time, there is currently no way to detect the possibility of a duplicated device.

Workaround: Manually run the Deduplication task after importing devices if you have imported two devices with identical IP addresses into two separate CiscoWorks NCM Cores at approximately the same time. The duplicated devices will be set to **Inactive**. (Refer to Chapter 7, Scheduling Tasks, in the CiscoWorks NCM 1.3 SP1 User's Guide for information on running the Deduplication task.)

Multimaster Distributed System on SQL Server

If you see a conflict for which the **reason_text** field does not reference a constraint name, it is possible that CiscoWorks NCM automatically resolved the conflict. However, you might have to manually resolve the conflict. In the former case, simply delete the conflict. In the latter case, make the appropriate corrections and then delete the conflict. The following is an example of a **reason_text** field from a conflict that does not reference a constraint name:

```
reason_text A row insert at 'red-dalmssql102.ds2880db2' could not be
propagated to 'RED-DALMSSQL101.ds2880db1'. This failure can be caused by a
constraint violation. The merge process was unable to synchronize the row.
```

CiscoWorks NCM Core Gateways

You cannot configure redundant CiscoWorks NCM Core Gateways in the same CiscoWorks NCM Realm as a single CiscoWorks NCM Core.

Workaround: Edit the **adjustable_options.rcx** file and add the other CiscoWorks NCM Core Gateways' IP address(es):

```
<array name="rpc/allowed_ips">
<value>10.255.54.10</value>
</array>
```

Detect Network Devices Task

The CiscoWorks NCM system prevents you from inadvertently running more than one Detect Network Devices task concurrently. Although the Detect Network Devices task generates only a minimal level of traffic, CiscoWorks NCM provides this protection to help minimize additional traffic when running duplicate or additional Detect Network Devices tasks simultaneously. If a second or third Detect Network Devices task is scheduled while an earlier Detect Network Devices task is running, CiscoWorks NCM will place the new task(s) in the **Waiting** state. The task(s) will run individually after the first Detect Network Devices task has completed.

Batch Editing Parent Device Groups or Device Groups with No Devices Results in Invalid Error Message

When you batch edit parent device groups or device groups/partitions that have no devices, an invalid error message is displayed: You do not have Modify Device Permission for any of the devices you selected.

Workaround: To batch edit all devices in a parent device group, do a batch edit against each child group in the parent device group.

Use of the Dollar Sign (\$) in Perl Code

If you convert a Telnet/SSH Proxy session that contains a dollar sign (\$) to Perl (such as a script that puts a \$ in the banner), CiscoWorks NCM does not properly escape the dollar sign (\$) in the generated Perl code.

Workaround: Edit the script and put a backslash (\) in front of the dollar sign (\$).

Diagramming

CiscoWorks NCM applies an absolute value for the **text height** attribute for interface and port labels shown in Visio diagrams. When the Visio VDX file is loaded, Visio assigns an incorrect formula to the **text height** attribute. As a result, when you have more than two lines of annotated text (i.e. a label) for an interface or port and you attempt to copy and paste, the label of the new interface or port is displayed improperly and could hide the interface or port icon.

Workaround: Click the **Text Tool** option on the Visio tool bar and move the label so as to expose the interface or port icon.

Passing Your CiscoWorks NCM Password to Advanced Scripts

When using advanced scripts, `$tc_user_password$` does not work.

Workaround: Use `$Password$` instead of `$tc_user_password$`. Note that `$Password$` can only be used in the Parameters part of the advanced script, so you'll need to add code to your script to get the password from the command line arguments when the script runs.

Multimaster Distributed System External Authentication

When using external authentication in a Multimaster Distributed System environment, the External Authentication Type, for example TACACS+ or Active Directory, is global (i.e., shared between all CiscoWorks NCM Cores). Specific authentication server information is CiscoWorks NCM Core specific.

Workaround: Set the **External Authentication Type** to **None** on the **Administrative Settings > User Authentication** page. Configure each CiscoWorks NCM Core individually with authentication server information or Active Directory setup. After all CiscoWorks NCM Cores have been configured, set the **External Authentication Type** on any CiscoWorks NCM Core. The External Authentication Type setting is replicated to all CiscoWorks NCM Cores.

