



Release Notes for CiscoWorks Network Compliance Manager, 1.4.02

Revised: May, 2009, OL-19103-02

These release notes include important information regarding CiscoWorks Network Compliance Manager (NCM), Release 1.4.02.



Note

The CiscoWorks NCM 1.4.02 release requires Driver Packs dated April 2009 (or later) to operate properly.

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:

- [What’s Been Fixed in CiscoWorks NCM 1.4.02, page 2](#)
- [Documentation Addendum, page 5](#)
- [Features in CiscoWorks NCM 1.4, page 8](#)
- [What’s Been Fixed in CiscoWorks NCM 1.4, page 9](#)
- [Supported Platforms, page 13](#)
- [Supported Databases, page 14](#)
- [Additional CiscoWorks NCM Configurations, page 15](#)
- [Additional Required Applications, page 16](#)
- [Hardware Requirements, page 17](#)
- [Caveats, page 18](#)
- [Resolved Problems, page 29](#)
- [Known Limitations and Problems, page 30](#)
- [Accessing the CiscoWorks NCM Documentation Set, page 32](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 33](#)
- [Notices, page 33](#)

What’s Been Fixed in CiscoWorks NCM 1.4.02

The following issues have been fixed in CiscoWorks NCM 1.4.02.

Table 1 *Issues Fixed in CiscoWorks NCM 1.4.02*

Bug Summary	Fix Description
Issues with devices using console TCP port(s) in the same remote Realm Gateway.	You can now edit the Core Gateway properties file and the remote Realm Gateway properties file to enable the console TCP port(s) to be reachable.
Users without privileges are able to view device configurations.	Users without privileges can no longer view device configurations.
Unable to archive the last successful IP address.	The last successful IP address is now tried first.
The anchor to set the Cisco.com password appears as HMTL instead of a link on the Download Software Image page.	The anchor to set the Cisco.com password now appears as a link on the Download Software Image page.
An error message occurs when trying to delete an event rule.	You can now delete an event rule.
The Deploy Config task fails when there is an issue with a Policy Manager regular expression.	You can now run the Deploy Config task even if there is an issue with a Policy Manager regular expression.

Table 1 **Issues Fixed in CiscoWorks NCM 1.4.02 (continued)**

Bug Summary	Fix Description
Unable to write advanced auto-remediation scripts.	Advanced scripts now work as auto-remediation scripts.
Password rules are not parsed if they are assigned to the default partition and to a dynamic group.	You can now assign a password rule to the default partition and to a dynamic group.
When using TACACS integration, CiscoWorks NCM fails when using a backslash character (\) in a username.	You can now include a backslash character (\) in a username.
Cannot generate the "All Devices Without Driver Assigned" report.	You can now generate the "All Devices Without Driver Assigned" report.
SSH library with keyboard interactive support is not available.	Added new updated SSH library with keyboard interactive support.
CiscoWorks NCM does not check for missing Parent groups.	CiscoWorks NCM now checks for missing Parent groups.
Passwords are not masked when a "limited access" user searches for a configuration.	Passwords are now masked when a "limited access" user searches for a configuration.
Event-driven group recalculation adds incorrect devices to groups.	Event-driven group recalculation now adds the correct devices to groups.
Searching for, and then saving the search results as a new device group, fails.	You can now search and save search results as a new device group.
User permissions are inconsistent on task pages.	User permissions are now correct on task pages.
Users with View permissions for a partition can view device groups belonging to other partitions.	Users without View permissions can no longer view device groups in other partitions.
Users are able to create a partition without View permissions.	Users can no longer create partitions without View permissions.
Error message is displayed after searching for policies.	Users can no longer select policies for which they do not have permission.
Tasks executed in remote Realms should not use the Secure Copy Protocol (SCP).	Tasks executed in remote Realms can no longer use the Secure Copy Protocol (SCP).
Users can configure device access settings without selecting device-specific passwords.	Device access settings are no longer available without selecting device-specific passwords.
Errors occur when updating user groups.	User groups are now successfully updated.
Tasks fail due to non-support of per-task credentials.	All tasks now support per-task credentials.
No confirmation is displayed when deleting Device Templates.	There is now confirmation displayed when deleting Device Templates.
Users with no privileges to view private groups can edit them.	Private groups are no longer displayed unless you have privileges to view them.
Auto-remediation scripts cause issues with compliance checking and snapshot tasks.	You can now run auto-remediation scripts with compliance checking and snapshot tasks.
When searching for policy compliance issues, policies are shown as applied, even if they are not.	You can now successfully search for policy compliance issues.
The proxy shell's input buffer can overflow.	The proxy shell now functions properly.

