HP NNM Integration User Guide for CiscoWorks
Network Compliance Manager

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
     800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-16538-03
# Table of Contents

## Getting Started
- Features and Benefits .................................................. 3
- NCM and NNM Co-residency ........................................... 4
- Ports ............................................................................. 4

## Chapter 1: Using NCM with NNM 7.5x
- Connecting to NCM from NNM 7.5x ................................. 6
- Viewing NCM Configuration Alarms ............................... 9
- Viewing Device and Configuration Information ................ 11
- Viewing Configuration Change in NCM ............................ 12
- Importing NNM Devices into the NCM Database ............. 12

## Chapter 2: Using NCM with NNMi 8.1x
- Connecting to NCM from NNMi 8.1x ................................. 14
- Upgrading the HP Network Node Manager (NNMi) 8.1x Connector .......................................................... 16
- Viewing NCM Device Information ................................ 16
- Viewing NCM Device Configuration .............................. 17
- Viewing NCM Device Configuration Diffs ....................... 17
- Viewing NCM Device Configuration History ................... 17
- Viewing the NCM Policy Compliance Report .................. 18
- Using Telnet or SSH to access NCM devices ................... 18
- Launching NCM Command Scripts ................................ 18
- Launching NCM Diagnostics ......................................... 19
- NCM Event Rules .......................................................... 19
- Importing NNMi 8.1x Devices into the NCM Database ...... 22

## Appendix A: Logs & Troubleshooting
- Setting the Logging Level for Troubleshooting ................ 23
- NCM and NNM Credentials .......................................... 24
- Password Encryption .................................................... 24
- Missing Integration URL Actions ................................... 25
- NCM Server IP Address ................................................ 25

## Appendix B: Tracing Events

## Index
Getting Started

This guide provides information on integrating HP Network Node Manager (NNMi) with CiscoWorks Network Compliance Manager (NCM) on Windows, Linux, and Solaris platforms. The guide is intended for network engineers and network administrators. The information presented assumes that the reader is familiar with both NNMi and NCM.

Features and Benefits

NNMi integration provides the following features and benefits in a system already running both NNMi and NCM software:

- **Alarm integration** — NNMi integration communicates NCM configuration change information to the NNMi console, enabling you to quickly identify whether configuration changes may have caused network problems. From within NNMi, you can quickly access NCM functionality to view specific configuration changes and device information, identify who made the change, and roll back to the previous configuration to restore network operation. Because a majority of network outages are caused by device configuration errors, this feature can enhance both problem identification and response time in resolving network downtime.

- **Access to NCM configuration history from the NNMi** — From NNMi, a device-level menu provides access to NCM features for reviewing configuration changes. For any device in the NCM database, this feature displays configuration changes side-by-side so you can easily view changes. You can also view configuration history.

- **Operations efficiency** — Network operations personnel can monitor and investigate information from two data sources from within a single screen.
NCM and NNM Co-residentcy

For NCM and NNM co-residency, NNM must be installed first, otherwise NCM will not know to use ports that do not conflict with NNM. In addition, the NCM installation will fail.

The hardware and software requirements for NCM and NNM co-residency should include both NCM and NNM requirements in terms of how many devices NCM and NNM are managing. Co-residency server sizing is a combination of both NCM and NNM as if they were individual installs.

Ports

When NCM is installed on a NNM server, the following ports will change:

- Http port: 80 to 8080
- Https port: 443 to 8443
- Jnp service port: 1099 to 9099
- RMI naming service port: 1098 to 9098
- RMI object port: 4444 to 9444
- RMI server bind polling port: 4445 to 9445
- Jboss web service port: 8083 to 8883
Chapter 1: Using NCM with NNM 7.5x

HP Network Node Manager (NNM) 7.5x integration combines the configuration change detection capabilities of CiscoWorks Network Compliance Manager (NCM) with the network monitoring capabilities of NNM, placing more information at your fingertips when problems occur.

Without exiting NNM, you can connect to NCM, login, and view information about NCM-managed devices and configuration change events. Once in NCM, you can perform any NCM functions for which you have the necessary permissions.