Multimaster Distributed System Performance

When running a Distributed System, if you are deleting many objects simultaneously, the system may take a while to push transactions for large delete operations.

Duplicate IP Addresses with Multiple Sites

If your system is configured with multiple Sites in different Realms, you could see duplicate IP addresses if you select the Multiple Devices/Groups option on a New Task page when browsing the Inventory Group using the Device Selector.

Workaround: Using the Device Selector, browse to devices using the specific Site Group.

RADIUS External Authentication

When setting up a user to authenticate using RADIUS, if the RADIUS server does not respond, CiscoWorks NCM still authenticates the user against the CiscoWorks NCM local password, even if you instruct CiscoWorks NCM not to fail-over on external authentication.

Unresponsive Script Warning Message in Mozilla Firefox 1.5

When uploading a software image (New/Edit Software Image Set page) or any CiscoWorks NCM page that requires file uploading, if you are using Mozilla Firefox 1.5 and the file size is relatively large, you could see a warning message during uploading that indicates a script may be busy or has stopped responding.

Workaround: Click **Continue**. If you want to avoid this warning message in the future:

1. Enter **about:config** in Firefox's address bar.
2. Scroll down to the **DOM.*** section.
3. Locate the value for **dom.max_script_run_time**.
4. Edit the default value **5** to something higher, for example **20**.

Juniper Devices with SCP Enabled do not Capture Running Configurations

If your Juniper device has SCP enabled, the copied configuration may not be the one running on the device.

Workaround: Always use CiscoWorks NCM to manage configuration changes or save the configuration on the Juniper device.

Scripts: Output Results in HTML Format

When executing an advanced script or a **Run External Application** task, any text that the advanced script or external application writes to **stdout** is stored in CiscoWorks NCM as the task result. Typically, this output is treated and displayed as plaintext. As a result, before CiscoWorks NCM displays the task results, it will escape any characters that would affect the HTML rendering, for example converting `<` to **<**.

However, you may want to create an advanced script that outputs its results in HTML format. In this case, none of the output characters would be escaped, so the results displayed would include any applicable HTML formatting. To indicate to CiscoWorks NCM that your script outputs HTML results, the first item that your script writes to **stdout** must be **<html>**. If your script output begins with anything other than **<html>**, the script results will be treated as plaintext.

Nmap Scanning

Careful consideration should be taken when identifying the network range you are going to scan. Some network topologies can result in very long scans. In addition, it is recommended that you do not scan Internet addresses. If you think your Nmap scan will take more than a few minutes, you can use several Nmap options, for example **--max_scan_delay <milliseconds>**, setting **<milliseconds>** to a value between **1** and **1000**. Nmap will throttle up to 1000ms max as packets are dropped.

Keep in mind that Nmap settings can be changed using the Administrative Settings option under Admin on the menu bar, and selecting the Device Access option. Please refer to the Nmap documentation at www.insecure.org for detailed Nmap information.

Cisco Catalyst Switches

Cisco has recently reported an issue with their Catalyst switches running CatOS 8.3(3). Cisco has found that these devices could crash when you connect to them via SSHv2 (for example from an SSH client, such as SecureCRT or Putty). By default, CiscoWorks NCM uses SSHv2 as the primary access method to network devices. Therefore, there is a substantial risk that a Catalyst switch running 8.3(3) could be reset when managed by CiscoWorks NCM.

Workaround: Upgrade your Cisco Catalyst to CatOS 8.3(4). If this is not possible, edit your Catalyst devices running 8.3(3) in CiscoWorks NCM to use only SSHv1 or Telnet for device access.

SecurID Software Token Software, Version 3.0.5

If the CiscoWorks NCM server is installed with the 3.0.5 SecurID token software, turn off copy protection when exporting SecurID software token keys on the RSA server. Otherwise, CiscoWorks NCM reports an error when accessing SecurID software tokens. A patched version of the SecurID software is available at RSA's website <http://www.rsasecurity.com>.