Table 1 *Issues Fixed in CiscoWorks NCM 1.4.02 (continued)*

Bug Summary	Fix Description
Searching for advanced diagnostics does not work.	You can now search for advance diagnostics.
There is no way to select the only use console port option to access devices.	You can now specify Telnet console port access to devices.
Error messages are displayed when viewing image recommendations.	Viewing image recommendations now functions correctly.
The Discover Driver option is missing in Bare-metal command scripts.	The Discover Driver option is now available in Bare-metal command scripts.
When there is more than one model assigned to an image set, the image set is not displayed in the Deployment table when running the Update Device Software task.	All image sets are now displayed in the Deployment table when running the Update Device Software task.
The Snapshot task can fail after deleting a user.	The Snapshot task now functions correctly.
Policy exceptions by hostname result in a NPE exception on deactivated devices.	Deactivated devices are now removed prior to adding new devices.
The Delete Task button does not function correctly.	The Delete Task button now functions correctly.
Incorrect change attribution with multiple users using AAA and Syslog.	Multiple users can now use AAA and Syslog without issues.
Arrow keys in the Proxy respond slowly.	The sleep time when handling escape sequences from arrow keys can now be configured so the Proxy responds more quickly.
When using Deploy to Running with commit options on Cisco IOS XR 3.7.1, the commit options are not sent properly.	The Deploy to Running with commit options on Cisco IOS XR 3.7.1 now functions properly.
Snapshot tasks using the getconfiguration_scpserver variable do not use the proper IP.	Snapshot tasks can now include the getconfiguration_scpserver variable.
Command scripts are displayed for users that should not be able to view them.	Command scripts are no longer displayed for unauthorized users.
The Service Pack Installer does not update (overwrite) the contents of the addins folder.	The Service Pack Installer now updates (overwrites) the contents of the addins folder.
Command scripts created from the Run Interface script do not require approval.	Command scripts created from the Run Interface script now require approval.
Deploying the Remote Agent to the Satellite Gateway fails if the root prompt is not pound sign (#).	Deploy Remote Agent now works correctly for root prompts with percent (%), pound sign (#), and greater than (>).
You cannot create a new policy rule with more than 5,000 characters in the text block.	You can now create a new policy rule with large text blocks.
Moving a device to a different Realm does not always work.	You can now move a device to a partition in a remote Realm.
SecurID device authentication fails.	SecurID device authentication no longer fails.

Table 1 *Issues Fixed in CiscoWorks NCM 1.4.02 (continued)*

Bug Summary	Fix Description
Network Status reports do not display policy rule violations.	Network Status reports now display policy rule violations.
Moving entities from a partition that is to be deleted to another partition affects all existing device groups and user groups.	You can now move entities from one partition to another without affecting all existing device groups and user groups.
Import/Export scripts and the Diagnostics link is enabled on the Command Scripts and Diagnostics pages regardless of a user's privileges.	You can now only Import/Export scripts and Diagnostics with the proper privileges.
Device Template provisioning does not work if there are no variables.	Device Template provisioning now functions properly.
Device Template provisioning does not work if there are no variables.	Device Template provisioning now functions properly.
Disabled accounts can login when using RSA as external authentication.	Disabled accounts can no longer login when using RSA as external authentication.
You cannot access devices using the Telnet console port.	You can now use the Telnet console port for accessing devices.
Bastion host does not function properly.	Bastion Host now functions properly.
Config Block compliance policies do not function properly.	Config Block compliance policies now function properly.

Documentation Addendum

This section contains the most recent CiscoWorks NCM 1.4.02 information that will be incorporated into the next version of the CiscoWorks NCM User's Guide and online Help files.

Task-specific Logs

Although all CiscoWorks NCM users can create a task-specific log, only users with Administrative privileges can view and download them. If you do not have the proper privileges to view and download logs, contact your CiscoWorks NCM system administrator, and if necessary have him or her provide the log information to Support.

Device Access Settings

When defining device password rules, although you are able to define multiple values for each device access setting, you should only specify one value per device access setting. If you specify a device access setting more than once, only one of the values is used, and there is no specific determination of which value will be used.

SecurID

When using SecurID to login to CiscoWorks NCM, CiscoWorks NCM supports the following token algorithms and token versions:

- AES SDTID 3.0
- SID SDTID 2.0

Manage View/Manage Partition Permissions

On the New Group and Edit Group pages, you can no longer grant **Manage View** or **Manage Partition** permissions to a user group. As a result, unless you are the CiscoWorks NCM administrator, you do not have either the **Manage View** or **Manage Partition** permission.

Password Rules

Device password rules can only be applied to **public** device groups. You cannot apply a password rule to **private** device groups.

Managing Devices Via a Console Server

If you are managing devices via a console server in a remote Realm, you must edit the Core Gateway properties file and the remote Realm Gateway properties file to enable the console TCP port(s) to be reachable.

The Core Gateway properties file is located on the Core Gateway host at:

```
/etc/opt/opsware/opswgw-GWNAME/opswgw.properties.
```

The EgressFilter entry looks like the following:

```
opswgw.EgressFilter=tcp:*:22:NAS:,tcp:*:23:NAS:,tcp:*:513:NAS:,tcp:*:8443:NAS:,tcp:*:443:NAS:,tcp:*:80:NAS:
```

To enable access to your console TCP ports, for example TCP port 7003, you need to append the following to the end of the above string:

```
,tcp:*:7003:NAS:
```



Note

You can add more than one port if necessary.

When complete, the result should look like the following:

```
opswgw.EgressFilter=tcp:*:22:NAS:,tcp:*:23:NAS:,tcp:*:513:NAS:,tcp:*:8443:NAS:,tcp:*:443:NAS:,tcp:*:80:NAS:,tcp:*:7003:NAS:,tcp:*:7004:NAS:,tcp:*:7005:NAS:
```

After saving your changes, restart the Core Gateway. Enter:

```
/etc/init.d/opswgw-GWNAME restart
```

Incorrect Port Counts

If port counts are incorrect, do the following to configure which port types are counted:

1. Stop CiscoWorks NCM.
2. Update the `<CWNCM Install Directory>/jre/adjustable_options.rcx` file and add the following entries anywhere between the `<options>` and `</options>` tags:

```
<array name="PortCount/PortTypes">
<value>Ethernet</value>
<value>FastEthernet</value>
<value>GigEthernet</value>
<value>FDDI</value>
<value>Lex</value>
<value>TokenRing</value>
<value>VGAnyLan</value>
<value>Pos</value>
<value>Serial</value>
<value>HSSI</value>
<value>ATM</value>
<value>Dialer</value>
<value>BRI</value>
<value>DSL</value>
<value>TenGigabitEthernet</value>
<value>GigEthernetTrunk</value>
</array>
```



Note Edit the above list as appropriate for the interface/port types that you want counted.