NNM integration adds several features and capabilities to the NNM and HPOV Launcher, enabling you to drill down into the network to find the details you need to quickly resolve problems.

In both the NNM and HPOV Launcher, NCM and NNM integration adds a new toolbar icon and two configuration menu items for opening connections to NCM, and adds three right-click menu items for viewing configuration information on devices managed by NCM. These tools enable you to:

- Launch NCM from an icon on the NNM toolbar or tab
- View detailed device information, including the vendor, model, modules, operating system version, and recent diagnostic result
- View device configuration changes and configuration history
- Compare configurations (typically the most recent and last previous configurations) to see what changed, why, and who made the changes

**Note:** These features are not available for network devices that are not configured in NCM or for NCM devices for which change detection is disabled.

For information on NCM/NNM co-residency, refer to “NCM and NNM Co-residentcy” on page 4.
Connecting to NCM from NNM 7.5x

NNM 7.5x integration supports Windows and Solaris platforms. Default browser settings are used. NCM and NNM 7.5x can be integrated in two ways:

- NCM and NNM are installed on separate servers (Standalone Mode)
- NCM and NNM are installed in the same server (Co-residency Mode)

If you are using Standalone Mode, you need to install one of the following Connector components:

- `ncm_nnm_connector_windows.exe`
- `ncm_nnm_connector_solaris.bin`

If you are using Co-residency Mode, you need to install one of the following Connector components:

- `ncm_nnm_coresidency_windows.exe`
- `ncm_nnm_coresidency_solaris.bin`

The Connector installer identifies where NNM 7.5x is located and installs the necessary components (including config files, icons, scripts, and so on) into different locations on NNM 7.5x. Device import is done during the installation, if applicable. After installation, additional icons and a right-mouse button click menu are displayed.

**Note:** If the Connector installer cannot find an existing version of NNM 7.5x, the installer quits. As a result, nothing is installed.
To connect to NCM from NNM, do the following:

1. On a Windows platform, click Start and select Programs --> HP OpenView --> Network Node Manager Admin --> Network Node Manager. The Root window opens. (**Note:** On a Solaris platform, enter: `# <nnm_install_directory>/OV/bin/ovw &`)

2. Click the HP icon at the top of the page. The CiscoWorks Network Compliance Manager login page opens.

3. Enter your NCM Username and Password and click Login. The NCM Home page opens.

4. Navigate to the HP Launcher window by selecting the Tools option and selecting HP Launcher from the drop-down menu. In the HP OpenView Launcher window, a new HP tab is added and a NCM menu is displayed when you select the tab, as shown below.

[Diagram of the HP Launcher window with the NCM menu highlighted.]

**Does not appear if running on a Solaris platform.**
To view device configuration changes in NCM from NNM, do the following:

1. In NNM, double click the Internet icon in the map. The current network segment is displayed.

2. Right click on a device and select the “View Configuration Change in NCM” option from the menu. The figure below shows a sample display.

3. Select the “View Configuration Change in NCM” option. The NCM Compare Device Configurations page opens. (Note that the “Launch NCM” item has been added to the NNM Tool menu.)
Chapter 1: Using NCM with NNM 7.5x

Viewing NCM Configuration Alarms

The new alarm category, Configuration Alarms, filters all NCM configuration change information to the Alarm Browser so you can view only NCM configuration alarms. In addition, NCM configuration alarms appear along with other system alarms when you select “All Alarms” on the Alarms Categories page as shown below.

A sample All Alarms Browser page is shown below.
**Note:** You can set color preferences in the All Alarms Browser to distinguish the NCM configuration alarms. By default, these alarms have no color assigned and appear as black text on a white field.

While configuration alarms are generated by all NCM events, this is a configurable feature in NCM. For a list of NCM events that generate alarms to the NNM display, refer to the *User Guide for Network Compliance Manager 1.5*.

**Note:** If you right-click on an entry, the Details page opens.
Viewing Device and Configuration Information

To view information that can help you determine the cause of network problems, after drilling down into the network to the device level, right-click the device to access the NCM menu options for viewing configuration and device details, as shown below.

