

HP Network Node Manager i-Series Software

For the Windows®, HP-UX, Linux, and Solaris operating systems

Software Version: NNMi 8.1x patch 4 (8.12)

[Online Help: Help for Administrators](#)

Document Release Date: June 2009

Software Release Date: June 2009



PDF Version of NNMi Online Help

This document is a PDF version of the NNMi online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Note: Some topics do not convert properly to PDF format. You may encounter formatting problems or unreadable text in certain document locations. Those problem topics can be successfully printed from within the online help.

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

For information about third-party license agreements, see the license-agreements directory on the product installation media.

Copyright Notices

© Copyright 2009 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

This product includes ASM Bytecode Manipulation Framework software developed by Institute National de Recherche en Informatique et Automatique (INRIA). Copyright © 2000-2005 INRIA, France Telecom. All Rights Reserved.

This product includes Commons Discovery software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 2002-2009 The Apache Software Foundation. All Rights Reserved.

This product includes Netscape JavaScript Browser Detection Library software, Copyright © Netscape Communications 1999-2001

This product includes Xerces-J xml parser software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999-2002 The Apache Software Foundation. All rights reserved.

This product includes software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). Xpp-3 Copyright © 2002 Extreme! Lab, Indiana University. All rights reserved.

Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Java™ is a US trademark of Sun Microsystems, Inc.

Oracle® is a registered trademark of Oracle Corporation and/or its affiliates.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing

restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, see the license-agreements directory on the NNMi product DVD.

Table of Contents

PDF Version of NNMi Online Help	2
Legal Notices	3
Table of Contents	5
Introduction for NNMi Administrators	14
Administrator Tools in the Console.....	15
Quick Start Configuration Wizard.....	15
Configuration Workspaces.....	16
Lookup Fields.....	18
Use the Quick Find Window.....	19
Use Autocomplete.....	19
Create a Configuration Object Instance Using the Form Toolbar.....	20
Delete One or More Objects.....	20
Perform Automated Tasks.....	21
Actions Provided by NNMi.....	22
NNMi Processes and Services.....	25
About Each NNMi Process.....	26
Verify that NNMi Processes Are Running.....	26
Stop or Start an NNMi Process.....	26
About Each NNMi Service.....	26
Verify that NNMi Services Are Running.....	28
Stop or Start NNMi Services.....	30
Use NNMi Help Anywhere, Anytime	31
Controlling Access to NNMi	32
Configure Sign-In Access.....	32
Roles Provided in NNMi.....	32
Determine which NNMi Role to Assign.....	33
Control Menu Access.....	34
Control Access with NNMi Accounts.....	35
Change Password, Name, or Role Assignment.....	36
Control Access Using Both Directory Service and NNMi.....	37
Change Role Assignment for a Directory Service User Name.....	39
Control Access with a Directory Service.....	40

Disable a User's Access to NNMi.....	41
Troubleshoot NNMi Access.....	41
Restore the System Role.....	41
Set Up Command Line Access.....	42
Audit NNMi User Activity.....	43
Communicate to Your Team.....	44
Open the Console.....	44
Sign In to the Console.....	46
Sign Out from the Console.....	46
Configuring Communication Protocol.....	47
Configure Default SNMP and ICMP Protocol Settings.....	47
Timeout / Retry Behavior Example for SNMP.....	50
Timeout / Retry Behavior Example for ICMP.....	51
Configure Default Community Strings (SNMPv1 or SNMPv2c).....	51
Default Community String Form.....	52
Configure the Default Device Credentials (NNM iSPI NET).....	53
Configure Default SNMPv3 Settings.....	54
Default SNMPv3 Settings form.....	55
Configure Regions (Communication Settings).....	56
Communication Region Form.....	57
Configure Address Ranges for Regions.....	60
Configure Hostname Filters for Regions.....	61
Configure Community Strings for Regions.....	62
Configure Credential Settings for Regions (NNM iSPI NET).....	64
Configure SNMPv3 Settings for Regions.....	65
Communication Region SNMPv3 Settings form.....	65
Configure Specific Nodes (Communication Settings).....	66
Specific Node Settings Form (Communication Settings).....	67
Configure Community Strings for Nodes.....	72
Configure Credential Settings for Nodes (NNM iSPI NET).....	73
Load Specific Node Settings from a File.....	74
Verify Your Communication Settings.....	75
Discovering Your Network.....	76
How Spiral Discovery Works.....	77
Discovery Intervals.....	79

Discovery Node Name Choices	79
Node Name Decision Tree.....	81
Discovery Seeds (as a starting point).....	82
Ping Sweep (as a starting point).....	82
Auto-Discovery Rules.....	83
Filters to Exclude Certain IP Addresses.....	83
Subnet Connection Rules.....	84
Device Profiles and Discovery.....	85
Prerequisites for Discovery.....	86
SNMP Prerequisites.....	86
Well-Configured DNS Prerequisite.....	86
Use nslookup to Verify DNS Server Configurations.....	87
Exclude Problem Devices from nmlookup.....	87
Determine Your Approach to Discovery.....	88
Do Not Use Auto-Discovery Rules.....	88
Routers and Switches Discovered.....	89
All SNMP Devices Discovered.....	90
Everything Discovered.....	91
All Devices from a Specific Vendor Discovered.....	92
Limit Sources of Neighbor Information.....	93
Exclude Problem IP Addresses from Discovery.....	94
Specific System Object IDs Not Discovered.....	94
Configure Device Profiles.....	95
Configure Discovery.....	96
Adjust the Discovery Interval.....	98
Configure Ping Sweep Global Settings.....	98
Configure the Node Name Strategy.....	99
Configure Auto-Discovery Rules.....	101
Configure Basic Settings for the Auto-Discovery Rule.....	102
IP Address Ranges for Auto-Discovery.....	104
SNMP System Object ID Ranges for Discovery.....	106
Configure an Excluded IP Addresses Filter.....	108
Configure Subnet Connection Rules.....	109
Subnet Connection Rules Provided by NNMi.....	111
Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered.....	112

In the Console, Configure Discovery Seeds.....	113
With a Seed File, Add Multiple Discovery Seeds.....	114
From the Command Line, Add Discovery Seeds.....	115
Examine Discovery Results.....	116
Check Initial Progress of Discovery.....	117
Node Discovery State Check.....	117
Verify Success of Discovery Seeds.....	117
Discovery Seed Results.....	118
Examine Discovery Inventory.....	120
Examine Layer 2 Discovery Results.....	120
Examine Layer 3 Discovery Results.....	121
Keep Your Topology Accurate.....	122
Delete Nodes.....	122
Delete Discovery Seeds.....	123
Add or Delete a Layer 2 Connection.....	124
Creating Groups of Nodes or Interfaces.....	126
Create Node Groups.....	126
In the Console, Create Node Groups.....	127
Specify Node Group Additional Filters.....	128
Add Boolean Operators in the Additional Filters Editor.....	134
In a Text File, Define Node Groups.....	137
Define Custom Attributes on Nodes (NNM iSPI Net).....	138
Create Interface Groups.....	139
Add New IfTypes (Interface Types) to the List.....	140
Specify Interface Group Additional Filters.....	141
Node Groups Provided by NNMi.....	147
Node Groups As Predefined View Filters.....	147
Island Node Groups.....	149
Interface Groups Provided by NNMi.....	149
Monitoring Network Health.....	151
About the State Poller.....	151
The NNMi Causal Engine and Monitoring.....	152
Configure Monitoring Behavior.....	152
Set Global Monitoring.....	153
Set Default Monitoring.....	154

Configure Interface Monitoring.....	158
Configure Threshold Monitoring for Interfaces (NNM iSPI for Performance).....	162
Determine Reasonable Threshold Settings (NNM iSPI for Performance).....	165
Examples of Threshold Monitoring (NNM iSPI for Performance).....	165
Configure Node Monitoring.....	168
Configure Threshold Monitoring for Nodes (NNM iSPI for Performance).....	172
Determine Reasonable Threshold Settings (NNM iSPI for Performance).....	175
Examples of Threshold Monitoring (NNM iSPI for Performance).....	175
Configure Node Group Status.....	178
Configure Percentage Values for the Target Status.....	179
Node Group Status Settings Form.....	179
Monitor Router Redundancy Groups (NNMi Advanced).....	181
Current Health of the State Poller Service.....	181
Verify Monitoring Configuration Settings.....	181
Stop or Start Managing a Node, Interface, or Address.....	184
View the Management Mode for an Object in Your Network.....	185
Using the (Management Mode) Nodes View.....	187
Using the (Management Mode) Interfaces View.....	187
Using the (Management Mode) IP Addresses View.....	187
Using the Managed Nodes View.....	188
Using the Managed Interfaces View.....	188
Using the IP Managed Addresses View.....	189
Using the Not Managed Nodes View.....	189
Using the Not Managed Interfaces View.....	190
Using the Not Managed Addresses View.....	190
Using the Out of Service Nodes View.....	190
Using the Out of Service Interfaces View.....	191
Using the Out of Service Addresses View.....	191
How NNMi Assigns the Management Mode to an Interface or Address.....	192
Understand the Effects of Setting the Management Mode to Not Managed or Out of Service.....	193
Configuring the NNMi User Interface.....	195
Configuring Maps.....	198
Define Node Group Map Settings.....	198
Node Group Map Settings Form.....	199
Configure Basic Settings for a Node Group Map.....	200

Configure the Connectivity to be Displayed for a Node Group Map.....	202
Configure Background Image Information for a Node Group Map.....	203
Background Image Sources in Node Group Maps.....	205
Scale Background Images in Node Group Maps.....	206
Troubleshoot URLs When Specifying a Background Image.....	206
Configure a Path View Map.....	206
Configuring Incidents.....	211
How NNMi Gathers Incidents.....	211
The NNMi Causal Engine and Incidents.....	212
About the Event Pipeline.....	213
Incident Configurations Provided by NNMi.....	214
Custom Incident Attributes Provided by NNMi.....	214
SNMP Trap Incident Configurations Provided by NNMi.....	216
Remote NNM 6.x/7.x Event Configurations Provided by NNMi.....	226
Management Event Configurations Provided by NNMi.....	229
Incident Pair (Pairwise) Configurations Provided by NNM.....	237
Configure Network Devices to Send SNMP Notifications to NNMi.....	238
Configure SNMP Trap Forwarding.....	239
Configure NNMi Security Settings for SNMPv3 Trap Forwarding.....	239
Configure Trap Forwarding Filters.....	241
Trap Forwarding Filters Form.....	241
Trap Forwarding Filter Expression Form.....	242
Configure Trap Forwarding Destinations.....	243
Trap Forwarding Destination Form.....	244
Trap Forwarding Filter Association Form.....	245
SNMP Trap Varbinds Provided by NNMi.....	246
Configure SNMP Trap Incidents.....	246
Load SNMP Trap Definitions.....	247
SNMP Trap Configuration Form.....	248
Specify the Incident Configuration Name.....	249
Specify the SNMP Object ID.....	249
SNMP Object ID Format for SNMPv2c Traps.....	250
SNMP Object ID Format for SNMPv1 Generic Traps.....	250
SNMP Object ID Format for a Specific SNMPv1 Trap.....	251
Display an SNMP Trap or NNM 6.x/7.x Events as a Root Cause Incident.....	251

Specify Category and Family Attribute Values for Organizing Your Incidents	251
Create an Incident Category	253
Create an Incident Family	254
Specify the Incident Severity	255
Specify Your Incident Message Format	255
Valid Parameters for Configuring Incident Messages	256
Include Custom Incident Attributes in Your Message Format	259
Specify a Description for Your Incident Configuration	260
Specify an Author for Your Incident Configuration	260
Configure Remote NNM 6.x/7.x Events	261
Configure Remote NNM 6.x and 7.x Management Stations	262
Remote NNMi Event Form	263
Configure How Management Events Are Displayed	264
Management Event Form	265
Reduce the Number of Incoming Incidents	266
Control which Incoming Traps Are Visible in Incident Views	268
Correlate Duplicate Incidents (Deduplication Configuration)	269
Deduplication Comparison Parameters Form	271
Track Incident Frequency (Rate: Time Period and Count)	273
Rate Comparison Parameters Form	274
About Pairwise Configurations	276
Incident Pair (Pairwise) Configurations Provided by NNM	276
Prerequisites for Pairwise Configurations	278
Pairwise Configuration Form (Correlate Pairs of Incidents)	279
Pair Item Configuration Form (Identify Incident Pairs)	281
Configure an Action for an Incident	283
Lifecycle Transition Action Form	284
Valid Parameters for Configuring Incident Actions	285
Handling Special Characters in Action Arguments	288
Example Jython Methods Provided by NNMi	290
Configure Diagnostics for an Incident (NNM iSPI NET)	291
Configuration Per Node Group Form (NNM iSPI NET)	292
Diagnostic Selection Form (NNM iSPI NET)	293
Diagnostics (Flows) Provided by NNMi (NNM iSPI NET)	295
Generate Interface Disabled Incidents	298

Generate Performance Threshold Incidents (NNM iSPI for Performance).....	298
Use HP Route Analytics Management System Data in Path View (NNMi Advanced).....	300
Configure One or More Route Analytics Management Systems (NNMi Advanced).....	300
Extending NNMi Capabilities.....	302
Add Custom Attributes to a Node or Interface Object	302
Control the Actions Menu.....	303
Configure URL Action Basic Behavior.....	303
URL Actions Author.....	304
Configure URL Action Details.....	305
Syntax and Limitations for URL Actions.....	306
Database Object Identifiers for URL Actions.....	311
Custom Incident Attributes in URL Actions.....	311
Capability Attributes in URL Actions.....	312
Custom Attributes in URL Actions.....	313
Environment Attributes in URL Actions.....	315
Specify Optional URL Action Filters.....	315
Purchase an HP Smart Plug-in.....	319
Purchase Integrations with Other HP Products.....	320
Integrating NNMi Elsewhere with URLs.....	321
Authentication Requirements for launch URLs Access.....	321
Access to Forms.....	322
Access to Workspaces.....	322
Access to Commands.....	323
Launch the Console (showMain).....	324
Launch a View (showView).....	324
Launch an Incident View.....	327
Launch a Topology Maps Workspace View.....	330
Launch a Monitoring Workspace View.....	335
Launch a Troubleshooting Workspace View.....	338
Launch an Inventory Workspace View.....	343
Launch a Management Mode Workspace Views.....	346
Launch a Configuration Workspace View.....	349
Launch a Form (showForm).....	350
Launch a Node Form.....	351
Launch an Interface Form.....	353

Launch an IP Address Form.....	355
Launch a Subnet Form.....	356
Launch an Incident Form.....	357
Launch a Node Group Form.....	358
Launch a Configuration Form.....	360
Launch Menu Items (runTool).....	361
Launch the Actions: Ping Command.....	362
Launch the Actions: Trace Route Command.....	362
Launch the Actions: Communication Configuration Command.....	363
Launch the Actions: Monitoring Settings Command.....	364
Launch the Actions: Status Poll Command.....	367
Launch the Actions: Configuration Poll Command.....	367
Launch the Actions: Status Details Command (for Node Groups).....	368
Launch the Tools: NNMi Status Command.....	369
Launch the Tools: Sign In/Out Audit Log Command.....	370
Launch the File: Sign-Out Command.....	370
Confirm that NNMi Is Running (cmd=isRunning).....	370
Maintaining NNMi.....	372
Track Your NNMi Licenses.....	372
Export and Import Configuration Settings.....	373
Export/Import Behavior and Dependencies.....	373
Export a Snapshot of Your Configuration Settings.....	377
Import Configuration Files to Restore Previous Settings.....	378
Transfer Configuration Settings to Another NNMi Management Server.....	379
Troubleshooting Imports of Configuration Files.....	382
Back Up and Restore NNMi.....	385
Back Up NNMi Data and Files.....	385
Restore NNMi Data and Files.....	386
Archive and Delete Incidents.....	387
Appendix A: Glossary Terms.....	390
Appendix B: Index.....	392

Introduction for NNMi Administrators


As an NNMi administrator, you can use the console to configure the items described in the following table.

Configure NNMi

What You Can Configure	Description
Sign-In Access to NNMi	<p>Using the User Accounts and Roles option in the Configuration workspace, provide and control access to NNMi . Configure a name and password for each user. Assign a role to each user.</p> <p>Tip: If your environment manages user names and passwords with a directory service, NNMi can be configured to use Lightweight Directory Access Protocol (LDAP) instead of the settings in the Configuration → User Accounts and Roles view.</p> <p>See "Controlling Access to NNMi" (on page 32) for more information.</p>
ICMP and SNMP Communication Protocols	<p>Using the Communication Configuration option in the Configuration workspace, provide the SNMPv1 or SNMPv2c community strings for your network environment, or provide the SNMPv3 user names for your network environment. Configure NNMi settings for timeout, retry, and port usage for ICMP and SNMP traffic. See "Configuring Communication Protocol" (on page 47) for more information.</p>
Discovery	<p>Using the Discovery Configuration option in the Configuration workspace, configure NNMi to discover only those devices that are important to you and your team. See "Discovering Your Network" (on page 76) for more information.</p>
Filters	<p>Using the Node Groups and Interface Groups options in the Configuration workspaces, define filters. These filters identify groups of devices. Use the filters to quickly locate information in views. See "Creating Groups of Nodes or Interfaces" (on page 126) for more information.</p> <p>You can also monitor the health of each group, see "Configure Monitoring Behavior" (on page 152).</p>
Monitoring Network Health	<p>Using the Monitoring Configuration option in the Configuration workspace, define how and how often important devices are monitored by NNMi . See "Monitoring Network Health" (on page 151) for more information.</p>
Incidents	<p>Using the Incident Configuration option in the Configuration workspace, review the many predefined incident configurations provided by NNMi . Edit any of the configurations provided by NNMi or create your own . See "Configuring Incidents" (on page 211) for more information.</p>
Actions Menu	<p>Using the URL Actions option in the Configuration workspace, configure the Actions menu. Add actions that you want to provide to your team. Modify the Actions provided by NNMi . See "Extending NNMi Capabilities" (on page 302) for more information.</p>
Management Stations	<p>Using the Management Stations option in the Configuration workspace, configure how events that are received from NNM 6.x or 7.x management stations are handled by NNMi . See "Configure Remote NNM 6.x and 7.x Management Stations" (on page 262) for more information.</p>

NNMi provides a variety of tools to assist you with these configuration tasks. Each of these tools is described in the following table. You can extend NNMi using an HP Smart Plug-in (iSPI) as described in ["Extending NNMi Capabilities" \(on page 302\)](#).

NNMi Administrator Tools

Tool	Description
Configuration Workspaces	The console provides a workspace for each kind of item you can configure in NNMi . See the preceding "Configure NNMi " table for more information.
Lookup Fields	Provided in forms, fields that include the  icon provide access to a list of all available attribute values, and in some locations enable you to create attribute values. See "Lookup Fields" (on page 18) for more information.
Actions	Used to perform automated tasks on a single object or on a group of objects. For example, you can use the Actions menu to change the Management Mode of one or more nodes from Managed to Out of Service . Actions are available from table views, map views, and forms. See "Perform Automated Tasks" (on page 21) for more information
NNMi Processes and Services	NNMi is built on a group of processes and services. You can list these processes and services. You can stop and start individual processes and services. See "NNMi Processes and Services" (on page 25) for more information.

Administrator Tools in the Console

When configuring settings for NNMi, you create configuration object instances. For example, to create a new URL action, you must create a new URL action instance. As another example, to specify configuration settings for discovery, you might create object instances that contain ranges of IP addresses that you want NNMi to use as hints for Spiral Discovery.

The console provides the following tools to assist you with configuration tasks:

- ["Configuration Workspaces" \(on page 16\)](#)
- ["Lookup Fields" \(on page 18\)](#)
- ["Create a Configuration Object Instance Using the Form Toolbar" \(on page 20\)](#)
- ["Delete One or More Objects" \(on page 20\)](#)

Quick Start Configuration Wizard

Note: Before you use the Quick Start Configuration Wizard, complete the initial configuration checklist. See [Help](#) → [Documentation Library](#) → [Installation Guide](#) for more information.

The Quick Start Configuration Wizard automatically runs immediately after Network Node Manager (NNMi) installation completes. Use the Quick Start Configuration Wizard to configure NNMi in a limited (or test) environment. The Quick Start Configuration Wizard helps you to complete the following initial set up tasks:

- Provide the community strings for your SNMPv1 or SNMPv2c environment
- Provide the USM settings for your SNMPv3 environment

- Discover a limited range of network nodes
- Set up an initial administrator account

You can launch the wizard using the following URL:

Note: If the NNMi Web server uses the https protocol, use `https` instead of `http`. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/quickstart/`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: HP recommends that you run the Quick Start Configuration Wizard only one time immediately after NNMi installation.

After using the Quick Start Configuration Wizard to set up a test network, see "[Configuration Workspaces](#)" (on page 16) for information about completing additional NNMi configuration tasks.

Configuration Workspaces

NNMi administrators use the Configuration workspaces to configure the following items related to NNMi.


Note: On tables in configuration forms, if the cursor changes to indicate a hyperlink when you mouse over a column heading, you are able to sort the column's data. You cannot change the sort on some of the tables on the forms in the configuration workspace.

NNMi Configuration Workspaces

Name	Description
Communication Configuration	Used to configure how NNMi uses ICMP and SNMP in your network environment.
Discovery Configuration	Used to specify the devices to be discovered.
Monitoring Configuration	Used to enable the NNMi State Poller.
Incident Configuration	Used to specify the information displayed with an incident, including its name, the message you want to be displayed, the way it should be categorized, its initial status, and how you want to identify duplicate traps.
Status Configuration	Enables an NNMi administrator to configure Node Group status calculations using either of the following methods: <ul style="list-style-type: none">• Assign the Node Group the most severe status of any Node Group member. This is the default.• Configure the percentage thresholds for one or more Node Group target statuses.
User Interface Configuration	Enables an NNMi administrator to configure the following user interface features: <ul style="list-style-type: none">• The console time out interval• The maximum number of nodes that display on a map• Whether NNMi displays unlicensed features that require a special license, such as






Name	Description
	NNMi Advanced
Node Groups	Used to group your devices for viewing and monitoring purposes.
Node Group Map Settings	<p>Used to specify the Node Group and background image to be used in a Node Group map. Map settings include the following:</p> <ul style="list-style-type: none"> • Node group name • The order in which Node Group maps should appear in the Topology workspace • Minimum role for saving edited locations for each node in the map • Refresh information • Connectivity information • Background image URL • Background image scale
Interface Groups	Used to group your devices for viewing and monitoring purposes.
RAMS Servers	Used to specify the RAMS appliance and the associated RAMS database to be used with NNMi when calculating a Path View between devices with IPv4 addresses.
Management Stations	Used to configure NNM 6.x or 7.x management stations so that they forward events to NNMi.
User Accounts and Roles	<p>Used to assign NNMi users to NNMi roles.</p> <p>Note: If NNMi role assignments are stored in your environment's directory service database, this view is not needed and is not visible. See "Control Access with a Directory Service" (on page 40).</p>
User Principals	<p>This view stores NNMi user names. Principal object instances are automatically created when you configure access to the NNMi console (using the User Accounts and Roles view) according to the following scenarios: "Control Access with NNMi Accounts" (on page 35) and "Control Access Using Both Directory Service and NNMi" (on page 37).</p> <p>Note: If NNMi role assignments are stored in your environment's directory service database, this view is not needed and should remain empty. See "Control Access with a Directory Service" (on page 40).</p>
URL Actions	Used to add actions to the Actions menu that you want to be available to your operators or to other administrators.
IfTypes	Provides a list of interface types. NNMi administrators use these ifTypes to define Interface Groups.
Device Profiles	Stores information about a type or family of device. Device profile information includes the SNMP object ID, model, and vendor. Use the Device Profile workspace to see and edit device profile information.

Lookup Fields



Lookup fields have the following icon: .

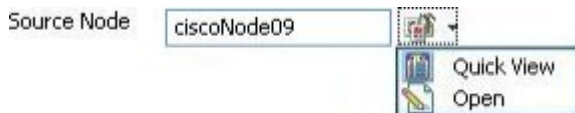
The Lookup field represents an associated object instance. For example, an Incident form has an associated Source Node attribute. Information about this source node is available in and accessed through the Lookup field.


Possible Drop-Down Menu Options in Lookup Fields

Option	Description
 Quick View	See a subset of information about the selected object. (Use  Open to see all available information about this object.)
 Quick Find	Display a list of valid choices for populating the current attribute field.
 Open	Open the form for the related object instance that is currently selected in the lookup field. Review all attributes of the related object. Depending on your role, you can edit these attributes.
 New	Create a new object instance to relate to the current object.

You can use Lookup fields in a variety of ways:

- **Read-only fields - to provide additional information about the associated object.** Click  Quick View or  Open to see the details of this object.




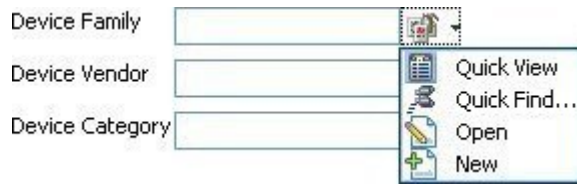
- **Selection fields - to change the association to another object instance.** Click  Quick Find to select from a list of previously configured objects ("[Use the Quick Find Window](#)" (on page 19)).





Or type a case-sensitive string into the input box ("[Use Autocomplete](#)" (on page 19)).



- **Read-write fields - create an entirely new object instance for this association.** Click  New. An empty form opens for you to fill in, creating a new object instance.



Use the Quick Find Window

The  Quick Find option is available only in Lookup fields that are modifiable. Use the  Quick Find option to see the list of available object instances appropriate for populating the current Lookup field.

To list all existing object instances that could be related to the current object:





1. From the lookup field of interest, click the  Look up icon:



2. Select  Quick Find.

NNMi displays a table view of object instances that are available to associate with to the current object instance.

3. In the Quick Find window, do one of the following:

- Click the  Make Empty icon to remove an association with this object. The Quick Find window closes, and the current lookup field is empty.
- Click the  Select This Item icon that precedes the table row containing an object instance. The Quick Find window closes, and the object instance you selected populates the current lookup field.
- Click the  Quick View icon to display a subset of available object attributes.
- Click the  Close icon to return to the previous form.

Use Autocomplete

The autocomplete feature is available only in Lookup fields that are modifiable. As you type, NNMi lists the available object instances for populating the current Lookup field.

To use the autocomplete feature:

1. Start typing the first few letters (case-sensitive) of the name of the object you want to associate with the current one.



The Lookup field displays a drop-down list below the input field. This list includes all potential existing objects with names that match the letters as you enter them.

Device Family	All	
Device Vendor	Allied Telesis	
Device Category	Allot Communications	
	Allot Communications NetEnforcer	

2. Use the scroll arrows or the mouse to select from the displayed list.


The selected object populates the lookup field and is now associated with the current object.

Create a Configuration Object Instance Using the Form Toolbar


You can save time by generating a new form from within another form. The new form is based on the object type for the original form and contains only the default values set by NNMi for particular attributes for that object. Any attributes that have no default value appear blank.

This tool is useful when you want to create multiple object instances that have similar attribute values.

To create a new object instance using the form toolbar:

1. Open the form representing the object of interest.
2. From the form toolbar, click the  Save and New icon.

A new form appears that contains the default attribute values for the object type represented by the original form.

3. Select the  **Save and Close** icon to save your changes and return to the view.


Delete One or More Objects

Each row in a table view and each symbol in a map view represents an instance of the object type being displayed. For example, in a node view, each row of the table represents an instance of a node in your network.

NNMi administrators can delete object instances. For example, you might need to delete a node that is no longer being managed.

All objects related to the deleted object are also deleted. For example, if a node object is deleted, all of its interfaces, network addresses, and its SNMP Agent are deleted. Related connections with either zero or one end points remaining are deleted. Related subnets and VLANs with zero remaining members are deleted.


To delete an object instance:

1. Select the object of interest:
 - In a table view, select the check box in the row that represents the object.
 - In a map view, click the map symbol.
 - In a form, proceed to step 2.
2. To delete the object, click the  Delete icon.

The object is deleted from the NNMi database and removed from the current view.

To delete multiple object instances:

1. Select the objects of interest:

- In a table view, do one of the following:
 - Select the check box in the row that represents each object you want to delete.
 - Select the check box above the check-box column to select all objects in the view.
 - In a map view, CTRL-Click each map symbol.
2. To delete the objects, click the  Delete icon.

Note: For Node objects, you can use this method to delete up to 20 nodes at one time. You can use the command line method to delete any number of nodes. See ["Delete Nodes" \(on page 122\)](#) for more information.

Tip: For all other objects, you can delete any number.

Each object is deleted from the NNMi database and removed from the current view.

Perform Automated Tasks

Use the Actions menu to perform automated tasks on a single object or on a group of objects. For example, you can use the Actions menu to change the Management Mode of one or more nodes from **Managed to Out of Service**.

Actions are available within table views, map views, or forms. When in a view, you can access actions from the console main menu toolbar. If you are in a view that is launched in a separate window, you can access actions from the view window menu bar. When in a form, you access actions from the form menu bar.


Note: Only those actions that apply to the current object appear in the **Actions** menu. For example, in an incident view, close one or more incidents by using the **Close** action.

To invoke an action from a table or map view:

1. Select the object of interest:
 - In a table view, select the check box that precedes the object information.
 - In a map view, single-click the object.
2. In the menu toolbar, click **Actions**.
3. Select an action from the list of available actions.

For example, from an incident view, select **Actions** → **In Progress** to change the lifecycle state of an incident to **In Progress**.

To invoke an action from a form:

1. If you do not have a form open:
 - a. From the workspace navigation panel, select the table view you want to access.
 - b. In the table view, locate the object (a row in the table).
 - c. Click the  Open icon in that row to open the object instance (for example, node).
2. In the menu toolbar, click **Actions**.
3. Select an action from the list of available actions.

For example, from an incident view, select **Actions** → **In Progress** to change the lifecycle state of an incident to **In Progress**.

Note: If you are running an action from a form, the action takes effect immediately. This means you do not have to select **Save**.

If you are accessing an action from a map, note the following:

- You must select a node, interface, or address before you can access the following actions:
 - Manage
 - Out of Service
 - Unmanage
- You must select a node or interface to access the **Manage (Reset All)** action.
- (NNM iSPI NET). You must select a node to access the **Show Attached End Nodes** action. See [Display End Nodes Attached to a Switch](#) for more information.

See ["Actions Provided by NNMi" \(on page 22\)](#) for information about the actions provided by NNMi.

Actions Provided by NNMi

The following tables describe the actions provided by NNMi:

[Actions Provided for Incidents](#)

[Actions Provided for Nodes](#)

[Actions Provided for Interfaces](#)

[Actions Provided for Addresses](#)

[Actions Provided for Node Groups](#)

As shown in the table, the actions available depend on the object selected.

Note: You can also use the Actions menu to access views and possibly NNM 6.x/7.x features. See [Access NNM 6.x and 7.x Features](#) for more information about the available NNM 6.x/7.x actions.

Actions Provided for Incidents

Action	Description
Close	Changes the lifecycle state to Closed for the selected incident.
Completed	Changes the lifecycle state to Completed for the selected incident.
Configuration Poll	Launches a real-time configuration check of the selected device to detect any changes since the last discovery cycle.
Delete	Deletes the selected object or objects.
Node Group Map	<p>Displays the lowest level Node Group map to which the Source Node belongs. For example, if the node belongs to a Child Node Group, the Child Node Group displays.</p> <p>If the Source Node is a member of more than one Node Group at the lowest level, NNMi prompts you to select the Node Group map you want to display.</p> <p>If the incident's Source Object is an Island Node Group, NNMi displays the Island Node Group map.</p> <p>Note: Incidents whose Source Object is an Island Node Group include Remote site in the incident message. See "Help for Operators" for more information.</p> <p>When the selected Source Node is not a member of any Node Group, and you select the</p>

Action	Description
	Node Group Map action, NNMi displays an information message.
Node Group Members	<i>Island Node Group incidents only.</i> Displays a table of the nodes that are members of the Island Node Group that is the Source Object for the selected incident. Note: Incidents whose Source Object is an Island Node Group include Remote site in the incident message.
Own Incident	Assigns the incident to the current user. This user name appears in the Assigned To column of the incident view.
In Progress	Changes the lifecycle state to In Progress for the selected incident.
Ping	Tests whether a node is reachable using the ping command.
Run Diagnostics	If you have NNM iSPI NET, gathers diagnostic information from the Source Node.
Source Node	Displays the node form of the source node object instance.
Source Object	Displays the form of the source object instance.
Status Poll	Launches a real-time check of the state of the selected device. If the state has changed, NNMi calculates an updated status reading for the selected device.
Trace Route	Traces a route path using the traceroute command.
Telnet	Establishes a connection to a node to view or change configuration information.
Unassign Incident	Removes the user name from the Assigned To column of the incident view.

Actions Provided for Nodes

Action	Description
Communication Settings	Displays the communication configuration information for the selected node.
Configuration Poll	Launches a real-time configuration check of the selected device to detect any changes since the last discovery cycle.
Delete	Deletes the selected object or objects (maximum 20). To delete more than 20 nodes, see the nnmnodedelete.ovpl Reference Page.
Manage	Changes the Management Mode of the selected node to Managed . Leaves the Direct Management Mode of any contained interfaces and addresses unchanged.
Manage (Reset All)	Changes the Management Mode of the selected node to Managed . Sets the Direct Management Mode of all contained interfaces and addresses to Inherited .
Monitoring Settings	Checks the monitoring configuration settings that were set for a particular node, interface, or IP address.
Node Group Map	Displays a current map of the node group to which the node belongs. The map shows all nodes that belong to the node group.

Action	Description
Out of Service	Changes the Management Mode of the selected node to Out of Service . Leaves the Direct Management Mode of any contained interfaces or addresses unchanged.
Ping	Tests whether a node is reachable using the ping command.
Run Diagnostics	If you have <i>NNM iSPI NET</i> , gathers diagnostic information on the current node.
Show Attached End Nodes	If you have <i>NNM iSPI NET</i> , displays information about the end nodes that NNMi determines are attached to the specified switch.
Status Poll	Launches a real-time check of the state of the selected device. If the state has changed, NNMi calculates an updated status reading for the selected device.
Telnet	Establishes a connection to a node to view or change configuration information.
Trace Route	Traces a route path using the traceroute command.
Unmanage	Changes the Management Mode of the node to Not Managed . Leaves the Direct Management Mode of any contained interfaces and addresses unchanged.

Actions Provided for Interfaces

Action	Description
Manage	Changes the Direct Management Mode of the interface to Inherited . Leaves the Direct Management Mode of any associated addresses unchanged.
Manage (Reset All)	Changes the Management Mode of the interface to Inherited . Changes the Direct Management Mode of any associated addresses to Inherited .
Monitoring Settings	Checks the monitoring configuration settings that were set for a particular node, interface, or address.
Node Group Map	Displays a current map of the Node Group to which the node (containing this interface) belongs. The map shows all nodes that belong to the Node Group.
Out of Service	Changes the Management Mode of the interface to Out of Service .
Unmanage	Changes the Management Mode of the interface to Not Managed . Leaves the Direct Management Mode of any associated addresses unchanged.

Actions Provided for Addresses

Action	Description
Configuration Poll	Launches a real-time configuration check of the selected device to detect any changes since the last discovery cycle.
Manage	Changes the Direct Management Mode of the address to Inherited .
Monitoring Settings	Checks the monitoring configuration settings that were set for a particular node, interface, or address.

Action	Description
Configuration Poll	Launches a real-time configuration check of the selected device to detect any changes since the last discovery cycle.
Node Group Map	Displays a current map of the Node Group to which the node (containing this IP address) belongs. The map shows all nodes that belong to the Node Group.
Out of Service	Changes the management mode of the address to Out of Service .
Ping	Tests whether a node is reachable using the ping command.
Telnet	Establishes a connection to a node to view or change configuration information.
Trace Route	Traces a route path using the traceroute command.
Unmanage	Changes the management mode of the address to Not Managed .

Actions Provided for Node Groups

Action	Description
Node Group Map	Displays a current map of all nodes that belong to the selected Node Group.
Show All Incidents	Checks for any Incidents associated with the selected Node Group.
Show All Open Incidents	Checks for any open Incidents associated with the selected Node Group.
Show Members	Displays a list of all nodes that belong to the selected Node Group.
Status Details	Launches a real-time status check of the selected Node Group to detect any changes since the last discovery cycle.

Actions Provided for Router Redundancy Member, Tracked Object, and Node Component

Action	Description
Monitoring Settings	Checks the monitoring configuration settings that were set for the Router Redundancy Member, Tracked Object, or Node Component.

NNMi Processes and Services

NNMi is built on a group of processes and services. For information about each process or service, see the following:

- ["About Each NNMi Process" \(on page 26\)](#)
- ["About Each NNMi Service" \(on page 26\)](#)

To verify that everything is running properly, you can use the ovstatus command:

- ["Verify that NNMi Processes Are Running" \(on page 26\)](#)

About Each NNMi Process

HP Network Node Manager Processes

Process Name	Description
OVsPMD	The control process that manages all the other NNMi processes.
pmd	Event Post Master daemon. This process routes events from the producers to the consumers. Producers of events are NNM 6.x/7.x management stations and processes. Consumers of events are the event pipeline and third party applications.
ovjboss	The process that controls the jboss application server that contains all of the NNMi Services (see "About Each NNMi Service" (on page 26) for more information).
nmsdbmgr	NMS Database Manager. Controls the NNMi embedded database, including periodic database connectivity testing.

Verify that NNMi Processes Are Running

After you install Network Node Manager, a group of processes run on the NNMi management server.

To verify that all NNMi processes are running, do one of the following:

1. Select **Tools** → **NNMi Status** to display a report.
2. At the command line, type: **ovstatus -c**

See the [ovstatus](#) Reference Page for more information.

Review the list of processes to ensure that all are running. For more information about each process, see ["About Each NNMi Process" \(on page 26\)](#).

Stop or Start an NNMi Process

You can stop and start NNMi processes from the command line. See the [ovstop](#) and [ovstart](#) Reference Pages for more information.

To stop or start an NNMi process:

At the command line, type the appropriate command:

ovstop <process name>

ovstart <process name>

To generate a list of process names, see ["Verify that NNMi Processes Are Running" \(on page 26\)](#).