3. Replace `<CWNCM Install Directory>` with the location where CiscoWorks NCM has been installed.
4. Update the `<CWNCM Install Directory>/jre/adjustable_options.rcx` file and add the following entry anywhere between the `<options>` and `</options>` tags:

```
<option name="snapshot/force_update_model_data">true</option>
```



Note This option causes CiscoWorks NCM to recompute the port counts (and other device data) on every checkpoint snapshot even if there is no configuration change.

5. Restart CiscoWorks NCM.
6. Run a Snapshot task against Inventory to update the port counts.
7. Check the **Make snapshot a checkpoint** option on the **New Task** page. This will recompute the port counts for existing devices.

**Note**

After running the Snapshot task, you might want to remove `<option name="snapshot/force_update_model_data">true</option>` from the `<CWNCM Install Directory>/jre/adjustable_options.rcx` file to improve performance.

Java Plug-in Version

If the Connect function fails and the CiscoWorks NCM server hangs, check what version of Java you have running on your Windows system. This is an issue with the Java Plug-in to your Web browser. The issue is not on the CiscoWorks NCM server.

To check what version of Java you are running:

1. Navigate **Start - > Control Panel**.
2. Double-click **Java**.
3. In the **General** tab, click the **About...** button.
4. If you have Version 6 Update 11 or later, you must install an older JRE on your Windows system. Version 6 Update 10 and earlier are known to work.

Features in CiscoWorks NCM 1.4

CiscoWorks NCM Release 1.4 contains a number of new features and enhancements, including:

- MySQL 5.0 support—MySQL 5.0 is supported by CiscoWorks NCM 1.4 and included as part of the installer.
- Upgraded Secure Shell (SSH) Protocol library and Secure Copy (SCP) support—CiscoWorks NCM 1.4 includes upgrades of SSHv1 and SSHv2 libraries to J2SSH's Maverick package. This upgrade increases flexibility, extensibility, and security of network device management.
- Updated operating system and database support—Support is added for SUSE 10 and RHEL AS 5. Support is removed for SUSE 9, RHEL AS 3.x, Solaris 9, and Windows 2000. Support is removed for Oracle 9i, Microsoft SQL Server 2000, and MySQL 3.x.
- Bare Metal Provisioning—Provisions devices out-of-the-box. Using a “bare metal” driver, you can execute scripts against a bare metal device to bring a fully-configured device onto your production network.
- Network Device Templates—Creates a configuration template without having an actual device present. With Network Device templates, you can perform compliance checks, create policy rules, view and compare configurations (even between templates and actual devices), set password rules, and so on before you add the device to the production network.
- Security Partitions—Establishes a set of CiscoWorks NCM objects per partition to specify more granular permissions. CiscoWorks NCM objects can include devices, users, command scripts, device password rules, policies, software images, etc. Security Partitions can be combined with a permissions model, group hierarchy, distribution of devices across CiscoWorks NCM Cores, and network diagramming.
- Auto-Remediation scripts—Defines variables in the script that reference data from regular expression pattern groups in a violated policy rule. The Auto-remediation pop-up window accesses the data on the Policy Rule page to show variable mappings, generate sample code, and validate the

script before it is saved. Unlike standard command scripts, Auto-remediation scripts uses a new language syntax to iterate over matches. Auto-remediation scripts are processed and converted into command scripts that are run on network devices.

- NNMi Integration—Integrates CiscoWorks NCM with NNMi to reside on a single server. As a result, you can:
 - Launch device policy compliance report from NNMi
 - Launch command scripts and diagnostics from NNMi
 - Link to out of the box command scripts and diagnostics with NNMi
 - Designate out of service for devices undergoing change activity
 - Auto-propagate changed community strings to NNMi
 - Auto-config new devices for required NNMi management settings
 - Alert user of duplex & speed miss-match states
- VoIP support—Key elements of VoIP management include:
 - Auto-Detect VoIP, MPLS, PoE and BGP configuration elements within network devices
 - Interface QoS and ACL configuration sections are automatically parsed and displayed in the interface configuration summary for the specific interface
 - A device driver for Cisco Call Manager allowing configuration compliance checks and basic device diagnostics
- Software Image Management (SWIM) process on Gateway server—Displays SWIM-centric data for remote devices. However, remote devices are defined as devices reachable only through an CiscoWorks NCM gateway.

What's Been Fixed in CiscoWorks NCM 1.4

The following issues have been fixed in CiscoWorks NCM 1.4.

Table 2 *Issues Fixed in CiscoWorks NCM 1.4*

Bug Summary	Fix Description
Changes to command scripts do not propagate to Email & Notification tasks	When an event rule triggers a Run Command Script task, the latest version of that command script is used if the command script still exists in the system. If the command script has been deleted, the version of the command script at the time the event rule was created is used.
Failed CLI connection protocols retried multiple times	If a CLI connection method fails, CiscoWorks NCM no longer retries it multiple times.
CLI Discover Driver command should run an actual task with a TaskID	You can now schedule to run a task by the TaskID when using the CLI Discover Driver command.
SCP configuration deployments for Cisco IOS devices fail	SCP configuration deployments of configurations for Cisco IOS devices are now supported.