When you select any NCM right-click menu items, you are prompted to log-in to NCM before the information you selected is displayed. Generally, you will only have to login once during a session.
Viewing Configuration Change in NCM

Viewing configuration changes in NCM opens the NCM Compare Device Configurations page. The most recent configuration captured by NCM is displayed alongside the previous configuration. As a result, you can easily review line-by-line changes.

The options at the top of the page can help you focus on particular information. Changes are highlighted in color to show lines changed, inserted, and deleted.

**Important!** If real-time change detection is disabled for any device, the most recent configuration will be the configuration captured by NCM at the last device polling interval. If configuration changes were made following that interval this may not be the current configuration.

Importing NNM Devices into the NCM Database

To import NNM device information into the NCM database:

On the NNM server, go to the NCM root directory. The defaults are:

- `c:\NCM` on Windows
- `/opt/NCM` on Solaris

On Windows, run `hpov_export_import.bat`.

On Solaris, run `hpov_export_import.sh`. 
Chapter 2: Using NCM with NNMi 8.1x

HP Network Node Manager (NNMi) 8.1x integration combines the configuration change detection capabilities of CiscoWorks Network Compliance Manager (NCM) with the network monitoring capabilities of NNMi 8.1x, placing more information at your fingertips when problems occur.

Without exiting NNMi 8.1x, you can connect to NCM, login, and view information about NCM-managed devices and configuration change events. Once in NCM, you can perform any NCM functions for which you have the necessary credentials.

NCM and NNMi 8.1x integration adds configuration menu items for opening connections to NCM, and adds menu items for viewing configuration information on devices managed by NCM. These tools enable you to:

- View detailed device information, including vendor, model, modules, operating system version, and recent diagnostic results
- View device configuration changes and configuration history
- Compare configurations (typically the most recent and last previous configurations) to see what changed, why, and who made the changes
- View device compliance information

**Note:** These features are not available for network devices that are not configured in NCM or for NCM devices for which change detection is disabled. In addition, when prompted for a NCM or NNMi hostname during installation, always use the IP address or the actual hostname, not localhost.

For information on NCM/NNM co-residency, refer to “NCM and NNM Co-residency” on page 4.
Connecting to NCM from NNMi 8.1x

NCM and NNMi 8.1x can be integrated in two ways:

- NCM and NNMi 8.1x are installed in separate servers (Standalone Mode)
- NCM and NNMi 8.1x are installed in the same server (Co-residency Mode)

If you are using Standalone Mode, you need to install one of the following Connector components:

- `na_nnm_connector_windows.exe`
- `na_nnm_connector_solaris.bin`
- `na_nnm_connector_linux.bin`

If you are using Co-residency Mode, you need to install one of the following Connector components:

- `na_nnm_coresidency_windows.exe`
- `na_nnm_coresidency_solaris.bin`
- `na_nnm_coresidency_linux.bin`

The Connector installer will detect where NNMi 8.1x is located and install the necessary components (including config files, java libs, scripts, and so on) into different locations on NNMi 8.1x. Device import is done during the installation if needed.

After installation, you will see additional URL actions from the NNMi 8.1x context menus. Keep in mind that if the installer cannot find an existing version of NNMi 8.1x, it will quit. As a result nothing is installed.

**Note:** After the NCM/NNMi 8.1x integration is installed, the NNMi 8.1x context sensitive menu to launch NCM does not appear until you re-login to NNMi 8.1x. In addition, when the Connector installer asks for the NNMi HTTP Port, it is referring to the HTTP port to which the NNMi client connects. By default, this is port 80 and can be configured during NNMi installation.
Chapter 2: Using NCM with NNMi 8.1x

To connect to NCM from NNMi 8.1x, do the following:

1. Login to NNMi 8.1x.
2. Select a node.
3. From Inventory/Node (Nodes view or Incident view), select Launch NCM from the Actions drop-down menu. The NCM Login page opens.
4. Enter your NCM User Name and Password and click Login. The NCM About page opens.
5. To view NCM device information, after selecting a node, select any of the following options from the Actions drop-down menu:
   - View NCM Device Information (refer to “Viewing NCM Device Information” on page 16)
   - View NCM Device Configuration (refer to “Viewing NCM Device Configuration” on page 17)
   - View NCM Device Configuration Diffs (refer to “Viewing NCM Device Configuration Diffs” on page 17)
   - View NCM Device Configuration History (refer to “Viewing NCM Device Configuration History” on page 17)
   - View NCM Policy Compliance Report (refer to “Viewing the NCM Policy Compliance Report” on page 18)
Upgrading the HP Network Node Manager (NNMi) 8.1x Connector