About Each NNMi Service

NNMi Services run inside the ovjboss process. The ovjboss process controls the jboss application server that contains all of the NNMi services.

HP Network Node Manager Services

ovjboss Service Name	Description
CommunicationParametersStatusService	Tracks internal statistics for measuring SNMP and ICMP configuration performance.

ovjboss Service Name	Description
IslandSpotterService	Auto discovers the Island Node Groups using Layer 2 connectivity information in the topology.
ManagedNodeLicenseManager	Managed Node License Manager. Responsible for ensuring that the number of managed nodes does not exceed the NNMi license capacity.
ModelChangeNotificationAdapter	Emits notifications when certain model changes happen (discovery seeds, global settings, Spiral Discovery configuration, management node).
MonitoringSettingsService	Calculates how to monitor each device based on the Monitoring Configuration settings.
NamedPoll	NMS Named Poll Service. Used to trigger immediate state polls for monitored objects. Used by the Causal Engine during neighbor analysis and interface up/down investigations.
NmsApa	NMS Active Problem Analyzer (APA) service determines the root cause of network problems and reports the root cause to the NMS Event Service. The Causal Engine is a key component of the NNMi APA service.
NmsDisco	<p>NMS Discovery Service. Adds new devices to the database and keeps the configuration of the managed devices up to date in the database by periodically rechecking the configuration of the devices.</p> <p>State Poller uses the Discovery service results to determine what to monitor.</p> <p>The Causal Engine depends on the Discovery service to monitor node configurations. The Causal Engine uses the configuration information when calculating status and root cause.</p> <p>NNMi uses the information provided by the Discovery service to maintain current device configuration information.</p>
NmsEvents	NMS Events Service. Populates and manages the information displayed in the incident table. The information displayed comes from the other NNMi services that are running on your system. The incidents are filtered so you see only the most important information about your network.
NmsEventsConfiguration	Handles incident configuration changes.
NmsModel	NMS Topology Model Service. Enables communication between NNMi services and the NNMi database.
SpmdjbossStart	The SpmdjbossStart service interacts with the OVSPMD process during startup (ovstart), shutdown (ovstop), and reporting on the status of the ovjboss services (ovstatus -v ovjboss).
StagedIcmp	Used by the State Poller to ping IP addresses using the Internet Control Message Protocol (ICMP). Also used by Auto-Discovery if Ping Sweep is enabled.

ovjboss Service Name	Description
StagedSnmp	Used by the State Poller and Discovery to perform Simple Network Management Protocol (SNMP) read-only queries.
StatePoller	NMS State Poller Service. State Poller collects measurements that assess the current state of discovered devices. This information is provided for the Causal Engine to use when calculating device health.

NNM iSPI NET Required.

ovjboss Service Name	Log File
RbaManager	Used by NNM iSPI NET. Controls diagnostics execution.

Verify that NNMi Services Are Running

After you install Network Node Manager, a group of services run on the NNMi management server. For information about each service, see ["About Each NNMi Service" \(on page 26\)](#).

To verify that all NNMi services are running, do one of the following:

- Select **Tools** → **NNMi Status** to display a report.
- At the command line, type:

ovstatus -v ovjboss

See the [ovstatus](#) Reference Page for more information.

Review the list of services to ensure that all are running.

"Service is started" means this service is working properly.

"Service is stopped" means this service/process is not running.

If you see any of the messages in this list, investigate the log files and look for the keyword **Exception** (within the log file for the parent `ovjboss` process and the log file for the specific service, possible services are listed in the [table](#) below):

- "Service is in created state"
- "Service is in failed state"
- "Service is in registered state"
- "Service is in destroyed state"
- "Service is in started state"
- "Service is in starting state"
- "Service is in stopped state"
- "Service is in stopping state"
- "Service is in unregistered state"

Log files are found in the following location:

- **Windows:**
`<drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO`

Software\log\nnm\

<drive> is the drive on which NNMi is installed.

• UNIX:

/var/opt/OV/log/nnm/

%g = Zero (0) for active log files. Any other number means an archived log file from previous restarts or from reaching log file size limits. See [logging.properties](#) for information about controlling the number of archives saved for each log file or for controlling the size of each log file.

%u = Zero (0) unless the parent `ovjboss` process failed during a logging session. While a service is logging information, the service creates a file named `<serviceName>.0.0.log.lck` (the lock file). The presence of this lock file prevents other services from writing to the `<serviceName>.0.0.log` file. The service deletes the lock file when it finishes logging. If a `<serviceName>.0.0.log.lck` file already exists, the service creates `<serviceName>.0.1.log.lck` file and writes to the `<serviceName>.0.1.log` file.

The parent `ovjboss` process generates the following log files:

- `ovjboss.log` and `ovjboss.log.old`
- `jbossServer.log` and `jbossServer.<date>.log`

Note: Each restart creates a new `ovjboss.log` and overwrites the `ovjboss.log.old`. Each day a new `jbossServer.log` file is created, and the previous day's file is renamed by inserting a date stamp `jbossServer.<date>.log`

The following table describes the `ovjboss` services and the log file each service generates.

Log File Names for Each ovjboss Service

ovjboss Service Name	Log File
CommunicationParametersStatusService	snmp.%g.%u.log
ManagedNodeLicenseManager	nmslic.%g.%u.log
ModelChangeNotificationAdapter	nmsmodel.%g.%u.log
MonitoringSettingsService	mon-config.%g.%u.log
NMSLogManager	admin.%g.%u.log
NamedPoll	statepoller.%g.%u.log
NmsApa	apa.%g.%u.log
NmsDisco	disco.%g.%u.log
NmsEvents	events.%g.%u.log
NmsEventsConfiguration	events.%g.%u.log
NmsModel	nmsmodel.%g.%u.log
NmsNotification	nmsmodel.%g.%u.log
NmsNotificationDestinationManager	nmsmodel.%g.%u.log
SpmjbossStart	admin.%g.%u.log

ovjboss Service Name	Log File
StagedIcmp	snmp.%g.%u.log
StagedSnmp	snmp.%g.%u.log
StatePoller	statepoller.%g.%u.log

Stop or Start NNMi Services

You can stop or start all NNMi services at the same time. You cannot start and stop individual services. See the [ovstop](#) and [ovstart](#) Reference Page for more information

To stop or start the NNMi services:

At the command line, type the command:

ovstop ovjboss

ovstart ovjboss

Use NNMi Help Anywhere, Anytime

The NNMi Help system can run independently from the console. Simply unzip the files into any convenient location.

To locate the NNMi Help files, on the NNMi management server, navigate to the location appropriate for the NNMi management server's operating system (see table).

Location of the NNMi Help System

Operating System	NNMi Help System Files
Windows	<drive>:\Program Files (x86)\HP\HP BTO Software\nonOV\jboss\nms\server\nms\deploy\nnmDocs_en.war <drive> is the drive on which NNMi is installed
UNIX	/opt/OV/nonOV/jboss/nms/server/nms/deploy/nnmDocs_en.war

To access Help independently from the console:

1. Copy the web archive file `nnmDocs_en.war` to any convenient location.
2. At the command prompt, navigate to the directory where you placed the `nnmDocs_en.war` file. To extract the help directory structure and files, type:

```
jar xvf nnmDocs_en.war
```

Tip: You can also use WinZip on Windows to decompress the `nnmDocs_en.war` file.

3. Navigate to and open the `/htmlHelp/nmHelp/nmHelp.html` file.
4. The NNMi Help system runs as usual in the default browser window.
- 5.

To Access a PDF version of the NNMi online help:

Go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport ID. To obtain an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Controlling Access to NNMi

As administrator, you control who accesses the NNMi console. The role you assign to each user determines which workspaces and actions are available within the NNMi console. To accomplish this, configure the following:

- ["Configure Sign-In Access" \(on page 32\)](#)
- ["Set Up Command Line Access" \(on page 42\)](#)
- ["Audit NNMi User Activity" \(on page 43\)](#)

Tip: You can configure the NNMi management server to use https/SSL so that data passed between client and server is encrypted. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

When configuration is complete, share information about NNMi with your team:

- ["Communicate to Your Team" \(on page 44\)](#)

Configure Sign-In Access

First decide which pre-defined NNMi role is appropriate for each user in your environment:

- ["Roles Provided in NNMi" \(on page 32\)](#)

Then choose how to configure access to the data required for NNMi logins:

1. ["Control Access with NNMi Accounts" \(on page 35\)](#)
User names, passwords, and role assignments are stored in the NNMi database.
2. ["Control Access Using Both Directory Service and NNMi" \(on page 37\)](#)
User names must be stored in both the directory service database and the NNMi database. Passwords are stored in the directory service database. Role assignments are stored in the NNMi database. NNMi communicates with the directory service using Lightweight Directory Access Protocol (LDAP).
3. ["Control Access with a Directory Service" \(on page 40\)](#)
User names, passwords, and role assignments are stored in the directory service. NNMi communicates with the directory service using Lightweight Directory Access Protocol (LDAP).

Which Database Stores the Information?

	User Name	Password	Role Mapping
1	NNMi	NNMi	NNMi
2	Both	Directory Service	NNMi
3	Directory Service	Directory Service	Directory Service

Roles Provided in NNMi

As NNMi administrator, you assign a preconfigured NNMi role to each NNMi user. (For more information, see ["Configure Sign-In Access" \(on page 32\)](#).)

User roles determine access to the NNMi console workspaces, forms, and actions. NNMi provides the following roles:

- Administrator
- Operator Level 2
- Operator Level 1
- Guest

You cannot create additional roles or change the names of the roles that NNMi provides.

Caution: Do not use the `system` role or Web Service Client role. NNMi provides the `system` role for accessing NNMi the first time during installation and for command line access (see ["Set Up Command Line Access" \(on page 42\)](#)). NNMi provides a special Web Service Client role to provide access for software that is integrated with NNMi.

For details about each predefined NNMi role:

- ["Determine which NNMi Role to Assign" \(on page 33\)](#)
- ["Access to Forms" \(on page 322\)](#)
- ["Access to Workspaces" \(on page 322\)](#)
- ["Access to Commands" \(on page 323\)](#)

Tip: NNMi administrators control which roles can access a small subset of Action menu items (see ["Control Menu Access" \(on page 34\)](#)) and set role permissions for Node Group map modifications (see ["Configure Basic Settings for a Node Group Map" \(on page 200\)](#)).

Determine which NNMi Role to Assign

Before configuring NNMi sign-in access for your team, determine which predefined NNMi role is appropriate for each team member. The roles are hierarchical, meaning the higher level roles include all privileges of the lower roles in the hierarchy (Administrator is highest, Guest is lowest). See also [additional information about how access to Actions is controlled by role](#).

As NNMi administrator, you can change a few aspects of role definitions:

- You can restrict access to certain URL actions (provide tighter security than the predefined NNMi roles enforce). See ["Configure URL Action Basic Behavior" \(on page 303\)](#) for more information about configuring actions.
- You can set role permissions for Node Group map modifications, see ["Configure Basic Settings for a Node Group Map" \(on page 200\)](#).

Role Permissions

Role	Workspaces	Actions Menu Items
Administrator	All workspaces (see the Views Provided by NNMi)	All actions available in other roles, plus Communication Settings
Operator Level 2	Incident Management, Topology Maps, Monitoring, Troubleshooting, Inventory, Management Mode, and Incident Browsing	All actions available in Operator Level 1 role, plus Telnet, Configuration Poll, Status Poll

Role	Workspaces	Actions Menu Items
Operator Level 1	Incident Management, Topology Maps, Monitoring, Troubleshooting, Inventory, and Incident Browsing	<p>Ping, Trace Route, Monitoring Settings</p> <p>NNM iSPI NET. Run Diagnostics</p> <p>Show Members, Show All Incidents, Show All Open Incidents (Node Group views only, see Node Group and Interface Groups for more information about Node Group actions.)</p> <p>6.x/7.x Neighbor View, 6.x/7.x Details, 6.x/7.x ovw, 6.x/7.x Home Base, 6.x/7.x Launcher, SNMP Viewer, Alarms (you must configure an NNM 6.x/7.x Management Station, see Access NNM 6.x and 7.x Features from NNMi for more information about 6.x/7.x actions.)</p>
Guest	<p>Read-only access to the same views as the Operator Level 1 role (see above).</p> <p>Because users assigned to Guest role have read-only access, they cannot make any changes to NNMi or to NNMi objects.</p>	No access to actions.
Web Service Client	Do not assign users on your team to the Web Service Client role. Any login attempt using this Role results in errors that require restarting your browser.	
system	Do not assign users on your team to the system role.	

Note: You control access to NNMi command line commands. See ["Set Up Command Line Access" \(on page 42\)](#) for more information.

See [About Workspaces](#) for more information about workspaces. See [Views Provided by NNMi](#) for more information about the views provided in each workspace.

Control Menu Access

Access to the [Tools](#) and [Actions](#) menu items is controlled by user role. (See ["Determine which NNMi Role to Assign" \(on page 33\)](#) for additional information about role limitations.)

Note: You can restrict access to certain URL actions (provide tighter security than the predefined NNMi roles enforce). See ["Configure URL Action Basic Behavior" \(on page 303\)](#) for more information about configuring actions.

Role Based Access the Tools Menu:

Access to the NNMi Tools menu items is determined by user role.

NNMi Tools Menu Access Limitations

Tools Menu Item	Lowest Role (Security Check)
Find Node	Not Applicable
NNMi Status	Operator Level 1
Sign In/Sign Out Audit Log	Administrator

Role Based Access the Actions Menu:

Access to the NNMi Actions menu is determined by user role.

Note: All menu items are visible, but an Access Denied message displays when any user with insufficient privileges tries to use a menu item. For example, both Level 1 or Level 2 Operators are denied access to the Communication Settings action. And Level 2 Operators can access the Monitoring Settings action, but Level 1 Operators are denied access.

URL Action Access Limitations

Action Menu Item	Default Role	Lowest Role (Security Check)
Ping (from server)	Operator Level 1	Operator Level 1
Traceroute (from server)	Operator Level 1	Operator Level 1
Telnet...(from client)	Operator Level 2	Operator Level 2
Communication Settings	Administrator	Administrator
Monitoring Settings	Operator Level1	Operator Level 1
Status Poll	Operator Level 2	Operator Level 2
Configuration Poll	Operator Level 2	Operator Level 2
Node Group Map	Guest	Guest
Show Members	Guest	Guest
Show All Incidents	Operator Level 1	Operator Level 1
Show All Open Incidents	Operator Level 1	Operator Level 1
Status Details	Operator Level 1	Operator Level 1

See [Investigate and Diagnose Network Problems](#) for more information about these actions.

Control Access with NNMi Accounts






To configure NNMi to store user names, passwords, and role assignments in the NNMi database, use the following instructions.


Which Database Stores the Information?

User Name	Password	Role Mapping
NNMi	NNMi	NNMi


Tip: If you prefer to configure NNMi logins to use data stored in the directory service database, see ["Control Access Using Both Directory Service and NNMi" \(on page 37\)](#) or ["Control Access with a Directory Service" \(on page 40\)](#).

To grant NNMi access to a user:

1. Navigate to the **Account Mapping** form.
 - a. From the workspaces navigation panel, select the **Configuration** workspace.
 - b. Select the **User Accounts and Roles** view.
 - c. Do one of the following:
 - To create new configuration, click the  New icon, and continue.
 - To edit an existing configuration, select a row, click the  Open icon, and continue.
2. Locate the **Account** attribute, and click the  Lookup icon. (See ["Using the Account Mapping Form"](#) for more information.)
 - To create new account, click the  New icon and provide the required user name and password. See ["Using the User Account Form"](#) for more information.) Then click  **Save and Close** to return to the **Account Mapping** form.

Tip: The user name you just created is added to the User Principals view.
 - To select an NNMi user configuration (user name and password), click the  Quick Find icon and make a selection.
3. Locate the **Role** attribute.

Select a predefined NNMi role from the drop-down menu. See ["Roles Provided in NNMi"](#) (on page 32) for more information.

Note: If you accidentally assign two different NNMi roles to the same NNMi user name, NNMi uses the higher level role.
4. Click  **Save and Close** to save your changes and return to the **User Accounts and Roles** view.

Related Topics

["Change Password, Name, or Role Assignment" \(on page 36\)](#)

["Disable a User's Access to NNMi" \(on page 41\)](#)

["Troubleshoot NNMi Access" \(on page 41\)](#)

Change Password, Name, or Role Assignment

If configuring NNMi to store user names, passwords, and role assignments in the NNMi database, use the following instructions.

Which Database Stores the Information?

User Name	Password	Role Mapping
NNMi	NNMi	NNMi

Note: If configuring NNMi to use the directory service database, see ["Change Role Assignment for a Directory Service User Name" \(on page 39\)](#) or ["Control Access with a Directory Service" \(on page 40\)](#).

Only NNMi administrators can change account details.





To change an NNMi user name:

You must ["Disable a User's Access to NNMi" \(on page 41\)](#), and then recreate the account mapping (see

["Control Access with NNMi Accounts" \(on page 35\)](#)).


Note: If you disable NNMi access for a user who is currently signed in to the NNMi console, the change does not take effect until the user signs in next time.


To change an NNMi password:

1. Navigate to the **User Accounts and Roles** view.
 - a. From the Workspaces navigation panel, select the **Configuration** workspace.
 - b. Select the **User Accounts and Roles** view.
2. Click the  Open icon in the row representing the account you want to edit.
3. To change the user's password, locate the **Account** attribute:
 - a. Click the  Lookup icon and select **Open** to access the [User Account](#) form.
 - b. Edit the **Password** value. Type up to 40 alpha-numeric characters, punctuation, spaces, and underline characters.
 - c. Click  **Save and Close** to return to the **Account Mapping** form.
4. Click  **Save and Close**. NNMi immediately implements your changes.

Note: If you change the password for a user who is currently signed in to the NNMi console, the change does not take effect until the user signs in next time.

To change an NNMi role assignment:

1. Navigate to the **User Accounts and Roles** view.
 - a. From the Workspaces navigation panel, select the **Configuration** workspace.
 - b. Select the **User Accounts and Roles** view.
2. Click the  Open icon in the row representing the account you want to edit.
3. To change the user's NNMi role assignment, locate the **Role** attribute.

Click the drop-down list and select the new role for the current NNMi user. See ["Determine which NNMi Role to Assign" \(on page 33\)](#) for more information about NNMi user roles and their privileges.
4. Click  **Save and Close**.

Note: If you change the role for a user who is currently signed in to the NNMi console, the change does not take effect until the user signs in next time.

Control Access Using Both Directory Service and NNMi

To configure NNMi to store role assignments in the NNMi database, but rely on your directory service for user names and passwords, use the following instructions. NNMi communicates with the directory service using Lightweight Directory Access Protocol (LDAP).

Which Database Stores the Information?

User Name	Password	Role Mapping
Both	Directory Service	NNMi

Tip: If you prefer to configure NNMi logins to only use data stored in the directory service database, see ["Control Access with a Directory Service" \(on page 40\)](#).


To enable NNMi to communicate with your environment's directory service:

1. Modify the `nms-ldap.properties` file. See the "Integrating NNMi with a Directory Service through LDAP" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>

Note: To make changes to a user name or password, you must now use the appropriate process for making changes to your environment's directory service software and make changes in NNMi (see ["Change Role Assignment for a Directory Service User Name" \(on page 39\)](#)).

2. **If you are switching from previously storing passwords in the NNMi database, do this step:**


Note: The password information is no longer required to be in the NNMi database.

- a. Navigate to the **User Principals** view:
 - i. From the workspace navigation panel, select the **Configuration** workspace.
 - ii. Select the **User Principals** view.
 - b. Delete all objects in the User Principals view:
 - i. Select all objects by clicking in the column heading row.
 - ii. Click the  button in the view toolbar.
 - c. Navigate to the **User Accounts and Roles** view:
 - i. From the workspace navigation panel, select the **Configuration** workspace.
 - ii. Select the **User Accounts and Roles** view.
 - d. Verify that there are no remaining objects in this view. (When you deleted Principal objects, any associated account objects were automatically removed.)
 - e. Continue with the next set of instructions.
3. **Establish the NNMi role mappings for directory service users:**
 - a. Navigate to the **User Accounts and Roles** view:
 - i. From the workspace navigation panel, select the **Configuration** workspace.
 - ii. Select the **User Accounts and Roles** view.
 - b. Repeat this step for each NNMi user.

Associate each user name from your environment's directory service with a predefined NNMi role.

Click the  New icon. See ["Using the Account Mapping Form"](#).


- o Locate the **Account** attribute.

Click the  New icon. Enter the user name exactly as it appears in your environment's directory service database (case-sensitive). See ["Using the Principal Form"](#).

Tip: The user name you just created is added to the User Principals view.

- o Locate the **Role** attribute.

Select a predefined NNMi role from the drop-down menu. See ["Roles Provided in NNMi" \(on page 32\)](#) for more information.

- o Click  **Save and Close** to save your role configuration changes and return to the **User Accounts and Roles** view.
- c. Access the **Incident Browsing** workspace.
- d. Open the **All Incidents** view.

Sort this view using the Assigned To (**AT**) column.

Verify that any *assigned* Incidents are associated with a valid user from the directory service database.

- o If the user names previously stored in the NNMi database are the same (case-sensitive) as those defined in your environment's directory service, no changes are required for Incident assignments.
- o If the user names have changed, reassign the Incidents to a valid user name (see [Assign an Incident](#)).

Change Role Assignment for a Directory Service User Name

If configuring NNMi to store user names and passwords in your environment's directory service, but to store role assignments in the NNMi database, use the following instructions. NNMi communicates with the directory service using Lightweight Directory Access Protocol (LDAP).

Which Database Stores the Information?

User Name	Password	Role Mapping
Both	Directory Service	NNMi

Note: To configure NNMi to use directory service for role assignments, see ["Control Access with a Directory Service" \(on page 40\)](#).

Only NNMi administrators can change the role assigned to each authorized directory service user name.

To change an NNMi role assignment:

1. Navigate to the **User Accounts and Roles** view.
 - a. From the Workspaces navigation panel, select the **Configuration** workspace.
 - b. Select the **User Accounts and Roles** view.

2. Click the  Open icon in the row representing the mapping you want to edit.

3. Locate the **Role** attribute.

Click the drop-down list and select the new NNMi role for the current user. See ["Determine which NNMi Role to Assign" \(on page 33\)](#) for more information about NNMi user roles and their privileges.

Note: If you accidentally assign two different NNMi roles to the same NNMi user name, NNMi uses the higher level role.

4. Click  **Save and Close**.

Note: If you change the role for a user who is currently signed in to the NNMi console, the change does not take effect until the user signs in next time.

Control Access with a Directory Service

To configure NNMi to rely on your environment's directory service for role assignments, user names, and passwords, use the following instructions. NNMi communicates with the directory service using Lightweight Directory Access Protocol (LDAP).

Which Database Stores the Information?

User Name	Password	Role Mapping
Directory Service	Directory Service	Directory Service


Tip: If you prefer to configure NNMi to store the role assignments in the NNMi database, see ["Control Access Using Both Directory Service and NNMi" \(on page 37\)](#).

To enable NNMi to communicate with your environment's directory service:

1. Modify the `nms-ldap.properties` file. See the "Integrating NNMi with a Directory Service through LDAP" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>

Note: To make changes to NNMi access (user name, password, or NNMi role assignment), you must now use the appropriate process for making changes to your environment's directory service software.

2. **If you are switching from previously storing this data in the NNMi database:**

- a. Navigate to the **User Principals** view:
 - i. From the workspace navigation panel, select the **Configuration** workspace.
 - ii. Select the **User Principals** view.
- b. Delete all objects in the view:
 - i. Select all objects by clicking in the column heading row.
 - ii. Click the  button in the view toolbar.
- c. Navigate to the **User Accounts and Roles** view:
 - i. From the workspace navigation panel, select the **Configuration** workspace.
 - ii. Select the **User Accounts and Roles** view.
- d. Verify that there are no remaining objects in this view. (When you deleted Principal objects, any associated Account Mapping and User Account objects were automatically removed.)
- e. Access the **Incident Browsing** workspace.
- f. Open the **All Incidents** view.

Sort this view using the Assigned To (**AT**) column.

Verify that any *assigned* Incidents are associated with a valid user from the directory service database.

- If the user names previously stored in the NNMi database are the same (case-sensitive) as those defined in your environment's directory service, no changes are required for Incident assignments.
- If the user names have changed, reassign the Incidents to a valid user name (see [Assign an Incident](#)).


Disable a User's Access to NNMi

Note: If you configured NNMi to store *role assignments* in your environment's directory service database (not the NNMi database), ignore this topic. To disable a user's access to NNMi, use the appropriate process required by your environment's directory service software (see ["Control Access with a Directory Service"](#) (on page 40)).

To deny a user's access to the console, delete their user configuration settings from the NNMi database.

Caution: If you delete the last NNMi user assigned to the `Administrator` role, no one can access the Configuration workspace. See ["Troubleshoot NNMi Access"](#) (on page 41) for more information about how to recover from this mistake.

To deny a user's access to NNMi:

1. Navigate to the **User Principals** view.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **User Principals** view.
2. Check the selection box () that precedes the row containing their user name.
3. Click the  Delete icon.

The user's configuration is automatically removed from *both* the User Principals view and the User Accounts and Roles view.

Tip: Access the Incident Browsing workspace. Open the All Incidents view. Sort this view using the Assigned To (AT) column. Reassign all Incidents associated with any user you deleted (see [Assign an Incident](#)).

Troubleshoot NNMi Access

If you have accidentally configured NNMi so that no one is assigned to the `Administrator` role (preventing anyone from being able to access the Configuration workspaces), use the `system` user account to correct the problem.

Sign in to the console using the password that was configured for the `system` account when NNMi was installed.

If you do not remember the password assigned to the `system` account, use the `nnmchangesyspw.ovpl` to reset the `system` password. See [nnmchangesyspw.ovpl](#) for more information.

Note: If you are still unable to log on to the console, verify that the `nms-roles.properties` file is in good working order. See ["Restore the System Role"](#) (on page 41) for more information.

Restore the System Role

NNMi provides an `nms-roles.properties` file that stores the `system` role assignment. This file is located in the following directory:

- **Windows:**

```
<drive>:Program Files (x86)\HP\HP BTO  
Software\nonOV\jboss\nms\server\nms\conf\props\nms-roles.properties
```

<drive> is the drive on which NNMi is installed

- **UNIX:**

`/opt/OV/nonOV/jboss/nms/server/nms/conf/props/nms-roles.properties`

You should not need to ever modify this file.

To verify the contents of this file:

1. With a text editor, open the `nms-roles.properties` file.
2. Verify that the following required line is present:
`system=admin`
3. Save and close the file.

Set Up Command Line Access

NNMi limits access to command line interface commands in one of two ways:

- Requiring user name and password.
- Requiring `system` role.

See **Help** → **Documentation Library** → **Reference Pages** for a list of command line commands. Check the appropriate Reference Page to determine which strategy applies.

Requiring User Name and Password

If you do not want to enter a user name and password at the command line, you can use the `nmsetcmduserpw.ovpl` command to specify the valid user name and password to be used in place of the `-u` (user name) and `-p` (password) options. The credentials defined using the `nmsetcmduserpw.ovpl` command are valid for command execution by the same user. See [nmsetcmduserpw.ovpl](#) for more information.

Requiring System Role

During installation, a special `system` user account is used to access NNMi for the first time. Thereafter, that special account should be used only for these purposes: to use some command line interface commands and to ["Troubleshoot NNMi Access" \(on page 41\)](#).

Command line interface commands that required the `system` user account must be issued from the NNMi management server, and you must have *read-only* or *read-write* access to the following files on the NNMi management server:

1. `nms-users.properties`
2. `nms-roles.properties`

Caution: Any user with read-write access to the `nms-users.properties` and `nms-roles.properties` files can potentially change the NNMi `system` user account password. (UNIX: by default, only the `root` user has read-write access to these files. Windows: by default, *any user name that is associated with the Administrators group* has read-write access to these files.)

To configure read-only or read-write access to the `nms-users.properties` and `nms-roles.properties` files. Follow the operating system instructions for changing file access permissions.

- **Windows:**

```
<drive>:\Program Files (x86)\HP\HP BTO  
Software\nonOV\jboss\nms\server\nms\conf\props\nms-roles.properties
```

```
<drive>:\Program Files (x86)\HP\HP BTO
```

```
Software\nonOV\jboss\nms\server\nms\conf\props\nms-users.properties
```

<drive> is the drive on which NNMi is installed

- **UNIX:**

```
/opt/OV/nonOV/jboss/nms/server/nms/conf/props/nms-roles.properties
```

```
/opt/OV/nonOV/jboss/nms/server/nms/conf/props/nms-users.properties
```

See "[Troubleshoot NNMi Access](#)" (on page 41) and "[Restore the System Role](#)" (on page 41) for more information about the `system` user account's role and password.

Audit NNMi User Activity

NNMi tracks a history of sign-in and sign-out activity for each NNMi user. This auditing information also includes a variety of information about user activity since the NNMi management server was last restarted.

NNMi stores the audit log files in the following directory:

- **Windows:**

```
<drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO  
Software\log\nnm\  
  
    signin.0.0.log  
    nnmui.0.0.log
```

<drive> is the drive on which NNMi is installed.

- **UNIX:**

```
/var/opt/OV/log/nnm/  
  
    signin.0.0.log  
    nnmui.0.0.log
```

Note: Log files are consecutively numbered. A new file is created each time you restart the NNMi management server. For example, <logFileName>.1.0.log and <logFileName>.2.0.log.

To see the most recent sign in audit report:

1. A tool is available to NNMi administrators. In the console menu bar, select **Tools** → **Sign In/Out Audit Log**.
2. The log provides a variety of information about recent account activity. For example:

```
Sign In/Sign Out AuditLog  
Jun 14, 2007 10:53:01.926 AM [ThreadID:719] com.hp.ov.ui.util. Sign-  
nInOutAuditLog logSignIn:  
  
INFO: Successful Sign In  
User: system  
Role: Administrator (ADMIN)  
Remote Host: <node IP address>  
Remote Port: 1549  
Locale: en_US  
Sign In/Out Audit Since 6/14/07 9:33 AM  
=====
```

Currently Signed In:

```
#1: system <node IP address> 6/14/07 10:53 AM (last access 6/14/07 10:53 AM)
No users currently signed out.
```

To configure the behavior of sign in information in the audit log files:

1. In a text editor, open the `logging.properties` file:
 - **Windows:**
`<drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\conf\ovjboss\logging.properties`
`<drive>` is the drive on which NNMi is installed.
 - **UNIX:**
`/var/opt/OV/shared/nnm/conf/ovjboss/logging.properties`
2. *Optional.* To disable sign in and sign out logging in the `signin.0.0.log` file, set `SignInOutAuditLog.level` to `OFF`:
`com.hp.ov.ui.util.SignInOutAuditLog.level = OFF`
3. *Optional.* To enable sign in and sign out logging in the `signin.0.0.log` file, set `SignInOutAuditLog.level` to `CONFIG`:
`com.hp.ov.ui.util.SignInOutAuditLog.level = CONFIG`
4. *Optional.* To disable sign in and sign out logging in the `nnmui.0.0.log` file, set `SignInOutAuditLog.useParentHandlers` to `false`:
`com.hp.ov.ui.util.SIgnInOutAuditLog.useParentHandlers = false`
5. Save and close the `logging.properties` file.
6. Before NNMi implements the change, you must follow the directions in the [logging.properties](#) reference page (**Help** → **Documentation Library** → **Reference Pages**, in the *File Formats* category).

Communicate to Your Team

After configuring user passwords and roles, communicate the following information to your team:

- ["Open the Console" \(on page 44\)](#)
- ["Sign In to the Console" \(on page 46\)](#)
- ["Sign Out from the Console" \(on page 46\)](#)

Open the Console

Provide each user with the following information:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

```
http://<serverName>:<portNumber>/nnm/
```

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

When your NNMi management server has more than one fully-qualified domain name, NNMi chooses one during the installation process. There are two ways to find out which domain name NNMi is using in your network environment:

- Click **Help** → **About HP Network Node Manager i-series**, find the Management Server section, Fully Qualified Domain Name (FQDN) attribute value.
- Use the `nnmofficialfqdn.ovpl` command. See the [nnmofficialfqdn.ovpl](#) Reference Page.

To determine the current port number configuration, look at the first line (`boss.http.port`) in the [nnm.ports.properties](#) file (see table for the location of this file).

Determine the NNMi Console Port Number

Operating System	Identify Current Port Number
Windows	<code><drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\conf\nnm.ports.properties</code>
UNIX	<code>/var/opt/OV/shared/nnm/conf/nnm.ports.properties</code>

`<drive>` is the drive on which NNMi is installed.

Communicate the following browser requirements for your team to use the NNMi console:

- Use Microsoft Internet Explorer 7.0 or later or Mozilla Firefox 2.0 or later.
- Pop-ups, cookies, and JavaScript must be enabled.
- Each user's screen resolution must be 1024x768 pixels or higher.
- When using Microsoft Internet Explorer as your browser, you can access multiple browser sessions of NNMi. Use a different user name for each browser session.
- When using Mozilla Firefox as your browser, multiple browser sessions all point to the same window.

Note: Users can bookmark the URL for the NNMi console. Use the URL for the NNMi console rather than the NNMi Welcome page. See [About the NNMi Console](#) for more information about the NNMi console.

To open the console:


1. Type the following URL (Uniform Resource Locator) into your browser navigation bar:
`http://<serverName>:<portNumber>/nnm/`
2. Sign in with the following name and password:
`<name you configured>`
`<password you configured>`

Note: The sign in prompt cannot be disabled, but you can include name and password in the URL. See ["Launch the Console \(showMain\)" \(on page 324\)](#).

3. Click the **Sign In** button. (See ["Sign In to the Console" \(on page 46\)](#) if you need more information.)
4. The console opens in a new window.
5. *Optional.* Close the NNMi Welcome page.

Note: If you do not close the NNMi Welcome page or sign out, you can relaunch the console from the NNMi Welcome Page without signing in again.

To refresh the console window:

Click the  Refresh icon in the tool bar of any NNMi window.

Sign In to the Console

After entering the URL for the console, users are prompted for a user name and password.

To sign in to the Console:

1. At the **User Name** prompt, enter the assigned user name.
2. At the **Password** prompt, enter the currently assigned password.
3. Click the **Sign In** button.

Each user name is assigned to an NNMi role. The role determines what users can do with the NNMi console. ["Determine which NNMi Role to Assign" \(on page 33\)](#) for more information.

The user name and the associated role appear in the upper right corner of the console as shown in the example below:



Sign Out from the Console

To sign out from the console:

1. Select **File** → **Sign Out**.
2. Click **OK**.

Note the following:

- Sign in is not preserved across user sessions. After signing out, each user must sign in again.
- You must sign out of each browser session that is running NNMi. For example, if you have signed in twice with two different browsers, signing out in one browser does not cause you to lose access in the other browser.
- NNMi automatically signs out any user after four hours of inactivity.

Configuring Communication Protocol


NNMi uses the following protocols to discover your network and monitor the health of your network environment:

- Simple Network Management Protocol (SNMP) read-only queries, also known as "Get" commands
 - SNMPv1 and SNMPv2c require the use of a community string to authenticate messages that are sent between NNMi and SNMP agents. NNMi cannot discover information about the SNMPv1 and SNMPv2c devices in your network environment until you provide the appropriate community strings. During discovery and monitoring, NNMi uses the community strings you provide in the Communication Configuration workspace. When a device is first discovered, NNMi tries all appropriate community strings and makes a record of the first community string that works. To keep network traffic to a minimum, from then on NNMi uses the recorded community string when communicating with that device using SNMP. If at some point the device no longer responds to the recorded community string, NNMi tries all appropriate community strings and makes a record of the first community string that now works.
 - SNMPv3 requires the use of user-based security model (USM) user names instead of community strings to authenticate messages that are sent between NNMi and SNMP agents. NNMi cannot discover information about the SNMPv3 devices in your network environment until you provide the appropriate user name and authentication. During discovery and monitoring, NNMi uses the user name and authentication you provide in the Communication Configuration workspace. When a device is first discovered, NNMi tries all appropriate USM user names and makes a record of the first USM user name that works. To keep network traffic to a minimum, from then on NNMi uses the recorded USM user name when communicating with that device using SNMP. If at some point the device no longer responds to the recorded USM user name, NNMi tries all appropriate USM user names and makes a record of the USM user name that now works.
- Internet Control Message Protocol (ICMP) ping commands

Note: If NNMi discovers a device for which no SNMP authentication was provided in the Communication Configuration workspace, that device is treated as a non-SNMP device.

You control the amount of traffic NNMi generates on your network. You can modify the settings to meet your needs.

To configure the way NNMi uses ICMP and SNMP protocols, do the following:

1. Navigate to the **Communication Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Communication Configuration**.
2. Make your configuration choices. Click here for a list of choices .
3. Click  **Save and Close**. Your changes are available for the next Discovery or Monitoring cycle.

Note: You control how often the Discovery Service runs by designating the **Rediscovery Interval** setting. See ["Adjust the Discovery Interval" \(on page 98\)](#) for more information.


Configure Default SNMP and ICMP Protocol Settings

NNMi generates network traffic using ICMP and SNMP protocols to discover and monitor your network environment. Default settings for the use of these protocols are provided, for example timeout and retry behavior settings.

To configure the default communication protocol settings for your environment:

1. Navigate to the **Communication Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Communication Configuration**.
2. Locate the **Default Settings** groups.
3. Make your configuration choices (see [SNMP table](#), [ICMP table](#)).

For an explanation of how NNMi implements timeout and retry configurations, see ["Timeout / Retry Behavior Example for SNMP" \(on page 50\)](#).