Table 2 *Issues Fixed in CiscoWorks NCM 1.4 (continued)*

Bug Summary	Fix Description
<i>\$tc_user_password\$</i> is unusable in advanced Perl scripts	You can now use <i>\$tc_user_password\$</i> in advanced Perl scripts (also accepted for login to the CLI or API).
API enhancements to user management	<p>User management capabilities have been enhanced to include new CLI commands and API calls, including:</p> <ul style="list-style-type: none"> • add user • mod user privileges • mod user info • activate/deactivate user • add user group • mod user group • add user to group • del user from group • del user • groupmod user group
Canceling a task on the Edit Task or Multi-task Edit page deletes the task	The Cancel Task button has been relabeled to Delete Task .
Devices in a remote Realm using the console server in the same remote Realm have issues	The console server for a device can now be in a different Realm than the Realm the device is in. CiscoWorks NCM now connects to the console server in the correct Realm.
Enable emailing configurations to a designated email address	You can now email configurations as text files to designated email addresses.
Administrative Settings submenu repeats	Multiple occurrences of menu items in the Administrative Settings submenu have been removed.
Visio diagrams do not open after generating them in CiscoWorks NCM	You can now generate Visio diagrams in CiscoWorks NCM.
Modifying a partition name is not reflected properly when using the API	You can now modify a partition name using the API.
Editing a software deployment task causes the deletion of the current software image to be reset	The Update Device Software task enables you to schedule the deployment of software to one or more devices. You can now delete the current software image when editing an update device software task.
High Availability Distributed System replication conflicts between the <i>RN_Auth_rule</i> tables	You can now change the password rule order on a CiscoWorks NCM Core. The change is replicated to other CiscoWorks NCM Cores.
Viewing device details for local MAC Addresses should show interface configuration information	On the Device MAC Addresses page, the View Details option now shows more information about the local interface.

Table 2 **Issues Fixed in CiscoWorks NCM 1.4 (continued)**

Bug Summary	Fix Description
Missing events for command scripts and diagnostic changes	The Command Script Changed and Diagnostic Changed events have been added.
Error calling CiscoWorks NCM WSDL API with Axis2	You can now call CiscoWorks NCM WSDL API using Axis2.
Auto-remediation scripts do not have access to policy failure details	Auto-remediation scripts now have access to policy failure details needed to correctly remediate.
Read-only access to policies does not include policy rules	Read-only access to policies now includes policy rules.
rlogin is not working on Solaris platforms	Snapshots through rlogin to a device have been fixed on Solaris platforms.
Changes to <i>soap.Api.request</i> incorrectly determine what columns to include	When the first row includes column NULL, subsequent rows did not include that column, regardless of whether it was NULL or not. Subsequent columns are now included.
<i>tc_tool</i> updates the URL for only one connection pool (Oracle)	When changing database connection information using <i>tc_tool</i> , CiscoWorks NCM no longer accesses both the old database and the new database. CiscoWorks NCM now accesses only the new database.
When using Active Directory, you cannot use Primary Group to authenticate	Active Directory authentication has been fixed to work with users whose primary group is the DOMAIN USERS group.
Image Sync does not handle boot images in a subdirectory	The Image Synchronization report now captures directory names. As a result, the Sync Image action captures the software image name.
Missing API call for modifying user groups	The mod user group API call has been added.
Add SSH support to the Perl API	SSH support has been added to the Perl API (not CLI). You can now use CONNECT Module between the client server and the CiscoWorks NCM application server.
<i>SNMPScanner.java</i> forces a CiscoWorks NCM reload to gather detect network logs at Trace	CiscoWorks NCM now detects when a logging level is changed to Trace.
Active Directory fails to login to CiscoWorks NCM if the user account has a “/” character in the Fullname field	You can now use the “/” character in a user's full name.
Deadlock in the SSH2 client during large input	CLI connections through CiscoWorks NCM can now handle large inputs.
Upgrading a CiscoWorks NCM system that is not running as root fails	You can now upgrade a CiscoWorks NCM system that is not running as root.
Using SecurID with SSH Version 2 fails	You can now use SecurID with SSH Version 2.

Table 2 Issues Fixed in CiscoWorks NCM 1.4 (continued)

Bug Summary	Fix Description
Console access to reuse existing socket connections is needed	CiscoWorks NCM now uses an existing connection to a console server if there is one. This is more efficient and avoids some failure scenarios.
Editing multi-task projects causes issues	You can now edit multi-task projects.
Admin setting to enable audit logs fails	You can now enable audit logs.
Task search results do not include the Results column	Task search results now include the Results column.
Regular expressions are not displayed correctly in policy rules	The rendering of regular expressions in the must contain only operator for policy rules has been fixed. The But must not have any additional lines section now properly displays regular expressions.
Searching for devices by password rule on SQL Server fails	You can now search for devices by password rule on SQL Server.
CSV output for the device compliance field is inconsistent with policy compliance search results	Device compliance search results are now the same in the CSV file and on the screen.
Issuing <i>mod device -ip 1.2.3.4 -asset somestring</i> revokes SSH as a connection method	The SSH connection method is no longer removed when the asset tag is added.
Changing dynamic group to static group causes problems	You can now change a dynamic group to static group.
Modifying diagnostic searches criteria fails	You can now modify diagnostic searches.
Pre/post-task Snapshot setting hints are not honored for one-time use scripts	Pre/post-task Snapshot setting hints are now honored for one-time use scripts.
Pre/post-task Snapshot setting hints are not honored for auto-remediation scripts	Pre/post-task Snapshot setting hints are now honored for auto-remediation scripts.
Need ability to expand session logs in task search results	You can now expand session logs in task search results.
CiscoWorks NCM managed devices are pointing to other devices' configuration	Deployment from one device to other devices did not clone the configuration. Instead, it pointed to other devices' configurations. This has been fixed. You can now clone configurations.
Cannot search for advanced diagnostics	You can now search for advanced diagnostics.
Dynamic group filter needs to be updated when referenced groups are deleted	You can now update dynamic group filters when the referenced groups are deleted.
Quick search should not include inactive devices	Quick search (the search box in the upper-left of the UI) no longer includes inactive devices in the search results.
Device boot dates are sometimes inaccurate	Device boot dates are now accurate.
The command script task comments field is empty on the Home page and the View Configuration page	The Recent Change section of the Home page now displays comments for command script tasks that result in a configuration change.