Canceling or Deleting Tasks

Some CiscoWorks NCM tasks will spawn external processes to run PERL or Expect scripts, or to run user-provided executables or shell scripts. Under certain circumstances, CiscoWorks NCM may not be able to kill these external processes when the spawning task is cancelled or deleted. This could include scripts that spawn sub-processes or processes that are coded to catch kill signals.

Workaround: Manually stop the external process on the CiscoWorks NCM server.

Deploy to Startup Config and Reboot not Supported via SNMP

CiscoWorks NCM can deploy a configuration file to the startup configuration and reboot the device via command line only. If the device is configured for SNMP access only (see the *CiscoWorks NCM 1.3 Device Driver Reference*), deploy startup and reboot will fail.

Software Center: Deploying Software

When deploying software to a device, it is possible for the configuration file currently on the device to no longer be acceptable to the device. This is more likely during an OS downgrade. (OS upgrades are usually handled via upwards compatibility.) It is always a good idea to test the functionality of a given OS version before deploying it on a production network. When downgrading OS versions, the device configuration file may need to be manually updated. It is very important to make this change before rebooting the device, otherwise the device could attempt to use the invalid configuration file and become unresponsive.

For the Aironet 1100, if you deploy software with the Reboot option, the Aironet 1100 might not restart correctly. In fact, the Aironet 1100 might be left inaccessible and the Deploy Software task could continue running for up to an hour. This can also occur when manually deploying software.

Workaround: Turn the device off and back on to restore connectivity. Alternatively, you can avoid the problem by turning the radio off before deploying software.

CiscoWorks NCM does not support BayRS software downgrades from 15.x to 14.x. Although the software update will function, the device configuration file after the reboot is not valid for the new software image. The device will need to be rebooted, and the configuration file saved with the new code via a console connection.

Workaround: You can pre-deploy a valid configuration file for a software update. The configuration file should be built by SiteManager for the particular version of code you are deploying.

Software Center: Downgrading Nortel OS and Rebooting Could Leave Device Inaccessible

When you deploy an earlier version of an OS to a Nortel device, you could experience unexpected results, including the device becoming inaccessible. This occurs because commands and configuration methods might have changed, and these might not work correctly for the earlier OS when downgrading.

Be sure to review the configuration file before downgrading and possibly test the procedure in a lab before migrating the change to your production network. You should also configure out-of-band access via a console port before downgrading a device OS.

Software Center: Cisco IOS devices

Software Center does not support 11.x drivers for Cisco IOS 11.x. Although it is possible to downgrade a Cisco device from 12.x to 11.x, it is not possible to upgrade from 11.x to 12.x. In addition, if you try to perform a software upgrade, the existing image on the device can be deleted, and the software update task will fail. Consequently, there is no way to upload an image to the device.

Workaround: Use a TFTP server to manually recover the lost image to the device.

Batch Insert ACL Line Option

When using the Batch Insert ACL Line option (**Devices > New Device Task > Batch Insert ACL Line**), the **Task Options** section on the New Task- Run Command Script page does not contain script content. While the Command Script to Run field correctly displays Cisco IOS Insert (or Remove) Line into (or from) ACL by handle, it does not present the script or script variables for execution until a device or device group for which the script supports is selected.

Software Center: Reboot Option

The Software Center reboot option is not supported when a BayRS device is configured to receive its configuration file from the network. The BayRS device returns an error message when CiscoWorks NCM attempts to reload the device.

```
[1:TN]$ boot - 1:config
Configuration source is network - override allowed only when source is local.
```

Workaround: Configure the BayRS device to use the locally stored configuration file.

Software Center: Cisco IOS 2500

There is a problem with the Cisco IOS 2500 that can affect the CiscoWorks NCM Software Update Center. With a Cisco IOS 2500, running Version 12.3(3) (distributed as c2500-i-1.123-3.bin), some file systems are inconsistently reported. The Software Update Center is not able to retrieve a list of files on devices running this software version. Additionally, the Software Update Center cannot deploy software to the Cisco IOS 2500 running Version 12.3(3) because the Software Update Center cannot query the device for the available locations (**dir ?** does not return **flash:** and **copy tftp ?** does not list **flash:**).