4. Click  **Save and Close**. Your changes are available for the next Discovery or Monitoring cycle.

Default SNMP Settings Attributes

Attribute	Description
Enable SNMP Address Discovery	<p>If <input checked="" type="checkbox"/> enabled, NNMi automatically identifies which management address (SNMP agent) to use for each device. If the initially configured address becomes unreachable, NNMi automatically locates another SNMP agent, if possible, and changes the management address attribute value.</p> <p>If <input type="checkbox"/> disabled, when the current management address (SNMP agent) becomes unreachable, NNMi reclassifies the node as a non-SNMP node until the previously configured management address is available again.</p>
SNMP Timeout	<p>(Seconds:Milliseconds) Maximum 1 millisecond less than a minute: 59 seconds 999 milliseconds.</p> <p>Time that NNMi waits for a response to an SNMP query before reissuing the request. Both the Discovery Process and the State Poller Service use this setting. For an explanation of how NNMi implements timeout and retry configurations, see "Timeout / Retry Behavior Example for SNMP" (on page 50).</p>
SNMP Retries Count	<p>Maximum number of retries that NNMi issues for an SNMP query before determining the query result to be "unresponsive". Zero means no retries. Both the Discovery Process and the State Poller Service use this setting.</p>
SNMP Port	<p>Default is 161. Specifies the management station's port that NNMi uses when generating SNMP traffic. Both the Discovery Process and the State Poller Service use this setting.</p>
SNMP Proxy Address	<p>Specify the IP address of your SNMP Proxy Server.</p> <p>You can set up SNMP Proxy Servers to allow communication with nodes that otherwise might be unreachable (for example, when a node to be managed is behind a firewall). The SNMP Proxy Server allows NNMi to manage these nodes in the same way as nodes that provide SNMP access directly.</p> <p>Note: To enable a proxy, you must also provide the port number of the SNMP Proxy Server.</p>
SNMP Proxy Port	<p>Port number on the SNMP Proxy Server. See SNMP Proxy Address (previous attribute).</p> <p>Note: To enable a proxy, you must also provide the address of the SNMP Proxy Server.</p>

Attribute	Description
SNMP Minimum Security Level	<p>For SNMPv1 or SNMPv2c, configure NNMi to use Community Strings in your network environment:</p> <ul style="list-style-type: none"> Community Only (SNMPv1) NNMi tries only SNMPv1 settings. Community Only (SNMPv1 or v2c) NNMi tries only SNMPv1/SNMPv2c settings. Community NNMi tries SNMPv1/SNMPv2c settings first, then tries SNMPv3 settings if any are configured. <p>For SNMPv3, configure NNMi to use the User-based Security Module (USM) level of security required in your network environment (if your environment also uses SNMPv1/SNMPv2c, select Community):</p> <ul style="list-style-type: none"> No Authentication, No Privacy Authentication, No Privacy Authentication, Privacy <p>See "Timeout / Retry Behavior Example for SNMP" (on page 50) for an explanation of NNMi behavior with each of these choices.</p>

Note: NNMi needs to know which SNMPv1 or SNMPv2c community strings are used in your environment (see ["Configure Default Community Strings \(SNMPv1 or SNMPv2c\)"](#) (on page 51)) and which SNMPv3 USM settings are used in your environment (see ["Configure Default SNMPv3 Settings"](#) (on page 54)).

Default ICMP Settings

Attribute	Description
ICMP Timeout	<p>(Seconds:Milliseconds) Maximum 1 millisecond less than a minute: 59 seconds 999 milliseconds.</p> <p>Time that NNMi waits for a response to an ICMP query before reissuing the request. For an explanation of how NNMi implements timeout and retry configurations, see "Timeout / Retry Behavior Example for ICMP" (on page 51).</p>
ICMP Retries Count	<p>Maximum number of retries that NNMi issues for an ICMP query before logging an error. Zero means no retries.</p>

Related Topics:

["Configure Default Community Strings \(SNMPv1 or SNMPv2c\)"](#) (on page 51)

["Configure Regions \(Communication Settings\)"](#) (on page 56)

["Configure Specific Nodes \(Communication Settings\)"](#) (on page 66).

Timeout / Retry Behavior Example for SNMP

When NNMi attempts to contact a device, your configuration settings for Timeout and Retry influence NNMi behavior.

NNMi attempts to obtain information about a hostname/IP-address using SNMP, then waits the configured timeout interval for a response. If not successful, NNMi increments the timeout interval before trying again. This process repeats until one of the following is true:

- The device responds to SNMP.
- The maximum configured number of SNMP Retries fails. For example, if your timeout is 2 seconds and your retry is 4:
 - NNMi attempts to communicate with a device and waits 2 seconds for a response.
 - If unsuccessful, NNMi tries again and waits 4 seconds for a response.
 - If unsuccessful, NNMi tries again and waits 6 seconds for a response.
 - If unsuccessful, NNMi tries again and waits 8 seconds for a response.

If no response, NNMi repeats this process using the next configured SNMP level.

- NNMi exhausts all possibilities. NNMi considers the hostname/IP-address to be a *non-SNMP* device until the next Discovery or Monitoring cycle.

Tip: It is best to use the same timeout/retry numbers for both ICMP and SNMP.

Your choice of SNMP Minimum Security Setting determines the range of possibilities:

- If your SNMP Minimum Security Setting is **Community Only (SNMPv1)**, NNMi uses only SNMPv1 to locate SNMP agents.
- If your SNMP Minimum Security Setting is **Community Only (SNMPv1 or v2c)**, NNMi cycles through the following until successful:
 - SNMPv2c
 - SNMPv1
- If your SNMP Minimum Security Setting is **Community**, NNMi cycles through the following until successful:
 - SNMPv2c
 - SNMPv1
 - SNMPv3 *No Authentication, No Privacy* settings (if any matching configurations, otherwise skip).
 - SNMPv3 *Authentication, No Privacy* settings (if any matching configurations, otherwise skip).
 - SNMPv3 *Authentication, Privacy* settings (if any matching configurations).
- If your SNMP Minimum Security Setting is **No Authentication, No Privacy**, NNMi cycles through the following until successful:
 - SNMPv3 *No Authentication, No Privacy* settings (if any matching configurations at this, otherwise skip)

SNMPv3 *Authentication, No Privacy* settings (if any matching configurations, otherwise skip).

SNMPv3 *Authentication, Privacy* settings (if any matching configurations).

- If your SNMP Minimum Security Setting is **Authentication, No Privacy**, NNMi cycles through the following until successful:

SNMPv3 *Authentication, No Privacy* settings (if any matching configurations, otherwise skip).

SNMPv3 *Authentication, Privacy* settings (if any matching configurations).

- If your SNMP Minimum Security Setting is **Authentication, Privacy**, NNMi cycles through the following until successful:

SNMPv3 *Authentication, Privacy* settings (if any matching configurations).

Timeout / Retry Behavior Example for ICMP

When NNMi attempts to contact a device, your configuration settings for Timeout and Retry influence NNMi behavior.

NNMi attempts to contact the device using ICMP, then waits the configured timeout interval for a response. If not successful, NNMi increments the timeout interval before trying again. This process repeats until one of the following is true:

- The device responds to ICMP.
- The maximum configured number of ICMP Retries fails. NNMi considers the device unreachable through ICMP until the next Discovery or Monitoring cycle. For example, if your timeout is 2 seconds and your retry is 4:
 - NNMi attempts to communicate with a device and waits 2 seconds for a response.
 - If unsuccessful, NNMi tries again and waits 4 seconds for a response.
 - If unsuccessful, NNMi tries again and waits 6 seconds for a response.
 - If unsuccessful, NNMi tries again and waits 8 seconds for a response.

Tip: It is best to use the same timeout/retry numbers for both ICMP and SNMP.

Configure Default Community Strings (SNMPv1 or SNMPv2c)

Use the Default Community Strings tab to provide default SNMPv1 and SNMPv2c passwords. For each address, NNMi checks the communication configuration settings in this order: [communication protocols for Specific Nodes](#), [communication protocols for Network Regions](#), and if no match is found, NNMi tries these default community strings. If NNMi discovers a device for which no SNMP settings are provided, that device is treated as a Non-SNMP device.

During initial discovery, NNMi tries many community strings until a match is found. After a match is identified for a node, the information is recorded to prevent future authentication errors.






Note: If you provide a community string for a [specific device](#), NNMi honors your choice and does not try any Region or Default community strings for that device.

NNMi uses SNMP read-only queries (Get commands) for ongoing discovery and monitoring of your network environment. SNMP community strings are the validation passwords used to authenticate messages sent from NNMi to an SNMP agent. NNMi uses SNMP to gather useful information about the devices in your network environment. After receiving an SNMP request, an SNMP agent compares the community string in the request to the community strings that are configured for that SNMP agent. The SNMP agent responds to the request only when the request is accompanied by a valid community string.

During NNMi installation, any community strings that were provided are automatically stored in the table on the Default Community Strings tab.

Provide any number of additional community strings that are used broadly in your environment (for example, by default). The order in which your community string settings appear in this table does not matter. NNMi checks all Default community strings in parallel.

To configure default SNMPv1 or SNMPv2c community strings for your environment:

1. Navigate to the **Communication Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Communication Configuration**.
2. Locate the **Default Community Strings** tab.
3. Do one of the following:
 - To establish a community string setting, click the  New icon, and continue.
 - To edit a community string setting, select a row, click the  Open icon, and continue.
 - To delete a community string setting, select a row and click the  Delete icon.
4. In the [Default Community String form](#), provide the required information.
5. Click  **Save and Close** to return to the Communication Configuration form.
6. Click  **Save and Close**. NNMi updates the affected SNMP Agent objects in the NNMi database. Your changes are available for the next Discovery or Monitoring cycle.






Default Community String Form

Provide any number of additional SNMPv1 or SNMPv2c community strings that are used broadly in your environment (for example, by default). The order in which your community string settings appear in this table does not matter. NNMi checks all Default community strings in parallel.

Note:For each address, NNMi checks the communication configuration settings in this order: [communication protocols for Specific Devices](#), [communication protocols for Network Regions](#), and if no match is found, NNMi tries the default community strings. If NNMi discovers a device for which no community string is provided, that device is treated as a Non-SNMP device.

To provide a default community string for your environment:

1. Navigate to the **Default Community String** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Communication Configuration**.
 - c. Navigate to the **Default Community Strings** tab.
 - d. Do one of the following:

- To establish a community string setting, click the  New icon, and continue.
 - To edit a community string setting, select a row, click the  Open icon, and continue.
2. Provide the community string (see [table](#)).
 3. Click either:
 -  **Save and Close** to return to the Communication Configuration form.
 -  Save and New to add another community string.
 4. Click  **Save and Close**. NNMi updates the affected SNMP Agent objects in the NNMi database. Your changes are available for the next Discovery or Monitoring cycle.

Default Community String

Attribute	Description
Read Community String	<p>The SNMP "get" (read-only) community string that is used in your network environment. Case-sensitive.</p> <p>Many proxy vendors use the community string for specifying remote target information. NNMi supports substitution parameters within community strings for SNMPv1 or SNMPv2 proxy environments. Click here for more information.</p> <p>Copy and paste these codes at the end of your Community String to provide the values required by your proxy environment. NNMi substitutes the actual attribute values from the NNMi database at runtime:</p> <p><code>\${contextName}</code> = Used for specifying VLAN context for switches (VLAN associated with the remote target node)</p> <p><code>\${managementAddress}</code> = Node form, Management Address attribute value (the remote target node)</p> <p><code>\${snmpPort}</code> = SNMP Agent form, UDP Port attribute value (SNMP agent associated with the remote target node)</p>




Configure the Default Device Credentials (NNM iSPI NET)

NNMi uses the Default Credentials setting to access devices when running Diagnostics either automatically or when the **Actions** → **Run Diagnostics** option is used. (See "[Configure Diagnostics for an Incident \(NNM iSPI NET\)](#)" (on page 291) and [Node Form: Diagnostics Tab](#) for more information.)

NNMi uses Shell (SSH or telnet) as the method for accessing devices with the credentials specified. NNMi uses SSH as the preferred communication method. If the SSH attempt fails, NNMi uses telnet.



To provide the default credentials setting:

1. Navigate to the **Default Device Credentials** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Communication Configuration**.
 - c. Navigate to the **Default Device Credentials** tab.

- d. Do one of the following:
 - To establish a credential setting, click the  New icon, and continue.
 - To edit a credential setting, select a row, click the  Open icon, and continue.
 - To delete a credential setting, select a row and click the  Delete icon
2. Provide *one* setting for the default attribute values (see [table](#)).

Caution: Populate only one row in this table.

Note: NNMi tries to use the [Specific Node Device Credentials](#). If none match, NNMi tries the [Region Device Credentials](#). If none match, NNMi tries the default credential settings provided here.

3. Click  **Save and Close** to return to the Communication Configuration form.
4. Click  **Save and Close**. Your changes are available for the next Discovery or Monitoring cycle.

Default Device Credential Attributes

Attribute	Description
User Name	Type the user name that you want NNMi to use for logging into devices by default (when no Region or Specific Node settings work).
Password	Type the password that you want NNMi to use for logging into devices by default (when no Region or Specific Node settings work). Note: NNMi encrypts the password and displays asterisks for this attribute. If you want to change the password, first clear the asterisks displayed in the Password attribute and enter the new Password value.

Configure Default SNMPv3 Settings

Use the Default SNMPv3 Settings tab to provide default SNMPv3 user-based security model (USM) settings. For each address, NNMi checks the communication configuration settings in this order: [communication protocols for Specific Nodes](#), [communication protocols for Network Regions](#), and if no match is found, NNMi tries these default user-based security model (USM) settings. If NNMi discovers a device for which no SNMP settings are provided, that device is treated as a Non-SNMP device.

During initial discovery, NNMi tries many SNMP configuration settings until a match is found. After a match is identified for a Node, the information is recorded to prevent future authentication errors.

Note: If you provide SNMPv3 user-based security model (USM) settings for a [specific device](#), NNMi honors your choice and does not try any Region or Default community strings for that device.

NNMi uses SNMP queries for ongoing discovery and monitoring of your network environment. SNMPv3 user-based security model (USM) settings are used to authenticate messages sent from NNMi to an SNMP agent. NNMi uses SNMP to gather useful information about the devices in your network environment. After receiving an SNMP request, an SNMP agent compares the SNMPv3 user-based security model (USM) settings in the request to the SNMPv3 user-based security model (USM) settings that are configured for that SNMP agent. The SNMP agent responds to the request only when the request is accompanied by valid SNMPv3 user-based security model (USM) settings.

Provide any number of additional SNMPv3 user-based security model (USM) settings that are used broadly in your environment (for example, by default). The order in which your SNMPv3 user-based secu-








urity model (USM) settings appear in this table does not matter. NNMi checks all Default SNMPv3 Settings at a particular security level in parallel.

NNMi uses Default SNMPv3 user-based security model (USM) settings to access devices.

To view the current list of default SNMPv3 USM settings:

1. Navigate to the **Default SNMPv3 Settings** tab.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Communication Configuration**.
 - c. Navigate to the **Default SNMPv3 Settings** tab.
2. The displayed table lists the Unique Name of each default SNMPv3 USM setting.

Note: NNMi tries to use the [Specific Node SNMPv3 Settings](#). If none match, NNMi tries the [Region SNMPv3 Settings](#). If none match, NNMi tries the default SMNPv3 settings provided [here](#).

3. You can do the following:
 - To establish a new setting, click the  New icon. See "[Default SNMPv3 Settings form](#)" (on page 55).
Click  **Save and Close** to return to the Default SNMPv3 Settings form.
 - To edit an existing setting, select a row, click the  Open icon. See "[Default SNMPv3 Settings form](#)" (on page 55).
Click  **Save and Close** to return to the Default SNMPv3 Settings form.
 - To delete an existing setting from the Default list, select a row and click the  Delete icon.
Note: The record remains in the database for possible use elsewhere and is simply removed from the Default list.
4. Click  **Save and Close** to return to the Communication Configuration form.
5. Click  **Save and Close**. NNMi updates the affected SNMP Agent objects in the NNMi database. Your changes are available for the next Discovery or Monitoring cycle.











Default SNMPv3 Settings form

NNMi can use SNMPv3 user-based security model (USM) settings to access devices.

NNMi tries to use the current SNMPv3 Settings attribute value from [Specific Node Settings](#). If none match, NNMi tries the [Region SNMPv3 Settings](#). If none match, NNMi tries the default SMNPv3 settings provided [here](#).

To configure a Default SNMPv3 Setting:

1. Navigate to the **Default SNMPv3 Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Communication Configuration**.
 - c. Navigate to the **Default SNMPv3 Settings** tab.
 - d. Do one of the following:

- To create default SNMPv3 Setting definition, click the  New icon.
 - To edit a default SNMPv3 Setting, select a row, click the  Open icon.
2. Click the SNMPv3 Settings  Lookup icon and select one of the options from the drop-down menu:
 -  Quick View to display summary information for the currently configured (selected) SNMPv3 Setting name.
 -  Quick Find to view and select from the list of all existing SNMPv3 Settings (for more information see ["Use the Quick Find Window" \(on page 19\)](#)).
 -  Open to display the details of the currently configured (selected) SNMPv3 Setting (see ["SNMPv3 Settings Form"](#) for more information).
 -  New to create a new SNMPv3 Setting (see ["SNMPv3 Settings Form"](#) for more information).
 3. Click  **Save and Close** to return to the Default SNMPv3 Settings form.
 4. Click  **Save and Close** to return to the Communication Configuration form.
 5. Click  **Save and Close**. NNMi updates the affected SNMP Agent objects in the NNMi database. Your changes are available for the next Discovery or Monitoring cycle.

Configure Regions (Communication Settings)

Configuring communication protocols for regions is optional.

NNMi includes a default region that covers all industry-standard private address spaces.

Note: If you provide an SNMPv1 or SNMPv2c community string or an SNMPv3 USM Setting for a specific device, NNMi honors your choice and does not try any Region or Default settings for that device.

Use the Regions tab to fine tune communication protocol usage and settings for particular regions of your network (for example, buildings, floors within those buildings, or workgroups within a particular floor). When you leave a field blank in a region definition, NNMi uses the next applicable configuration setting in the following order:






- The value for each field as defined in the first Region definition that matches, Regions are checked according to the Ordering number. The match with the lowest Ordering number applies.
- If no Region definition provides a value for an attribute, the default value is used.

Note: NNMi enables you to set up one or more SNMP Proxy Servers when an SNMP node is otherwise unreachable (for example, when a node you want to manage is behind a firewall). To enable NNMi to use the SNMP Proxy Server, when you configure communication protocols for network regions, you must include the IP address and port number on the SNMP Proxy Server. See ["Communication Region Form" \(on page 57\)](#) for more information.

If your communication protocol usage is too complex for Region definitions, see ["Configure Specific Nodes \(Communication Settings\)" \(on page 66\)](#).

To configure communication protocols for a particular region of your network:

1. Navigate to the **Communication Region** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Communication Configuration**.

- c. Navigate to the **Regions** tab.
- d. Do one of the following:
 - To establish a region definition, click the  New icon, and continue.
 - To edit a region definition, select a row, click the  Open icon, and continue.
 - To delete a region definition, select a row and click the  Delete icon.
2. Provide the required information. Define the regions with wildcard address, wildcard device names, or literal addresses and names. See ["Communication Region Form" \(on page 57\)](#).
3. Click  **Save and Close** to return to the Communication Configuration form.
4. Click  **Save and Close**. NNMi updates the affected SNMP Agent objects in the NNMi database. Your changes are available for the next Discovery or Monitoring cycle.

Related Topics:





["Configure Default SNMP and ICMP Protocol Settings" \(on page 47\)](#)

["Configure Default Community Strings \(SNMPv1 or SNMPv2c\)" \(on page 51\)](#)

["Configure Specific Nodes \(Communication Settings\)" \(on page 66\)](#)

Communication Region Form

To configure communication regions:

1. Navigate to the **Communication Region** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Communication Configuration**.
 - c. Navigate to the **Regions** tab.
 - d. Do one of the following:
 - To establish a region definition, click the  New icon, and continue.
 - To edit a region definition, select a row, click the  Open icon, and continue.
2. Provide the basic communication region definition (see the [Regional Basic Settings](#) table, [Regional SNMP Settings](#) table, and [Regional ICMP Settings](#) table).
3. Make your configuration choices. Click here for a list of choices .
4. Click  **Save and Close** to return to the Communication Configuration form.
5. Click  **Save and Close**. Your changes are available for the next Discovery or Monitoring cycle.

Regional Basic Settings

Attribute	Description
Name	A name for this region.
Ordering	A numeric value. NNMi checks for configuration settings in the order you define (lowest number first). NNMi uses the first match found for each address.

Attribute	Description
	<p>No duplicate Ordering numbers are allowed. Each Communication Region ordering number must be unique.</p> <p>Tip: It is recommended that ordering numbers are incremented by 10s or 100s to provide flexibility when adding new regions over time.</p>
Description	<p><i>Optional.</i> Provide any description that would be useful for communication purposes within your team.</p> <p>Type a maximum of 255 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p>

Regional SNMP Settings

Attribute	Description
Enable SNMP Communication	<p>If <input checked="" type="checkbox"/> enabled, the Discovery Process and State Poller Service generate network traffic with SNMP protocol to discover and monitor your network devices in this region.</p> <p>If <input type="checkbox"/> disabled, NNMi does not generate any SNMP traffic on your network in this region.</p> <p>Caution: At least one IP Address in each node must have SNMP enabled, otherwise no SNMP data is collected from that Node. With no SNMP data, Spiral Discovery interprets each IP Address as a separate node, Causal Engine calculates Status based only on IP address State, previously discovered Interfaces show a State attribute value of "Not Polled" and a Status attribute value of "No Status" with the Interface map-symbol color set to beige, and no new Interfaces are discovered.</p> <p>Note: See "Monitoring Network Health" (on page 151) for information about enabling/disabling SNMP communication specifically for the State Poller Service.</p>
Enable SNMP Address Discovery	<p>If <input checked="" type="checkbox"/> enabled, NNMi automatically identifies which management address (SNMP agent) to use for each device. If the initially configured address becomes unreachable, NNMi automatically locates another SNMP agent, if possible, and changes the management address attribute value.</p> <p>If <input type="checkbox"/> disabled, when the current management address (SNMP agent) becomes unreachable, NNMi reclassifies the node as a non-SNMP node until the previously configured management address is available again.</p>
SNMP Timeout	<p>(Seconds:Milliseconds) Maximum 1 millisecond less than a minute: 59 seconds 999 milliseconds.</p> <p>Time that NNMi waits for a response to an SNMP query before reissuing the request. Both the Discovery Process and the State Poller Service use this setting in this region. For an explanation of how NNMi implements timeout and retry configurations, see "Timeout / Retry Behavior Example for SNMP" (on page 50).</p>
SNMP Retries Count	<p>Maximum number of retries that NNMi issues for an SNMP query before determining the query result to be "unresponsive". Zero means no retries. Both the Discovery Process and the State Poller Service use this setting in this region.</p>
SNMP Port	<p>Default is 161. Specifies the management station's port that NNMi uses when generating SNMP traffic. Both the Discovery Process and the State Poller Service use this setting in this region.</p>

Attribute	Description
SNMP Proxy Address	<p>Specify the IP address of your SNMP Proxy Server.</p> <p>You can set up one or more SNMP Proxy Servers to allow communication with nodes that otherwise might be unreachable (for example, when a node to be managed is behind a firewall). The SNMP Proxy Server allows NNMi to manage these nodes in the same way as nodes that provide SNMP access directly.</p>
SNMP Proxy Port	<p>Port number on the SNMP Proxy Server. See SNMP Proxy Address (previous attribute).</p>
SNMP Minimum Security Level	<p>For SNMPv1 or SNMPv2c, configure NNMi to use Community Strings in your network environment:</p> <ul style="list-style-type: none"> • Community Only (SNMPv1) NNMi tries only SNMPv1 settings. • Community Only (SNMPv1 or v2c) NNMi tries only SNMPv1/SNMPv2c settings. • Community NNMi tries SNMPv1/SNMPv2c settings first, then tries SNMPv3 settings if any are configured. <p>For SNMPv3, configure NNMi to use the User-based Security Module (USM) level of security required in your network environment (if your environment also uses SNMPv1/SNMPv2c, select Community):</p> <ul style="list-style-type: none"> • No Authentication, No Privacy • Authentication, No Privacy • Authentication, Privacy <p>See "Timeout / Retry Behavior Example for SNMP" (on page 50) for an explanation of NNMi behavior with each of these choices.</p>






Regional ICMP Settings

Attribute	Description
Enable ICMP Communication	<p>If <input checked="" type="checkbox"/> enabled, NNMi generates network traffic with ICMP protocol in this region.</p> <p>If <input type="checkbox"/> disabled, NNMi does not generate any ICMP traffic on your network in this region:</p> <ul style="list-style-type: none"> • Addresses in this Region (both previously discovered and newly discovered) have a State attribute value of "Not Polled" and a Status attribute value of "No Status" with the IP Address map-symbol color set to beige. • Nodes with all IP addresses and interfaces showing a Status attribute value of "No Status" have a map-symbol background shape color set to beige. However, it is possible for a node to have IP addresses in multiple regions with multiple Status values. <p>Note: See "Monitoring Network Health" (on page 151) for information about enabling/disabling ICMP communication specifically for the State Poller Service.</p>
ICMP Timeout	<p>(Seconds:Milliseconds) Maximum 1 millisecond less than a minute: 59 seconds 999 milliseconds.</p>

Attribute	Description
	Time that NNMi waits for a response to an ICMP query before reissuing the request in this region. For an explanation of how NNMi implements timeout and retry configurations, see " Timeout / Retry Behavior Example for ICMP " (on page 51).
ICMP Retries Count	Maximum number of retries that NNMi issues for an ICMP query in this region before logging an error. Zero means no retries.




Configure Address Ranges for Regions

To configure an address range for this region:

1. Navigate to the **Region Included Address Range** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Communication Configuration**.
 - c. Navigate to the **Regions** tab.
 - d. Do one of the following:
 - To establish a region definition, click the  New icon, and continue.
 - To edit a region definition, select a row, click the  Open icon, and continue.
 - e. In the **Communication Region** form, navigate to the **Included Address Regions** tab.
 - f. Do one of the following:
 - To establish an address range setting, click the  New icon, and continue.
 - To edit an address range setting, select a row, click the  Open icon, and continue.
 - To delete an address range setting, select a row and click the  Delete icon.
2. Provide address range definition (see [table](#)).

If you provide multiple IP address ranges for a region, each device must pass at least one to meet the criteria.

Tip: If you provide both IP address ranges and hostname wildcards, each device must pass at least one in either category (not both) to meet the criteria.

3. Click  **Save and Close** to return to the Communication Region form.
4. Click  **Save and Close** to return to the Communication Configuration form.
5. Click  **Save and Close**. Your changes are available for the next Discovery or Monitoring cycle.

Address Range Definition Attribute






Attribute	Description
IP Range	Used to specify the range of IP addresses for this Communication Region. An IPv4 Address range is a modified dotted-notation where each octet is one of the following: <ul style="list-style-type: none"> • A specific octet value between 0 and 255

Attribute	Description
	<ul style="list-style-type: none">• A low-high range specification for the octet value (for example, "112-119")• An asterisk (*) wildcard character which is equivalent to the range expression "0-255"
	Note: The following two IPv4 addresses are considered invalid: 0.0.0.0 and 127.0.0.0
	Examples of valid IPv4 address wildcards include: 10.1.1.* 10.*.*.* 10.1.1.1-99 10.10.50-55.* 10.22.*.4 10.1-9.1-9.1-9




Configure Hostname Filters for Regions

Define the [Communication Region](#) with hostname patterns.

To establish a Hostname Filter setting:

1. Navigate to the **Region Hostname Filter** form.
 - From the workspace navigation panel, select the **Configuration** workspace.
 - Select the **Communication Configuration**.
 - Navigate to the **Regions** tab.
 - Do one of the following:
 - To create a region definition, click the  New icon.
 - To edit a region definition, select a row, click the  Open icon.
 - In the **Communication Region** form, access the **Hostname Filters** tab.
 - Do one of the following:
 - To create a hostname wildcard definition, click the  New icon.
 - To edit a hostname wildcard definition, select a row, click the  Open icon.
 - To delete a hostname wildcard setting, select a row and click the  Delete icon.
2. Type an appropriate hostname filter (see [table](#)).

If you provide multiple hostname wildcards for a region, each device must pass at least one to meet the criteria.

Tip: If you provide both hostname wildcards and IP address ranges, each device must pass at least one in either category (not both) to meet the criteria.
3. Click  **Save and Close** to return to the Communication Region form.
4. Click  **Save and Close** to return to the Communication Configuration form.
5. Click  **Save and Close**. Your changes are available for the next Discovery or Monitoring cycle. See "[Discovering Your Network](#)" (on page 76) and [Verify Device Configuration Details](#).

Node Hostname Filter Definition

Attribute	Description
Hostname Filter	<p>Enter a wildcard expression using ? (one character) and * (multiple characters).</p> <p>Wildcards are not case-sensitive. So a wildcard of ABC* would match devices with hostnames beginning with ABC*, abc*, and Abc*</p> <p>Caution: The Hostname attribute value on the Node form of the discovered node must match what is entered here (see the Hostname attribute the Node form help topic).</p> <p>If a device has multiple hostnames or no hostname, NNMi follows a set of rules to determine the hostname. Click here for details.</p> <ol style="list-style-type: none">1. If a hostname is available, it must resolve to a valid IP address. NNMi stores the fully-qualifiedhostname in the database as all lowercase characters.2. If more than one address is associated with a node, the loopback address¹ is used with the following exceptions:<ul style="list-style-type: none">■ NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).■ NNMi ignores any address that is virtual (HSRP/VRRP) or an Anycast Rendezvous Point IP Address².3. If a node has multiple loopback addresses, NNMi uses the loopback address with the lowest number that resolves to a hostname (for example, 10.16.42.197 is a lower number than 10.16.197.42).4. If no loopback address resolves to a hostname and the device supports SNMP, NNMi uses the current value from the Management Address attribute on the Node form.5. If the device does not support SNMP, the IP address or DNS name found during the current rediscovery cycle is used as the hostname. <p>This sequence is repeated during each rediscovery cycle. The hostname could change from cycle to cycle (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).</p>

Configure Community Strings for Regions









If more than one SNMPv1 or SNMPv2c "get" community string is used within this region, repeat this step any number of times. Order does not matter because all community strings defined for this Region are checked in parallel.

During initial discovery, NNMi tries many community strings until a match is found. After a match is identified for a Node, the information is recorded to prevent future authentication errors.

To provide a community string for this region:

¹The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

²Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

1. Navigate to the **Region Community String** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Communication Configuration**.
 - c. Navigate to the **Regions** tab.
 - d. Do one of the following:
 - To establish a region definition, click the  New icon, and continue.
 - To edit a region definition, select a row, click the  Open icon, and continue.
 - e. In the **Communication Region** form, navigate to the **Community Strings** tab.
 - f. Do one of the following:
 - To establish a community string setting, click the  New icon, and continue.
 - To edit a community string setting, select a row, click the  Open icon, and continue.
 - To delete a community string setting, select a row and click the  Delete icon
 2. Provide a community string for this region (see [table](#)).
- Note:** If you do not provide any community strings, NNMi uses the [Default Community Strings](#).
3. Click  **Save and Close** to return to the Communication Region form.
 4. Click  **Save and Close** to return to the Communication Configuration form.
 5. Click  **Save and Close**. NNMi updates the affected SNMP Agent objects in the NNMi database. Your changes are available for the next Discovery or Monitoring cycle.

SNMPv1 or SNMPv2c Community String for this Region






Attribute	Description
Read Community String	<p>The SNMPv1 or SNMPv2c "get" (read-only) community string that is used for this region. Case-sensitive.</p> <p>Tip: If no values appear in this table, the default settings are used (see "Configure Default Community Strings (SNMPv1 or SNMPv2c)" (on page 51)).</p> <p>Many proxy vendors use the community string for specifying remote target information. NNMi supports substitution parameters within community strings for SNMPv1 or SNMPv2 proxy environments. Click here for more information.</p> <p>Copy and paste these codes at the end of your Community String to provide the values required by your proxy environment. NNMi substitutes the actual attribute values from the NNMi database at runtime:</p> <p><code>\${contextName}</code> = Used for specifying VLAN context for switches (VLAN associated with the remote target node)</p> <p><code>\${managementAddress}</code> = Node form, Management Address attribute value (the remote target node)</p> <p><code>\${snmpPort}</code> = SNMP Agent form, UDP Port attribute value (SNMP agent associated with the remote target node)</p>

Configure Credential Settings for Regions (NNM iSPI NET)




NNMi uses Default Credential Settings to access devices when running Diagnostics either automatically or when the **Actions** → **Run Diagnostics** option is used. (See "[Configure Diagnostics for an Incident \(NNM iSPI NET\)](#)" (on page 291) and [Node Form: Diagnostics Tab](#) for more information.)

NNMi uses Shell (SSH or telnet) as the method for accessing devices with the credentials specified. NNMi uses SSH as the preferred communication method. If the SSH attempt fails, NNMi uses telnet.

To provide credential settings for this region:

1. Navigate to the **Region Device Credentials** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Communication Configuration**.
 - c. Navigate to the **Regions** tab.
 - d. Do one of the following:
 - To establish a region definition, click the  New icon, and continue.
 - To edit a region definition, select a row, click the  Open icon, and continue.
 - e. In the **Communication Region** form, navigate to the **Device Credentials** tab.
 - f. Do one of the following:
 - To establish a credential setting, click the  New icon, and continue.
 - To edit a credential setting, select a row, click the  Open icon, and continue.
 - To delete a credential setting, select a row and click the  Delete icon
2. Provide the attribute values of credentials for this region (see [table](#)).

Note: NNMi tries to use the [Specific Node Device Credentials](#). If none match, NNMi tries the Region Device Credential settings provided here. If none match, NNMi tries the [Default Device Credentials](#).

3. Click  **Save and Close** to return to the Communication Region form.
4. Click  **Save and Close** to return to the Communication Configuration form.
5. Click  **Save and Close**.



Device Credential Attributes for this Region

Attribute	Description
User Name	Type the user name that you want NNMi to use for logging into devices in this Communication Region.
Password	Type the password that you want NNMi to use for logging into devices in this Communication Region. Note: NNMi encrypts the password and displays asterisks for this attribute. If you want to change the password, first clear the asterisks displayed in the Password attribute and enter the new Password value.

Configure SNMPv3 Settings for Regions

NNMi can use SNMPv3 user-based security model (USM) settings to access devices.


To view the current list of SNMPv3 USM settings for a Region:


1. Navigate to the **SNMPv3 Settings** tab on the Communication Region form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Communication Configuration**.
 - c. Navigate to the **Regions** tab.
 - d. Do one of the following:
 - To create a region definition, click the  New icon.
 - To edit a region definition, select a row, click the  Open icon.
 - e. In the **Communication Region** form, access the **SNMPv3 Settings** tab.


2. The displayed table lists the Unique Name of each SNMPv3 USM setting for this region.


Note: NNMi tries to use the [Specific Node SNMPv3 Settings](#). If none match, NNMi tries the Region SNMPv3 Settings provided here. If none match, NNMi tries the [default SMNPv3 settings](#).


3. You can also do the following:

- To establish a new setting, click the  New icon. See "[Communication Region SNMPv3 Settings form](#)" (on page 65).


Click  **Save and Close** to return to the Communication Region form.

- To edit an existing setting, select a row, click the  Open icon. See "[Communication Region SNMPv3 Settings form](#)" (on page 65).

Click  **Save and Close** to return to the Communication Region form.

- To delete a setting from the Region's list, select a row and click the  Delete icon.

Note:The record remains in the database for possible use elsewhere and is simply removed from this Communication Region's list.

4. Click  **Save and Close** to return to the Communication Configuration form.

5. Click  **Save and Close**. Your changes are available for the next Discovery or Monitoring cycle.






Communication Region SNMPv3 Settings form










NNMi can use SNMPv3 user-based security model (USM) settings to access devices.

NNMi tries to use the current SNMPv3 Settings attribute value from [Specific Node Settings](#). If none match, NNMi tries the Region SNMPv3 Settings provided here. If none match, NNMi tries the [default SMNPv3 settings](#).

To configure an SNMPv3 Setting for a Region:

1. Navigate to the **Communication Region SNMPv3 Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.

- b. Select the **Communication Configuration**.
 - c. Navigate to the **Regions** tab.
 - d. Do one of the following:
 - To create a region definition, click the  New icon.
 - To edit a region definition, select a row, click the  Open icon.
 - e. In the **Communication Region** form, navigate to the **SNMPv3 Settings** tab.
 - f. Do one of the following:
 - To create an SNMPv3 Setting definition, click the  New icon.
 - To edit an SNMPv3 Setting, select a row, click the  Open icon.
 - To remove an SNMPv3 Setting from this Region, select a row, click the  Delete icon.

Note: The record remains in the database for possible use elsewhere and is simply removed from this Communication Region's list.
2. Click the SNMPv3 Settings  Lookup icon and select one of the options from the drop-down menu:
 -  Quick View to display summary information for the currently configured (selected) SNMPv3 Setting name.
 -  Quick Find to view and select from the list of all existing SNMPv3 Settings (for more information see ["Use the Quick Find Window" \(on page 19\)](#)).
 -  Open to display the details of the currently configured (selected) SNMPv3 Setting (see ["SNMPv3 Settings Form"](#) for more information).
 -  New to create a new SNMPv3 Setting (see ["SNMPv3 Settings Form"](#) for more information).
 3. Click  **Save and Close** to return to the Communication Region SNMPv3 Settings form.
 4. Click  **Save and Close** to return to the Communication Region form.
 5. Click  **Save and Close** to return to the Communication Configuration form.
 6. Click  **Save and Close**. Your changes are available for the next Discovery or Monitoring cycle.

Configure Specific Nodes (Communication Settings)

Configuring communication protocols for specific devices is optional.

Use the Specific Node Settings tab to fine tune communication protocol usage and settings for a particular device within your environment. For example, provide settings for your most important devices, or disable communication with the least important devices.

When you leave a field blank, NNMi uses the next applicable configuration setting for that field in the following order:

- The value configured for a Region that includes this device. If multiple Region definitions include this device (for example, buildings, floors within those buildings, or workgroups within a particular floor), the first match applies (the matching region with the lowest Ordering number) . See ["Configure"](#) .

[Regions \(Communication Settings\)" \(on page 56\).](#)

- The default value for this field (see "[Configure Default SNMP and ICMP Protocol Settings" \(on page 47\)](#) , "[Configure Default Community Strings \(SNMPv1 or SNMPv2c\)" \(on page 51\)](#) , "[Configure the Default Device Credentials \(NNM iSPI NET\)" \(on page 53\)](#) , and "[Configure Default SNMPv3 Settings" \(on page 54\)](#)).