If you have installed the NNMi 8.1x connector and are upgrading to NCM 7.50.02, you must upgrade your NNMi 8.1x connector. To upgrade the NNMi 8.1x connector:

On Windows, you must first uninstall the NNMi 8.1x connector.
   1. In the Control Panel, select “add or remove programs”.
   2. Select to remove/uninstall the NCM - HP Network Node Manager Connector.
   3. Follow the on-screen instructions. Note that some files will remain.

On Linux or Solaris, there is no need to uninstall the NNMi 8.1x connector.
   1. Run the NCM 1.5 Service Pack installer to update NCM.
   2. Re-install the updated NNMi 8.1x connector.

Viewing NCM Device Information

When you click the View NCM Device Information option, the Device Details page opens. The Device Details page enables you to perform device-specific tasks. For example, if you click the Current Configuration option from the View drop-down menu, the Current Configuration page opens, where you can deploy the configuration to the running configuration on the device. Refer to the User Guide for Network Compliance Manager 1.5 for detailed information.
Viewing NCM Device Configuration

When you click the View NCM Device Configuration option, the Current Configuration page opens. If you select the “Compare to previous” link, the Compare Device Configurations page opens. The most recent configuration captured by NCM is displayed, alongside the previous configuration. As a result, you can easily review line-by-line changes. Selecting the options at the top of the page can help you focus on specific information. Refer to the User Guide for Network Compliance Manager 1.5 for detailed information.

**Note:** If real-time change detection is disabled for any device, the most recent configuration will be the configuration captured by NCM at the last device polling interval. If configuration changes were made following that interval this may not be the current configuration.

Viewing NCM Device Configuration Diffs

If you click the View NCM Device Configuration Diffs option, the Compare Device Configuration page displays two configurations for the same device side-by-side. Additions, deletions, and changes are highlighted in two columns, with line numbers on the left. Each configuration is identified by its unique IP address and the date/time on which the configuration snapshot was taken. Refer to the User Guide for Network Compliance Manager 1.5 for detailed information.

Viewing NCM Device Configuration History

If you click the View NCM Device Configuration History option, the NCM Device Configurations History page opens. On this page, you can view the configuration and compare the configuration to a previous version. Refer to the User Guide for Network Compliance Manager 1.5 for detailed information.
Viewing the NCM Policy Compliance Report

If you click the View NCM Policy Compliance Report option, the Policy, Rule and Compliance Search Results page opens, where you can view information on:

- Device Hostnames and IP Addresses
- Policies
- Policy Rules
- Device Compliant States

Refer to the *User Guide for Network Compliance Manager 1.5* for detailed information.

Using Telnet or SSH to access NCM devices

To use Telnet or SSH to access NCM devices from NNMi 8.1x, do the following:

1. Login to NNMi 8.1x.
2. From Inventory/Node (Nodes view or Incident view), select either the “Telnet to NCM Device” option or the “SSH to NCM Device” option. A Telnet or SSH window opens.

Refer to the *User Guide for Network Compliance Manager 1.5* for detailed information.

Launching NCM Command Scripts

If you click the Launch NCM Command Scripts option, the New Task - Run Command Script page opens, where you can select command scripts and schedule when the task is to start. Refer to the *User Guide for Network Compliance Manager 1.5* for detailed information.
Launching NCM Diagnostics

If you click the Launch NCM Diagnostics option, the New Task - Run Diagnostics page opens, where you can select diagnostics and schedule when the task will be started. Refer to the *User Guide for Network Compliance Manager 1.5* for detailed information.