Workaround: Although the Software Update Center cannot execute a software upgrade to the Cisco IOS 2500 running Version 12.3(3) by specifying a single device (the missing flash: slot information prohibits it), you can perform a software upgrade by creating a device group that contains only the Cisco IOS 2500, and then execute a software upgrade to that group.

Tasks: A task Scheduled for the 31st Might Run on the 1st

If you schedule a monthly recurring task for the 31st of every month and that task runs during a month that contains fewer than 31 days, CiscoWorks NCM will run the task on the 1st, 2nd, or 3rd day of the next month depending on how many days less than 31 the previous month contains. For example, if you schedule a task in February (with 28 days) for the 30th, the task will actually run on March 2nd. If you want to run the task on the last day of the month, you must set the date correctly.

Inventory: Data from Device Overwrites Manually Entered Values

Certain data on the Device Details page (and other pages) is auto-populated. If you manually change the data, CiscoWorks NCM overwrites the values when the next snapshot occurs. The device-specific values are listed in the CiscoWorks NCM Device Driver Reference per device.

The automatically populated data includes:

- Domain Name
- Host Name
- Model
- Serial Number
- Location
- Vendor

Tasks: Running External Application Tasks Presents a Possible Security Risk

All Run External Application tasks run the application with root (UNIX) or system (Windows) privileges. This is a potential security risk that should be acknowledged by the System Administrator before using the Run External Application feature. Contact Technical Support to learn how to run CiscoWorks NCM without root/system privileges.

Console Server: SSH access is not Supported

CiscoWorks NCM does not support console server access via SSH. If you use a console server to access a device, you must use the Telnet connectivity. In other words, on the New Device page/Edit Device page, if **Use to access device** is checked in the Console Server Information section, you should make sure that the **Telnet** option in the Connection Information section is also checked.

Extreme Devices: Configuration Comments can Cause Misconfiguration

On Extreme devices, adding inline comments between multi-line commands, such as user account commands or set banner commands, can cause serious problems if the resulting configuration is deployed.

Workaround: Do not add inline comments between multi-line commands. Add comments on the line above the start of a command.

Diagnostics: When to Run Icmp Tests

Use ICMP tests only to verify connectivity occasionally or after a change. They are not a replacement for monitoring software. You should schedule ICMP tests no more than once per 10 minutes.

Scripts: Cannot Save Template or Command Scripts with a Period in the Name

Command Scripts, Templates, and Custom Diagnostics cannot have a period in the name. Use underscores or dashes in place of a period.

Scripts: Cannot Save Command Scripts with Quote Marks in the Name

Do not use quote marks when naming command scripts. If you do, you will not be able to select and run the command script.

Reports: Checkpointing can Cause Reports to be Inflated

The **Make Snapshot a Checkpoint** option on the Snapshot Task page (**Task > New Task > Take Snapshot**), stores the configuration file regardless of whether it changed. However, even if there is no change, the snapshot still appears as a configuration change on the Home page, Summary reports, Configuration Change search results, and so on. As a result, the number of configuration changes includes the check-pointed configurations, and therefore these counts may not be accurate.

Syslog Messages

Certain Syslog messages (compliant with the Syslog RFC) sent from devices could have the same sender IP address as the IP address in the Syslog messages. In this case, CiscoWorks NCM does not process the Syslog messages or schedules events. As a result, change detection will not work as expected on these devices.

Sending Reports to External Email Addresses

Even though you may have properly configured CiscoWorks NCM to contact your SMTP server, for network security reasons your SMTP server might have been configured to reject messages from the CiscoWorks NCM server address. In this case, you would see the following error message, and any CiscoWorks NCM messages would not be delivered.

```
Error occurred when sending email. Please check the email address and/or your SMTP
server settings.
```

If this occurs, you will need to configure the SMTP server to enable the CiscoWorks NCM server to relay email messages through it.

NetScreen Devices

NetScreen devices could timeout during the discovery process. This does not occur on all platforms, however.

Workaround: Edit the NetScreen device information and set the **standard_timeout** device variable to five seconds. This will enable the NetScreen device to discover via the Command Line Interface (CLI).