Note: NNMi enables you to set up one or more SNMP Proxy Servers in the cases where an SNMP node is otherwise unreachable (for example, when a node you want to manage is behind a firewall). To enable NNMi to use the SNMP Proxy Server, when you configure communication protocols for specific devices, you must include the IP address and port number on the SNMP Proxy Server. See "[Specific Node Settings Form \(Communication Settings\)" \(on page 67\)](#) for more information.

To configure specific devices, you have two choices:






- "[Specific Node Settings Form \(Communication Settings\)" \(on page 67\).](#)
- "[Load Specific Node Settings from a File" \(on page 74\)](#)

Specific Node Settings Form (Communication Settings)

Create specific node settings to control the way NNMi monitors your most important devices or least important devices.

Tip: If no value is provided for an attribute in the Communication Node form, NNMi uses the applicable [Region settings](#) and if none match, NNMi uses the [default settings](#).

To configure communication protocol settings for a specific node:

1. Access the **Specific Node Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Communication Configuration**.
 - c. Navigate to the **Specific Node Settings** tab.
 - d. Do one of the following:
 - To establish settings for a node, click the  New icon, and continue.
 - To edit settings for a node, select a row, click the  Open icons, and continue.
 - To delete settings for a node, select a row and click the  Delete icon.
2. Provide the communication protocol settings for the node (see the [Basic Settings](#) table, [SNMP Settings](#) table, and [ICMP Settings](#) table).
3. *Optional.* Make additional configuration choices. Click here for a list of choices .
4. Click  **Save and Close** to return to the Communication Configuration form.
5. Click  **Save and Close**. Your changes are available for the next Discovery or Monitoring cycle.

Basic Settings for this Device

Attribute	Description
Target Hostname	<p>Caution: The Hostname attribute value on the Node form of the discovered node must match what is entered here (see the Hostname attribute the Node form help topic).</p> <p>If a device has multiple hostnames or no hostname, NNMi follows a set of rules to determine the hostname. Click here for details.</p> <ol style="list-style-type: none">1. If a hostname is available, it must resolve to a valid IP address. NNMi stores the fully-qualifiedhostname in the database as all lowercase characters.2. If more than one address is associated with a node, the loopback address¹ is used with the following exceptions:<ul style="list-style-type: none">■ NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).■ NNMi ignores any address that is virtual (HSRP/VRRP) or an Anycast Rendezvous Point IP Address².3. If a node has multiple loopback addresses, NNMi uses the loopback address with the lowest number that resolves to a hostname (for example, 10.16.42.197 is a lower number than 10.16.197.42).4. If no loopback address resolves to a hostname and the device supports SNMP, NNMi uses the current value from the Management Address attribute on the Node form.5. If the device does not support SNMP, the IP address or DNS name found during the current rediscovery cycle is used as the hostname. <p>This sequence is repeated during each rediscovery cycle. The hostname could change from cycle to cycle (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).</p>
Preferred Management Address	<p>Specify the address you want NNMi to use for SNMP communications with this device. If you enter an invalid or unreachable address, the device is not discovered or monitored.</p> <p>If this attribute is left empty (null), NNMi dynamically selects the address based on responses from the device's SNMP agent.</p>

¹The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

²Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

Attribute	Description
	<p>When NNMi determines the Management Address, NNMi handles cases where the SNMP agent supports multiple IP addresses by following a set of rules. Click here for details.</p> <ol style="list-style-type: none"> 1. If the node has only one loopback address¹, that address is used with the following exceptions: <ul style="list-style-type: none"> ■ NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*). ■ NNMi ignores any address that is virtual (HSRP/VRRP), an Anycast Rendezvous Point IP Address², or whose interface is administratively down. 2. If an SNMP agent supports multiple loopback addresses, NNMi uses the loopback address with the lowest number to which this SNMP agent responds (for example, 10.16.42.197 is a lower number than 10.16.197.42). 3. If no loopback address is supported, NNMi uses the address that meets the following criteria: <ul style="list-style-type: none"> ■ During initial discovery, NNMi uses the first address to which the associated SNMP agent responded. <p>Note: The <i>first address</i> might be <i>either</i> a discovery seed address or an ARP cache address gathered in the path to this node.</p> ■ During any other discovery cycle, NNMi uses the current Management Address value. <p>For this sequence, if the SNMP agent does not respond to any of the above addresses, NNMi automatically repeats the sequence with SNMPv2c, SNMPv1, and SNMPv3 (according to the current NNMi Communication Configuration settings established by your NNMi administrator).</p> <p>This sequence is repeated during each configuration polling cycle. And the address could change over time (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).</p>






SNMP Settings for this Device

Attribute	Description
Enable SNMP Communication	<p>If <input checked="" type="checkbox"/> enabled, the Discovery Process and State Poller Service generate network traffic with SNMP protocol to discover and monitor this device.</p> <p>If <input type="checkbox"/> disabled, NNMi does not generate any SNMP traffic to this device.</p>

¹The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

²Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

Attribute	Description
	<p>Caution: With no SNMP data, Spiral Discovery interprets each IP Address as a separate node, Causal Engine calculates Status based only on IP address State, previously discovered Interfaces show a State attribute value of "Not Polled" and a Status attribute value of "No Status" with the Interface map-symbol color set to beige, and no new Interfaces are discovered.</p> <p>Note: Your choice might be overridden if Monitoring Configuration settings disable SNMP usage for the State Poller Service, see "Set Global Monitoring" (on page 153) or "Configure Monitoring Behavior" (on page 152).</p>
Enable SNMP Address Discovery	<p>If <input checked="" type="checkbox"/> enabled, NNMi automatically identifies which management address (SNMP agent) to use for each device. If the initially configured address becomes unreachable, NNMi automatically locates another SNMP agent, if possible, and changes the management address attribute value.</p> <p>If <input type="checkbox"/> disabled, when the current management address (SNMP agent) becomes unreachable, NNMi reclassifies the node as a non-SNMP node until the previously configured management address is available again.</p>
SNMP Timeout	<p>(Seconds:Milliseconds) Maximum 1 millisecond less than a minute: 59 seconds 999 milliseconds.</p> <p>Time that NNMi waits for a response to an SNMP query before reissuing the request. Both the Discovery Process and the State Poller Service use this setting for this device. For an explanation of how NNMi implements timeout and retry configurations, see "Timeout / Retry Behavior Example for SNMP" (on page 50).</p>
SNMP Retries Count	<p>Maximum number of retries that NNMi issues for an SNMP query before determining the query result to be "unresponsive". Zero means no retries. Both the Discovery Process and the State Poller Service use this setting for this device.</p>
SNMP Port	<p>Default is 161. Specifies the management station's port that NNMi uses when generating SNMP traffic. Both the Discovery Process and the State Poller Service use this setting for this device.</p>
SNMP Proxy Address	<p>Specify the IP address of your SNMP Proxy Server.</p> <p>You can set up one or more SNMP Proxy Servers to enable communication with nodes that otherwise might be unreachable (for example, when a node to be managed is behind a firewall). The SNMP Proxy Server allows NNMi to manage these nodes in the same way as nodes that provide SNMP access directly.</p>
SNMP Proxy Port	<p>Port number on the SNMP Proxy Server. See SNMP Proxy Address (previous attribute).</p>

Attribute	Description
SNMPv3 Settings	<p>Click the SNMPv3 Settings  Lookup icon and select one of the options from the drop-down menu:</p> <ul style="list-style-type: none">  Quick View to display summary information for the currently configured (selected) SNMPv3 Setting name.  Quick Find to view and select from the list of all existing SNMPv3 Settings (for more information see "Use the Quick Find Window" (on page 19)).  Open to display the details of the currently configured (selected) SNMPv3 Setting.  New to create a new SNMPv3 Setting. <p>The SNMPv3 Settings form opens. See "SNMPv3 Settings Form" for information about each attribute.</p>

ICMP Settings for this Device

Attribute	Description
Enable ICMP Communication	<p>If <input checked="" type="checkbox"/> enabled, NNMi generates network traffic with ICMP protocol to this device.</p> <p>If <input type="checkbox"/> disabled, NNMi does not generate any ICMP traffic to this device:</p> <ul style="list-style-type: none"> Addresses in this Node (both previously discovered and newly discovered) have a State attribute value of "Not Polled" and a Status attribute value of "No Status" with the IP Address map-symbol color set to beige. If both ICMP and SNMP are disabled, the Node has a Status attribute value of "No Status" have a map-symbol background shape color set to beige. <p>Note: Your choice might be overridden if Monitoring Configuration settings disable ICMP usage for the State Poller Service, see "Set Global Monitoring" (on page 153) or "Configure Monitoring Behavior" (on page 152).</p>
ICMP Timeout	<p>(Seconds:Milliseconds) Maximum 1 millisecond less than a minute: 59 seconds 999 milliseconds.</p> <p>Time that NNMi waits for a response to an ICMP query before reissuing the request to this device. For an explanation of how NNMi implements timeout and retry configurations, see "Timeout / Retry Behavior Example for ICMP" (on page 51).</p>
ICMP Retries Count	<p>Maximum number of retries that NNMi issues for an ICMP query to this device before logging an error. Zero means no retries.</p>

Related Topics:

["Configure Default SNMP and ICMP Protocol Settings" \(on page 47\)](#)



["Configure Default Community Strings \(SNMPv1 or SNMPv2c\)" \(on page 51\)](#)



["Configure Regions \(Communication Settings\)" \(on page 56\)](#)

Configure Community Strings for Nodes

Configure one SNMPv1 or SNMPv2c "get" community string for each node.

To provide a community string for a specific device:

1. Navigate to the **Specific Node Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Communication Configuration**.
 - c. Navigate to the **Specific Node Settings** tab.
 - d. Do one of the following:
 - To establish a node definition, click the  New icon, and continue.
 - To edit a node definition, select a row, click the  Open icon, and continue.
 - e. In the **Specific Node Settings** form, navigate to the **Community Strings** tab.
2. Provide a community string for this region (see [table](#)).

Tip: : If you do not provide any community strings, NNMi uses the applicable [Region settings](#) and if none match, NNMi uses the [default settings](#) .
3. Click  **Save and Close** to return to the Communication Configuration form.
4. Click  **Save and Close**. NNMi updates the affected SNMP Agent objects in the NNMi database. Your changes are available for the next Discovery or Monitoring cycle.

SNMPv1 or SNMPv2c Community String for this Device






Attribute	Description
Read Community String	<p>The SNMPv1 or SNMPv2c "get" (read-only) community string that is used for this device. Case-sensitive.</p> <p>Many proxy vendors use the community string for specifying remote target information. NNMi supports substitution parameters within community strings for SNMPv1 or SNMPv2 proxy environments. Click here for more information.</p> <p>Copy and paste these codes at the end of your Community String to provide the values required by your proxy environment. NNMi substitutes the actual attribute values from the NNMi database at runtime:</p> <p><code>\${contextName}</code> = Used for specifying VLAN context for switches (VLAN associated with the remote target node)</p> <p><code>\${managementAddress}</code> = Node form, Management Address attribute value (the remote target node)</p> <p><code>\${snmpPort}</code> = SNMP Agent form, UDP Port attribute value (SNMP agent associated with the remote target node)</p>




Configure Credential Settings for Nodes (NNM iSPI NET)

NNMi uses Default Credential Settings to access devices when running Diagnostics either automatically or when the **Actions** → **Run Diagnostics** option is used. (See "[Configure Diagnostics for an Incident \(NNM iSPI NET\)](#)" (on page 291) and [Node Form: Diagnostics Tab](#) for more information.)

NNMi uses Shell (SSH or telnet) as the method for accessing devices with the credentials specified. NNMi uses SSH as the preferred communication method. If the SSH attempt fails, NNMi uses telnet.

To provide credential settings for a specific node:

1. Navigate to the **Specific Node Device Credentials** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Communication Configuration**.
 - c. Navigate to the **Specific Node Settings** tab.
 - d. Do one of the following:
 - To establish a definition, click the  New icon, and continue.
 - To edit a definition, select a row, click the  Open icon, and continue.
 - e. In the **Specific Nodes Settings** form, navigate to the **Device Credentials** tab.
 - f. Do one of the following:
 - To establish a credential setting, click the  New icon, and continue.
 - To edit a credential setting, select a row, click the  Open icon, and continue.
 - To delete a credential setting, select a row and click the  Delete icon
2. Provide the attribute values of credentials for this node (see [table](#)).

Note: NNMi tries to use the Specific Node Device Credentials provided here. If none match, NNMi tries the [Region Device Credential](#) settings. If none match, NNMi tries the [Default Device Credentials](#).
3. Click  **Save and Close** to return to the Specific Node Settings form.
4. Click  **Save and Close** to return to the Communication Configuration form.
5. Click  **Save and Close**.

Specific Node Device Credential Attributes

Attribute	Description
User Name	Type the user name that you want NNMi to use for logging into this device.
Password	Type the password that you want NNMi to use for logging into this device. Note: NNMi encrypts the password and displays asterisks for this attribute. If you want to change the password, first clear the asterisks displayed in the Password attribute and enter the new Password value.

Load Specific Node Settings from a File

Import a list of devices, using a command line command. You also have the option of importing the SNMPv1 or SNMPv2c community string for each device or the SNMPv3 USM settings. This is useful when your SNMP is managed by a change control mechanism. You can bulk insert the SNMP assignments into NNMi. Each assignment shows up as an individual entry in the table on the **Communication Configuration** form's **Specific Node Settings** tab.

To import SNMP assignments:

1. On the NNMi management server's hard drive, create a text file according to the specifications in the [nnmcommload.ovpl](#) reference page. Create one line for each device. For more information, see [nnmcommload.ovpl](#)

To add comments to your file, place a # character at the beginning of each comment line.

Note: When you load this file, the data in the file overwrites any previously entered information about each hostname.

2. Use the following command line command to load the information into the NNMi database:

Windows:

```
<drive>:\Program Files (x86)\HP\HP BTO Software\bin\nnmcommload.ovpl -u <NNMi-adminUserName> -p <NNMiadminPassword> -file <path/filename>
```

<drive> is the drive on which NNMi is installed

UNIX:

```
/opt/OV/bin/nnmcommload.ovpl -u <NNMiadminUserName> -p <NNMiadminPassword> -file <path/filename>
```

3. Verify that the import worked properly:
 - a. From the workspace navigation panel, select the Configuration workspace.
 - b. Select Communication Configuration.
 - c. Access the Specific Node Settings tab.
4. Review each entry in the table to verify that the import was successful.

To verify the SNMP configuration for an IP Address, at the command line, type:

Note: For more information, see [nnmcommconf.ovpl](#)

Windows:

```
<drive>:\Program Files (x86)\HP\HP BTO Software\bin\nnmcommconf.ovpl -u <NNMi-adminUsername> -p <NNMiadminPassword> -proto snmp -host <node IP address>
```

<drive> is the drive on which NNMi is installed

UNIX:

```
/opt/OV/bin/nnmcommconf.ovpl -u <NNMiadminUsername> -p <NNMiadminPassword> -proto snmp -host <node IP address>
```

To verify the ICMP configuration for an IP Address, at the command line, type:

Note: For more information, see [nnmcommconf.ovpl](#)

Windows:

```
<drive>:\Program Files (x86)\HP\HP BTO Software\bin\nnmcommconf.ovpl -u <NNMi-adminUsername> -p <NNMiadminPassword> -proto icmp -host <node IP address>
```

<drive> is the drive on which NNMi is installed

UNIX:

```
/opt/OV/bin/nnmcommconf.ovpl -u <NNMiadminUsername> -p <NNMiadminPassword> -proto icmp -host <node IP address>
```

Verify Your Communication Settings

After you configure your communication settings, you can check to determine what parameters NNMi is using to communicate with a node of interest.

Use the **Actions** → **Communication Settings** menu item to display a report.

NNMi displays the communication configuration information for the node selected, including the SNMP and ICMP configuration information.



To navigate to a table view and select a node:

1. From the workspace navigation panel, select the workspace of interest. For example, **Inventory**.
2. Select the view that contains the node whose communication settings you want to check. For example, **Nodes**.
3. From the table view, select the check box that precedes the node whose configuration you want to check.
4. Select **Actions** → **Communication Settings**.

To navigate to a map view and select a node:

1. Navigate to the table view.
2. From a table view, select the check box that precedes the node of interest.
3. Select the **Actions** menu.
4. From the drop-down menu, select the map view of interest.
5. From the map view, click the node whose configuration you want to check.
6. Select **Actions** → **Communication Settings**.

To select a node from a form:

1. From a table view, click the  Open icon that precedes the node of interest.
2. From a map view, click the node of interest on the map and click the  Open icon.
3. Select **Actions** → **Communication Settings**.

See "[Configuring Communication Protocol](#)" (on page 47) for information about configuring communication settings.

Related Topics

[nnmcommconf.ovpl](#)

Discovering Your Network

Configure NNMi to discover only the nodes that are important to you and your team.

Using a wide range of protocols and techniques, NNMi Spiral Discovery gathers a wealth of information about your network inventory, ascertains the relationships between devices (such as subnets and VLANs), and accurately maps out the connectivity between those devices. The NNMi Causal Engine determines the current status of each device (plus each associated interface and address within that device) and proactively notifies you when NNMi detects any trouble or potential trouble.

This dynamic discovery process continues over time. When things change in your network management domain, Spiral Discovery automatically updates information according to a schedule that you set. The topology maps always reflect accurate timely information about any changes in your network.

Note: Review and complete the prerequisites before configuring discovery, "[Prerequisites for Discovery](#)" ([on page 86](#)).

You decide which nodes are discovered and how often NNMi checks for new devices in your network (see "[Determine Your Approach to Discovery](#)" ([on page 88](#)) for ideas). The steps required depend on what you want to do:

- "[Adjust the Discovery Interval](#)" ([on page 98](#)) – *Optional*. The time NNMi waits between the discovery cycles that keep your network information current. By default, NNMi updates information about devices and connections every 24 hours.
- "[Configure the Node Name Strategy](#)" ([on page 99](#)) – *Optional*. Choose the node naming strategy for NNMi to use for the map icons and in the Name column of the table views.
- "[Configure Auto-Discovery Rules](#)" ([on page 101](#)) – *Optional*. Specify whether you want NNMi to automatically discover groups of network devices (identified by IP address ranges and MIB II sysObjectIDs). NNMi extends discovery by using requests for Address Resolution Protocol (ARP) cache information about neighbors. NNMi uses a variety of protocols to gather information from all neighbor devices. See "[Auto-Discovery Rules](#)" ([on page 83](#)) for more details.

Specify whether NNMi uses [Ping Sweep](#) (ICMP ping) or your [Discovery Seeds](#) as starting points for gathering information about neighboring devices.

NNMi discovers any devices that comply with your rule configurations, and creates a record of each device in the NNMi database. If the device supports SNMP, all addresses for that device are combined into one Node object. If the device does not support SNMP, NNMi queries DNS to determine the host name. If this hostname matches another non-SNMP node, NNMi merges the information to create only one node with multiple associated addresses.

- "[Configure an Excluded IP Addresses Filter](#)" ([on page 108](#)) – *Optional*. Specify addresses that you do not want NNMi to discover.
- "[Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered](#)" ([on page 112](#)) – *Optional*. Use Discovery Seeds to accomplish either of the following purposes:
 - Limit Spiral Discovery to only the seeds that you specify.
 - Provide seeds as starting points for your Auto-Discovery Rules.

For details about how Spiral Discovery works:

For a list of the types of things NNMi can discover, see [About Map Symbols](#).

From the information collected, NNMi constructs a model of your network configuration in the database, and displays this information in the map views. See [View Maps of Network Connectivity](#) for more information about the available map views.

How Spiral Discovery Works

NNMi uses a variety of network protocols (read-only queries) within your defined network management domain to gather information about each discovered device. You see the real-time accumulation of information as it is collected, rather than waiting until NNMi discovers your entire network environment.

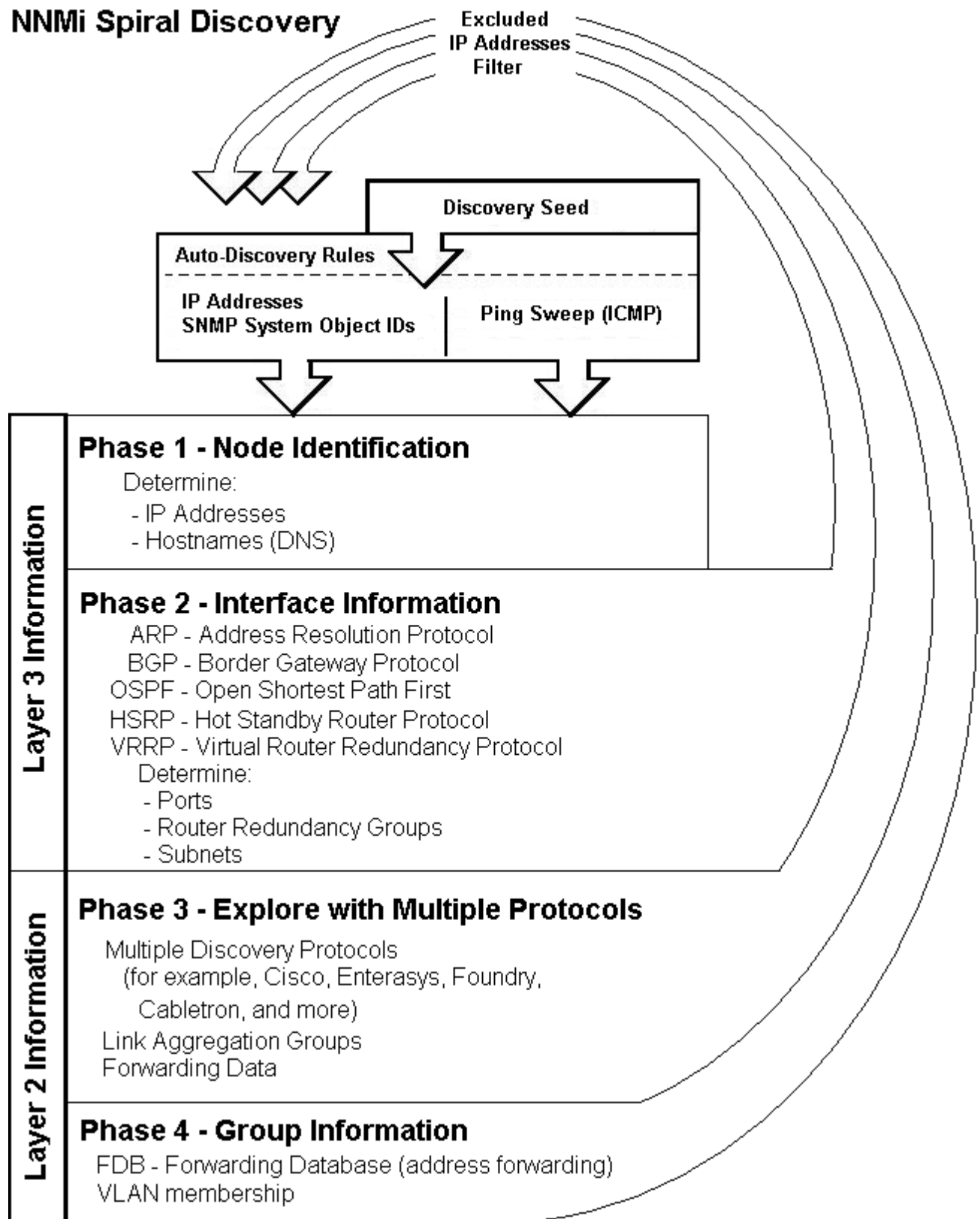
Spiral Discovery dynamically gathers two categories of information from each discovered node:

1. Information about the node — NNMi gathers detailed information about each device. You can review this data on the device's [Node form](#). Examples of configuration details include IP address, subnet information, sysObjectID, number of interfaces, and version of SNMP supported.
2. Connectivity details — NNMi gathers information about how devices are connected to each other on [Layer 2](#)¹ and [Layer 3](#)² of your network.

¹Refers to the Data Link layer of the multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer moves data across the physical links in the network. The switches and bridges are devices that redirect data messages at the layer 2 level, using the destination Media Access Control (MAC) address to determine where to direct the message.

²Refers to the Network layer of the multilayered communication model, Open Systems Interconnection (OSI). The Network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding incoming messages to local host domains. The router and switch-router are the devices that redirect data messages at the Layer 3 level. Everything in a subnet is connected at the Layer 3 (IP) level.

NNMi Spiral Discovery



Spiral Discovery checks for changes according to a schedule determined by the [Discovery Interval](#). NNMi administrators can set the schedule to meet any service-level agreement (SLA) commitments.

After NNMi completes initial discovery of your network, ongoing discovery takes over according to the Discovery Interval:

- If a new node is added to your defined network management domain, NNMi dynamically updates the topology database and maps. The node form provides details of the new node's configuration. The maps reflect the new connectivity information.
- If configuration settings change on an existing node, NNMi dynamically updates the database and maps to reflect the changes.

The only exception is when non-SNMP addresses that had the same DNS hostname are changed to have separate DNS hostnames, NNMi must completely rediscover the non-SNMP nodes to correctly update the database objects (node, interface, address, connection, and incidents). The NNMi administrator must delete the old non-SNMP node object and force NNMi to rediscover the new node configurations. See ["Delete Nodes" \(on page 122\)](#).

Tip: At any time, you can initiate an on-demand rediscovery poll to gather the most current information about a previously discovered device. Select a node and click the **Actions** → **Configuration Poll** command, or use the `nnmconfigpoll.ovpl` command.

A number of NNMi tools let NNMi administrators control how Spiral Discovery works.

For details about how Spiral Discovery works:

Discovery Intervals

Specify how often your entire network is checked for the latest information.

This interval controls how often NNMi generates network traffic to gather the following information:

- Information about the nodes, addresses, and interfaces you configure for discovery.
- Information about Level 2 connectivity between interfaces and VLANs in your network.
- Information about Level 3 connectivity between addresses in your network.

Make sure that you allow plenty of time for the interval so that Spiral Discovery cycles do not overlap. The larger your network environment, the longer the time required to complete a Spiral Discovery cycle.

See ["Adjust the Discovery Interval" \(on page 98\)](#) to learn how to set the discovery interval.

For details about how Spiral Discovery works:

Discovery Node Name Choices

Control how the **Name** attribute on node forms is populated during discovery. This Name value is used to identify the object in NNMi maps and table views. You specify a hierarchy for discovery to use. You configure three levels in the hierarchy. See ["Node Name Decision Tree" \(on page 81\)](#).

You can designate any of the following for each level of the node Name decision hierarchy:

- **DNS Names.** Discovery uses the results of hostname resolution.

If a device has multiple hostnames or no hostname, NNMi follows a set of rules to determine the hostname. Click here for details.

- a. If a hostname is available, it must resolve to a valid IP address. NNMi stores the fully-

qualifiedhostname in the database as all lowercase characters.

- b. If more than one address is associated with a node, the **loopback address**¹ is used with the following exceptions:
 - o NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).
 - o NNMi ignores any address that is virtual (HSRP/VRRP) or an **Anycast Rendezvous Point IP Address**².
- c. If a node has multiple loopback addresses, NNMi uses the loopback address with the lowest number that resolves to a hostname (for example, 10.16.42.197 is a lower number than 10.16.197.42).
- d. If no loopback address resolves to a hostname and the device supports SNMP, NNMi uses the current value from the Management Address attribute on the Node form.
- e. If the device does not support SNMP, the IP address or DNS name found during the current rediscovery cycle is used as the hostname.

This sequence is repeated during each rediscovery cycle. The hostname could change from cycle to cycle (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).

- **MIB II sysName Values.** Device administrators set the sysName. Discovery avoids populating the NNMi database with multiple devices having the same manufacturer's default sysName. If a sysName matches or starts with the manufacturer's default factory setting (case-sensitive), discovery ignores sysName as a choice for the Name attribute of the node. NNMi ships with a Device Profile for each device type. The Device Profile includes a record of the manufacturer's default sysName.

Caution: You can override this choice using the Device Profile's Advanced settings, Never Use sysName attribute. See "[Configure Device Profiles](#)" (on page 95) for more information.

- **IP addresses.** The addresses are gathered from [discovery seed addresses](#) that you provided, [ping sweep](#) configurations, or neighbor addresses gathered using [Auto-DiscoveryRules](#). Discovery avoids potential confusion when a device has multiple IP addresses by following these rules:
 - If the device supports SNMP, the address of the responding SNMP agent is recorded (the Management Address) and the other addresses are associated with the node. See "[Specific Node Settings Form \(Communication Settings\)](#)" (on page 67) for more information about configuring the management address.
 - If the device does not support SNMP, NNMi queries DNS to determine the hostname. If this hostname matches another non-SNMP node, NNMi merges the information to create only one node with multiple associated addresses.

See "[Configure the Node Name Strategy](#)" (on page 99) to learn how to configure the NNMi node name strategy.

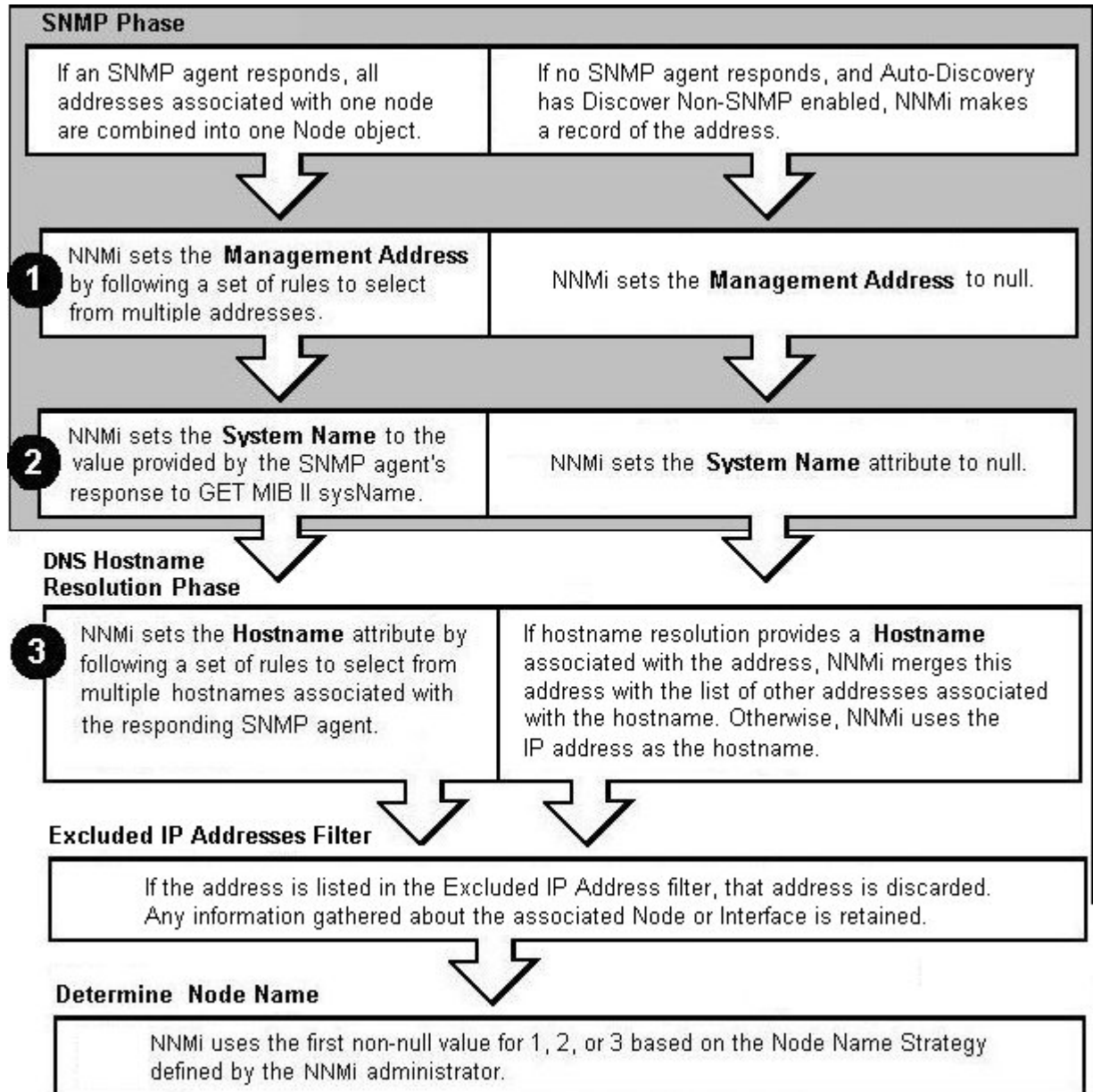
For details about how Spiral Discovery works:

¹The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

²Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

Node Name Decision Tree

For each discovered address, NNMi gathers multiple attributes that are used to implement your Node Name strategy. NNMi chooses the node Name based on the Management Address, System Name, and Hostname collected during discovery. The following diagram shows how NNMi determines values for these attributes.



For details about how Spiral Discovery works:

Discovery Seeds (as a starting point)

An optional discovery seed is a specific node that you want NNMi to discover. For example, a discovery seed might be a core router in your management environment.

Each discovery seed is identified by an IP address or hostname. When you add an optional discovery seed, NNMi immediately tries to discover that device (without waiting until the next regularly scheduled [discovery interval](#)). If discovery is not successful, NNMi tries again 10 minutes later, and continues trying. The time between each attempt is doubled until the time reaches 1 week or equals your current discovery interval.

Discovery seeds override [Auto-Discovery Rule](#) definitions. NNMi discovers seed addresses regardless of how you configure Auto-Discovery Rules or the [Excluded IP Addresses](#) filter.

Note: Nodes configured as discovery seeds are always discovered and added to the topology database. If you change your mind and [delete a discovery seed](#) configuration, the node is not automatically deleted from the topology database. See "[Delete Nodes](#)" (on page 122).

If you configure one or more Auto-Discovery Rules, note the following:

- If **Discover Included Nodes** is enabled for an Auto-Discovery Rule, NNMi uses each discovery seed as a starting point to gather information about neighboring devices and expand discovery.

Note: You can use the [Ping Sweep](#) option in your Auto-Discovery Rules in addition to or instead of Discovery Seeds.

- If **Discover Included Nodes** is disabled for an Auto-Discovery Rule, no devices matching that rule's criteria are discovered and added to the topology database unless:
 - The device's address is a discovery seed.
 - The device's address is reported as a neighbor to another discovered address.

See "[Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered](#)" (on page 112) to learn how to establish discovery seeds.

For details about how Spiral Discovery works:

Ping Sweep (as a starting point)

You have two choices for Auto-Discovery starting points. Use either or both to best advantage in your network environment:

- [Discovery Seeds](#) (You designate specific IP addresses or hostnames where Auto-Discovery starts gathering neighbor information.)
- Ping Sweep (NNMi issues ICMP pings to certain addresses gathered from neighbor information.)

Ping Sweep sends ICMP ping commands to IP addresses in the ranges defined in your Auto-Discovery rules. Ping Sweep enforces the following limits to the ICMP pings:

- For each specific IP address range, NNMi issues pings across a maximum of the last two octets in the IPv4 address range. This is equivalent to a /16 subnet
- ICMP pings are limited to 500 at one time. This avoids flooding your network or tripping spam detection tools.

Ping Sweep is useful in wide area networks such as ATM, Frame Relay, and Point-to-Point that do not contain an Address Resolution Protocol (ARP) cache.

You configure the Ping Sweep feature at two levels:

- ["Configure Ping Sweep Global Settings" \(on page 98\)](#)
- ["IP Address Ranges for Auto-Discovery" \(on page 104\)](#) (Ping Sweep configuration for each rule)

For details about how Spiral Discovery works:

Auto-Discovery Rules

Auto-Discovery Rules control the extent of automatic discovery. You choose the starting points for automatic discovery (either [Discovery Seeds](#) or [Ping Sweep](#), or both).

- If **Discover Included Nodes** is disabled for a particular Auto-Discovery Rule, nodes that match the Rule criteria are affected as follows:
 - *IP Address* ranges are not used for gathering neighbor information, see ["Limit Sources of Neighbor Information" \(on page 93\)](#).
 - *System Object ID* ranges are excluded from discovery. For examples, see ["Specific System Object IDs Not Discovered" \(on page 94\)](#).
- If **Discover Included Nodes** is enabled for a particular Auto-Discovery Rule, a variety of protocols are used to gather information about the neighbors adjacent to each discovered device. Spiral Discovery then requests neighbor information from each new neighbor. This sequence continues until the boundaries identified by your rule definition are reached.

See ["Configure Auto-Discovery Rules" \(on page 101\)](#) to learn how to establish the rules that control automatic discovery.

When defining Auto-Discovery Rules, you must provide *at least one* Auto-Discovery Rule that includes an IP address range to define the limits of your management domain. By default NNMi discovers routers and switches. You can expand the number of device types that NNMi discovers by including one or more System Object ID Ranges (based on MIB II sysObjectID values). Your address ranges and system object ID ranges determine which discovered addresses are added to the NNMi database.

NNMi gathers information about neighboring devices using ARP cache, DNS, and the following protocols:

- **BGP** — Border Gateway Protocol
- **CDP** — Cisco Discovery Protocol
- **EIGRP** — Cisco Enhanced Interior Gateway Routing Protocol
- **ENDP** — Enterasys Discovery Protocol (also known as CDP - Cabletron Discovery Protocol)
- **FDP** — Foundry Discovery Protocol
- **OSPF** — Open Shortest Path First

In Wide Area Networks (WANs) such as ATM, Frame Relay, and Point-to-Point (where ARP cache is not available), the optional [Ping Sweep](#) feature locates nodes for Auto-Discovery to use when gathering neighbor information and evaluating [subnet connection rules](#).

For details about how Spiral Discovery works:

Filters to Exclude Certain IP Addresses

When configuring Spiral Discovery in NNMi, sometimes it is useful to exclude certain addresses or ranges of addresses from discovery and monitoring. For example:

- There are multiple Nortel switches in your environment. They each have a non-routable IP address of 192.168.168.168 that is defined by the manufacturer. This special address is used to establish the default VLAN for the switch. However, NNMi discovers this duplicate address and establishes a lot of unnecessary connections on the Layer 3 Neighbor View map.
- Your service provider does not allow ICMP or SNMP traffic from your NNMi installation. That range of addresses can easily be excluded to prevent violating your contractual agreement with the vendor.
- The Provider Edge (PE) routers have addresses that NNMi ICMP ping commands cannot reach or have addresses that you want to exclude from Subnet views.