Table 2 *Issues Fixed in CiscoWorks NCM 1.4 (continued)*

Bug Summary	Fix Description
Settings tasks with a range or reoccurrence setting does not always work	You can now set tasks with a range or reoccurrence setting.
Saving passwords with <i>tc_tools</i> does not work with non-standard ports	You can now save passwords with <i>tc_tools</i> to work with non-standard ports.
Editing a user profile when integrating with Active Directory causes errors	You can now edit a user profile when integrating with Active Directory.
Policy Manager Must Contain Only check does not catch missing and extra lines in the same configuration	The Policy Manager Must Contain Only check now flags missing and extra lines in the same configuration.

Supported Platforms

CiscoWorks NCM 1.4 can be installed on the following platforms:

Vendor	OS	Version	Architecture
Microsoft	Windows Server, Enterprise Edition (32-bit and 64-bit)	2003	i386
Sun Microsystems	Solaris (patch 118833-36 or later)	10	Dual UltraSparc IIIi+, 1.3 GHz
Red Hat	RH AS 4 32-bit, and RH AS 5 32-bit and 64-bit	4 and 5	i386
SuSE	Enterprise Linux Server	10.0	i386



Note CiscoWorks NCM is a 32-bit application that runs in 32-bit mode on 64-bit operating systems.

The following operation systems are no longer supported:

- Windows 2000
- Solaris 9
- Red Hat AS3
- SuSE 9

When upgrading to CiscoWorks NCM 1.4, if you are going from a deprecated operating system, for example Windows 2000 or Solaris 9, to a supported CiscoWorks NCM 1.4 operating system, do the following:

-
- Step 1** Back up the CiscoWorks NCM folder.
- Step 2** Upgrade the operating system.
- Step 3** Follow the CiscoWorks NCM 1.4 upgrade steps.
-



Note For all operating system upgrades, please refer to the vendor documentation and your system support personnel. Cisco is not responsible for issues that might arise during third-party product upgrades.

Supported Databases

When installing CiscoWorks NCM, the database can be installed on any platform. CiscoWorks NCM supports the following databases:

Database	Notes
Oracle 10g (10.2.0.4) Standard Edition	If you are running CiscoWorks NCM in a Distributed System environment, you will need Oracle Enterprise Edition.
Microsoft SQL Server 2005 Standard Edition	
MySQL 5.0.41 or later versions, including 5.0.58	MySQL 5.0.58 ships with CiscoWorks NCM.



Note 64-bit Oracle and SQL Server are supported.

The following databases are no longer supported:

- Oracle 9i and Oracle 9.2
- Microsoft SQL Server 2000
- MySQL 3



Note Existing MySQL 3.x databases can be upgraded to MySQL 5.0.41 or later using the MySQL Upgrade Installer. Refer to the *Installation and Upgrade Guide for CiscoWorks Network Compliance Manager, 1.4* for information.

When upgrading to CiscoWorks NCM 1.4, if you are going from a deprecated version of the database, for example Oracle 9i, to a supported version of the database, do the following:

- Step 1** Back up the CiscoWorks NCM database.
- Step 2** Upgrade the database.
- Step 3** Follow the CiscoWorks NCM 1.4 upgrade steps.



Note For all database upgrades, please refer to the documentation provided by the appropriate vendor and your DBA. Cisco is not responsible for issues that might arise during third-party product upgrades.

Additional CiscoWorks NCM Configurations

If you have configured a High Availability Distributed System environment, the database requirements for Oracle and Microsoft SQL Server include:

Database	Restrictions
Oracle Enterprise Edition 10.2.0.2 and 10.2.0.4	No more than five CiscoWorks NCM Cores can be configured.
SQL Server Standard Edition 2005 SP2 or higher	No more than two CiscoWorks NCM Cores can be configured. The maximum number of devices should not exceed 6,500.

Refer to the *High Availability Distributed System on Oracle Configuration Guide for CiscoWorks Network Compliance Manager* or the *High Availability Distributed System on Microsoft SQL Configuration Guide for CiscoWorks Network Compliance Manager* for information on configuring a High Availability Distributed System environment.

If you have configured a Satellite environment, CiscoWorks NCM supports the following platforms:

Vendor	OS	Version	Architecture
Red Hat	RHEL AS (32-bit)	3 and 4	i386
Novell	SuSE Enterprise Linux Server	9	i386
Sun Microsystems	Solaris (patch 118833-36 or later)	9 and 10	Sun Sparc



Note

SuSE Linux 9 and Solaris 9 are supported with Satellite; however, these two operating systems are not supported in CiscoWorks NCM 1.4 Core. These two operating systems are only valid to run the satellite remote gateway.