When monitoring NetScreen devices, for CiscoWorks NCM to detect that the device's interfaces are administratively down, the interface must be configured as down using the **set interface untrust ident-reset** command.

Scripts: Command Scripts and Templates for Cisco Aironet VxWorks Devices

CiscoWorks NCM supports command scripts and templates for Cisco Aironet wireless access points running VxWorks software (for example OS versions 11.23T & 12.01T1). Because scripts and templates are deployed differently to Cisco Aironet devices, CiscoWorks NCM uses TFTP to deploy a file containing the script to the device. Some OS versions on Cisco Aironet devices accept only a limited size file via TFTP. In these cases, any excess commands are ignored and will not be run on the device. However, the script will still report successful execution. Devices exhibiting this behavior will accept no more than approximately 130 lines of text and ignore the rest without reporting an error.

Workaround: Use scripts smaller than 100 lines, or use multiple scripts to deploy larger sets of configuration commands to the device. If possible, upgrade the device to a newer version of code, ideally a version of IOS (12.2).

BayRS device can lose ability to provide snapshot

Occasionally, the BayRS device can enter a state in which it cannot provide a snapshot. Snapshot tasks fail with the following error message:

```
File retrieval error
```

Workaround: Rebooting the BayRS device restores the normal state on the device.

Known Limitations and Problems

This section contains information about the limitations and problems known to exist in the CiscoWorks NCM 1.3 SP1 product.

CSCse09644—The **cwncm_import** script does not parse the hostname as present in the CSV file.

Description: When exporting some devices from DCR into the CSV file using **dcr_export.sh** or from Device Management UI of LMS, the **cwncm_import** script does not parse the hostname (present) in the CSV file; instead, it substitutes the IP Address as the hostname for all these imported devices.

Workaround: You can manually change the Hostname by looking up the corresponding name in the CSV file. This issue will be fixed in a future release.

CSCse11820— Installation hangs if you provide incorrect Database credentials.

Description: Oracle is installed successfully and you proceed with CiscoWorks NCM installation. If you provide any incorrect database credentials (port number, DB name, or password) while configuring the CiscoWorks NCM Database, then CiscoWorks NCM hangs while trying to connect to the database.

Workaround: Stop the installation using the Windows task manager. Restart the installation and enter the correct credentials.

CSCse16848—Duplicate entries are seen in the software updates report.

Description: When adding more than one image set from **Devices > Device tools > Software Images**, the weekly report incorrectly reports two successful updates when this is not the case.

Workaround: There is no known workaround for this issue.

CSCsh28136—Installer fails to copy licenses from a directory whose name has spaces.

Workaround: Make sure that the directory and directory path where the license files are being copied do not have spaces in their names. If you must use directory and directory path names containing spaces, make sure to quote the entire path.

CSCsk95754—SNMPv3 Engine Id check is not needed.

Description: For a device which has SNMP-v3 configured, from Inventory, select the device. Navigate **View > Device Details > Software Upgrade Recommendation**. Select any image to launch the details. Following warning message will be displayed in the details:

```
SWIM1094: SNMP-V3 parameters is incorrect or not available for the device. Check
whether the SNMP-V3 password, SNMP-V3 algorithm, and SNMP-V3 engine ID is
configured for the device.
```

Workaround: Ignore the message if the SNMP-V3 password and SNMP-V3 Algorithm are configured correctly.

CSCsl38283—Snapshot fails if banners are present on the device on the Linux platform.

Workaround: Removing the banner on the device should solve the problem.

CSCsl39839—**Detect Network Devices** will not detect devices with SNMPv3 configuration.

Description: Devices configured with SNMPv3 parameters will not be discovered when you perform the **Detect Network Devices** task.

Workaround: Configure SNMPv2 parameters on devices to discover them using the **Detect Network Devices** task.

Accessing the CiscoWorks NCM Documentation Set

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 SP1 you will need.



Tip

To cut and paste a two-line URL into the address field of your browser, you must cut and paste each line separately to get the entire URL without a break.



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 Network Compliance Manager *might* not include links to the latest documents.

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>

Notices

The following notices 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:

Copyright © 1998-2007 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:

Copyright © 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].

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0804R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.