Note: The node and interface associated with any address identified in your Excluded IP Address filter shows up in the topology database and maps.

Carefully select the addresses for your Excluded IP Addresses filter. Do not populate the Excluded IP Addresses filter with the addresses associated with SNMPv1/SNMPv2c agents or SNMPv3 engines (the Management Addresses). See ["Configure an Excluded IP Addresses Filter" \(on page 108\)](#) to learn how to exclude an address or range of addresses from discovery.

For details about how Spiral Discovery works:

Subnet Connection Rules

Sometimes it is useful to monitor connections in the following categories:

- Virtual tunnel connections within your management domain.
- Connections to remote sites (across a Service Provider's network or a WAN).

NNMi accomplishes this by following special rules for subnets with prefix lengths between 28 and 31. These special rules are called Subnet Connection Rules. NNMi provides a group of predefined Subnet Connection Rules (see ["Subnet Connection Rules Provided by NNMi" \(on page 111\)](#)). You can edit an existing Subnet Connection Rule or create your own (see ["Configure Subnet Connection Rules" \(on page 109\)](#)).

If you limit Spiral Discovery to only your Discovery Seeds, NNMi uses the Subnet Connection Rules to detect connections among those devices.

If you use Auto-Discovery rules to configure Spiral Discovery, when NNMi detects a subnet prefix between 28 and 31, NNMi uses the Subnet Connection Rules:

1. NNMi checks for an applicable Subnet Connection Rule (see ["Subnet Connection Rules Provided by NNMi" \(on page 111\)](#)).
2. If a match is found, Spiral Discovery checks the topology database for existing data about each IPv4 address in the subnet. If no data is found for a particular IPv4 address, NNMi issues an SNMP query to the new IPv4 address. The number of available IPv4 addresses for each valid prefix length is described in the following table:

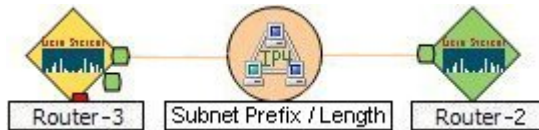
Valid Minimum Prefix Length Values (Subnet Mask Length)

Valid Minimum IPv4 Prefix Length Values	Number of Usable IPv4 Addresses
28	14 (16-2=14)*
29	6 (8-2=6)*
30	2 (4-2=2)*
31	2

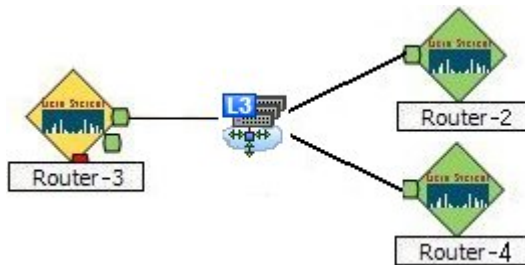
* Two IPv4 addresses are reserved in each subnet. The first IPv4 address is used for the network itself and the last IPv4 address is reserved for broadcast.

3. NNMi checks the Excluded IP Addresses list. Any addresses in the list are dropped. For details, see ["Filters to Exclude Certain IP Addresses" \(on page 83\)](#).
4. New IPv4 addresses that respond to SNMP are added to the topology database and available for monitoring purposes. New IPv4 addresses that do not respond to SNMP are ignored.
5. If the IPv4 address on each end of a connection has an associated interface, NNMi uses the subnet connection rule to display the connection on map views.

In a Layer 3 Neighbor View map, if NNMi discovers an interface that is connected to more than one interface, the results of your subnet connection rule look like the following:



In a Layer 2 Neighbor View map, if NNMi discovers an interface that is connected to more than one interface, the results of your subnet connection rule look like the following:



See ["Configure Subnet Connection Rules" \(on page 109\)](#) to learn how to configure Subnet Connection Rules.

For details about how Spiral Discovery works:

Device Profiles and Discovery

You can modify the settings in the Device Profiles to fine-tune Spiral Discovery and the device symbols on the maps.

You can also use the **Configuration** → **Device Profiles** view to see the list of all known system object IDs (MIBII sysObjectIDs) at the time NNMi released. This list of system object IDs is useful if you want to expand the range of devices that NNMi discovers. By default, NNMi discovers only routers and switches (see ["SNMP System Object ID Ranges for Discovery" \(on page 106\)](#)).

See the Advanced Settings section of ["Configure Device Profiles" \(on page 95\)](#) for more information.

For details about how Spiral Discovery works:

Prerequisites for Discovery

NNMi uses SNMP and DNS while discovering and monitoring devices in your network environment. To ensure accurate network topology information, verify that these prerequisites are working properly:

- ["SNMP Prerequisites" \(on page 86\)](#)
- ["Well-Configured DNS Prerequisite" \(on page 86\)](#)

SNMP Prerequisites

Spiral Discovery uses SNMP while detecting devices and connections among the devices in your network environment. NNMi also uses SNMP as part of monitoring and reporting on the health of devices in your network environment.

NNMi supports the following SNMP versions:

- SNMPv1
- SNMPv2c
- SNMPv3

NNMi uses information gathered from Routers to establish subnet membership for Layer 3 connections. Make sure that important Routers in your network environment are SNMP enabled.

NNMi uses either of the following criteria to identify a Router:

- Each Router responds with appropriate values for sysServices (1.3.6.1.2.1.1.7) and ipForwarding (1.3.6.1.2.1.4.1). See RFC1213-MIB for details.
- Identify Routers with the [Device Profile configuration settings](#) for a particular device type.

You must provide the appropriate SNMP Community Strings to NNMi. See ["Configuring Communication Protocol" \(on page 47\)](#).

Before configuring NNMi discovery, complete the following steps:

1. Enable SNMP communication on important devices in your network (each device that you want NNMi to actively monitor).

See the manufacturer's documentation for information about how to configure SNMP on each of your devices.

- Configure the SNMP agents.
- Establish Read-Only community strings for SNMPv1 or SNMPv2c.
- Establish the appropriate SNMPv3 User-based Security Module (USM) level of security for authentication and privacy.

2. Configure NNMi to use the appropriate community strings or USM settings for your network environment. See ["Configuring Communication Protocol" \(on page 47\)](#).

Well-Configured DNS Prerequisite

NNMi uses Domain Name System (DNS) to determine relationships between hostnames and IP addresses. This can result in a large number of `nslookup` requests.

Tip: To improve the response time for `nslookup`, deploy a secondary DNS service on the NNMi management server or another system on the same subnet as the NNMi management server. Configure this secondary DNS service to mirror the information from the primary DNS service. Another option is to use `*/etc/hosts` instead of DNS in small environments.

Use nslookup to Verify DNS Server Configurations

Verify that your DNS servers are well configured to prevent long delays when resolving `nslookup` requests. This means the DNS server responding to NNMi `nslookup` requests has these qualities:

- The DNS server is an authoritative server and does not forward DNS requests.
- The DNS server has consistent *hostname-to-IP address* mappings and *IP address-to-hostname* mappings.
- If your network uses multiple DNS servers, all respond consistently to any particular `nslookup` request.

Caution: Round-robin DNS (used to do load balancing of web application servers) is not appropriate because any given hostname can map to different IP addresses over time.

On the NNMi management server, verify that the following are configured appropriately for your environment:

- **All operating systems:** Locate your `*/etc/hosts` file and ensure that the host file contains a minimum of two entries. When an `nslookup` command is not successful, this file takes over:

```
127.0.0.1 (loopback localhost)
<NNMi_server_address> (the IP address of the NNMi management server)
```