Refer to the *Satellite User's Guide for CiscoWorks Network Compliance Manager* for information on configuring a Satellite environment.

If you are running CiscoWorks NCM in a Virtual Environment (VM), CiscoWorks NCM supports the following platforms:

Vendor	OS	Version
Sun Microsystems	Solaris Zones	10
VMWare ESX 3.0.x	Windows	2003, SP1



Note Troubleshooting and performance issues related to VMWare cannot be resolved via Cisco Support. As a result, VMWare performance tuning practices must be used. Refer to your VMWare documentation for information.

Keep the following in mind when running CiscoWorks NCM in a VM:

- Running CiscoWorks NCM and the database in the same VM is not recommended.
- Running the database for the CiscoWorks NCM High Availability Core in a VM is not recommended.
- The maximum number of devices is 3,000.
- The maximum number of concurrent tasks is less than 20.
- The minimum VMWare Guest requirements include:
 - 2.6 GHz CPU
 - 4 GB dedicated RAM
 - 40 to 60 GB HD
 - 100 Mbps or higher dedicated Ethernet port
 - Linux RHEL AS 3 and 4
- CiscoWorks NCM is not certified to run with Oracle in a VMWare instance.
- CiscoWorks NCM is not certified to run in an environment where VMotion is used with the VMs.

Additional Required Applications

You will need to install the following applications:

- CiscoWorks NCM supports the following browsers:
 - Mozilla Firefox 2.0 or 3.0
 - Internet Explorer 6.x, 7.0



Note Mozilla Firefox 1.x is no longer supported.

- Microsoft Excel 2000 or higher, if you are viewing Summary Reports from the CiscoWorks NCM server.
- Adobe® Acrobat Reader™ version 4.0 or higher if you are viewing CiscoWorks NCM documentation from the CiscoWorks NCM server.
- ActivePerl 5.8.x (for Windows).

- Perl 5.8.x (for Solaris and Linux). Keep in mind that the CiscoWorks NCM Convert to Perl script feature uses Perl.

**Note**

Third-party products mentioned in this documentation are manufactured by vendors independent of Cisco. Cisco makes no warranty, implied or otherwise, regarding the performance or reliability of these products. We provide third-party contact information to help you find technical support. However, third-party contact information is subject to change without notice and, therefore, Cisco can in no way guarantee the accuracy of this contact information.

Hardware Requirements

CiscoWorks NCM requires the following minimum hardware:

Application Server

CPU	Intel Xeon or equivalent, 3.0+ GHz (Windows, Linux), Dual UltraSparc IIIi+, 1.3 GHz (Solaris)
Memory	4 GB RAM
Swap Space	4 GB
Disk	40 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Database Server

CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	4 GB RAM
Swap Space	4 GB
Disk	60 to 100 GB, Single Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Caveats

Please read the following regarding usability issues before using CiscoWorks NCM 1.4.

Solaris and SecurID

Configuring CiscoWorks NCM to use SecurID as the authentication method can cause the management service to crash. The SecurID libraries provided by RSA are the source of the problem. Currently, the problem can occur on Solaris 10 with a version string of **SunOS 5.10 Generic_118833-22**, while version **SunOS 5.10 Generic_120011-14** works fine. Please update your OS to at least this version if you are experiencing problems with SecurID on Solaris until this issue can be resolved.

SSH Library

In CiscoWorks NCM 1.4, the SSH library was updated. However, this library does not currently support keyboard interactive. As a result, CiscoWorks NCM 1.4 does not support SecurID authentication over SSH to devices.

Using SCP with Devices in Remote Realms

Devices in remote Realms cannot use the Secure Copy (SCP) Transfer Protocol because in most cases, the remote Gateway Satellite Agent cannot use SSH/SCP port 22, since the Gateway OS is already using the port.

Workaround: Disable SCP for devices in remote Realms.

Using SCP on Linux and Solaris

The Secure Copy (SCP) Transfer Protocol enables you to securely transfer files between a local and remote host or between two remote hosts using the Secure Shell (SSH) protocol. When using SCP on a Linux platform, you will need to modify your system's SSH daemon (SSHD) to run on an alternate port and restart the SSHD service. Port 8022 is recommended.

Once the system's SSHD is reconfigured, you can restart CiscoWorks NCM so that it can bind to Port 22. System administrators will need to `ssh -p 8022 username@host` to login via the system's SSHD after the change is made.



Note

Use `ssh username@host` for a direct connection to the CiscoWorks NCM proxy.

When logged-in to CiscoWorks NCM, you can navigate to the Device Access page (**Admin- > Administrative Settings- > Device Access**). Scroll down to the **SSH Device Access** field. Enter a **SSH User** and **SSH Password**. The device driver will use this information when copying files to the CiscoWorks NCM server.



Note

The device specific settings must be configured to enable SCP and SSH to function properly. In addition, the device and the device driver must support SCP to use the CiscoWorks NCM SSH server for SCP.

To use SCP with remote Realms, the SCP connection must be made back to the managing CiscoWorks NCM server. A SCP connection to the CiscoWorks NCM Gateway will not succeed because the CiscoWorks NCM Gateway runs the Linux and Solaris system SSHD. The CiscoWorks NCM Gateway sets the host to the CiscoWorks NCM Gateway and not the managing CiscoWorks NCM Core. This can

be overridden by setting an access variable (TFTPServer) to the IP address of the managing CiscoWorks NCM Core. Refer to the *User's Guide for CiscoWorks Network Compliance Manager, 1.4* for detailed information.