NCM Event Rules

NNMi 8.1x can receive the following event rules from NCM:

- **NCM/NNM Integration via SNMP traps** — This event rule triggers events when a new device is added or a device configuration is changed. The event will send an SNMP v1 trap to NNMi 8.1x.
- **INT_NNM.AsyncAddSeed** — This event rule triggers events when a new device is added. This event calls NNMi 8.1x Web service AddSeed and adds a new device to NNMi 8.1x.
- **INT_NNM.AsyncRediscoverHost** — This event rule triggers events when a device configuration is changed. This event calls NNMi 8.1x Web service RediscoverHost to get the latest status for the device.
- **INT_NNM.SyncOutOfService** — This event rule triggers events when a task is started and sets the device in the 'out of service' state. After the task completes, it sets the device back to the 'in service' state. This event calls the NNMi 8.1x Web service. By default, Reboot Device, Update Software, and Password Change trigger this event and should be selected from the 3rd Party Integrations page. Refer to the *User Guide for Network Compliance Manager 1.5* for information.
- **INT_NNM.SyncSnmpCommunityStringPropagate** — This event rule triggers events when the 'Last Used Device Password Changed' is changed. This event calls the NNMi 8.1x Web service to update NNMi 8.1x with the community strings NCM is using to manage the device. By default, SNMP community string propagate option is disabled from 3rd Party Integration page. Refer to the *User Guide for Network Compliance Manager 1.5* for information.

*Note:* Do not delete these event rules.
The following figures show sample NCM/NNMi 8.1x event pages.
Importing NNMi 8.1x Devices into the NCM Database

To import NNMi 8.1x device information into the NCM database:
On the NNMi 8.1x server, go to the NCM root directory. The defaults are:
- `C:\NCM` (Windows)
- `opt/NCM` (Linux and Solaris)
On Windows, run `nnmimport.bat`.
On Linux or Solaris, run `nnmimport.sh`.

**Note:** Running this periodically will help ensure your NNMi 8.1x and NCM device inventory is in sync.
Appendix A: Logs & Troubleshooting

This appendix provides information and procedures on setting the logging level for troubleshooting and provides information on specific issues that could arise during installation.

Setting the Logging Level for Troubleshooting

NNM integration writes the following log information to the output files specified during installation:

<table>
<thead>
<tr>
<th>Log type</th>
<th>Log Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>external/hpov</td>
<td>Errors encountered in importing device information from NNM to NCM.</td>
</tr>
<tr>
<td>api</td>
<td></td>
</tr>
<tr>
<td>device/import</td>
<td></td>
</tr>
</tbody>
</table>

The logging level is set in the configuration options of the `commandline.rcx` file installed at setup. During normal operation, HP recommends that the logging level remain at the default value, 75, which provides error messages. Accepted values are 0 to 100.

During troubleshooting, you can change this value to 0 (zero) to collect trace level debugging information that will assist you and Customer Support in resolving the problem. You may be advised to turn up two or more logging levels in concert depending on the type of problem you are seeing.

To reset the logging level, edit the `commandlineclient.rcx` configuration file. The default location of this file is `C:\NCM\jre` on your NNM server. Each log has its own "level" variable:

- `log/external/connector/hpov/level`
- `log/api/level`
- `log//device import/level`
NCM and NNM Credentials

For standalone installation, the `client_nnm.rcx` file in the `<NCM_INSTALL>/jre` directory contains NCM and NNM credentials in either plaintext or encrypted (default) format. If either set of credentials change, you can update the file and reload server options from the NCM CLI.

The `client_nnm.rcx` file exists on both the NCM and NNM servers. As a result, device imports from NNM can be initiated from both servers. For co-residency, the `.rcx` file is renamed as `client_ncm_nnm.rcx`.