Windows: The following registry key determines the location of this file:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DataBasePath
```

UNIX: This file is in the `/etc` directory.

- **Windows:** Use the Control Panel to navigate to your Network and Internet Connections configuration, Network Connections, Local Area Connections, Support tab, and click the Details button. Verify that all identified DNS servers provide consistent *hostname-to-IP address* mappings and *IP address-to-hostname* mappings.
- **UNIX:** Ensure that the `nslookup` search path resolves to the `nsswitch.conf` file. See the `nsswitch.conf(4)` manpage that was provided with your operating system. Verify that all identified DNS servers provide consistent *hostname-to-IP address* mappings and *IP address-to-hostname* mappings.

Exclude Problem Devices from nmlookup

You can populate two files that instruct `nslookup` to exclude certain addresses. The benefits of doing this are as follows:

- Speed up Spiral Discovery.
- Keep network traffic generated by NNMi to a minimum.

If you know there are problems with the DNS configuration in your network domain (hostnames or addresses that do not resolve properly), instruct NNMi to avoid `nslookup` requests for unimportant devices.

To identify problem devices, create the following two files prior to configuring NNMi discovery. NNMi never issues a DNS request for hostnames or IP addresses identified in these files:

- [hostNoLookup.conf](#) (enter fully-qualified hostnames or wildcards that identify groups of hostnames)
- [ipNoLookup.conf](#) (enter fully-qualified IP addresses or wildcards that identify groups of IP addresses)

Use an ASCII editor to populate the files. Place the files in the following location on the NNMi management server:

- **Windows:**
`<drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\conf\
<drive>` is the drive on which NNMi is installed.
- **UNIX:**
`/var/opt/OV/shared/nnm/conf/`

Determine Your Approach to Discovery

Discover and monitor only the network devices that you and your team consider to be important. Take any approach that makes sense to you.

Tip: See the following examples for ideas. Print one or more of the following topics to use as a guide when you are configuring NNMi discovery.

Maintain absolute control over what is discovered.

- ["Do Not Use Auto-Discovery Rules" \(on page 88\)](#)

Configure Spiral Discovery to make decisions about what is discovered.

Create one or more Auto-Discovery Rules that define the boundaries of what is important to you and your team:

- ["Routers and Switches Discovered" \(on page 89\)](#) (Auto-Discovery Rules default behavior)
- ["All SNMP Devices Discovered" \(on page 90\)](#) (more than Routers and Switches)
- ["Everything Discovered" \(on page 91\)](#) (all SNMP enabled devices and all Non-SNMP devices)

Fine tune Spiral Discovery behavior.

Identify the things your team is not interested in monitoring:

- ["All Devices from a Specific Vendor Discovered" \(on page 92\)](#)
- ["Limit Sources of Neighbor Information" \(on page 93\)](#)
- ["Exclude Problem IP Addresses from Discovery" \(on page 94\)](#)
- ["Specific System Object IDs Not Discovered" \(on page 94\)](#)

Do Not Use Auto-Discovery Rules

If you want NNMi to discover only what you specify, use these guidelines.

Note: After you set your configuration according to these guidelines, when a new device is added to your network, NNMi does not discover that device unless you configure another discovery seed to identify that device.

Configuration Steps to Discover Only What You Specify

Task	How
Do not include any Auto-Discovery Rules .	None are required for this strategy.
In the Discovery Seeds settings, designate the hostname or IP address of each device you want NNMi to discover and configure NNMi to monitor your SNMP devices. See "Monitoring Network Health" (on page 151) .	"In the Console, Configure Discovery Seeds" (on page 113)

Note: You control how often Spiral Discovery checks the discovered nodes based on a **Rediscovery Interval** setting. See ["Adjust the Discovery Interval" \(on page 98\)](#) for more information.

Routers and Switches Discovered

If you want Spiral Discovery to automatically find devices on your network, use these guidelines. By default, Spiral Discovery Rules apply only to routers and switches. If you want to discover more devices, see ["All SNMP Devices Discovered" \(on page 90\)](#) or ["Everything Discovered" \(on page 91\)](#).

Note: After you set your configuration according to these guidelines, when a new router or switch is added to your network, you do not need to do anything. NNMi discovers it during the next discovery cycle.

Configuration Steps to Discover Only Routers and Switches

Task	How
<p>Create an Auto-Discovery Rule. Set the following attribute values:</p> <ul style="list-style-type: none"> Enter Ordering <input type="text" value="500"/> <p>It is recommended that you use Ordering number 500. This provides flexibility if you want to expand or limit Spiral Discovery behavior later by creating additional rules with higher or lower Ordering numbers.</p> Enable <input checked="" type="checkbox"/> Discover Included Nodes Disable <input type="checkbox"/> Discover Any SNMP Device Disable <input type="checkbox"/> Discover Non-SNMP Devices <p>Note: Discover Included Nodes is enabled by default.</p>	"Configure Auto-Discovery Rules" (on page 101)
<p>Create one or more IP Ranges settings that identify the entire scope of the addresses in your network domain:</p> <p>Enter IP Range <input type="text" value="<IPv4 range>"/> (at least one)</p> <p>Set Range Type <input type="text" value="Include in rule"/></p>	"IP Address Ranges for Auto-Discovery" (on page 104)
<p><i>Optional.</i> NNMi can use <input checked="" type="checkbox"/> Enable Ping Sweep (instead of or in addition to discovery seeds, see below) to gather neighbor information.</p>	"Ping Sweep (as a starting point)" (on page 82)

Task	How
<p>If you want Spiral Discovery to find all routers and switches. Do not create any System Object ID Ranges.</p> <p>If you want to limit Spiral Discovery to only the vendor/make/model of routers and switches that you specify, create one or more System Object ID Ranges. Your list <i>must include everything</i> you want Spiral Discovery to find.</p>	<p>"SNMP System Object ID Ranges for Discovery" (on page 106)</p> <p>Tip: Navigate to the Configuration workspace, and select the Device Profiles view to see all known system object IDs at the time NNMi released.</p>
<p><i>Optional.</i> In the Discovery Seeds settings, designate one or more hostnames or addresses. Consider using devices with the largest neighbor data. For example, a good choice would be a core router. The discovery seeds become the starting points from which Spiral Discovery explores your network.</p>	<p>"In the Console, Configure Discovery Seeds" (on page 113)</p>

Note: You control how often Spiral Discovery runs by designating the **Rediscovery Interval** setting. See ["Adjust the Discovery Interval" \(on page 98\)](#) for more information.

If you want to fine tune the Spiral Discovery results, see:

- ["All Devices from a Specific Vendor Discovered" \(on page 92\)](#) (more than routers and switches from the vendor)
- ["Limit Sources of Neighbor Information" \(on page 93\)](#) (less than all routers and switches)
- ["Specific System Object IDs Not Discovered" \(on page 94\)](#) (less than all routers and switches)
- ["Exclude Problem IP Addresses from Discovery" \(on page 94\)](#)

All SNMP Devices Discovered

If you want Spiral Discovery to find any device that has a working SNMP agent, use these guidelines. However, this strategy may cause you to reach your license limit very quickly. Consider defining additional Auto-Discovery Rules to limit this strategy. (See ["Specific System Object IDs Not Discovered" \(on page 94\)](#), or ["Limit Sources of Neighbor Information" \(on page 93\)](#). See also ["Filters to Exclude Certain IP Addresses" \(on page 83\)](#)).

Note: When a new SNMP-supported device is added to your network, you do not need to do anything. NNMi discovers it during the next discovery cycle.

Configuration Steps to Discover All Devices that Have SNMP Agents

Task	How
<p>Create an Auto-Discovery Rule. Set the following attribute values:</p> <ul style="list-style-type: none"> • Enter Ordering <input type="text" value="500"/> <p>It is recommended that you use Ordering number 500. This provides flexibility if you want to expand or limit Spiral Discovery behavior later by creating additional rules with higher or lower Ordering numbers.</p> • Enable <input checked="" type="checkbox"/> Discover Included Nodes • Enable <input checked="" type="checkbox"/> Discover Any SNMP Device • Disable <input type="checkbox"/> Discover Non-SNMP Devices 	<p>"Configure Auto-Discovery Rules" (on page 101)</p>
<p>Note: This strategy may cause you to reach your license limit very quickly.</p>	

Task	How
<p>Create one or more IP Range settings that identify the entire scope of the addresses in your network domain:</p> <p>Enter IP Range <input type="text" value="<IPv4 range>"/> (at least one)</p> <p>Set Range Type <input type="text" value="Include in rule"/></p>	<p>"IP Address Ranges for Auto-Discovery" (on page 104)</p>
<p><i>Optional.</i> NNMi can use <input checked="" type="checkbox"/> Enable Ping Sweep (instead of or in addition to discovery seeds, see below) to gather neighbor information.</p>	<p>"Ping Sweep (as a starting point)" (on page 82)</p>
<p>Do not create any System Object ID Ranges. When Discover Any SNMP Device is enabled and no ranges are specified, <i>all SNMP devices</i> are discovered (every sysObjectID that responds to an SNMP query).</p>	
<p><i>Optional.</i> In the Discovery Seeds settings, designate one or more hostnames or addresses. Consider using devices with the largest neighbor data. For example, a good choice would be a core router. The discovery seeds become the starting points for Spiral Discovery.</p>	<p>"In the Console, Configure Discovery Seeds" (on page 113)</p>

Note: You control how often Spiral Discovery runs by designating the **Rediscovery Interval** setting. ["Adjust the Discovery Interval" \(on page 98\)](#) for more information.

Everything Discovered

If you want Spiral Discovery to find all devices in your network, use these guidelines. However, this strategy may cause you to reach your license limit very quickly. Consider defining additional Auto-Discovery Rules to limit this strategy. (See ["All Devices from a Specific Vendor Discovered" \(on page 92\)](#), ["Specific System Object IDs Not Discovered" \(on page 94\)](#), or ["Limit Sources of Neighbor Information" \(on page 93\)](#). See also ["Filters to Exclude Certain IP Addresses" \(on page 83\)](#)).

If the device does not support SNMP, NNMi queries DNS to determine the hostname. If this hostname matches another non-SNMP node, NNMi merges the information to create only one node with multiple associated addresses to keep your license count low.

Note: After you set your configuration according to these guidelines, when a new device is added to your network, you do not need to do anything. NNMi discovers it during the next discovery cycle.

Configuration Steps to Discover Everything

Task	How
<p>Create an Auto-Discovery Rule. Set the following attribute values:</p> <ul style="list-style-type: none"> Enter Ordering <input type="text" value="500"/> <p>It is recommended that you use Ordering number 500. This provides flexibility if you want to expand or limit Spiral Discovery behavior later by creating additional rules with higher or lower Ordering numbers.</p> Enable <input checked="" type="checkbox"/> Discover Included Nodes Enable <input checked="" type="checkbox"/> Discover Any SNMP Device Enable <input checked="" type="checkbox"/> Discover Non-SNMP Devices <p>Note: This strategy may cause you to reach your license limit very quickly. Consider</p>	<p>"Configure Auto-Discovery Rules" (on page 101)</p>

Task	How
adding your non-SNMP devices using seeds instead of selecting the Discover Non-SNMP Devices option.	
Create one or more IP Ranges settings that identify the entire scope of the addresses in your network domain: Enter IP Range <input type="text" value="<IPv4 range>"/> (at least one is required) Set Range Type <input type="text" value="Include in rule"/>	"IP Address Ranges for Auto-Discovery" (on page 104)
<i>Optional.</i> NNMi can use <input checked="" type="checkbox"/> Enable Ping Sweep (instead of or in addition to discovery seeds, see below) to gather neighbor information.	"Ping Sweep (as a starting point)" (on page 82)
Do not include any System Object ID Ranges . When Discover All SNMP Devices is enabled and no ranges are specified, <i>all SNMP devices</i> are discovered (every sysObjectID that responds to an SNMP query).	
<i>Optional.</i> In the Discovery Seeds settings, designate one or more hostnames or addresses. Consider using devices with the largest neighbor data. For example, a good choice would be a core router. The discovery seeds become the starting points for Spiral Discovery.	"In the Console, Configure Discovery Seeds" (on page 113)

Note: You control how often Spiral Discovery runs by designating the **Rediscovery Interval** setting. See ["Adjust the Discovery Interval" \(on page 98\)](#) for more information.

All Devices from a Specific Vendor Discovered

If you want to expand Spiral Discovery to all devices manufactured by a specific vendor (more than routers and switches), use these guidelines.

To implement this strategy, you must create two Auto-Discovery Rules (see prerequisite). The prerequisite rule configures Spiral Discovery to find any router or switch, regardless of vendor.

Note: After you set your configuration according to these guidelines, when a new device is added to your network, you do not need to do anything. NNMi discovers or skips devices according to your configuration choices.

Prerequisite: Create an Auto-Discovery Rule that uses IP address ranges to specify the outer limits of your network management domain. This rule instructs Spiral Discovery to find devices manufactured by *any* vendor. See ["Routers and Switches Discovered" \(on page 89\)](#), ["All SNMP Devices Discovered" \(on page 90\)](#) or ["Everything Discovered" \(on page 91\)](#).

Configuration Steps to Discover All Devices from Specific Vendors

Task	How
Create an Auto-Discovery Rule . Set the following attribute values: <ul style="list-style-type: none"> Enter Ordering <input type="text" value="400"/> <p>It is recommended that you use Ordering number 400. This rule must have a lower number than the prerequisite rule.</p> Enable <input checked="" type="checkbox"/> Discover Included Nodes 	"Configure Auto-Discovery Rules" (on page 101)

Task	How
<ul style="list-style-type: none"> • Enable <input checked="" type="checkbox"/> Discover Any SNMP Device • Disable <input type="checkbox"/> Discover Non-SNMP Devices <p>Create one or more IP Ranges settings that identify the entire scope of the addresses in your network domain:</p> <p>Enter IP Range <input type="text" value="<IPv4 range>"/> (at least one)</p> <p>Set Range Type <input type="text" value="Include in rule"/></p>	<p>"IP Address Ranges for Auto-Discovery" (on page 104)</p>
<p>When Discover Any SNMP Devices is enabled and you specify one or more System Object ID Ranges, <i>only</i> the sysObjectIDs you specify are discovered.</p> <p>Create one or more System Object ID Ranges settings. Enter the SNMP sysObjectID prefix that identifies each vendor whose devices you want to discover.</p> <p>For example, to include all HP devices, use the following prefix: 1.3.6.1.4.1.11.</p> <p>Enter System Object ID Prefix <input type="text" value="<sysObjectID>"/></p> <p>Set Range Type <input type="text" value="Include in rule"/></p>	<p>"SNMP System Object ID Ranges for Discovery" (on page 106)</p> <p>Tip: Navigate to the Configuration workspace, and select the Device Profiles view to see all known system object IDs at the time NNMi released.</p>

Note: You control how often Spiral Discovery runs by designating the **Rediscovery Interval** setting. ["Adjust the Discovery Interval" \(on page 98\)](#) for more information.

Limit Sources of Neighbor Information

If you want Auto-Discovery to never request neighbor information from certain addresses within your management domain, use these guidelines. In other words, Auto-Discovery will not use these addresses as resources for further discovery.

Note: The addresses identified in your IP address Range might show up in the topology database if their neighbors provide information about them.

To implement this strategy, you must create two Auto-Discovery Rules (see prerequisite).

Prerequisite: Create an Auto-Discovery Rule that uses IP address ranges to specify the outer limits of your network management domain. See ["Routers and Switches Discovered" \(on page 89\)](#), ["All SNMP Devices Discovered" \(on page 90\)](#) or ["Everything Discovered" \(on page 91\)](#).

Configuration Steps to Exclude Some IP addresses from Providing Neighbor Data

Task	How To
<p>Create an Auto-Discovery Rule. Set the following attribute values:</p> <ul style="list-style-type: none"> • Enter Ordering <input type="text" value="100"/> <p>It is recommended that you use Ordering number 100. This rule must have a lower number than the prerequisite rule.</p>	<p>"Configure Auto-Discovery Rules" (on page 101)</p>

Task	How To
<ul style="list-style-type: none"> Disable <input type="checkbox"/> Discover Included Nodes Disable <input type="checkbox"/> Discover Any SNMP Device Disable <input type="checkbox"/> Discover Non-SNMP Devices <p>Note: This strategy instructs NNMi to "not gather neighbor information " from certain addresses.</p>	
<p>Create one or more IP Ranges settings that identify all addresses from which Auto-Discovery never requests neighbor information.</p> <p>Enter IP Range <input type="text" value="<IPv4 range>"/> (at least one)</p> <p>Set Range Type <input type="text" value="Include in rule"/></p>	<p>"IP Address Ranges for Auto-Discovery" (on page 104)</p>
<p>Create a list of IP addresses that NNMi should never discover.</p>	<p>"Configure an Excluded IP Addresses Filter" (on page 108)</p>

Note: You control how often Spiral Discovery runs by designating the **Rediscovery Interval** setting. See ["Adjust the Discovery Interval" \(on page 98\)](#) for more information.

Exclude Problem IP Addresses from Discovery

If you want Spiral Discovery to never discover certain IP addresses, use these guidelines.

Note: The node and interface associated with any address identified in your Excluded IP Address filter are added to the topology database and maps.

Configuration Steps to Exclude Certain IP Addresses from Spiral Discovery

Task	How To
<p>Create at least one Excluded IP Addresses filter.</p>	<p>"Configure an Excluded IP Addresses Filter" (on page 108)</p>

Note: You control how often Spiral Discovery runs by designating the **Rediscovery Interval** setting. See ["Adjust the Discovery Interval" \(on page 98\)](#) for more information.

Specific System Object IDs Not Discovered

If you want to limit Spiral Discovery to never discover certain device makes/models, use these guidelines. You must be able to identify the devices using SNMP system object IDs.

To implement this strategy, you must create two Auto-Discovery Rules (see prerequisite).

Note: After you set your configuration according to these guidelines, when a new device is added to your network, you do not need to do anything. NNMi discovers or skips devices according to your configuration choices.

Prerequisite: Create an Auto-Discovery Rule that uses IP address ranges to specify the outer limits of your network management domain. See ["Routers and Switches Discovered" \(on page 89\)](#), ["All SNMP Devices Discovered" \(on page 90\)](#) or ["Everything Discovered" \(on page 91\)](#).

Configuration Steps to Exclude Some System Object IDs from Spiral Discovery

Task	How To
<p>Create an Auto-Discovery Rule. Set the following attribute values:</p> <ul style="list-style-type: none"> Enter Ordering <input type="text" value="200"/>. It is recommended that you use Ordering number 200. This rule must have a lower number than the prerequisite rule. Disable <input type="checkbox"/> Discover Included Nodes Disable <input type="checkbox"/> Discover Any SNMP Device Disable <input type="checkbox"/> Discover Non-SNMP Devices <p>Note: This strategy instructs NNMi to "not discover" certain things.</p>	<p>"Configure Auto-Discovery Rules" (on page 101)</p>
<p>Do not include any IP Ranges. When no IP address ranges are defined within an Auto-Discovery Rule, your system object ID ranges take precedence over all Auto-Discovery Rules that have higher Ordering numbers than this Auto-Discovery Rule.</p> <p>Note: NNMi automatically treats any Auto-Discovery Rules without any IP Range as if <input type="checkbox"/> Discover Included Nodes were disabled.</p>	
<p>Create one or more System Object ID Ranges settings. Enter the SNMP sysObjectID that identifies the make/model of the SNMP device that you do not want to discover.</p> <p>Enter System Object ID Prefix <input type="text" value="<sysObjectID>"/></p> <p>Set Range Type <input type="text" value="Include in rule"/></p>	<p>"SNMP System Object ID Ranges for Discovery" (on page 106)</p> <p>Tip: Navigate to the Configuration workspace, and select the Device Profiles view to see all known system object IDs at the time NNMi released.</p>

Note: You control how often Spiral Discovery runs by designating the **Rediscovery Interval** setting. See ["Adjust the Discovery Interval" \(on page 98\)](#) for more information.

Configure Device Profiles

According to industry standards (RFC 1213, MIB II), each combination of vendor, device type, and model number is assigned a unique SNMP system object ID (sysObjectID). For example, all Cisco 6500 series switches have the same sysObjectID prefix: .1.3.6.1.4.1.9.*

HP provides well over three thousand preconfigured Device Profiles, one for each known sysObjectID at the time NNMi released.



NNMi uses Device Profiles (which equate to sysObjectIDs) to control certain types of behavior:

- [Spiral Discovery](#) determines the closest matching device profile, and uses the device profile settings to control certain attribute values for the discovered device. The Device Profile also influences the following:
 - Auto-Discovery Rules can provide a list of sysObjectIDs that expand the default discovery behavior (beyond routers and switches) or prevent troublesome device types from being discovered.

- The Node Name value might be affected, depending on your choices, see "[Configure the Node Name Strategy](#)" (on page 99).
- When Node Groups are defined based on system object IDs, the [State Poller Service](#) monitors devices based on attribute values in the device profiles. Device Profile settings determine how State Poller detects renumbered interfaces.
- In [Map views](#), the background shape of map icons is determined by the Device Category. See [About Map Symbols](#) for an example of each available shape. There is also a [Force Device](#) attribute that enables category overrides in troublesome situations.


Tip: To quickly locate the device profile settings for a particular network device, sort or filter the Device Profiles view by clicking the heading for the Device Vendor, Device Model, or Device Category columns.

To access the device profile definition for a particular device type:

1. Navigate to the **Device Profile** view.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Device Profiles** view.
2. Do one of the following:
 - To create a device profile, click the  New icon.
 - To edit a device profile, select a row, click the  Open icon.
3. Modify the settings as needed:
 - The [basic settings](#) Device Category attribute value modifies NNMi behavior for Spiral Discovery and map symbols.
 - The [advanced settings](#) control NNMi behavior for Spiral Discovery and Node name selection. For example, instruct NNMi to treat a certain device type as a Router.

If you make changes, remember to place your name in the Author attribute. See [Device Profile Author form](#).

Caution: When you make a change, NNMi must update all references to device profiles. This can take some time and slow down your system. Consider making this change during a slow time in your network environment.

4. Click  **Save and Close**. NNMi applies your changes during the next regularly scheduled discovery cycle. To apply the changes immediately, use **Actions** → **Configuration Poll**. See [Using Actions to Perform Tasks](#) for more information.

Configure Discovery


NNMi uses Simple Network Management Protocol (SNMP read-only queries), and a variety of communication protocols to discover the devices within the network management domain that you define. See "[How Spiral Discovery Works](#)" (on page 77) for more information.

By default, NNMi does the following (and you can change these default settings):

- Drops all non-SNMP nodes from discovery.
- Discovers routers and switches.

If you want NNMi to discover non-SNMP devices or more than routers and switches, use Auto-Discovery Rules that configure discovery behavior to meet your needs. Or add the specific devices as discovery seeds.

To configure the NNMi Discovery Process, do the following:

1. Complete all prerequisites. See ["Prerequisites for Discovery" \(on page 86\)](#).
2. Navigate to the **Discovery Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
3. Make your configuration choices (see [table](#)).
4. Click  **Save and Close**. Spiral Discovery implements your changes during the next regularly scheduled [discovery interval](#). To apply the changes immediately, use **Actions** → **Configuration Poll**. See [Using Actions to Perform Tasks](#) for more information.

Discovery Configuration Tasks

Task	How
"Determine Your Approach to Discovery" (on page 88)	<p>Read these guidelines to understand how to configure discovery for the types of devices you want to discover, including the following:</p> <p>For strategies to discover devices:</p> <p>For strategies to prevent specific devices from being discovered:</p>
"Adjust the Discovery Interval" (on page 98)	<i>Optional.</i> Use the Discovery Configuration workspace to modify the global discovery interval setting. The Global Control setting for Rediscovery Interval controls the frequency that NNMi uses for network discovery traffic.
"Configure Ping Sweep Global Settings" (on page 98)	<i>Optional.</i> Use the Discovery Configuration workspace to configure the starting points for Auto-Discovery. The choices are Discovery Seeds or Ping Sweep within Auto-Discovery Rules (ICMP ping commands) or both. The Global Control settings for Spiral Discovery Ping Sweep Control provide control across all Auto-Discovery Rules.
"Configure the Node Name Strategy" (on page 99)	<i>Optional.</i> Use the Discovery Configuration workspace to specify a node naming strategy. The Global Control settings for Node Name enable you to choose the most meaningful name for devices in your environment.
"Configure Auto-Discovery Rules" (on page 101)	<i>Optional.</i> Use the Auto-Discovery Rules tab to specify any IP address ranges or MIB II sysObjectID ranges (or both) that you want NNMi to use for automatic discovery. Within each Rule you can specify whether Ping Sweep is used as a starting point (in addition to or instead of discovery seeds).
"Configure an Excluded IP Addresses Filter" (on page 108)	<i>Optional.</i> Use the Excluded IP Addresses tab to provide a list of specific addresses or ranges of addresses that you want NNMi to never discover or monitor.
"Configure Subnet Connection Rules" (on page 109)	<i>Optional.</i> Use the Subnet Connection Rules tab to connect interfaces on devices that <i>do not respond</i> to Layer 2 Discovery protocols (for example, WAN edge devices).
"Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered" (on page 112)	<p><i>Optional.</i> Use the Discovery Seeds tab to specify nodes to be discovered or to indicate which nodes are used as starting points for your Auto-Discovery Rules.</p> <p>Tip: Use the Discovery Seeds tab to verify that NNMi successfully located each Discovery Seed that you provided. See "Discovery Seed Results" (on page 118).</p>

Task	How
------	-----

Adjust the Discovery Interval

When configuring Spiral Discovery, you determine how often network traffic is generated to gather and verify information about your network management domain. This time interval controls how frequently information is gathered about nodes, interfaces, IP addresses, subnets, VLANs, and connections in the network. See ["Discovery Intervals" \(on page 79\)](#) for more information.

To adjust the discovery cycle interval:

1. Navigate to the **Discovery Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
2. Locate the **Global Control** settings.
3. In the **Rediscovery Interval** attribute, set the time interval that Spiral Discovery waits between information gathering cycles.

The default is 24 hours between cycles. The minimum is 1 hour.

Make sure that you allow plenty of time for the interval so that Spiral Discovery cycles do not overlap. The larger your network environment, the longer the time required to complete a Spiral Discovery cycle.

4. Click  **Save and Close** to apply your changes.

Configure Ping Sweep Global Settings

You have two choices for Auto-Discovery starting points. Use either or both to best advantage in your network environment:

- **Discovery Seeds:** You designate specific IP addresses or hostnames where Auto-Discovery starts gathering neighbor information.

For details see ["Discovery Seeds \(as a starting point\)" \(on page 82\)](#). For information about creating Discovery Seeds, see ["Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered" \(on page 112\)](#).

- **Ping Sweep:** NNMi issues ICMP pings to certain addresses to find new nodes. For details, see ["Ping Sweep \(as a starting point\)" \(on page 82\)](#).

Ping Sweep uses the current default ICMP interval and timeout settings from the Communications Configuration settings. See ["Configure Default SNMP and ICMP Protocol Settings" \(on page 47\)](#).

To configure the global Auto-Discovery setting for Ping Sweep:

1. Navigate to the **Discovery Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
2. Navigate to the **Global Control** settings.
3. Designate the global setting for **Ping Sweep**. Your choice determines how Spiral Discovery uses


ICMP ping commands for the discovery process in your network environment:

- **Each Rule (as configured)**— The instructions for Ping Sweep within each Auto-Discovery Rule configuration are followed exactly.

To configure Ping Sweep for a specific Auto-Discovery Rule, see "[IP Address Ranges for Auto-Discovery](#)" (on page 104).

- **All Rules**— Ping Sweep is applied for all of your current Auto-Discovery Rules. This overrides the Ping Sweep settings within each rule.
- **None of the Rules**— Ping Sweep is not used for any of your current Auto-Discovery Rules. This overrides the Ping Sweep settings within each rule. This is useful to temporarily suspend issuing any ping commands within your network.

Note: If things don't work as expected, check whether ICMP is allowed (see if "[Communication Region Form](#)" (on page 57)).

4. Designate the **Sweep Interval** (days/hours) that controls how often Spiral Discovery reissues ICMP Ping for each address.
5. Click  **Save and Close**. Spiral Discovery implements your changes during the next regularly scheduled [discovery interval](#).

Configure the Node Name Strategy

When configuring discovery in NNMi, you control how the Name attribute on the Node form is populated. For details see "[Discovery Node Name Choices](#)" (on page 79).

To resolve issues about choosing the Name value, NNMi follows a sequence of rules. If NNMi is unable to determine a Name based on your three choices, the node name is determined using the NNMi factory defaults for these three choices (see list in step 3).

The node Name shows up beneath the node symbol on the maps and in the Name column on table views.

To control how node names are determined for your network devices:

1. Navigate to the **Discovery Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
2. Locate the **Node Name Resolution** attributes on the left side of the form (see [table](#)).
3. Specify the three-level hierarchy for node naming decisions.

Short name and full name are related. The short name is everything before the first period in the full name. For example, full name `cisco5500.abc.xyz.com` and the short name `cisco5500`.

Select among the following choices. Use each choice only one time:

- **Short DNS Name** – (*first by default*) Use the group of characters prior to the first period in your in-house DNS naming standards.

If a device has multiple hostnames or no hostname, NNMi follows a set of rules to determine the hostname. Click here for details.


- i. If a hostname is available, it must resolve to a valid IP address. NNMi stores the fully-qualifiedhostname in the database as all lowercase characters.

- ii. If more than one address is associated with a node, the **loopback address**¹ is used with the following exceptions:
 - o NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).
 - o NNMi ignores any address that is virtual (HSRP/VRRP) or an **Anycast Rendezvous Point IP Address**².
- iii. If a node has multiple loopback addresses, NNMi uses the loopback address with the lowest number that resolves to a hostname (for example, 10.16.42.197 is a lower number than 10.16.197.42).
- iv. If no loopback address resolves to a hostname and the device supports SNMP, NNMi uses the current value from the Management Address attribute on the Node form.
- v. If the device does not support SNMP, the IP address or DNS name found during the current rediscovery cycle is used as the hostname.

This sequence is repeated during each rediscovery cycle. The hostname could change from cycle to cycle (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).

- **Fully Qualified DNS Name** – Use the full in-house DNS naming standards.
- **Short sysName** – (*second by default*) Use the group of characters prior to the first period in the current MIB II sysName value established by the administrator for each SNMP enabled device. See ["Discovery Node Name Choices" \(on page 79\)](#) for possible issues with using sysName.
- **Full sysName** – Use the full current MIB II sysName value established by the administrator for each SNMP enabled device.
- **IP Address** – (*third by default*) Use the IP address. If the node responds to SNMP, the SNMP Management Address is used. For non-SNMP nodes, name is set to either a discovery seed address associated with this node or a neighbor address gathered by Spiral Discovery along the path to this node.

Note: If you listed the address in your Excluded IP Address filter, Spiral Discovery skips that address. See ["Exclude Problem IP Addresses from Discovery" \(on page 94\)](#).

4. Click  **Save and Close**. Spiral Discovery implements your changes during the next regularly scheduled [discovery interval](#). To apply the changes immediately, use **Actions** → **Configuration Poll**. See [Using Actions to Perform Tasks](#) for more information.

Node Name Resolution Settings

Attribute	Description
First Choice	Click the drop-down list and choose the predefined node name strategy you want discovery to use first.

¹The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

²Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

Attribute	Description
Second Choice	Click the drop-down list and choose the predefined node name strategy you want discovery to use if the first choice fails.
Third Choice	Click the drop-down list and choose the predefined node name strategy you want discovery to use if the second choice fails.

Configure Auto-Discovery Rules


Auto-Discovery Rule configuration settings control Spiral Discovery behavior (for details see ["Auto-Discovery Rules" \(on page 83\)](#)):

- Rules define the outer limits of discovery.
- Rules expand or reduce the types of devices that are discovered and added to the topology database.

Before you start, have a clear idea of what you want to accomplish, see ["Determine Your Approach to Discovery" \(on page 88\)](#).

If you do not configure any Auto-Discovery Rules, Spiral Discovery is limited to only discovery seeds. See ["Discovery Seeds \(as a starting point\)" \(on page 82\)](#) for more information.

To configure Auto-Discovery Rules, do the following:

1. Complete all prerequisites. See ["Prerequisites for Discovery" \(on page 86\)](#).
2. Navigate to the **Auto-Discovery Rules** tab.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
 - c. Select the **Auto-Discovery Rules** tab.
3. Make your configuration choices (see [table](#)).
4. Click  **Save and Close**. Spiral Discovery implements your changes during the next regularly scheduled [discovery interval](#). To apply the changes immediately, use **Actions** → **Configuration Poll**. See [Using Actions to Perform Tasks](#) for more information.




Auto-Discovery Rule Configuration Tasks

Task	How
"Configure Basic Settings for the Auto-Discovery Rule" (on page 102)	Provide the basic requirements for an Auto-Discovery Rule configuration. This includes name and Ordering number. You designate how ICMP and SNMP are used for this segment of discovery.
"IP Address Ranges for Auto-Discovery" (on page 104)	<i>Optional.</i> Use IP addresses with wildcards to specify the area you want Spiral Discovery to find in your network environment. You decide whether Ping Sweep is used for this segment of discovery.
"SNMP System Object ID Ranges for Discovery" (on page 106)	<i>Optional.</i> Use industry standard System Object IDs to control Spiral Discovery: <ul style="list-style-type: none"> • Expand Spiral Discovery to include more device types than the default routers and switches . • Instruct Spiral Discovery to never discover specific troublesome models of routers, switches, or other devices.



Configure Basic Settings for the Auto-Discovery Rule

The Auto-Discovery Rule settings determine which methods Spiral Discovery applies when discovering the part of your network defined in the rule.

To configure this Auto-Discovery Rule:

1. Navigate to the **Auto-Discovery Rule** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
 - c. Locate the **Auto-Discovery Rules** tab.
 - d. Do one of the following:
 - To establish a rule, click the  New icon, and continue.
 - To edit a rule, select a row, click the  Open icon, and continue.
 - To delete a rule, select a row, and click the  Delete icon.
2. Provide the required basic settings (see the [Basics for this Auto-Discovery Rule](#) table).
3. Provide the behavior settings for this rule (see the [Auto-Discovery Behavior for this Rule](#) table).
4. There are many ways to implement discovery. Before you start this step, "[Determine Your Approach to Discovery](#)" (on page 88).

Configure one or more ranges, to identify the devices you want to discover.

- "[IP Address Ranges for Auto-Discovery](#)" (on page 104)
 - "[SNMP System Object ID Ranges for Discovery](#)" (on page 106)
5. Click  **Save and Close** to return to the **Discovery Configuration** form.
 6. Click  **Save and Close**. Spiral Discovery implements your changes during the next regularly scheduled [discovery interval](#).
 7. *Optional:* Open the **Discovery Configuration** workspace again and provide a discovery seed for each address range of this region. Core routers make the best seeds. See "[Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered](#)" (on page 112).

Basics for this Auto-Discovery Rule

Task	How
Name	Give this Auto-Discovery Rule a meaningful name.
Ordering	<p>Determine the order in which the Auto-Discovery Rules are applied. No Duplicate Ordering numbers are allowed. Each Auto-Discovery Rule ordering number must be unique.</p> <p>Tip: It is recommended that ordering numbers are incremented by 10s or 100s to provide flexibility when adding new rules over time.</p> <p>IP address ranges: If a device falls within two Auto-Discovery Rules, the Auto-Discovery Rule with the lowest ordering number applies. For example, if an Auto-Discovery Rule includes certain IP addresses, then no other Auto-Discovery Rules with higher ordering numbers apply to those addresses.</p> <p>System Object ID ranges:</p>

Task	How
	<ul style="list-style-type: none"> If no IP address range is included in this Auto-Discovery Rule, then the system object ID settings take precedence over all Auto-Discovery Rules that have higher Ordering numbers than this Auto-Discovery Rule. If an IP address range is included in this Auto-Discovery Rule, your system object ID range applies only within this Auto-Discovery Rule.
Notes	<p>Provide any additional useful information about this Auto-Discovery Rule.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p>

Auto-Discovery Behavior for this Rule

Task	How
Discover Included Nodes	<p>If <input checked="" type="checkbox"/> enabled, Auto-Discovery gathers information about neighboring devices and adds devices to the NNMi database if they meet the rule's criteria. For more information see "Auto-Discovery Rules" (on page 83).</p> <p>Note: Auto-Discovery requires at least one IP address range with the Range Type attribute set to Include. Routers and switches are discovered by default. If enabled, Discover Any SNMP Device and Discover Non-SNMP Devices extend discovery to more than routers and switches.</p> <p>If <input type="checkbox"/> disabled, Auto-Discovery ignores devices in this rule unless those devices are specifically identified in the discovery seeds configuration settings.</p>
Enable Ping Sweep	<p>If <input checked="" type="checkbox"/> enabled, Auto-Discovery issues a wide range of ICMP ping commands to determine starting points for Spiral Discovery. For details, see "Ping Sweep (as a starting point)" (on page 82).</p> <p>If <input type="checkbox"/> disabled, Auto-Discovery depends on Discovery Seeds as starting points for Spiral Discovery. For details, see "Discovery Seeds (as a starting point)" (on page 82).</p>
Discover Any SNMP Device	<p>Note: This value is ignored if Discover Included Nodes is unchecked. However, if you configure any device as a discovery seed, discovery always adds that device to the database.</p> <p>If <input checked="" type="checkbox"/> enabled, discovery gathers information about any device that responds to SNMP queries (in addition to routers or switches that are discovered by default). These nodes appear on maps and are monitored.</p> <p>If <input type="checkbox"/> disabled, discovery ignores all device types except routers, switches, discovery seeds, and device types specified in your system object ID ranges. (Routers and switches are identified by the settings in the device profile.)</p>
Discover Non-SNMP Devices	<p>Note: This value is ignored if Discover Included Nodes is unchecked. However, if you configure any device as a discovery seed, discovery always adds that device to the database.</p> <p>Non-SNMP devices are those that do not respond to SNMP queries.</p> <p>If you enable Discover Non-SNMP Devices, note the following:</p> <ul style="list-style-type: none"> If you do not want NNMi to discover every node in your network, make sure your Auto-Discovery Rules correctly limit the scope of the discovery. See "Determine Your Approach to Discovery" (on page 88) for more information.

Task	How
	<ul style="list-style-type: none">• Selecting this option may cause you to reach your license limit very quickly.• If NNMi determines that a non-SNMP node has a hostname matching another non-SNMP node, NNMi merges the information to create only one node and includes any additional IP address information under the same node. <p>Non-SNMP nodes might be inaccurately represented under the following circumstances:</p> <ul style="list-style-type: none">▪ One or more non-SNMP nodes in your network use the same hostname.▪ The same non-SNMP node has multiple hostnames.▪ A non-SNMP node name changes (see "Delete Nodes" (on page 122)). <p>If <input checked="" type="checkbox"/> enabled, addresses that do not respond to SNMP queries are added to the database.</p> <p>If <input type="checkbox"/> disabled, discovery ignores any address that does not respond to SNMP queries.</p>

IP Address Ranges for Auto-Discovery

Auto-Discovery IP address ranges determine the outer limits for the area controlled by the current Auto-Discovery Rule. You can create multiple IP ranges within one Auto-Discovery Rule. Before you start, have a clear idea of what you want to accomplish, see ["Determine Your Approach to Discovery" \(on page 88\)](#).

If **Discover Included Nodes** is disabled for the rule, click here for additional information about IP address ranges when defining a rule with Discover Included Nodes disabled.

- Spiral Discovery *does not gather neighbor information* from the addresses identified in any IP address range included in this rule. The addresses, themselves, may still show up in the topology database.

Note: Neighbor information is still gathered from IP addresses specifically identified in the [discovery seeds](#) configuration settings.

- IP address ranges are optional. However, when no IP address range is provided:
 - One or more system object ID (MIB II sysObjectIDs) ranges must be defined. This technique constricts or extends the types of devices affected by this rule. See ["SNMP System Object ID Ranges for Discovery" \(on page 106\)](#) for more information.
 - The system object ID range criteria applies to all Discovery Rules with higher Ordering numbers.






If **Discover Included Nodes** is enabled for the rule, click here for additional information about IP address ranges when defining a rule with Discover Included Nodes enabled.

- At least one IP address range is required to be designated as an **Include in rule** range type. Auto-Discovery *gathers neighbor information* from those addresses to extend discovery.
- *Optional.* You can configure NNMi to ignore subsets of those IP addresses (an **Ignored by rule** range, which means that those addresses are available for other Auto-Discovery Rules).
- *Optional.* Specify system object ID (MIB II sysObjectIDs) ranges to be included or ignored. This technique constricts or extends the types of devices affected by this rule. See ["SNMP System Object ID Ranges for Discovery" \(on page 106\)](#) for more information.




NNMi discovers any devices that comply with your rule configurations, and creates a record of each device in the NNMi database. If the device supports SNMP, all addresses for that device are combined into one Node object. If the device does not support SNMP, NNMi queries DNS to determine the hostname. If this

hostname matches another non-SNMP node, NNMi merges the information to create only one node with multiple associated addresses.

To specify an IP address range:

1. Navigate to the **Auto-Discovery IP Range** form.
 - a. In the **Workspace** navigation panel, open the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
 - c. Select the **Auto-Discovery Rule** tab.
 - d. Do one of the following:
 - To establish an Auto-Discovery Rule, click the  New icon.
 - To edit an Auto-Discovery Rule, select a row, and click the  Open icon.
 - a. Select the **IP Ranges** tab.
 - b. Do one of the following:
 - To create an IP range, click the  New icon, and continue.
 - To edit an IP range, select a row, and click the  Open icon, and continue.
 - To delete an IP range, select a row, and click the  Delete icon.
2. Decide whether Ping Sweep is used in this segment of network discovery:
 - **Enable Ping Sweep**
Auto-Discovery issues a wide range of ICMP ping commands to determine starting points for Spiral Discovery. For details, see ["Ping Sweep \(as a starting point\)" \(on page 82\)](#).
 - **Enable Ping Sweep**
Auto-Discovery depends on Discovery Seeds as starting points for Spiral Discovery. For details, see ["Discovery Seeds \(as a starting point\)" \(on page 82\)](#).

Note: There are two ways to override this choice. If things don't work as expected, check whether Ping Sweep is disabled (see ["Configure Ping Sweep Global Settings" \(on page 98\)](#)) and check whether ICMP is allowed (see if ["Communication Region Form" \(on page 57\)](#)).
3. Provide the IP address range information for this Auto-Discovery Rule (see [table](#)).

Note: If you choose to not include any IP address ranges in a particular Auto-Discovery Rule, then you must provide at least one system object ID range (see ["SNMP System Object ID Ranges for Discovery" \(on page 106\)](#)). And Auto-Discovery Rules without any IP Range must have **Discover Included Nodes** disabled in the Auto-Discovery Rule form.
4. Click  **Save and Close** to return to the **Auto-Discovery Rule** form.
5. Click  **Save and Close** to return to the **Discovery Configuration** form.
6. Click  **Save and Close**. Spiral Discovery implements your changes during the next regularly scheduled [discovery interval](#).

Discovery IP Range Form

Name	Description
IP Range	<p>Used to specify a range of IP addresses for this Auto-Discovery Rule.</p> <p>Note: If you enter an IP address value that represents only one IP address, Auto-Discovery gathers neighbor information only from the address you enter. (Discovery extends only one hop out from this address.)</p> <p>An IPv4 Address range is a modified dotted-notation where each octet is one of the following:</p> <ul style="list-style-type: none">• A specific octet value between 0 and 255• A low-high range specification for the octet value (for example, "112-119")• An asterisk (*) wildcard character which is equivalent to the range expression "0-255" <p>Note: The following two IPv4 addresses are considered invalid: 0.0.0.0 and 127.0.0.0</p> <p>Examples of valid IPv4 address wildcards include:</p> <pre>10.1.1.* 10.*.*.* 10.1.1.1-99 10.10.50-55.* 10.22.*.4 10.1-9.1-9.1-9</pre> <p>Caution: If Ping Sweep is enabled for this rule (see step 2 above), NNMi only uses Ping Sweep across a maximum of the last two octets (/16) of the network specified by each IP Range.</p>
Range Type	<p>Include in rule - The current Auto-Discovery Rule settings apply to the addresses in this range.</p> <p>Ignored by rule - The current Auto-Discovery Rule settings do not apply to the addresses in this range. Use the Ignored by rule setting to identify a subset of addresses within a larger range. The addresses in the ignored range are available to conform to an Auto-Discovery Rule with a higher ordering number.</p>

SNMP System Object ID Ranges for Discovery

Vendors are assigned a system object ID (RFC 1213 MIB II sysObjectID) for each type of network device that they manufacture. This system object ID number is unique for each combination of vendor, device type, and model number. For example, all Cisco 6509 routers have the same system object ID.

Tip: See "[Configure Device Profiles](#)" (on page 95) for more information about system object IDs. In the Device Profiles view (in the **Configuration** workspace), you can quickly and easily locate the system object IDs of devices in your network environment.

System object ID ranges are powerful tools for expanding or limiting discovery behavior. For example, expand discovery to include more than the default routers and switches, or limit discovery by excluding specific models of routers and switches. Before you start, have a clear idea of what you want to accomplish, see "[Determine Your Approach to Discovery](#)" (on page 88).

When using system object ID ranges, note the following:

- When one or more IP address ranges are defined within the Auto-Discovery Rule, your system object ID ranges apply only within the current Auto-Discovery Rule.






- When no IP address ranges are defined within the Auto-Discovery Rule, your system object ID ranges take precedence over all Auto-Discovery Rules that have higher Ordering numbers than this Auto-Discovery Rule.
- To enable Discover Included Nodes in this rule, at least one IP address range is required. Before any discovered node is added to the topology database, it must match both IP address range and system object ID range specifications.

The following table includes examples of how you might want to expand or limit your Spiral Discovery scope using System Object ID Ranges.

Controlling Spiral Discovery with System Object ID Ranges

Task	Related Topics
Expand Spiral Discovery to include device types in addition to routers and switches.	"All Devices from a Specific Vendor Discovered" (on page 92)
Globally exclude one or more specific device types from Spiral Discovery.	"Specific System Object IDs Not Discovered" (on page 94)

To specify a system object ID range:

1. Navigate to the **Discovery System Object ID Range** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
 - c. Select the **Auto-Discovery Rule** tab.
 - d. Do one of the following:
 - To create an Auto-Discovery Rule, click the  New icon.
 - To edit an Auto-Discovery Rule, click the  Open icon.
 - e. In the **Auto-Discovery Rule** form, select the **System Object ID Ranges** tab.
 - f. Do one of the following:
 - To create a system object ID range, click the  New icon, and continue.
 - To edit a system object ID range, click the  Open icon, and continue.
 - To delete a system object ID range, click the  Delete icon.
2. Provide one or more System Object ID ranges for this Auto-Discovery Rule (see the [table](#)).

Use multiple System Object ID ranges to fine tune your discovery settings.

Note: If you do not include any System Object ID ranges in a particular Auto-Discovery Rule, then you must provide at least one IP address range in that particular Auto-Discovery Rule (see ["IP Address Ranges for Auto-Discovery" \(on page 104\)](#)).


Example 1. In an Auto-Discovery Rule with Discover Included Nodes enabled:

- Create a definition that includes all HP devices. Use the System Object ID prefix 1.3.6.1.4.1.11 and set the Range Type to *Include in rule*.

- Create a definition that excludes any HP Printers. Use the System Object ID prefix 1.3.6.1.4.1.11.2.3.9 and set the Range Type to *Ignored by rule*. (Order does not matter, now the printers are always ignored.)


Example 2. In an Auto-Discovery Rule with Discover Included Nodes disabled:


- Create a definition that excludes any HP Printers. Use the System Object ID prefix 1.3.6.1.4.1.11.2.3.9 and set the Range Type to *Include in rule*.
- Skip step 4, below. HP printers are not discovered within the IP address range of any Auto-Discovery Rules with higher ordering numbers than this rule.


3. Click  **Save and Close** to return to the **Auto-Discovery Rule** form.

4. Provide any IP ranges (see ["IP Address Ranges for Auto-Discovery" \(on page 104\)](#)):

- Optional if Discover Included Nodes is disabled in the Auto-Discovery Rule form.
- Required if Discover Included Nodes is enabled in the Auto-Discovery Rule form.

Click  **Save and Close** to return to the **Auto-Discovery Rule** form.

5. Click  **Save and Close** to return to the **Discovery Configuration** form.

6. Click  **Save and Close**. Spiral Discovery implements your changes during the next regularly scheduled [discovery interval](#).

Discovery System Object ID Range Definition





Attribute	Description
System Object ID Prefix	<p>Enter a prefix of an SNMP system object ID, or enter the entire SNMP system object ID. A partial entry becomes a wildcard.</p> <p>For example, if you enter 1.3.6.1.4.1.11, discovery finds all HP devices. If you enter 1.3.6.1.4.1.9, discovery finds all Cisco devices.</p> <p>Note: Do not use dashes or asterisks (*) in your system object ID value.</p>
Range Type	<p>Include in rule - Instructs Auto-Discovery to find devices matching this system object ID range.</p> <p>Ignored by rule - Instructs Auto-Discovery to ignore devices matching this system object ID range.</p>
Notes	<p>Add any information about this rule that would be useful to you and your team.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p>

Configure an Excluded IP Addresses Filter

Sometimes there are IP addresses or ranges of IP addresses in your environment that you do not want NNMi to discover or monitor. For details and examples, see ["Filters to Exclude Certain IP Addresses" \(on page 83\)](#).

Tip: If you have a large number of IP addresses that you want to exclude from Spiral Discovery, see the [nnmdiscocfg.ovpl](#) Reference Page.

To excluded specific IP addresses from the discovery process:

1. Navigate to the **Excluded IP Address** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
 - c. Select the **Excluded IP Addresses** tab.
 - d. Do one of the following:
 - To exclude an address or range of addresses from Spiral Discovery, click the  New icon, and continue.
 - To edit an excluded address setting, click the  Open icon, and continue.
 - To delete an excluded address setting, select a row, and click the  Delete icon.
2. In the **IP Address Range** field, type an IP address or range of addresses. For example, 27-29.*.*.*
Maximum 255 characters.
The following wildcard characters are allowed:
 - Asterisk (*) represents any string
 - Question mark (?) represents a single character
3. Click  **Save and Close**. Spiral Discovery implements your changes during the next regularly scheduled [discovery interval](#). To apply the changes immediately, use **Actions** → **Configuration Poll**. See [Using Actions to Perform Tasks](#) for more information.

Configure Subnet Connection Rules

For an explanation of how Subnet Connection Rules work, see "[Subnet Connection Rules](#)" (on page 84).

If important subnets in your network environment are not automatically connected by Spiral Discovery, edit a Subnet Connection Rule or create your own.






The following are typical situations that require Subnet Connection Rules:

- Point-to-point or point-to-multipoint connections between interfaces within subnets that have a prefix length ranging from 28-31.
- Tunnel or other virtual connections between interfaces within subnets that have a prefix length ranging from 28-31.

NNMi uses Subnet Connection Rules to detect connections between interfaces associated with IPv4 addresses that *do not respond* to Layer 2 Discovery protocols (see the list of Topology Source protocols in [Layer 2 Connection Form](#)). Subnet Connection Rules take priority over the Layer 2 Discovery protocol results. For special cases, you can override a Subnet Connection Rule by using the Connection Editor command line tool, see the [nnmconnedit.ovpl](#) Reference Page for more information.

When Spiral Discovery detects a subnet, NNMi uses the matching Subnet Connection Rule to request information about all possible IPv4 addresses (potentially detecting previously undiscovered IPv4 addresses). NNMi checks the Excluded IP Addresses list. Any addresses in the list are dropped (for details, see "[Filters to Exclude Certain IP Addresses](#)" (on page 83)). Then NNMi creates connections among any interfaces associated with any newly discovered IPv4 addresses.

To configure Subnet Connection Rules:

1. Navigate to the **Subnet Connection Rule** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
 - c. Select the **Subnet Connection Rules** tab.
 - d. Do one of the following:
 - To establish a rule, click the  New icon, and continue.
 - To edit a rule, click the  Open icon, and continue.
 - To delete a rule, select a row, and click the  Delete icon.
2. Provide the required basic settings ([see Basics table](#)).
3. Provide the Subnet Connection behavior settings for this rule ([see Details table](#)).
4. Click  **Save and Close** to return to the **Discovery Configuration** form.
5. Click  **Save and Close** to apply the configuration. Spiral Discovery implements your changes during the next regularly scheduled [discovery interval](#).

Basics for this Subnet Connection Rule

Task	How
Name	Type a meaningful name for this Subnet Connection Rule. Note: This name is prepended to the Layer 2 connection name (when you request Quick View information about the connection on the Layer 2 Neighbor View map). If a subnet matches more than one rule, NNMi randomly chooses from among the matching rules.
Enable	If enabled <input checked="" type="checkbox"/> , NNMi uses the Subnet Connection Rule to create connections between interfaces associated with the IPv4 addresses within the specified subnets. If disabled <input type="checkbox"/> , NNMi ignores the Subnet Connection Rule.

Details for this Subnet Connection Rule

Task	How										
Minimum IPv4 Prefix Length	<p>Specify the minimum prefix length (subnet mask length) for the subnet where you want Spiral Discovery to create Layer 2 connections. Spiral Discovery creates connections between interfaces associated with IPv4 addresses that have subnet prefix lengths equal to or greater than the specified value and meet the other specified criteria.</p> <table border="1"> <thead> <tr> <th>Valid Minimum IPv4 Prefix Length Values</th> <th>Number of Usable IPv4 Addresses</th> </tr> </thead> <tbody> <tr> <td>28</td> <td>14 (16-2=14)*</td> </tr> <tr> <td>29</td> <td>6 (8-2=6)*</td> </tr> <tr> <td>30</td> <td>2 (4-2=2)*</td> </tr> <tr> <td>31</td> <td>2</td> </tr> </tbody> </table> <p>* Two IPv4 addresses are reserved in each subnet. The first IPv4 address is used for the network itself and the last IPv4 address is reserved for broadcast.</p>	Valid Minimum IPv4 Prefix Length Values	Number of Usable IPv4 Addresses	28	14 (16-2=14)*	29	6 (8-2=6)*	30	2 (4-2=2)*	31	2
Valid Minimum IPv4 Prefix Length Values	Number of Usable IPv4 Addresses										
28	14 (16-2=14)*										
29	6 (8-2=6)*										
30	2 (4-2=2)*										
31	2										
IfType	<p><i>Optional.</i> Use this Interface MIB variable as an additional filter to identify the types of interfaces to include when creating the subnet connections. For example, if you want connections only between frameRelay interfaces, select <code>frameRelay</code> as the IfType.</p>										
IfName	<p><i>Optional.</i> Use this Interface MIB variable as an additional filter to identify the interfaces to include when creating the subnet connections. This attribute is useful if you have a naming convention that is used to identify a set of interfaces. For example, <code>lan0</code>.</p> <p>Maximum 255 characters. The following wildcard characters are allowed: asterisk (*) represents any string, and question mark (?) represents a single character.</p>										
IfDescription	<p><i>Optional.</i> Use this Interface MIB variable as an additional filter to identify the interfaces to include when creating the subnet connections. For example, you might want to select a particular set of interfaces that have the same vendor description.</p> <p>Maximum 255 characters. The following wildcard characters are allowed: asterisk (*) represents any string, and question mark (?) represents a single character.</p>										
IfAlias	<p><i>Optional.</i> Use this Interface MIB variable as an additional filter to identify the interfaces to include when creating the subnet connections. This attribute is useful if you have an alias naming convention that is used to identify a set of interfaces. For example, <code>Connection to remote store in Hawaii</code>.</p> <p>Maximum 255 characters. The following wildcard characters are allowed: asterisk (*) represents any string, and question mark (?) represents a single character.</p>										

Related Topics

[Interpret Root Cause Messages](#)

Subnet Connection Rules Provided by NNMi

NNMi provides the Subnet Connection Rules described in the following table (for more information, see "[Subnet Connection Rules](#)" (on page 84)).

The *Small Subnets* Rule ensures that NNMi detects IPv4 addresses within subnets of this size, regardless of the interface type. The remaining Subnet Connection Rules create connections based on interface type and the specified subnet size.

Tip: See [IfTypes \(Interface Types\) Form](#) for more information about interface types.

To create new Subnet Connection Rules (or modify the ones provided), see "[Configure Subnet Connection Rules](#)" (on page 109).

Subnet Connection Rules Provided by NNMi

Rule Name	Minimum IPv4 Prefix Length (Subnet Mask Length)	Interface Type (#)
Asynchronous Transfer Mode	28	atm (37)
Digital Signal 0	28	ds0 (81)
Digital Signal 1	28	ds1 (18)
Digital Signal 3	28	ds3 (30)
Digital Subscriber Loop over ISDN	28	idsl (154)
Frame Relay Interfaces	28	frameRelay (32)
Integrated Services Digital Network	28	isdn (63)
Multiprotocol Label Switching	28	mpls (166)
Point to Point	28	ppp (23)
Small Subnets	30	
Serial Line Internet Protocol	28	slip (28)
Serial Point to Point	28	propPointToPointSerial (22)
Synchronous Optical Networking	28	sonnet (39)

Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered

Note: Discovery seeds are optional. Before you start this task, "[Determine Your Approach to Discovery](#)" (on page 88) and complete the prerequisites ("[Prerequisites for Discovery](#)" (on page 86)).

Nodes specified as discovery seeds are always discovered and added to the topology database. As soon as you enter one or more optional discovery seeds, discovery begins.

If you create Auto-Discovery Rules, NNMi uses neighbor information gathered from each discovery seed to extend discovery. See "[Discovery Seeds \(as a starting point\)](#)" (on page 82) for more information. NNMi can also use Ping Sweep (instead of or in addition to discovery seeds) to gather neighbor information. See "[Ping Sweep \(as a starting point\)](#)" (on page 82).

If you want Spiral Discovery to automatically find devices on your network, before you begin adding discovery seeds:

- Configure at least one Auto-Discovery Rule. See "[Configure Auto-Discovery Rules](#)" (on page 101).
- Configure any number of Auto-Discovery Rules to maintain fine control over the scope of Spiral Discovery.

A discovery seed is an IP address or hostname. Consider devices with the largest neighbor data in your network environment. For example, a good choice would be a core router connected to a network you want to discover.

If you change your mind and delete a discovery seed from Discovery Configuration, the corresponding node is not deleted from the topology database. See ["Delete Nodes" \(on page 122\)](#) for information about removing the entire node record from the topology database.

To configure discovery seeds do one or more of the following:

- ["In the Console, Configure Discovery Seeds" \(on page 113\)](#)
- ["With a Seed File, Add Multiple Discovery Seeds" \(on page 114\)](#)
- ["From the Command Line, Add Discovery Seeds" \(on page 115\)](#)

Related Topics




["Discovery Seed Results" \(on page 118\)](#)

["Delete Discovery Seeds" \(on page 123\)](#)

In the Console, Configure Discovery Seeds

There are many ways to provide discovery seeds. Discovery seeds are optional. See ["Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered" \(on page 112\)](#) for more information.

To add an optional discovery seed using the console:

1. Navigate to the **Discovery Seeds** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
 - c. Locate the **Discovery Seeds** tab.
 - d. Do one of the following:
 - To add a discovery seed, click the  New icon.
 - To edit a discovery seed, click the  Open icon the precedes the discovery seed you want to edit.
 - To delete a discovery seed, select a row, and click the  Delete icon (see ["Delete Discovery Seeds" \(on page 123\)](#) and ["Delete Nodes" \(on page 122\)](#) for more information).


2. Provide appropriate information (see [table](#)).


NNMi uses information gathered from Routers to establish subnet membership for Layer 3 connections. Make sure that important Routers in your network environment are SNMP enabled.


NNMi uses either of the following criteria to identify a Router:

- Each Router responds with appropriate values for sysServices (1.3.6.1.2.1.1.7) and ipForwarding (1.3.6.1.2.1.4.1). See RFC1213-MIB for details.
- Identify Routers with the [Device Profile configuration settings](#) for a particular device type.

You must provide the appropriate SNMP Community Strings to NNMi. See ["Configuring Communication Protocol" \(on page 47\)](#).

3. Click  **Save and Close** to return to the Discovery Configuration form.

Tip: Click the  Save and New icon to continue to adding discovery seeds.

4. Click  **Save and Close**. As soon as you enter one or more optional discovery seeds, discovery begins.

Discovery Seed Definition

Attribute	Definition
Hostname / IP	<p>Note: NNMi does not validate your entry when you use this method to add discovery seeds. Use the nnmloadseeds.ovpl command to validate your discovery seed entries.</p> <p>To identify the node, enter one of the following:</p> <ul style="list-style-type: none">• Fully-qualified hostname of the discovery seed• IP address of the discovery seed, specify a physical address <p>When providing IPv4 addresses as discovery seeds, the following IPv4 addresses are considered invalid:</p> <ul style="list-style-type: none">• 255.255.255.255• IP addresses that begin or end with 0 (zero)
Discovery Seed Results	An automatically generated value. The most recent discovery status for this discovery seed. See "Discovery Seed Results" (on page 118) for details.
Last Modified	The date and time of the last change in Discovery Seed Results.
Notes	<p>Provide any additional information about this discovery seed that would be useful to you or your team.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p>

With a Seed File, Add Multiple Discovery Seeds

There are many ways to provide discovery seeds. Discovery seeds are optional. See ["Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered" \(on page 112\)](#) for more information.

Use a seed file to simultaneously add large numbers of discovery seeds. Your seed file contains one line for each discovery seed. For example:

```
12.2.111.104# cisco5500
12.2.112.268# cisco6509
12.2.119.205# cisco5500
```

Note: Any comments included after the # in a seed file become Notes attribute values for the discovery seeds.

To identify a discovery seed, enter one of the following:

- **Fully-qualified hostname** of the discovery seed
- **IP address** of the discovery seed, specify a physical address

When providing IPv4 addresses as discovery seeds, the following IP addresses are considered invalid:

- 255.255.255.255
- IP addresses that begin or end with 0 (zero)

NNMi uses information gathered from Routers to establish subnet membership for Layer 3 connections. Make sure that important Routers in your network environment are SNMP enabled.

NNMi uses either of the following criteria to identify a Router:

- Each Router responds with appropriate values for sysServices (1.3.6.1.2.1.1.7) and ipForwarding (1.3.6.1.2.1.4.1). See RFC1213-MIB for details.
- Identify Routers with the [Device Profile configuration settings](#) for a particular device type.

You must provide the appropriate SNMP Community Strings to NNMi. See "[Configuring Communication Protocol](#)" (on page 47).

To create a seed file:

In a text editor, type each entry on a separate line in the following format:

```
<IP_address> or <hostname> # (optional comment to help identify the node)
```

- *<IP_address>* = the IP address of the node
- *<hostname>* = the fully-qualified DNS hostname or short DNS hostname of the node

To add discovery seeds by loading a seed file:

Use the `nnmloadseeds.ovpl` command:

Windows:

```
<drive>:\Program Files (x86)\HP\HP BTO Software\bin\nnmloadseeds.ovpl -f <path>\<file_name>
```

<drive> is the drive on which NNMi is installed

<path>/<file_name> = the name of the file that contains your discovery seeds

UNIX:

```
/opt/OV/bin/nnmloadseeds.ovpl -f <path>/<file_name>
```

A message displays, showing the number of added, invalid, and ignored discovery seeds. For example:

```
26 seeds added  
0 seeds invalid  
0 seeds duplicated
```

See the [nnmloadseeds.ovpl](#) Reference Page for more information.

Related Topics

["Discovery Seed Results" \(on page 118\)](#)

["Delete Discovery Seeds" \(on page 123\)](#)

From the Command Line, Add Discovery Seeds

There are many ways to provide discovery seeds. Discovery seeds are optional. See "[Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered](#)" (on page 112) for more information.

You can add optional discovery seeds using the [nnmloadseeds.ovpl](#) command:

`<seed_list>` = the discovery seed entries (fully-qualified DNS hostname, short DNS hostname, or IP address)

Windows:

```
<drive>:\Program Files (x86)\HP\HP BTO Software\bin\nnmloadseeds.ovpl -n <seed_list>
```

`<drive>` is the drive on which NNMi is installed

UNIX:

```
/opt/OV/bin/nnmloadseeds.ovpl -n <seed_list>
```

In the following example, the devices with a hostname of cisco4 and cisco5, and a device with the IP address of 12.6.91.5 are added as discovery seeds.