Using SCP

The SSH protocol runs on port 22. Secure Copy (SCP) is a data transfer mechanism that uses the SSH protocol. By default, Linux and Solaris installs run on port 8022. Windows installs run on port 22. For Windows installs, if the port is switched to 8022, there could be connectivity issues. (Because most devices do not allow for the specification of an alternate port, this issue is uncommon.)



Note

SCP will not work if the device is in a remote Realm and access to the device is managed via a CiscoWorks NCM Satellite. You must run the CiscoWorks NCM SSHD proxy on port 22. If you use port 8022 on any platform, SCP copies from a device to CiscoWorks NCM will not work. Refer to the *Satellite User's Guide for CiscoWorks Network Compliance Manager* for information on configuring CiscoWorks NCM Satellites.

Using a Non-English Operating System

When running CiscoWorks NCM 1.4 on a non-English operating system, unreadable text is displayed in the **Password Information** section on the Edit Device page when you select a Partition from the drop-down menu.

Auto-remediation Scripts

When creating an Auto-remediation script on the New Policy Rule page, if you input extended characters in the **Rule Conditions** field, it will produce unreadable text.

Proxy Interface

If you login to CiscoWorks NCM as a limited access user and attempt to connect to a device via the proxy interface, you will be dropped at the username/password prompt.

Searching for Diagnostics

When searching for diagnostics, in the list of diagnostic types, there are two options for the CiscoWorks NCM Topology Data Gathering diagnostic: CiscoWorks NCM Topology Data Gathering and Topology. Selecting either will search for the CiscoWorks NCM Topology Data Gathering diagnostic.

SNMP Timeouts

Using SNMP device discovery over networks with latency can cause SNMP timeouts. To resolve this issue:

1. Login to CiscoWorks NCM.
2. Navigate **Admin- > Administrative Settings- > Device Access**. The Administrative Settings - Device Access page opens.
3. Scroll down to the **Detect Network Devices Task Settings** section and set SNMP Timeout to a higher value, for example 2500 (milliseconds).

-sync Option

When Workflow is enabled, attempting to run a CLI or API task with the `-sync` option will fail with a **No such directory** error.

Running CiscoWorks NCM as Non-root

On a Unix platform, if you are running CiscoWorks NCM as non-root, after installing the CiscoWorks NCM Service Pack, you must enter:

```
chown -R $user $CWNCM_root
```

```
find $CWNCM_root -type d -exec ls -ld {} \; |grep '^d..-' | awk '{print $9}' | xargs chmod u+x
```

(Where `$CWNCM_root` is the root CiscoWorks NCM directory and `$user` is the username with which to start the CiscoWorks NCM Management Engine.)

Database Passwords

Any CiscoWorks NCM user input cannot contain multiple dollar signs (\$\$). As a result, if the password you use to connect to the database contains multiple dollar signs, you must modify the password before installing CiscoWorks NCM.

Installation Address

The IPv4 address range 169.254.0.0/16 is reserved for link-local usage (referred to as APIPA: Automatic Private Internet Protocol Addressing, by Microsoft) and is not applicable addressing for a network application server such as CiscoWorks NCM. For more information, refer to <http://www.ietf.org/rfc3330> and [rfc3927](http://www.ietf.org/rfc3927).

SSH Communication

CiscoWorks NCM 1.4 utilizes a new set of keys for SSH communication. In previous releases, CiscoWorks NCM used one Digital Signature Algorithm (DSA) key for all installations. When you install CiscoWorks NCM 1.4, CiscoWorks NCM creates two new 1024 bit keys. The first key uses the DSA algorithm. The second key uses the RSA algorithm. These keys are used when you connects to CiscoWorks NCM via SSH.

Custom Data Setup

Custom data fields enable you to assign useful data to specific devices, configurations, users, and so on. This gives you added flexibility and enables you to integrate CiscoWorks NCM with other applications.

To add custom data, navigate **Admin- > Custom Data Setup**. The Custom Data Setup page opens. Custom data field can include alphanumeric and underscores. While you can use dashes, custom data field names with dashes cannot be used with the `tc_device_custom` device variables in custom scripts.

Advanced ACL Scripts

Selecting the **Update Script** button 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 the **Update Script** button 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. [159198]

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 the 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.

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.

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.

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>
```

Oracle Database Errors Cause Failed Tasks and Other Issues

Oracle database errors cause failed tasks and other issues due to a bug in the JDBC Oracle driver. As a result, it is possible for the driver to cause database errors—causing tasks to fail and other issues. The error message information is OALL8 is in an inconsistent state.

Workaround: It is recommend that you update your version of Oracle Database Server.

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. Navigate **Devices**- > **Device Tools**- > **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**.

High Availability 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. One device will be automatically de-duplicated and set to **Inactive**. (Refer to Chapter 7, Scheduling Tasks, in the *User's Guide for CiscoWorks Network Compliance Manager, 1.4* for information on running the Deduplication task.)

High Availability 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.
```

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 & 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.

High Availability 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.

High Availability Distributed System External Authentication

When using external authentication in a High Availability 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.

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 the Continue button. 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 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 Device Driver Reference), deploy startup and reboot will fail.

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: 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: 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.

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

Cisco has discovered a problem with the Cisco IOS 2500 that can affect CiscoWorks NCM's Software Update Center. With a Cisco IOS 2500, running Version 12.3(3) (distributed as c2500-i-l.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 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.

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.

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.

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 could 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.

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.

Resolved Problems

The following table lists the problems that were resolved in CiscoWorks Network Compliance Manager, Release 1.4.