Password Encryption

To encrypt a password, using the ConnectorTool utility:

1. Change to the `<NCM_INSTALL>` directory.
2. Run the following command:

   ```bash
   <NCM_INSTALL>/jre/bin/java -cp <NCM_INSTALL>/client/truecontrol-client.jar com.rendition.tools.ConnectorTool -encrypt xxxxxxx
   ```

   The following example (Windows platform) shows how to encrypt the 'rendition' password:

   ```bash
   c:\NCM\jre\bin\java -cp c:\NCM\client\truecontrol-client.jar com.rendition.tools.ConnectorTool -encrypt rendition
   ```

   The string 'rendition' is encrypted in single quotation mark:

   ```bash
   'K2IGjPQjw6/K3tKNW9KFLg=='
   ```

3. Copy the encrypted password to the `.rcx` file.
Appendix A: Logs & Troubleshooting

Missing Integration URL Actions
If right-click menus do not appear in NNM after installing the NNM Integration software:

1. cd to the c:\Program Files (x86)\HP\HP BTO Software\bin NNM 8.x directory:

2. Run the following command:
   `nnmconfigimport.ovpl -u xxxx -p xxxx -f urlactions.xml`

Note: Right-click menus will not work unless devices are imported from NNMi to NCM because NCM needs the UUID information from NNMi to associate with NCM managed devices.

NCM Server IP Address
If the NCM server changes its IP Address or DNS, do the following to update the information in the NNMi 8.10 menus:

1. NNM --> Configuration --> Url Actions --> View

2. Select each NCM menu item and change the URL.
Appendix B: Tracing Events

This appendix provides information on tracing events, required software applications, and configuring NCM to send SNMP traps.

To trace input events, run:

```
%HPOV_HOME%\bin>ecsmgr -log_events input on
```

All input events are written to:

```
%HPOV_HOME%\log\ecs\1\ecsin.evt0 file
```

To trace output events, run:

```
%HPOV_HOME%\bin>ecsmgr -log_events stream on
```

All output events are written to:

```
%HPOV_HOME%\log\ecs\1\default_sout.evt0 file
```

All discarded events are written to:

```
%HPOV_HOME%\log\ecs\1\default_sdis.evt0 file
```

To discontinue logging events, run:

```
%HPOV_HOME%\bin>ecsmgr -log_events input off
%HPOV_HOME%\bin>ecsmgr -log_events stream off
```

To do run-time trace logic to view how correlation worked, run:

```
%HPOV_HOME%\bin>ecsmgr -fact_update Composer "C:\Program Files\HP OpenView\contrib\ecs\CO\CompTraceOn.fs
%HPOV_HOME%\bin>ecsmgr -i 1 -trace 65536
%HPOV_HOME%\bin>pmdmgr -Secss\;T0xffffffff
```
All output events are written to:
%HPOV_HOME%\log\pmd.tc0 file

To discontinue logging run-time tracing, run:
%HPOV_HOME%\bin>ecsmgr -fact_update Composer "C:\Program Files\HP OpenView\contrib\ecs\CO\CompTraceOff.fs"
%HPOV_HOME%\bin>ecsmgr -i 1 -trace 0
%HPOV_HOME%\bin>pmdmgr -Secss;T0x0
Index

A
Alarms
Categories 10
Configuring 9
Integration 3

C
client_ncm_nnm.rcx file 24
client_nnm.rcx file 24
Configuration change
Comparing 12
Viewing in NCM 12
Configuring alarms 9
Connecting to NCM from NNM 6
Connecting to NCM from NNMi 14

D
Device configuration
Diffs 17
History 17
Viewing changes 12
Viewing in NCM 11

I
Importing devices 12
IP addresses 25

L
Launching NCM command scripts 18
Launching NCM diagnostics 19
Log files 23

N
NCM
Alarms 9
Benefits 3
Database maintenance 3
Features 5, 13
Integrating with NNM 5
Integrating with NNMi 13
NCM events rules 19
NCM/NNM co-residency
Ports 4
Requirements 4
NCM/NNM credentials 24
Network Node Manager (NNM)
Connecting to NCM 7
Features 3
Network Node Manager (NNMi)
Connecting to NCM 15
NNM Integration
Benefits 3
Features 5
NNM Launcher 12
NNMi Integration
Using SSH 18
Using Telnet 18

P
Password encryption 24
Policy compliance report 18
Ports 4

S
SSH 18

T
Telnet 18
Tracing events 27
Troubleshooting
Missing menus 25
NCM installation 23
NCM/NNM credentials 24
Password encryption 24
Server IP address 25
Setting logging level 23

V
Viewing device information 11