Table 3 **Problems Resolved in CiscoWorks NCM Release 1.4**

DDTS Number	Description
CSCse09644	The cwncm_import script does not parse the hostname as present in the CSV file.
CSCse11820	Installation hangs if you provide incorrect Database credentials.
CSCse16848	Duplicate entries are seen in the software updates report.
CSCsh28136	Installer fails to copy licenses from a directory whose name has spaces.

Table 3 *Problems Resolved in CiscoWorks NCM Release 1.4 (continued)*

DDTS Number	Description
CSCsl38283	Snapshot fails if banners are present on the device on the Linux platform.
CSCsr66733	Image set screen for IOS XR does not have label for tar file type.
CSCsr66899	Update image on IOS XR failed due to non-pie type.
CSCsr66970	Solaris installation is not compatible with SecureCRT.
CSCsr66985	During initial launch of Windows installer, the OpsWare Network Automation System 7.21 splash screen is displayed.

Known Limitations and Problems

This section contains information about the limitations and problems known to exist in CiscoWorks NCM, Release 1.4.

Licensing not found issue

Description: If while logging into CiscoWorks NCM Server, the server throws an error saying **No Valid License found**, then check the following:

- a) Make sure that all license files are installed under CiscoWorks NCM install folder.
- b) Make sure that there are no lingering expired license file(s), especially Evaluation license in the CiscoWorks NCM install folder.
- c) Make sure that the output of the command `<CWNCM_install_Dir>/server/ext/wrapper/bin/lmutil lmhostid` output matches the hostid on the license file. Do not modify the license file.

CSCsg74160—CiscoWorks NCM 1.1 installation fails with Microsoft Japanese SQL Server 2K/2005.

Description: CiscoWorks NCM 1.1 installation fails on Japanese Windows 2K or 23 with Japanese SQL Server 2K/2005 and you are not able to continue the installation, after specifying **sa** in **Database Admin Login** dialog.

Workaround: Change **sa** User's Language to **English**. Then proceed with the installation.

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.

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.

CSCsr66918—While deploying the IOS XR image on device, the option to **Reboot device after image update**, is not suitable for IOS XR.

Description: Cisco IOS XR Software requires Install Commit / Install Activate after the image(s) successfully deployed to the device. The old model deploy, reboot does not work with IOS XR.

Workaround: The **Reboot device after deploying software** option adds unnecessary delay time. Do not set this option for IOS XR devices.

CSCsr66956—Device disk space is incorrectly shown for IOS XR/CRS-1.

Workaround: Ignore the information given by CiscoWorks NCM and manually verify whether enough disk space is available by connecting directly to the device.

CSCsx03029—Need a way to exit Service Pack installer.

Description: When upgrading from CiscoWorks NCM 1.3 SP2 to CiscoWorks NCM 1.4, once the Service Pack installation is started, you cannot gracefully exit the installer before the installation completes.

Workaround: Kill the installer process.

CSCsx18134—User will see previous CWNCM version on the License information page.

Description: After upgrading from CiscoWorks NCM 1.3 SPx to CiscoWorks NCM 1.4, the License information page does not display the correct CiscoWorks NCM version number.

Workaround: There is no workaround. This is a cosmetic with no functional effect.

CSCsx18560—Service Pack installer for CiscoWorks NCM 1.4 will not update CNC and EOX.

Description: Service Pack Installation used to upgrade the existing CiscoWorks NCM 1.3.x to CiscoWorks NCM 1.4 does not upgrade CNC and EOX,

Workaround: Follow the instructions in the Service Pack Installation Guide to overwrite the files.

CSCsx30597—Error message shown with html code.

Description: Warning message generated from using invalid Cisco.com credentials is posted twice: Once in regular text and once in HTML format

Workaround: Use a valid Cisco.com credentials.

CSCsx30625—The CiscoWorks NCM Doc folder contains wrong version or branded documents.

Description: The `<CWNCM_install>/docs` folder contains incorrect versions of CiscoWorks NCM documents.

Workaround: 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

CSCsx30638—Link to CiscoWorks NCM documentation from Docs UI page is not reliable.

Description: The **Docs** tab visible from within CiscoWorks NCM *might* not include links to the latest documents.

Workaround: 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

CSCsx35323—Cannot SSH to CiscoWorks NCM server.

Description: In some Windows environments, you can not connect to CiscoWorks NCM server using SSH. The SSH server within the CiscoWorks NCM process (Truecontrol Management Engine) fails to start.

Workaround: None at this time.

CSCsx38253—SWIM process status is incorrect.

Description: From a terminal, enter `/etc/init.d/truecontrol status` to make sure all services are running normally. Navigate **Admin > Start/Stop Services**, and stop the Software Image Management Server.

The error message displays: **Unable to stop the TrueControl SWIM Server service.**

From a terminal, `/etc/init.d/truecontrol status` shows that the SWIM process is not running.

Workaround: Ignore the error message panel. Directly check the TrueControl SWIM server status with the Services application on Windows platforms and `/etc/init.d/truecontrol status` on Linux or Solaris platforms.

CSCsx39856—Deploy Remote Agent to Satellite Gateway failed.

Description: Deploy Remote Agent fails with root shell prompt in the format such as `ncm-sol2:/>` on the satellite gateway. It seems that Expect could not resolve the combination of characters from that prompt. This situation only appears on Linux and Solaris platforms.

Workaround: Avoid using Unix system prompt with a combination of characters such as `ncm-sol2:/>`. The prime suspect characters are `:/`.

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

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (ey@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, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; 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, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, 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. (0903R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.