```
nnmloadseeds.ovpl -n cisco4 cisco5 12.6.91.5
```

Note: Identify the discovery seed by either a resolvable hostname or an IP address.

When adding individual discovery seeds using the **nnmloadseeds.ovpl** command:

- **Fully-qualified hostname** of the discovery seed
- **IP address** of the discovery seed, specify a physical address

When providing IPv4 addresses as discovery seeds, the following IP addresses are considered invalid:

- 255.255.255.255
- IP addresses that begin or end with 0 (zero)

Communicate any additional IP address requirements to your team to avoid unexpected discovery results.

NNMi uses information gathered from Routers to establish subnet membership for Layer 3 connections. Make sure that important Routers in your network environment are SNMP enabled.

NNMi uses either of the following criteria to identify a Router:

- Each Router responds with appropriate values for sysServices (1.3.6.1.2.1.1.7) and ipForwarding (1.3.6.1.2.1.4.1). See RFC1213-MIB for details.
- Identify Routers with the [Device Profile configuration settings](#) for a particular device type.

You must provide the appropriate SNMP Community Strings to NNMi. See ["Configuring Communication Protocol" \(on page 47\)](#).

Related Topics

["Discovery Seed Results" \(on page 118\)](#)

["Delete Discovery Seeds" \(on page 123\)](#)

Examine Discovery Results

When verifying discovery, you can do any of the following tasks:

- ["Check Initial Progress of Discovery" \(on page 117\)](#)
- ["Verify Success of Discovery Seeds" \(on page 117\)](#)
- ["Examine Discovery Inventory " \(on page 120\)](#)
- ["Examine Layer 2 Discovery Results" \(on page 120\)](#)
- ["Examine Layer 3 Discovery Results" \(on page 121\)](#)

Related Topics

["Node Discovery State Check" \(on page 117\)](#)

["Discovery Seed Results" \(on page 118\)](#)

Check Initial Progress of Discovery

During your initial discovery, you can check Spiral Discovery's progress by using the **Help** → **About HP Network Node Manager i-series** menu item.

Check this several times during a one hour period. The numbers in the Nodes, SNMP agents, Interfaces, IP addresses, and Layer 2 Connections fields stabilize when initial discovery is complete. A report on the health of the State Poller Service is also presented on this window.


You can also see discovery state for a node. See ["Node Discovery State Check" \(on page 117\)](#) for more information.

Note: If you configure one or more Auto-Discovery Rules and you get unexpected results, check your ordering numbers. See ["Configure Auto-Discovery Rules" \(on page 101\)](#) for more information.

Node Discovery State Check

You can verify the current discovery state for a node.

To see the current Discovery State for a node:

1. Navigate to a **Node** form.
 - a. From the workspaces navigation panel, select the workspace of interest. For example, **Inventory**.
 - b. Select the node view of interest. For example **Nodes**.
 - c. Select a node and click the  Open icon.
2. Locate the **Discovery State** attribute (in the Discovery section on the left side of the form).

Possible values include:

- **Newly Created** – Indicates the node and its IP addresses are in the NNMi database, but further information needs to be collected before state and status are determined.
- **Discovery Completed** – Indicates that discovery gathered all required information for the node.
- **Rediscovery in Process** – Indicates discovery is updating the information collected for the node.

Verify Success of Discovery Seeds

The discovery seeds provide the starting point for discovery.

To verify that each discovery seed was successfully discovered:

1. Navigate to the **Discovery Configuration** form.
 - From the workspace navigation panel, select the **Configuration** workspace.
 - Select the **Discovery Configuration**.
2. Locate the **Discovery Seeds** tab.

3. Check the value in the Discovery Seed Results column on each row of the table. A value of **Node Created** indicates the successful discovery of each discovery seed. See "[Discovery Seed Results](#)" (on page 118) for the meaning of other values and how to correct discovery problems.

Discovery Seed Results

When you add a discovery seed, the Discovery Service immediately tries to discover it (without waiting until the next regularly scheduled [discovery interval](#)). If discovery is not successful, NNMi tries again 10 minutes later, and continues trying. The time between each try is doubled until it reaches 1 week or equals your current discovery interval.

To see the current discovery results for each specified discovery seed:

1. Navigate to the **Discovery Configuration** form
 - From the workspace navigation panel, select the **Configuration** workspace.
 - Select **Discovery Configuration**.
2. Locate the **Discovery Seeds** tab. The table lists each discovery seed and the result that NNMi gathered when contacting the discovery seed.
3. Check the value in the **Discovery Seed Results** column on each row of the table.

Discovery Seed Results Values

Discovery Results	Description
New seed	You just entered a new discovery seed. When discovery begins, Discovery Results changes to "In progress". If the "New seed" value does not change, check to see if the Discovery Service needs to be restarted, see " Verify that NNMi Services Are Running " (on page 28).
In progress	Discovery is in progress.
Node created	The discovery seed is successfully discovered and a new Node is created in the database.
Node created (Non-SNMP device)	<p>The hostname or IP address you provided is a non-SNMP device. The Node was discovered and added to the database, but no SNMP information is available because no SNMP agent responded.</p> <p>If this result is unexpected, the device might currently be down. Initiate an on-demand discovery poll using Actions → Configuration Poll, click here for more information. Or try the following:</p> <p>Check whether the IP address is accessible</p> <ol style="list-style-type: none"> 1. Type the following command to verify that the address is accessible: <code>ping <nodename></code> <p>Check the Access Control List</p> <ol style="list-style-type: none"> 1. Access the Node, and open the Access Control List (ACL). 2. Verify that the NNMi management server address is in the list. <p>Ensure that SNMP is working</p> <ol style="list-style-type: none"> 1. Type the following command to verify that the address has an SNMP agent. Supply

Discovery Results	Description
	<p>one specific MIB variable to limit network traffic to one object rather than requesting all possible SNMP values. For example, use the VendorID prefix with SNMPv1 or SNMPv2c:</p> <pre>nnmsnmpwalk -c <communityString> <nodename or IP address> <VendorID></pre> <ol style="list-style-type: none"> 2. If the nnmsnmpwalk fails: <ol style="list-style-type: none"> a. Use telnet to check the device's SNMP configuration to verify that SNMP is enabled. b. Verify that the address of the NNMi management server is listed in the SNMP Agent's Access list. <p>Check your communication configuration</p> <ol style="list-style-type: none"> 1. Verify that SNMP communication is enabled for this device: "Configuring Communication Protocol" (on page 47). 2. Verify that the device has a properly configured SNMPv1 or SNMPv2c read-only community string, or that the device has a properly configured SNMPv3 USM security setting. <p>Note: <i>NNMi makes one attempt to contact each discovery seed.</i> After you correct the problem that caused NNMi to specify the seed as a non-SNMP device, NNMi updates the Node record during the next discovery cycle. However, this Discovery Results entry does not change, but everything is working properly.</p>
Node not created (Duplicate seed)	The address or hostname you provided is a Node that already exists in the database.
Node not created (DNS name resolution failed)	The hostname you provided for this discovery seed cannot be resolved to a valid IP address through DNS.

Discovery Results	Description
Node not created (License exceeded)	Discovery rejected this discovery seed because the number of devices previously discovered reached your license limit.
Failed	<p>Contact with of this discovery seed failed due to an internal NNMi error. The problem might be related to discovery or to a system wide issue, such as running out of memory or having trouble with database access. Check the discovery log file (see "Verify that NNMi Services Are Running" (on page 28)):</p> <ul style="list-style-type: none">• Windows: <code><drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\log\nnm\disco.0.0.log</code> <code><drive></code> is the drive on which NNMi is installed.• UNIX: <code>/var/opt/OV/log/nnm/disco.0.0.log</code>

Related Topics:

["Specify Discovery Seeds: Initial Routers or Specific Nodes to be Discovered" \(on page 112\)](#)

Examine Discovery Inventory

The best method for examining your discovered inventory depends on how you configure discovery.

To examine your Discovery Inventory:

1. In the **Workspace** navigation panel, open the **Inventory** workspace.
2. Select the **IP Addresses** view.
3. *Optional.* Verify that each IP address you identified as a [discovery seed](#) is listed.
4. Verify that the set of IP addresses you expect to see are visible (based on any address ranges where [Discover Included Nodes](#) is enabled or disabled).
5. To check on the current discovery state for a particular node, see ["Node Discovery State Check" \(on page 117\)](#).

Note: If you configure one or more Auto-Discovery Rules and you get unexpected results, check your ordering numbers. See ["Configure Auto-Discovery Rules" \(on page 101\)](#) for more information.

Related Topics

[Using the IP Addresses View](#)

[Using the Nodes View](#)

Examine Layer 2 Discovery Results

Layer 2 represents your network's physical connections and LAN switch traffic routes.


To examine Layer 2 inventory and connectivity results:

1. In the **Workspace** navigation panel, open the **Inventory** workspace.
2. Select the **Nodes** view.

3. Select the node of interest.
4. Select **Actions** → **Layer 2 Neighbor View**.
5. Use the **Number of Hops** field to expand the area shown on the map.
6. Examine your network connectivity to ensure it is as expected. See ["Add or Delete a Layer 2 Connection" \(on page 124\)](#) if changes are required.

Note: If you configure one or more Auto-Discovery Rules and you get unexpected results, check your ordering numbers. See ["Configure Auto-Discovery Rules" \(on page 101\)](#) for more information.

To examine VLAN results:

1. In the **Workspace** navigation panel, open the **Inventory** workspace.
2. Select the **VLANs** view.
3. Select the VLAN of interest.
4. Click  Open to open the VLAN form.
5. Verify that the list includes all nodes and ports assigned to this VLAN.

Note: If you configure done or more Auto-Discovery Rules and you get unexpected results, check your ordering numbers. See ["Configure Auto-Discovery Rules" \(on page 101\)](#) for more information.

Related Topics

[Using the Layer 2 Neighbor View](#)

[Using the Layer 3 Neighbor View](#)

Examine Layer 3 Discovery Results

Layer 3 represents your network's router traffic.

To examine Layer 3 inventory results:

1. In the **Workspace** navigation panel, open the **Inventory** workspace.
2. Select the **Nodes** view.
3. Select the router of interest.
4. Select **Actions** → **Layer 3 Neighbor View**.
5. Use the **Number of Hops** field to expand the area shown on the map.
6. Examine your network connectivity to ensure it is as expected. If changes are required, try the following:
 - Use **Actions** → **Configuration Poll**. See [Using Actions to Perform Tasks](#) for more information.
 - Manually add or delete the connection See ["Add or Delete a Layer 2 Connection" \(on page 124\)](#).
 - Verify that the addresses on each end of the connection are not listed in the Excluded IP Address filter. See ["Configure an Excluded IP Addresses Filter" \(on page 108\)](#).

Note: If you configure one or more Auto-Discovery Rules and you get unexpected results, check your ordering number for each rule. See ["Configure Auto-Discovery Rules" \(on page 101\)](#) for more information.

Related Topics

[Using the Layer 2 Neighbor View](#)

[Using the Layer 3 Neighbor View](#)

Keep Your Topology Accurate

With NNMi, discovery is ongoing. After initial discovery, NNMi checks periodically to ensure that the maps accurately reflect the state of your network. NNMi also updates the database to reflect any changes.

By default, NNMi uses the following methods to keep the maps accurate:

Spiral Discovery. NNMi uses neighbor information gathered from various devices on your network to discover all devices connected to your network.

Scheduled Rediscovery. Discovery occurs automatically at the interval you define. See "[Adjust the Discovery Interval](#)" (on page 98) for more information about setting the discovery schedule.

Delete Nodes. As an administrator, you can also delete any nodes that you no longer use, or delete nodes to force NNMi to rediscover them. See "[Delete Nodes](#)" (on page 122) for more information.

Tip: NNMi also monitors the health of the discovered devices. The health is indicated by the color of the background shape of each device icon on the map. See "[Status Colors](#)" for more information. For information about how health monitoring works, see "[About the State Poller](#)" (on page 151) and "[Monitoring Network Health](#)" (on page 151).

Add or Delete Connections. If your network management domain includes ATM, Frame Relay, or MPLS links between wide area networks (WANs), you may need to use the connection editor to show the links in the Layer 2 Neighbor View maps within NNMi. For MPLS, you can provide multiple connections between two nodes. "[Add or Delete a Layer 2 Connection](#)" (on page 124).


Delete Nodes

NNMi administrators can delete nodes from a table view, map view, or Node form. For example:

- Remove any nodes that are no longer being used in the network.
- When non-SNMP addresses that had the same DNS hostname are changed to have separate DNS hostnames, NNMi must completely rediscover the non-SNMP nodes to correctly update the database objects (node, interface, address, connection, and incidents).

To understand the results of deleting a Node, click here for more information.


- NNMi cleans up the database by deleting the following objects:
 - Any objects representing things contained in the deleted Node (for example, all of that node's interfaces and IP addresses).
 - Any related objects that are empty after deleting the Node (for example, subnets).
 - Any connections with only zero or one end points after deleting the Node.
- During future discovery cycles, if the deleted Node meets the criteria for an Auto-Discovery Rule and appears in a monitored router's ARP cache, NNMi adds the Node back into the NNMi database during the next discovery cycle. To prevent this, create an Excluded IP Addresses filter for the addresses (see "[Configure an Excluded IP Addresses Filter](#)" (on page 108)).
- During future monitoring cycles, NNMi polls only objects currently in the database.
- Each Incident associated with the deleted Node is modified in the following ways:

- The **Status** attribute changes to **Closed**.
- The **Correlation Notes** indicate the deletion of the associated node, interface, or address.
- The **RCA State** attribute changes to **FALSE**.
- Incidents generated from traps (received from the deleted Node) appear in the Incident views, but remain unresolved.
- If you are viewing a Node that has recently been deleted by another user, the deleted Node appears as a transparent icon on the map until the map is refreshed using the  **Refresh** icon. After **Refresh**, the deleted node is removed from the map. NNMi does not automatically refresh the connectivity or set of nodes in a map view, except on the Network Overview map.

Note: If you delete a Node with many interfaces and VLANs, you may see an error message indicating that the Node could not be deleted. This means the database was busy with discovery. Try again between discovery cycles.

If a deleted Node is one of your seeds, delete that seed from the Discovery Seeds table as well. See ["Delete Discovery Seeds" \(on page 123\)](#).

To delete one or more nodes (maximum 20 at one time):

- In a table view, select the object of interest by selecting the check box in the row or rows that represents the objects of interest, and click the  Delete icon. Each selected node is deleted from the NNMi database and removed from the current view.
- In a map view, click the map symbol representing the node you want to delete, and click **File** → **Delete Node**. The node is deleted from the NNMi database and removed from the current view.
- In a Node form, select **File** → **Delete Node** and in the confirmation dialog, click **OK**. The form is automatically closed after NNMi deletes the Node.

To delete any number of nodes at one time:

See the [nnmnodedelete.ovpl](#) Reference Page.

Related Topics



[Using Table Views](#)

[Using Map Views](#)

Delete Discovery Seeds

There are two ways to delete discovery seeds from the NNMi Discovery configuration and the NNMi database.

To delete seeds using the Discovery Configuration view:

1. Navigate to the **Discovery Seeds** tab in the Discovery Configuration form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Discovery Configuration**.
 - c. Locate the **Discovery Seeds** tab.
2. To delete one or more discovery seeds, select any number of rows, and click the  Delete icon.
3. Click  **Save and Close**.

To delete any number of seeds at one time from the command line:

1. A user name and password are required with the `nnmseedelete.ovpl` command:

```
-u <NNMiadminUserName> -p <NNMiadminPassword>
```

If you do not want to enter a user name and password at the command line, you can use the [nnmsetcmduserpw.ovpl](#) command to specify the valid user name and password (instead of `-u` and `-p`). The credentials set using the `nnmsetcmduserpw.ovpl` command are valid for command execution by the same user.

2. At the command line of the NNMi management server, type the [nnmseedelete.ovpl](#) command.

Specify the host name or IP address (exactly as listed in the **Discovery Seeds** tab in the Discovery Configuration form).

```
nnmseedelete.ovpl -seed <IP-address/hostname>
```

Add or Delete a Layer 2 Connection

Tip: If your network management domain includes ATM, Frame Relay, or MPLS links between wide area networks (WANs), you may need to use the connection editor to show the links in the Layer 2 Neighbor View maps within NNMi. For MPLS, you can provide multiple connections between two nodes.

Use the NNMi [nnmconnedit.ovpl](#) command to add or delete connection data.

The `nnmconnedit.ovpl` command is used to generate a template XML file (shown in the following example). For each connection to be added or deleted, you provide information about the node and interface at both ends of the connection. Multiple `<connection>` elements are allowed within the template XML file.

```
<connectionedits>
<connection>
  <operation>add or delete</operation>
  <node>node Name, Hostname or management IP address</node>
  <interface>ifName, ifAlias, ifDescr or ifIndex</interface>
  <node>node Name, Hostname, or management IP address</node>
  <interface>ifName, ifAlias, ifDescr or ifIndex</interface>
</connection>
</connectionedits>
```

Required Layer 2 Connection Attributes in the Connection Editor File

Attribute	Description
operation	Specify whether the connection is to be added or deleted.
node	Identify the node using any of the following values: Note: NNMi converts all Hostname attribute values to lowercase in the NNMi database. Therefore, when entering a Hostname value, use all lowercase. <ul style="list-style-type: none">• node Name• Hostname (fully-qualified DNS name, all lowercase)• management IP address
interface	Identify the interface using one or more of the following (MIB-II) values: <ul style="list-style-type: none">• ifName• ifAlias

Attribute	Description
	<ul style="list-style-type: none">• <code>ifDescr</code>• <code>ifIndex</code> Note the following for <code>ifIndex</code>:<ul style="list-style-type: none">■ For interfaces in Non-SNMP nodes, always use the <code>ifIndex</code> value of 0 (zero).■ For interfaces in SNMP nodes, choose other MIB-II values to identify the interface because often automatic interface renumbering causes confusion.

To add or delete a connection:

1. For the devices at both ends of the connection, gather the data required to identify the device and interface.
2. On the NNMi management server, at the command line, generate a connections template file using either `add` to create an `add.xml` template file or `delete` to create a `delete.xml` template file.

In the following example, NNMi creates an `add.xml` file:

```
nnmconnect.ovpl -t add
```

Note: If you specify `add`, NNMi creates the template file named `add.xml`. If you use `delete`, the template file is named `delete.xml`.

3. Open the template file in a text editor and fill in the correct information for each node and interface.
4. On the NNMi management server, at the command line, load the new connection information into the NNMi database:

```
nnmconnect.ovpl -f <add|delete>.xml
```

For example, to load the `add.xml` template file, enter:

```
nnmconnect.ovpl -f add.xml
```

5. Open the Layer 2 Neighbor View map and verify the connection changes.

The connections you establish are listed in the Layer 2 Connections view in the Inventory workspace. To delete a connection, you must use the [nnmconnect.ovpl](#) command (no Delete action is available in the Layer 2 Connections view).

Creating Groups of Nodes or Interfaces

Groups of nodes or interfaces are used for a variety of purposes within NNMi. Use of these groups is optional.

- Use node and interface groups to specify monitoring configuration settings. See ["Monitoring Network Health" \(on page 151\)](#).
- Use node and interface groups to create custom view filters that help your team quickly sift through data in the NNMi views and identify the most important information.

You can use Node Groups and Interface Groups within both contexts (view and configuration) or create a separate set of groups to configure monitoring.

View Filter Possibilities

Filter	View: Object Type			
	Incident	Node	Interface	IP Address
Node Groups "Create Node Groups" (on page 126)	x	x	x	x
Interface Groups "Create Interface Groups" (on page 139)			x	x

Create Node Groups

Node Group definitions match the way your team identifies important network devices. Each node group is defined using one or more of the following:

- Device Filters (by any combination of category, vendor, family, profile)
- Additional Filters
- Additional Nodes (identified by Hostname)
- Child Node Groups

Note the following:

- When you provide both Device Filters and Additional Filters, nodes must match *all* specifications to belong to this Node Group.
- Any Additional Nodes you specify are always included in the Node Group.
- You can set Custom Attributes for nodes and then create Node Groups based on these Custom Attributes. See ["In a Text File, Define Node Groups" \(on page 137\)](#) and [nmmnetloadnodeattrs.ovpl](#) for more information.

Node Groups are used for a variety of purposes in NNMi:

- Filter node, interface, IP address, and incident views by Node Group.
- Control [how NNMi monitors network devices](#) using Node Groups. For example, configure a different health monitoring interval for each group.
- *NNM iSPI for Performance*. If you are using NNM iSPI for Performance, control performance monitoring and provide report filters by Node Group.

To create Node Groups, do one or more of the following:

- ["In the Console, Create Node Groups" \(on page 127\)](#)
- ["In a Text File, Define Node Groups" \(on page 137\)](#)

To verify the contents of a Node Group:

After the Node Group is saved, from the Node Group form, select **Actions** → **Show Members**.



NNMi automatically creates Island Node Groups whenever it detects changes in Layer 2 connections. An Island Node Group is a group of fully-connected nodes that NNMi displays in a group that is not connected to the rest of the topology. See ["Island Node Groups" \(on page 149\)](#) for more information.

In the Console, Create Node Groups




Node Groups are used for a variety of purposes in NNMi:

- Filter node, interface, IP address, and incident views by Node Group.
- Control [how NNMi monitors network devices](#) using Node Groups. For example, configure a different health monitoring interval for each group.
- *NNM iSPI for Performance*. If you are using NNM iSPI for Performance, control performance monitoring and provide report filters by Node Group.

To create a Node Group (if your role allows you to do this):

1. Navigate to the **Node Group** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Node Groups** view.
 - c. Do one of the following:
 - To create a Node Group, click the  New icon.
 - To edit a Node Group, select a row, click the  Open icon.
2. In the [Node Group form](#), provide attribute values in the [Basics](#) section.
3. *NNM iSPI for Performance*. Make the Node Group available within NNM iSPI for Performance (see [NNM iSPI for Performance table](#)).
4. Identify the nodes that belong to this Node Group.

Do one or more of the following:



- [Specify an SNMP Object ID strategy using the Device Filters tab.](#)
 - [Specify a Node Group filter expression using the Additional Filters tab.](#)
 - [Specify individual nodes using the Additional Nodes tab.](#)
 - [Specify Child Node Groups using the Child Node Groups tab.](#)
5. Click  **Save and Close** to return to the Node Group form.
 6. Click  **Save**.
 7. To view the members in the Node Group, select **Actions** → **Show Members**.
 8. Click  **Save and Close**.

If you configured this Node Group for Monitoring, NNMi applies your changes during the next monitoring cycle. "[Configure Monitoring Behavior](#)" (on page 152).

Note the following:

- You can create a Node Group using a comma separated values (CSV) text file. For example, if you have node group information in an Microsoft Excel spreadsheet, you can save this information as a .csv file and use the `nnmloadnodegroups.ovpl` command to add this node group information to NNMi. See the [nnmloadnodegroups.ovpl](#) Reference Page for more information about the `nnmloadnodegroups.ovpl` command, including the required format of the CSV file.
- NNMi monitors the status of each Node Group over time. To check Node Group status information, access the Node Group [Status](#) tab.

To review a Node Group definition:

1. From the workspace navigation panel, select the **Inventory** workspace.
2. Select the **Node Groups** view.
3. Locate the row representing the Node Group, click the  Open icon.
4. The [Node Group form](#) displays.
5. When finished, click the  Close icon.

[Special Actions are available](#) within the Node Group and Interface Group views.

Related Topics

["In a Text File, Define Node Groups" \(on page 137\)](#)



Specify Node Group Additional Filters

The Additional Filters Editor enables you to create expressions to further define the nodes to be included in a Node Group. Make sure to design any complex Additional Filters offline as a Boolean expression first. This method can help to minimize errors when entering your expressions using the Additional Filters editor.

If any Additional Filters are created, NNMi combines any Device Filters and Additional Filters using the AND Boolean operator as follows:

- NNMi first evaluates any Device Filters. Nodes must match *all* specifications to belong to this node group.
- NNMi then evaluates the Additional Filters expression. Nodes *must also match all* Additional Filters expression specifications to belong to this Node Group.

To create an Additional Filters expression:

1. Navigate to the **Node Group Form: Additional Filters** tab.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Node Group**.
 - c. Do one of the following:
 - To create a Node Group definition, click the  New icon.
 - To edit a Node Group definition, select a row, click the  Open icon.
 - d. In the Node Group form, select the **Additional Filters** tab.

2. Establish the appropriate settings for the Additional Filters you need (see the [Additional Filters Editor Components](#) and [Additional Filters Editor Buttons](#) table).

When creating any Additional Filters, note the following:

- Each set of expressions associated with a Boolean Operator is treated as if it were enclosed in parentheses and evaluated together.
- View the expression displayed under **Filter String** to see the logic of the expression as it is created.
- When using the AND operator to combine expressions that include Custom Attributes, include only one customAttrName/customAttrValue pair in a sub-expression.
- The AND and OR Boolean Operators must contain at least two expressions as shown in the example below.

AND


```
sysName like cisco*  
sysName != cisco2811
```

OR

```
sysLocation = Boston  
sysContact In (Johnson,Hickman)
```

NNMi evaluates the expression above as follows:

```
sysName like cisco* AND sysName != cisco2811 AND (sysLocation = Boston OR  
sysContact in (Johnson, Hickman))
```

- NNMi finds all nodes whose system Name begins with **cisco**, but does not include **cisco2811**
 - Of these nodes, NNMi then finds all nodes whose system location is **Boston** or whose system contact name includes **Johnson** or **Hickman**.
- The placement of your cursor and the subsequent text that is selected is important when performing operations using the Additional Filters Editor. For example, you append to, replace, or change the indentation of the expression that is selected.
 - The placement of your cursor and the subsequent text that is selected is especially important when adding your Boolean operators. See "[Add Boolean Operators in the Additional Filters Editor](#)" (on page 134) for more information.
3. Click  **Save and Close**.

Additional Filters Editor Components

Attribute	Description
Attribute	<p>The attribute name on which NNMi searches. Filterable attributes include the following. For more information about each one, click the link:</p> <p>Values from the Basic Attributes listed on the Node Form:</p> <ul style="list-style-type: none">• hostname (Hostname)• mgmtIPAddress (Management Address) <p>Values from the Node Form:General Tab:</p> <ul style="list-style-type: none">• sysName (System Name)• sysLocation (System Location)• sysContact (System Contact) <p>Addresses from the Node Form: IP Addresses Tab:</p> <ul style="list-style-type: none">• hostedIPAddress (Address) <p>Note: When you want to filter nodes based on an hostedIPAddress address range, use the between operator. When using the <code>hostedIPAddress</code> attribute with the greater than or equal to (<code>>=</code>) and less than or equal to (<code><=</code>) operators, NNMi finds all addresses that match the filter. Click here for an example. For example, the hostedIPAddress values 1.1.1.1 and 20.20.20.20, pass the filter: <code>hostedIPAddress >= 16.120.100.0</code> and <code>hostedIPAddress <= 16.120.100.255</code>.</p> <p>Unique Keys from the Node Form: Capabilities Tab:</p> <ul style="list-style-type: none">• capability (Unique Key of the Capability) <p>Values from the Node Form: Custom Attributes Tab:</p> <ul style="list-style-type: none">• customAttrName (Custom Attribute Name)• customAttrValue (Custom Attribute Value)

Operator The standard query language (SQL) operations to be used for the search.

Note: Only the `is null` Operator returns null values in its search.

Valid operators are described below.

- `=` Finds all values equal to the value specified. Click here for an example.
Example: `sysName=cisco2811` finds all devices with system name equal to **cisco2811**.
- `!=` Finds all values not equal to the value specified. Click here for an example.
Example: `sysName != cisco2811` finds all system names other than **cisco2811**.
- `<` Finds all values less than the value specified. Click here for an example.
Example: `mgmtIPAddress < 15.239.255.255` finds all IP address values less than **15.239.255.255**.
- `<=` Finds all values less than or equal to the value specified. Click here for an example.
Example: `mgmtIPAddress <= 15.239.255.255` finds all IP address values less than or equal to **15.239.255.255**.

Attribute	Description
-----------	-------------

- **>** Finds all values greater than the value specified. Click here for an example.
Example: `mgmtIPAddress > 15.238.0.0` finds all IP address values greater than **15.238.0.0**.
- **>=** Finds all values greater than or equal to the value specified. Click here for an example.
Example: `mgmtIPAddress >= 15.238.0.0` finds all IP address values greater than or equal to **15.238.0.0**.
- **between** Finds all values equal to and between the two values specified. Click here for an example.
Example: `mgmtIPAddress between 15.238.0.10 15.238.0.120` finds all IP address values equal to or greater than **15.238.0.10** and equal to or less than **15.238.0.120**.
- **in** Finds any match to at least one value in a list of values. Click here for an example.

Example:

```
sysName in
```



finds all systems with names that are **cisco2811** or **cisco5500**.

Note: As shown in the example, each value must be entered on a separate line.

NNMi displays the list of attributes using comma-separated values enclosed in parentheses, for example (**cisco2811, cisco550**). However, the comma-separated list is used only for display purposes. The actual delimiter is the new line.

- **is not null** Finds all non-blank values. Click here for an example.
Example: `sysName is not null` finds all systems that have a name value.
- **is null** Finds all blank values. Click here for an example.
Example: `sysName is null` finds all systems that do not have an assigned name value.
- **like** Finds matches using wildcard characters. Click here for more information about using wildcard characters.

The following attributes cannot be used with the `like` operator:

- `hostedIPAddress`
- `mgmtIPAddress`

The asterisk (*) character means *any number of characters of any type at this location*.

The question mark (?) character means *any single character of any type at this location*.

Examples:

- `sysName like cisco*` finds all system names that begin with **cisco**.
- `sysName like *.xyz.com` finds all system names that *end with* this specific domain.
- `sysName like *rtr*` finds all system names that *contain* **rtr**.

Attribute	Description
-----------	-------------

- `sysName like *cisco??*` finds all system names that *include* **cisco** followed by two characters.
- `sysName like ??rtr?bld5*` finds all system names that have *specific characters at an exact location*, positions 3-5 (rtr) and 7-10 (bld5).

- **not between** Finds all values except those between the two values specified. Click here for an example.

Example: `mgmtIPAddress not between 15.238.0.10 15.238.0.120` finds all IP address values less than **15.238.0.10** and greater than **15.238.0.120**.

- **not in** Finds all values except those included in the list of values. Click here for an example.

Example:

```
sysName not in
```



finds all system name values other than **cisco2811** and **cisco5500**.

Note: As shown in the example, each value must be entered on a separate line.

NNMi displays the list of attributes using comma-separated values enclosed in parentheses, for example, (**cisco2811**, **cisco5500**). However, the comma-separated list is used only for display purposes. The actual delimiter is the new line.

- **not like** Finds all that do not have the values specified (using wildcard strings). Click here for an example.

The following attributes cannot be used with the `not like` operator:

- `hostedIPAddress`
- `mgmtIPAddress`

The asterisk (*) character means *any number of characters of any type at this location*.

The question mark (?) character means *any single character of any type at this location*.

Examples:

- `sysName not like cisco*` finds all system names that do not begin with **cisco**.
- `sysName not like *.xyz.com` finds all system names that do not *end with* this specific domain.
- `sysName not like *rtr*` finds all system names that do not *contain* **rtr**.
- `sysName not like *cisco??*` finds all system names that do not *include* **cisco** followed by two characters.
- `sysName not like ??rtr?bld5*` finds all system names that do not have *specific characters at an exact location*, positions 3-5 (rtr) and 7-10 (bld5).

Attribute	Description
Attribute	<p>The attribute name on which NNMi searches. Filterable attributes include the following. For more information about each one, click the link:</p> <p>Values from the Basic Attributes listed on the Node Form:</p> <ul style="list-style-type: none"> • hostname (Hostname) • mgmtIPAddress (Management Address) <p>Values from the Node Form:General Tab:</p> <ul style="list-style-type: none"> • sysName (System Name) • sysLocation (System Location) • sysContact (System Contact) <p>Addresses from the Node Form: IP Addresses Tab:</p> <ul style="list-style-type: none"> • hostedIPAddress (Address) <p>Note: When you want to filter nodes based on an hostedIPAddress address range, use the <code>between</code> operator. When using the <code>hostedIPAddress</code> attribute with the greater than or equal to (<code>>=</code>) and less than or equal to (<code><=</code>) operators, NNMi finds all addresses that match the filter. Click here for an example. For example, the <code>hostedIPAddress</code> values 1.1.1.1 and 20.20.20.20, pass the filter: <code>hostedIPAddress >= 16.120.100.0</code> and <code>hostedIPAddress <= 16.120.100.255</code>.</p> <p>Unique Keys from the Node Form: Capabilities Tab:</p> <ul style="list-style-type: none"> • capability (Unique Key of the Capability) <p>Values from the Node Form: Custom Attributes Tab:</p> <ul style="list-style-type: none"> • customAttrName (Custom Attribute Name) • customAttrValue (Custom Attribute Value)
Value	<p>The value for which you want NNMi to search.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • The values you enter are case sensitive. <p>Note: NNMi converts all Hostname attribute values to lowercase in the NNMi database. Therefore, when entering a Hostname value, use all lowercase.</p> <ul style="list-style-type: none"> • NNMi displays a variable number of value fields depending on the Operator selected. For example, the <code>between</code> Operator causes two value fields to be displayed. • The <code>in</code> and <code>not in</code> operators require that each value be entered on a separate line. • When entering a value for the Capability attribute, copy and paste the Unique Key value from the Node form: Capability tab. <p>Note: When copying and pasting the Unique Key value, delete any leading or trailing blank spaces as the Unique Key value must be an exact match.</p>

Additional Filters Editor Buttons

Button	Description
Append	Appends the current expression (Attribute, Operator, and Value) to the selected expression already included in the filter string.
Replace	Replaces the selected expression with the expression displayed in the Attribute, Operator, and Value fields.
AND	Inserts the AND Boolean Operator in the selected cursor location. Note: View the expression displayed under Filter String to see the logic of the expression as it is created.
OR	Inserts the OR Boolean Operator in the current cursor location. Note: View the expression displayed under Filter String to see the logic of the expression as it is created.
AND <--> OR	Switches the selected Boolean Operator to either AND or OR. If the selected Boolean Operator is AND, the value is changed to OR. If the selected Boolean Operator is OR, the value is changed to AND.
Outdent	Moves a nested expression up one expression level. If your filter string includes only one nested expression, Outdent replaces the top-level expression. Click here for examples. Example 1 <pre>AND sysName like cisco* OR sysLocation = Boston</pre> Placing the cursor at <code>sysLocation = Boston</code> and selecting Outdent , results in: <pre>AND sysName like cisco* OR sysLocation = Boston</pre> Example 2 <pre>AND sysName like cisco*</pre> Placing the cursor at <code>sysName like cisco*</code> and selecting Outdent , results in: <pre>sysName like cisco*</pre>
Delete	Deletes the selected expression. Note: If the Boolean Operator is selected, the Additional Filters Editor deletes all expressions associated with the Boolean Operator.

Add Boolean Operators in the Additional Filters Editor

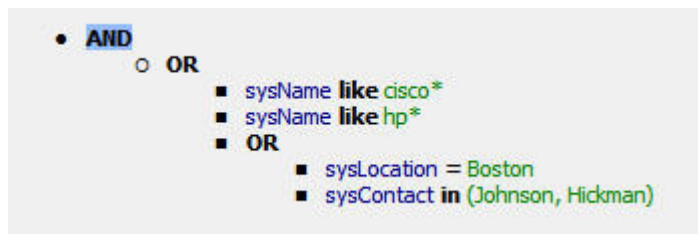
When adding or deleting Boolean Operators using the Additional Filters Editor, note the following:

- Add your highest level Boolean operator first. For example, **AND** is the highest level Boolean operator in the following expression

(sysName like cisco* OR sysName like hp*) **AND** (sysLocation = Boston OR sysContact in Johnson,Hickman)

- Add each additional Boolean Operator before the expressions to which it applies.
- Select the appropriate Boolean Operator in the expression before you add the expressions to which the Boolean Operator applies.
- When a Boolean Operator is selected and you click **Delete**, any expressions that are associated with the Boolean Operator are also deleted.

In the example expression below, If you select **AND** and then click **Delete**, the Additional Filters Editor deletes the entire expression.



[Click here for an example for creating Node Group Additional Filters.](#)

Node Group Additional Filters Expression Example

(sysName like cisco* OR sysName like hp*) **AND** (sysLocation = Boston OR sysContact in Johnson,Hickman)

To add the expression above, after you are in the Additional Filters Editor, follow these steps:

1. Click **AND**.
2. Click **OR**.
3. Select the **OR** you just added to the expression.
4. In the **Attribute** field select **sysName** from the drop-down list.
5. In the **Operator** field, select **like** from the drop-down list.
6. In the **Value** field, enter **cisco***.
7. Click **Append**.
8. In the **Attribute** field, select **sysName** from the drop-down list.
9. In the **Operator** field, select **like** from the drop-down list.
10. In the **Value** field, enter **hp***.
11. Click **Append**.
12. Select the **AND** that you previously added to the expression.
13. Click **OR**.
14. Select the **OR** you just added to the expression.
15. In the **Attribute** field, select **sysLocation** from the drop-down list.

16. In the **Operator** field, select **=** from the drop-down list.
17. In the **Value** field, enter **Boston**.
18. Click **Append**.
19. In the **Attribute** field, select **sysContact** from the drop-down list.
20. In the **Operator** field, select **in** from the drop-down list.
21. In the **Value** field:
 - a. enter **Johnson** and press **<Enter>**.
 - b. On the new line, enter **Hickman**.
22. Click **Append**.
23. Click **Save** to save your Additional Filters.
24. Select **Actions** → **Show Members** to view the members of the Node Group that is a result of this filter.

Click here for an example for creating an Interface Group Additional Filters.

Interface Group Additional Filters Expression Example

(ifName like ATMS* AND ifName != ATMS/0/A) **AND** (ifSpeed = 10 OR ifSpeed = 100)

To add the expression above, follow these steps:

1. Click **AND**.
2. Click **AND**.
3. Select the **AND** you just added to the expression.
4. In the **Attribute** field select **ifName** from the drop-down list.
5. In the **Operator** field, select **like** from the drop-down list.
6. In the **Value** field, enter **ATM***.
7. Click **Append**.
8. In the **Attribute** field, select **ifName** from the drop-down list.
9. In the **Operator** field, select **!=** from the drop-down list.
10. In the **Value** field, enter **ATMS/0/A**.
11. Click **Append**.
12. Select the first **AND** that you added to the expression.
13. Click **OR**.
14. Select the **OR** you just added to the expression.
15. In the **Attribute** field, select **ifSpeed** from the drop-down list.
16. In the **Operator** field, select **=** from the drop-down list.
17. In the **Value** field, enter **10**.
18. Click **Append**.

19. In the **Attribute** field, select **ifSpeed** from the drop-down list.
20. In the **Operator** field, select **=** from the drop-down list.
21. In the **Value** field, enter **100**.
22. Click **Append**.
23. Click **Save** to save your Additional Filters.
24. Select **Actions** → **Show Members** to view the members of the Node Group that is a result of this filter.

In a Text File, Define Node Groups

Node Groups are used for a variety of purposes in NNMi:

- Filter node, interface, IP address, and incident views by Node Group.
- Control [how NNMi monitors network devices](#) using Node Groups. For example, configure a different health monitoring interval for each group.
- *NNM iSPI for Performance*. If you are using NNM iSPI for Performance, control performance monitoring and provide report filters by Node Group.

You can create a Node Group using the NNMi console or a comma separated values (CSV) text file. For example, if you have Node Group information in a Microsoft Excel spreadsheet, you can save this information as a .csv file and use the `nnmloadnodegroups.ovpl` command to add this node group information to NNMi.

Note the following:

- NNMi uses the OR Boolean operator to combine any Node Group Device Filter and Additional Filter information in the CSV file.
- NNMi uses the AND Boolean operator to combine any Custom Attribute and Capability attribute values.
- If you include Node Group Device Filter and Additional Filter values as well as Custom Attribute and Capability values, NNMi first uses the AND Boolean operator to combine the Custom Attribute and Capability values and then uses the AND Boolean operator to combine these result with the Node Group filter (Device Filter and Additional Filter) results.
- See [nnmloadnodegroups.ovpl](#) for a complete list of the types of Node Group attribute values that `nnmloadnodegroups.ovpl` supports.

To create a Node Group using a comma separated values (CSV) text file, use the `nnmloadnodegroups.ovpl` command:

```
nnmloadnodegroups.ovpl -r [true|false] -u <NNMiadminUsername> -p <NNMi-adminPassword> -f <CSV file name>
```


`-r` is used to overwrite any existing Node Group configuration information. When `-r` is used with `true`, NNMi overwrites any existing Node Group configuration information. The default setting is `false`.



`CSV file name` is the name of the CSV file that contains the Node Group information. The CSV file requires that the information appear in a specific order and format. For example, to create a Node Group using a Device Filter, the information must appear in the column designated as the Device Filter column of the CSV file.

If you want to use a Device Filter to create a Node Group, you might need to access the NNMi graphical user interface to determine values to include in the .csv file. Therefore, note the following:

The `nnmloadnodegroups.ovpl` command requires that you use the SNMP object ID value to identify the Device Profile. You must use the Unique Key values for the following Device Filter information: 1) Device Family, 2) Device Vendor, and 3) Device Category. Click here for more information.

To determine the SNMP object ID or Unique Key value:

1. Navigate to the **Device Profile Configuration** table view.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Device Profile**.
2. *Optional.* Sort or filter the view by the attribute or attribute value you want to specify. For example, you might want to sort the table view using the Device Vendor attribute. See [Use Table Views](#) for more information about sorting and filtering table views.
3. Click the  Open icon that precedes the Device Profile of interest.
4. The **SNMP object ID** value appears on the Device Profile form.

If you want to view a Unique Key value, from the **Family**, **Vendor**, or **Category** attribute, click the  Lookup icon and select  Open.

NNMi displays the **Device Family**, **Device Vendor**, or **Device Category** form.

5. Use the value displayed in the **SNMP Object ID** or **Unique Key** attribute in the form.

See [nnmloadnodegroups.ovpl](#) Reference Page for more information about the `nnmloadnodegroups.ovpl` command, including additional requirements for the CSV file format.

Related Topics

["In the Console, Create Node Groups" \(on page 127\)](#)

Define Custom Attributes on Nodes (NNM iSPI Net)

The NNM iSPI Net `nnmnetloadnodeattrs.ovpl` enables you to load Custom Attributes from a comma-separated values (CVS) file. This feature is useful if you have a large number of nodes defined in an external data storage and you would like to load the attributes into NNMi. For example, if you have Node information in a Microsoft Excel spreadsheet and this information is not defined as a Node attribute in NNMi, you can save this information as a .csv file and use the `nnmnetloadnodeattrs.ovpl` command to add this node information to NNMi.

After the Custom Attributes are loaded into NNMi, you can use the NNMi console to create Node Groups containing nodes with the specified Custom Attribute Name (`custAttrName`) and Custom Attribute Value (`custAttrValue`) pair. For example, if you have a comma-separated value file that includes building locations, you can use the `nnmnetloadnodeattrs.ovpl` command to define **BldgLocation** as a Custom Attribute and load the location values for each node. You can then create a Node Group using **BldgLocation** as the `custAttrName` and the location of interest, such as **Building Five Upper**, as the `custAttrValue`. See ["In the Console, Create Node Groups" \(on page 127\)](#) for more information about creating Node Groups using the NNMi console.

To load Custom Attributes for Nodes using a comma-separate file:

```
nnmnetloadnodeattrs.ovpl -u <NNMiadminUsername> -p <NNMiadminPassword> -r  
[true|false] -f <CSV file name>
```

`-r` is used to overwrite any existing Node Custom Attribute information. When `-r` is used with `true`, NNMi overwrites any existing information. The default setting is `false`.

CSV file name is the name of the CSV file that contains the Node Custom Attribute information. The CSV file requires that the information appear in a specific order and format. See [nmmnetloadnodeattrs.ovpl](#) for more information.

You can also create Node Groups using a CVS file. See "[In a Text File, Define Node Groups](#)" (on page [137](#)) and [nmmloadnodegroups.ovpl](#) for more information.

Create Interface Groups










Interface Group definitions match the way your team identifies important network devices. Each interface group can include one or more interface-type specifications (based on industry-standard IANA ifType-MIB variables).




Optional. Associate a Node Group with an Interface Group. If you specify a Node Group, any interface in this group must be contained in a node that matches the specified Node Group.

Interface Groups are used for a variety of purposes in NNMi:

- Interface Groups are filters for interface and IP address views.
- Interface Groups can control [how NNMi monitors network devices](#). For example, instruct NNMi to never generate ICMP or SNMP queries to any interface used for Voice-Over-IP within your network.



To define an Interface Group (if your role allows you to do this):

1. Navigate to the **Interface Group** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Interface Groups** view.
 - c. Do one of the following:
 - To create an Interface Group, click the  New icon.
 - To edit an Interface Group, select a row, click the  Open icon.
2. Provide the definition for this interface group(see [Interface Group Form](#) help).
3. Navigate to the **Interface Type Filters** tab.
4. Identify one or more interface types that belong to this group:
 - To add an Interface Type filter, click the  New icon, and continue.
 - To change an Interface Type filter, select a row, click the  Open icon, and continue.
 - To delete an Interface Type filter, select a row and click the  Delete icon.
5. In the [Interface Type Filter form](#), click the  Lookup icon and select one of the options from the drop-down menu:
 -  Quick View to display summary information for the currently selected IfType.
 -  Quick Find to view and select from the list of all existing IfTypes (for more information see "[Use the Quick Find Window](#)" (on page 19)).
 -  Open to display the details of the currently selected IfType.

-  New to create a new IfType (see "[Add New IfTypes \(Interface Types\) to the List](#)" (on page 140)).
6. Click  **Save and Close** to return to the Interface Group form.
 7. Click  **Save and Close**.

If you configured this Interface Group for Monitoring, NNMi applies your changes during the next monitoring cycle. See "[Configure Monitoring Behavior](#)" (on page 152).

To review an Interface Group definition:

1. From the workspace navigation panel, select the **Inventory** workspace.
2. Select the **Interface Groups** view.
3. Locate the row representing the Interface Group, click the  Open icon.
4. The [Interface Group form](#) displays.
5. When finished, click the  Close icon.

[Special Actions are available](#) within the Node Group and Interface Group views.





Add New IfTypes (Interface Types) to the List






Interface Type definitions cover all known industry-standard IANA ifType-MIB variables at the time of the release of NNMi. Interface Groups are built with Interface Types. See "[Create Interface Groups](#)" (on page 139)

The Interface Types view is provided because:

- Occasionally new Interface Types are added between releases of NNMi. If your team acquires new devices that contain new interface types, you can add the new interface type to the NNMi list of Interface Type definitions.
- When NNMi discovers a new Interface Type, NNMi automatically adds a new entry in the Interface Types view. NNMi detects the assigned IANA ifType-MIB number. NNMi uses that number in both the IfType attribute and the number attribute values. Use this view to provide a more meaningful IfType text string and optional description.

To configure an IANA ifType-MIB definition:

1. Navigate to the **IfTypes** view:
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **IfTypes** view.
2. Do one of the following:
 - To create an Interface Type definition, click the  New icon, and continue.
 - To edit an Interface Type definition, select a row, click the  Open icon, and continue.
 - To delete an Interface Type definition, select a row and click the  Delete icon.
3. In the [Interface Type Filter form](#), click the  Lookup icon and select one of the options from the drop-down menu:

-  Quick View to display summary information for the currently selected IfType.
 -  Quick Find to view and select from the list of all existing IfTypes (for more information see ["Use the Quick Find Window" \(on page 19\)](#)).
 -  Open to display the details of the currently selected IfType.
 -  New to create a new IfType.
4. Click  **Save and Close**.



Specify Interface Group Additional Filters

The Additional Filters Editor enables you to create expressions to further define the interfaces to be included in an Interface Group. Make sure to design any complex Additional Filters offline as a Boolean expression first. This method can help to minimize errors when entering your expressions using the Additional Filters editor.

If any Additional Filters are created:

- NNMi first evaluates any Interface Type filter. Nodes must match *at least one* specification to belong to this Interface Group.
- NNMi then evaluates the Additional Filters expression. Nodes *must also match all* Additional Filters expression specifications to belong to this Interface Group.

To create any Additional Filters expression:

1. Navigate to the **Interface Group Form: Additional Filters** tab.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Interface Groups**.
 - c. Do one of the following:
 - To create an Interface Group definition, click the  New icon.
 - To edit an Interface Group definition, select a row, click the  Open icon.
 - d. In the Interface Group form, select the **Additional Filters** tab.
2. Establish the appropriate settings for the Additional Filters you need. (See the [Additional Filters Editor Components](#) and [Additional Filters Editor Buttons](#) table.)

When creating any Additional Filters, note the following:

- Each set of expressions associated with a Boolean Operator is treated as if it were enclosed in parentheses and evaluated together. View the expression displayed under **Filter String** to see the logic of the expression as it is created.
- When using the AND operator to combine expressions that include Custom Attributes, include only one customAttrName/customAttrValue pair in a sub-expression.
- The AND and OR Boolean Operators must contain at least two expressions as shown in the example below.

```
AND
  ifName like ATMS*
  ifName != ATMS/0/A
```

```
OR
  ifSpeed = 10000000
  ifSpeed = 100000000
```

Note: As shown in the example above, you must use the actual ifSpeed number.

NNMi evaluates the expression above as follows:

```
(ifName like ATMS* AND ifName != ATMS/0/A) AND (ifSpeed = 10000000 OR
ifSpeed = 100000000)
```

- NNMi finds all interfaces whose interface Name begins with **ATMS**, but does not include **ATMS/0/A**.
- Of these interfaces, NNM then finds all interfaces whose interface speed is **10 Mbps** or **100 Mbps**.
- The placement of your cursor and the subsequent text that is selected is important when performing operations using the Additional Filters Editor. For example, you append to, replace, or change the indentation of the expression that is selected.
- The placement of your cursor and the subsequent text that is selected is especially important when adding your Boolean operators. See "[Add Boolean Operators in the Additional Filters Editor](#)" (on page 134) for more information.

3. Click  **Save and Close**.

Additional Filters Editor Components

Attribute	Description
Attribute	<p>The attribute name on which NNMi searches. Filterable attributes include the following. For more information about each one, click the link:</p> <p>Values from the Basic Attributes listed on the Interface Form:</p> <ul style="list-style-type: none">• ifName (Name)• hostedOn (Host On Node) <p>Values from the Interface Form: General Tab:</p> <ul style="list-style-type: none">• ifAlias (InterfaceAlias)• ifDesc (InterfaceDescription)• ifIndex (InterfaceIndex)• ifSpeed (Interface Speed) <p>Addresses from the Interface Form: IP Addresses Tab:</p> <ul style="list-style-type: none">• ipAddress (IP Address associated with the interface) <p>Unique Keys from the Interface Form: Capabilities Tab:</p> <ul style="list-style-type: none">• capability (Unique Key of the Capability) <p>Values from the Interface Form: Custom Attributes Tab:</p> <ul style="list-style-type: none">• customAttrName (Custom Attribute Name)• customAttrValue (Custom Attribute Value)
Operator	<p>The standard query language (SQL) operations to be used for the search.</p>

Attribute	Description
-----------	-------------

Note: Only the `is null` Operator returns null values in its search.

Valid operators are described below.

- **=** Finds all values equal to the value specified. Click here for an example.
Example: `ifName=Fa0/14` finds all interface names that are equal to **Fa0/14**.
- **!=** Finds all values not equal to the value specified. Click here for an example.
Example: `ifName != lan0` finds all interface names other than **lan0**.
- **<** Finds all values less than the value specified. Click here for an example.
Example: `ifSpeed <= 100000000` finds all interfaces whose interface speed is less than **100 Mbps**.
- **<=** Finds all values less than or equal to the value specified. Click here for an example.
Example: `ifSpeed <= 100000000` finds all interfaces whose interface speed is less than or equal to **100 Mbps**.
- **>** Finds all values greater than the value specified. Click here for an example.
Example: `ifSpeed >= 10000000` finds all interfaces whose interface speed is greater than **10 Mbps**.
- **>=** Finds all values greater than or equal to the value specified. Click here for an example.
Example: `ifSpeed >= 10000000` finds all interfaces whose interface speed is greater than or equal to **10 Mbps**.
- **between** Finds all values equal to and between the two values specified. Click here for an example.
Example: `ifSpeed between 10000000 100000000` finds all interfaces whose interface speed is equal to or greater than **10 Mbps** and equal to or less than **100 Mbps**.
- **in** Finds any match to at least one value in a list of values. Click here for an example.

Example:

```
ifName in
```



A screenshot of a text input field. The field contains two lines of text: 'Fa0/14' on the first line and 'Fa0/15' on the second line. To the right of the input field is a small blue button with a white downward-pointing arrow, indicating a dropdown menu.

finds all interfaces with names that are **Fa0/14** or **Fa0/15**.

Note: As shown in the example, each value must be entered on a separate line.

NNMi displays the list of attributes using comma-separated values enclosed in parentheses, for example, (**Fa0/14**, **Fa0/15**). However, the comma-separated list is used only for display purposes. The actual delimiter is the new line.

- **is not null** Finds all non-blank values. Click here for an example.
Example: `ifName is not null` finds all interfaces that have a name value.
- **is null** Finds all blank values. Click here for an example.
Example: `ifName is null` finds all interfaces that do not have an assigned name value.

Attribute	Description
-----------	-------------

- **like** Finds matches using wildcard characters. Click here for more information about using wildcard characters.

The following attributes cannot be used with the `like` operator:

- `ifIndex`
- `ifSpeed`
- `IPAddress`

The asterisk (*) character means *any number of characters of any type at this location*.

The question mark (?) character means *any single character of any type at this location*.

Examples:

- `ifName like ATM*` finds all interface names that begin with **ATM**.
 - `ifName like *.xyz.com` finds all system names that *end with* this specific domain.
 - `ifName like *rtr*` finds all system names that *contain* **rtr**.
 - `ifName like *cisco??*` finds all system names that *include* **cisco** followed by two characters.
 - `ifName like ??rtr?bld5*` finds all system names that have *specific characters at an exact location*, positions 3-5 (**rtr**) and 7-10 (**bld5**).
- **not between** Finds all values except those between the two values specified. Click here for an example.

Example: `ifSpeed not between 10000000 100000000` finds all interfaces whose interface speed is less than **10 Mbps** and greater than **100 Mbps**.

- **not in** Finds all values except those included in the list of values. Click here for an example.

Example:

`ifName not in`



A screenshot of a text input field containing the text "Fa0/14" and "Fa0/15" on two separate lines. To the right of the text are two small blue arrow buttons, one pointing up and one pointing down, indicating a list or dropdown menu.

finds all interface name values other than **Fa0/14** or **Fa0/15**.

Note: As shown in the example, each value must be entered on a separate line.

NNMi displays the list of attributes using comma-separated values enclosed in parentheses, for example, (**Fa0/14, Fa0/15**). However, the comma-separated list is used only for display purposes. The actual delimiter is the new line.

- **not like** Finds all that do not have the values specified (using wildcard strings). Click here for an example.

The following attributes cannot be used with the `not like` operator:

- `ifIndex`
- `ifSpeed`
- `IPAddress`

Attribute	Description
	<p>The asterisk (*) character means <i>any number of characters of any type at this location</i>.</p> <p>The question mark (?) character means <i>any single character of any type at this location</i>.</p> <p>Examples:</p> <ul style="list-style-type: none">▪ <code>ifName not like ATM*</code> finds all interface names that do not begin with ATM.▪ <code>ifName not like *.xyz.com</code> finds all system names that do not <i>end with</i> this specific domain.▪ <code>ifName not like *rtr*</code> finds all system names that do not <i>contain</i> rtr.▪ <code>ifName not like *cisco??*</code> finds all system names that do not <i>include</i> cisco followed by two characters.▪ <code>ifName not like ??rtr?bld5*</code> finds all system names that do not have <i>specific characters at an exact location</i>, positions 3-5 (rtr) and 7-10 (bld5).

Attribute	Description
Attribute	<p>The attribute name on which NNMi searches. Filterable attributes include the following. For more information about each one, click the link:</p> <p>Values from the Basic Attributes listed on the Interface Form:</p> <ul style="list-style-type: none"> • ifName (Name) • hostedOn (Host On Node) <p>Values from the Interface Form: General Tab:</p> <ul style="list-style-type: none"> • ifAlias (InterfaceAlias) • ifDesc (InterfaceDescription) • ifIndex (InterfaceIndex) • ifSpeed (Interface Speed) <p>Addresses from the Interface Form: IP Addresses Tab:</p> <ul style="list-style-type: none"> • ipAddress (IP Address associated with the interface) <p>Unique Keys from the Interface Form: Capabilities Tab:</p> <ul style="list-style-type: none"> • capability (Unique Key of the Capability) <p>Values from the Interface Form: Custom Attributes Tab:</p> <ul style="list-style-type: none"> • customAttrName (Custom Attribute Name) • customAttrValue (Custom Attribute Value)
Value	<p>The value for which you want NNMi to search.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • The values you enter are case sensitive. • NNMi displays a variable number of value fields depending on the Operator selected. For example, the <code>between</code> Operator causes two value fields to be displayed. • The <code>in</code> and <code>not in</code> operators require that each value be entered on a separate line. • When entering a value for the Capability attribute, copy and paste the Unique Key value from the Interface form: Capability tab. <p>Note: When copying and pasting the Unique Key value, delete any leading or trailing blank spaces as the Unique Key value must be an exact match.</p>

Additional Filters Editor Buttons

Button	Description
Append	Appends the current expression (Attribute, Operator, and Value) to the selected expression already included in the filter string.
Replace	Replaces the selected expression with the expression displayed in the Attribute, Operator, and Value fields.
AND	<p>Inserts the AND Boolean Operator in the selected cursor location.</p> <p>Note: View the expression displayed under Filter String to see the logic of the expression as it is created.</p>

Button	Description
OR	<p>Inserts the OR Boolean Operator in the current cursor location.</p> <p>Note: View the expression displayed under Filter String to see the logic of the expression as it is created.</p>
AND < > OR	<p>Switches the selected Boolean Operator to either AND or OR. If the selected Boolean Operator is AND, the value is changed to OR. If the selected Boolean Operator is OR, the value is changed to AND.</p>
Outdent	<p>Moves a nested expression up one expression level. If your filter string includes only one nested expression, Outdent replaces the top-level expression. Click here for examples.</p> <p>Example 1</p> <pre>AND ifName like ATMS* OR ifSpeed = 10000000</pre> <p>Placing the cursor at <code>ifSpeed = 10000000</code> and selecting Outdent, results in:</p> <pre>AND ifName like ATMS* ifSpeed = 10000000</pre> <p>Example 2</p> <pre>AND ifName like ATMS*</pre> <p>Placing the cursor at <code>ifName like ATMS*</code> and selecting Outdent, results in:</p> <pre>ifName like ATMS*</pre>
Delete	<p>Deletes the selected expression.</p> <p>Note: If the Boolean Operator is selected, the Additional Filters Editor deletes all expressions associated with the Boolean Operator.</p>

Node Groups Provided by NNMi

NNMi Provides the following kinds of Node Groups:

- [Node Groups as Predefined View Filters](#). These Node Groups can also be used for Monitoring Configuration if you find them useful.
- ["Island Node Groups" \(on page 149\)](#). These Node Groups contain connected nodes that NNMi displays in a group that is not connected to the rest of the topology.

Node Groups As Predefined View Filters

NNMi provides the following Node Groups. You can configure these Node Groups with specific information about your management domain and change them to meet your needs.

Node Groups can be used to filter table and map views.

Node Groups Provided by NNMi

Name	Purpose
Important Nodes	<p>Caution: Do not delete this Node Group.</p> <p>This Node Group is used by the Causal Engine. Any devices in this group receive special treatment. When a current member of this group stops responding, the Causal Engine generates a "Node Down" incident and sets the device status to Critical. For example, when a WAN Edge Device is in the shadow of another problem (and, therefore, NNMi would normally not generate an incident about that WAN edge router), NNMi generates a "Node Down" incident because the router is listed in this Important Nodes group.</p> <p>This Node Group is empty by default. Consider populating this group with critical servers that run important applications and critical WAN routers.</p> <p><i>NNM iSPI for Performance.</i> This group automatically becomes a filter for Performance Reports (unless the group has no members). The NNMi administrator can change this default behavior. See "In the Console, Create Node Groups" (on page 127).</p>
Microsoft Windows Systems	<p>This Node Group includes any device manufactured by Microsoft. The Node Group definition is populated with one vendor entry. Any Microsoft devices within your management domain are automatically included in this Node Group.</p>
Networking Infrastructure Devices	<p>This Node Group is populated with a list of categories for network devices. Any devices within your management domain that match these categories are automatically included in this Node Group.</p> <p>Devices in this group are automatically monitored for Component Health fault metrics.</p> <p><i>NNM iSPI for Performance.</i> This group automatically becomes a filter for Performance Reports (unless the group has no members). The NNMi administrator can change this default behavior. See "In the Console, Create Node Groups" (on page 127).</p> <p><i>NNM iSPI NET.</i> By default, NNMi automatically uses diagnostic flows to monitor devices in this group.</p>
Non-SNMP Devices	<p>This Node Group includes any device that does not respond to SNMP. The Node Group definition is populated with one entry for a null MIB II sysObjectID value. Any device within your management domain that fails to respond to SNMP queries is automatically included in this Node Group.</p>
Routers	<p>This Node Group is populated with a list of categories for network devices that represent routers. Any router, switch-router, or gateway within your management domain is included in this Node Group. See Node Capabilities Provided by NNMi for more information.</p> <p>This filter is used to create the Routers Node Group map that NNMi provides by default in the Topology Maps workspace.</p> <p>Devices in this group are automatically monitored for Component Health fault metrics</p> <p><i>NNM iSPI for Performance.</i> Devices in this group are automatically monitored for performance, including Component Health performance metrics. This group automatically becomes a filter for Performance Reports.</p> <p>The NNMi administrator can change this default behavior. See "Set Default Monitoring" (on page 154), "Configure Node Monitoring" (on page 168), and "In the Console, Create Node Groups" (on page 127) for more information.</p>
Switches	<p>This Node Group is populated with a list of categories for network devices that represent switches. Any switch, ATM switch, or switch-router within your management domain is</p>

Name	Purpose
	included in this Node Group. See Node Capabilities Provided by NNMi for more information.
	This filter is used to create the Switches Node Group map that NNMi provides by default in the Topology Maps workspace.

Related Topics

["Island Node Groups" \(on page 149\)](#)

Island Node Groups

An Island Node Group is a group of fully-connected nodes that NNMi discovers and that are not connected to the rest of the topology.

An example of an environment with multiple Island Node Groups is a financial institution or retail store with many branches or stores. Each branch or store might be connected to other branches or stores with a WAN (Wide Area Network) connection. Each branch or store appears as an isolated island of nodes in the NNMi topology.

NNMi automatically updates Island Node Group discovery information whenever it detects changes in Layer 2 connections. NNMi uses the Discovery Interval to determine when the updates actually occur.

Note the following about Island Node Groups:

- NNMi selects a representative node in each Island Node Group as the Source Node associated with an Island Node Group incident. The representative node is selected using the following criteria:
 - Sort all routers in the Node Group alphabetically by name and choose the first one in the list
 - If no routers are in the Node Group, sort all nodes in the Node Group alphabetically by name and choose the first one in the list.
- Island Node Groups are identified using "Island" in the Node Group Name. NNMi also assigns each Island Node Group name a number to ensure the name is unique.
- Island Node Groups are managed internally. Therefore, NNMi administrators should not modify Island Node Group configurations. NNMi overrides any user changes the next time NNMi updates the Island Node Group discovery information.
- Island Node Groups must have at least two nodes.
- How the Status of Island Node Groups is calculated cannot be changed.

The only possible Status values for Island Node Groups are Unknown and Normal. Unknown indicates that NNMi cannot reach any nodes in the group. Normal indicates that NNMi can reach at least one node in the group.

Related Topics

["Node Groups As Predefined View Filters" \(on page 147\)](#)

Interface Groups Provided by NNMi

NNMi Provides the following Interface Groups as predefined view filters. These Interface Groups can also be used for Monitoring Configuration if you find them useful.

Feel free to populate these Interface Groups with specific information about your management domain and change them to meet your needs.

Interface Groups Provided by NNMi

Name	Purpose
ISDN Inter- faces	This Interface Group includes multiple interface types known to be commonly used for ISDN purposes. Any interface within your management domain that meets the defined criteria is automatically included in this Interface Group.
Link Aggre- gation	<i>NNMi Advanced</i> . This Interface Group includes all of the Link Aggregation Aggregator Interfaces discovered in the network. See Layer 2 Neighbor View Map Objects for more information about Aggregator Interfaces. Use Actions → Show Members to identify the Link Aggregation Aggregator Interfaces in this group.
Point to Point Inter- faces	This Interface Group includes multiple interface types known to be commonly used for point-to-point purposes. Any interface within your management domain that meets the defined criteria is automatically included in this Interface Group.
Software Loopback Interfaces	This Interface Group includes any interface that is IfType 24, software loopback from the IANA ifType-MIB. Any interface within your management domain that meets this loopback address ¹ criteria is automatically included in this Interface Group.
VLAN Inter- faces	This Interface Group includes interfaces of ifType I2vlan. The NNMi default Monitoring Configuration settings enable fault monitoring for these interfaces, but disable performance monitoring (because collection of performance data for VLAN interfaces tends to be problematic).
Voice Inter- faces	This Interface Group includes multiple interface types known to be commonly used for voice purposes. Any interface within your management domain that meets the defined criteria is automatically included in this Interface Group.

¹The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

Monitoring Network Health

Note: If you are using NNMi Advanced, also see ["Monitor Router Redundancy Groups \(NNMi Advanced\)" \(on page 181\)](#).

Before NNMi can monitor the health of your network, the following tasks must be completed:

- ["Configuring Communication Protocol" \(on page 47\)](#)
- ["Discovering Your Network" \(on page 76\)](#)

For the most flexibility, also complete these tasks:

- Review the ["Interface Groups Provided by NNMi" \(on page 149\)](#) and ["Node Groups Provided by NNMi" \(on page 147\)](#).
- Create your own groups by ["Creating Groups of Nodes or Interfaces" \(on page 126\)](#).

The State Poller and the Causal Engine work together to automatically monitor the health of your network. Many of the tasks you normally do to troubleshoot network problems are now automated. To learn more about how this works, see the following topics:

- ["About the State Poller" \(on page 151\)](#)
- ["The NNMi Causal Engine and Monitoring" \(on page 152\)](#)

You control which network devices NNMi monitors. By monitoring only the devices that are important within your network environment, you keep the amount of traffic generated by NNM to a minimum. You can configure NNMi to check devices with status *other than critical* less frequently (if at all) to prevent unimportant incidents from showing up in the Incident views.

To configure the polling policies that control how NNMi monitors devices in your network, see ["Configure Monitoring Behavior" \(on page 152\)](#). You can configure NNMi monitoring behavior to meet your needs.

About the State Poller

The State Poller Service monitors each discovered interface, address, and SNMP agent that is designated to be actively monitored in your management domain. State Poller can also be configured to provide Component Health monitoring and Router Redundancy Group monitoring.

State Poller gathers information in the following area and updates the **State** field on each object's form:

- Verifies that each monitored IP Address is responding to ICMP ping.
- Verifies that each monitored SNMP Agent is responding to SNMP queries.
- Issues an SNMP query for the following:
 - Each monitored interface, requesting the current value for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.)
 - Router Redundancy Groups.
 - Component Health data.
- By default, State Poller monitors interfaces connected to another known interface through a Layer 2 connection.
- You can extend monitoring to include the following:

- Unconnected interfaces
- Interfaces that have an IP address (for example a router interface that services mobile laptop machines)
- *NNM iSPI for Performance*. The State Poller also collects performance data and monitors thresholds. See ["Purchase an HP Smart Plug-in" \(on page 319\)](#).

The State Poller stores the results of the queries in the NNMi database and notifies the Causal Engine of any changes. The Causal Engine gathers additional information about the overall health of each interface and SNMP agent. Using this information the Causal Engine calculates the **Status** of each node, interface, and SNMP agent (see ["The NNMi Causal Engine and Monitoring" \(on page 152\)](#) for more information).








To configure the behavior of the State Poller, see ["Configure Monitoring Behavior" \(on page 152\)](#).

The NNMi Causal Engine and Monitoring

The Causal Engine actively gathers information about your network devices from incoming incidents and traps. The Causal Engine also uses the data gathered by [State Poller](#) and by [Discovery](#) to calculate the current health status of each node, interface, IP address, SNMP agent, and connection.

The health status is dynamic (based on what the environment looks like *now*).

The NNMi Causal Engine communicates device health information in the following ways:

- In the database, the Causal Engine stores a multitude of information about each device. You can access this information in the Node, Interface, IP Address, SNMP Agent, and connection forms.
- On the maps, the color of the background shape for each map icon changes to the color that represents the most currently calculated health status, based on the Causal Engine calculations for that node, interface, address, or connection ([click here for information about status colors](#)).
- On forms for Nodes, Interfaces, IP addresses, SNMP Agents, and connections, the Causal Engine updates the Status attribute to show the current status:  **Normal**,  **Warning**,  **Minor**,  **Major**,  **Critical**,  **Unknown**, or  **No Status**.
- The Status column in table views is updated.

The Causal Engine also uses health status information to determine root cause. See ["The NNMi Causal Engine and Incidents" \(on page 212\)](#) for more information about the Causal Engine, incidents, and root cause analysis.

Configure Monitoring Behavior

Certain devices in your network are the most important ones. You and your team must keep those devices up and running at all times. Adjust NNMi monitoring behavior to focus on the important devices and to check devices with status *other than critical* less frequently (if at all).

Note: NNMi does not poll any [private interface](#) or **Anycast Rendezvous Point IP Address**¹.

Based on your individual situation, adjust the NNMi behavior to meet your needs. NNMi applies your Monitoring Configuration settings in the following sequence:

¹Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

1. **Interface Settings:** NNMi monitors each of the Node's Interfaces and IP Addresses based on the first matching Interface Settings definition. The first match is the Interface Settings definition with the lowest Ordering number.
2. **Node Setting:** NNMi monitors each Node and each previously unmatched Interface or IP Address based on the first matching Node Settings definition. The first match is the Node Settings definition with the lowest Ordering number.

Note: Child node groups are included in the Ordering hierarchy. This means that if the parent node group has a lower Ordering number (for example, parent=10, child=20), then the monitoring configuration specified for the parent node group also applies to the nodes in the child node group. To override a parent node group monitoring configuration, set the Ordering number for the child node group to a number that is lower than the parent (for example, parent=20, child=10).
3. **Default Settings:** If no match is found for a Node, Interface, or IP Address in 1 or 2, NNMi applies the default Monitoring Configuration settings.

Tasks for Configuring the Monitoring Behavior


Task	How
"Set Global Monitoring" (on page 153) .	<i>Optional.</i> Use the Global Control group.
"Set Default Monitoring" (on page 154) .	Use the Default Settings tab to establish monitoring behavior for any devices that are discovered, but not included in any Node Settings or Interface Settings definitions.
"Configure Node Monitoring" (on page 168)	<i>Optional.</i> Use the Node Settings tab. Configure settings based on Node Groups to customize the way NNMi monitors certain groups of devices in your environment. Prerequisite: "Create Node Groups" (on page 126) .
Fine tune behavior for specific types of Interfaces, see "Configure Interface Monitoring" (on page 158) .	<i>Optional.</i> Use the Interface Settings tab. Configure settings based on Interface Groups to customize the way NNMi monitors certain interface types in your environment. Prerequisite: "Create Interface Groups" (on page 139) .

Set Global Monitoring

Note: To suspend all SNMP traffic generated by NNMi, rather than only the State Poller Service SNMP traffic, see ["Communication Region Form" \(on page 57\)](#) and ["Specific Node Settings Form \(Communication Settings\)" \(on page 67\)](#).

To temporarily turn off all NNMi monitoring activity without tampering with your customized monitoring configuration settings:

1. Navigate to the **Monitoring Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Monitoring Configuration**.
2. Locate the **Global Control** group box.
3. Clear the check box preceding each setting that you want to enable or disable (see [table](#)).

4. Click  **Save and Close**. NNMi applies your changes. The next regularly scheduled monitoring cycle uses the new settings.

Global Control


Name	Description
Enable State Polling	<p>If <input checked="" type="checkbox"/> enabled, State Poller monitors all managed interfaces, IP addresses, and SNMP agents by issuing ICMP pings and SNMP read-only queries for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the overall health of the device and is supplied by the SNMP Agent.) You can also configure NNMi so that State Poller gathers additional information about Component Health and Router Redundancy Groups.</p> <p>If <input type="checkbox"/> disabled:</p> <ul style="list-style-type: none">• Previously discovered devices remain with the last calculated state/status.• Newly discovered devices are set to "No Status" with map-symbol background shape color set to beige.
Enable Component Health Monitoring	<p>If <input checked="" type="checkbox"/> enabled, State Poller monitors Component Health metrics for all managed nodes. See Node Form: Component Health Tab for more information about Component Health metrics.</p> <p>Note: Component Health monitoring is enabled by default.</p> <p>If <input type="checkbox"/> disabled:</p> <ul style="list-style-type: none">• Previously discovered devices are assigned a State of Not Polled and a Status of No Status for Component Health metrics.• Component Health metrics for newly discovered devices are assigned a State of Not Polled and a Status of No Status.
Enable Router Redundancy Group Monitoring (NNMi Advanced)	<p>If <input checked="" type="checkbox"/> enabled, NNMi monitors all managed Router Redundancy Groups. See Router Redundancy Group View (NNMi Advanced) for more information about Router Redundancy Groups.</p> <p>Note: Router Redundancy Group monitoring is enabled by default.</p> <p>If <input type="checkbox"/> disabled:</p> <ul style="list-style-type: none">• Previously discovered Router Redundancy Groups are assigned a State of Not Polled and a Status of No Status.• Newly discovered Router Redundancy Groups are assigned a State of Not Polled and a Status of No Status.

Set Default Monitoring

The choices you make for "defaults" apply only to devices whose interfaces, IP addresses, SNMP agents (Management Addresses), tracked objects, router redundancy groups, or component health monitoring settings are not covered by any Interface Settings or Node Settings definitions.

To establish default NNMi monitoring behavior:

1. Navigate to the **Defaults Settings** tab.
 - a. From the workspace navigation panel, select the **Configuration** workspace.

- b. Select **Monitoring Configuration**.
 - c. Locate the **Defaults Settings** tab.
2. Locate the **Default Fault Monitoring** group box.
3. Configure the Default Fault Monitoring behavior (see [Default Fault Monitoring table](#)).
4. *NNM iSPI for Performance*. If the NNM iSPI for Performance is installed, locate the **Default Performance Monitoring** group box.
Configure the Default Performance Monitoring behavior (see [Default Performance Monitoring table](#)).
5. By default, NNMi monitors only interfaces that are connected to other interfaces. When SNMP polling is enabled, NNMi automatically detects most connections. See ["Add or Delete a Layer 2 Connection" \(on page 124\)](#) for information about manual overrides.
Optional. If you want to expand default monitoring behavior to include unconnected Interfaces, indicate your choices in the extend the scope of polling beyond connected Interfaces group box (see [Default Extend the Scope of Polling Beyond Connected Interfaces table](#)).
6. *Optional*. To establish custom monitoring behavior for one or more groups of interfaces, configure Interface Settings, see ["Configure Interface Monitoring" \(on page 158\)](#).
7. *Optional*. To establish custom monitoring behavior for one or more groups of nodes, configure Node Settings, see ["Configure Node Monitoring" \(on page 168\)](#).
8. Click  **Save and Close**. NNMi applies your changes. The next regularly scheduled monitoring cycle uses the new settings.

Default Fault Monitoring

Attribute	Description
Enable ICMP Fault Polling Note: This monitoring option is useful for devices that do not support SNMP. By default, this feature is enabled for the "Non-SNMP Devices" Node Group .	If <input checked="" type="checkbox"/> enabled, State Poller issues ICMP (ping) requests to verify the availability of each managed IP address. Note: In the Global Control section of this form, the Enable State Polling attribute must be enabled, too. If <input type="checkbox"/> disabled, State Poller suspends ICMP polling of all IP addresses: <ul style="list-style-type: none"> • IP addresses (both previously discovered and newly discovered) have a State attribute value of "Not Polled" and a Status attribute value of "No Status" with the color of the IP address map-symbol set to beige. See Layer 3 Neighbor View. • If both ICMP and SNMP are disabled for a Node, the Node has a Status attribute value of "No Status" and the color of the Node map-symbol background shape is set to beige. Tip: To turn off ICMP polling within a subset of your network environment, use the Communication Configuration workspace Region definitions. For example, you can easily turn off ICMP communication to all private addresses (use the Private IP Addresses region). You can also define your own Regions that identify any unreachable addresses in your management domain.
Enable SNMP Fault Polling	If <input checked="" type="checkbox"/> enabled, State Poller monitors all interfaces by issuing SNMP read-only queries to devices assigned to this level of the monitoring hierarchy. By default, any connected interface is monitored for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.) If you have <i>unconnected</i>

Attribute	Description
	<p>interfaces that you want to monitor, expand NNMi monitoring behavior with the Poll Unconnected Interfaces and the Poll Interfaces Hosting IP Addresses attributes.</p> <p>Note: The following attributes must also be enabled:</p> <ul style="list-style-type: none"> • In the Global Control section of this form, the Enable State Polling attribute must be enabled, too. See Layer 2 Neighbor View. (See "Set Global Monitoring" (on page 153) for more information.) • In the Communication Configuration view, enable State Poller queries with the applicable Enable SNMP Communication attributes (see "Configuring Communication Protocol" (on page 47) for more information). <p>If <input type="checkbox"/> disabled, for devices assigned to this level of the monitoring hierarchy:</p> <ul style="list-style-type: none"> • Causal Engine calculates Status based only on IP address State. • The following previously discovered objects change to a State attribute value of "Not Polled" and a Status attribute value of "No Status": <ul style="list-style-type: none"> ▪ Interfaces (plus any related map-symbol changes to a beige color) ▪ Router Redundancy Groups (plus any related map-symbol changes to a beige color) ▪ Any fault-related items listed on the Node form, Component Health tab
<p>Enable Component Health Fault Polling</p> <p>Note: By default, this feature is enabled for the "Routers" and "Networking Infrastructure Devices" Node Groups.</p>	<p>Use this attribute to poll Component Health fault metrics. Component Health fault metrics include the following: Fan, Power Supply, Temperature, and Voltage.</p> <p>Note: Component Health Fault Polling is disabled by default.</p> <p>If <input checked="" type="checkbox"/> enabled, NNMi gathers fault data related to the Component Health fault metrics in devices assigned to this level of the monitoring hierarchy.</p> <p>If <input type="checkbox"/> disabled, NNMi does not extend data collection behavior to include Component Health fault data about devices assigned to this level of the monitoring hierarchy.</p> <p>Note: NNMi uses the same polling interval set for the Fault Polling Interval.</p>
<p>Fault Polling Interval</p>	<p>The time that State Poller waits between issuing queries to gather information for any of the following that are enabled: ICMP Polling, SNMP Polling, Poll Unconnected Interfaces, and Poll Interfaces Hosting IP addresses.</p> <p>Note: NNMi monitors SNMP agents (Management Addresses) according to this Fault Polling Interval, <i>even if ICMP Polling, SNMP Polling, Poll Unconnected Interfaces, and Poll Interfaces Hosting IP addresses are all disabled</i>. To prevent an SNMP Agent's address from being monitored, one of the following must be true: State Polling is disabled, current Communication Configuration settings turn off SNMP for the SNMP agent's address, or the parent Node is set to Not Managed or Out of Service.</p>

NNM iSPI for Performance. Default Performance Monitoring

Attribute	Description
Enable SNMP Interface Performance Polling	<p><i>NNM iSPI for Performance.</i> Use this attribute to extend the range of polling data that NNMi collects. NNM iSPI for Performance uses the additional data in a series of performance reports. See "Purchase an HP Smart Plug-in" (on page 319) for more information. When enabled, network traffic increases on your network because NNMi gathers performance data about each member of this group on a regular schedule.</p> <p>If <input checked="" type="checkbox"/> enabled, NNMi gathers performance data from Interfaces, CPU, memory, and buffers in devices assigned to this level of the monitoring hierarchy.</p> <p>If <input type="checkbox"/> disabled, NNMi does not extend data collection behavior to include performance data about devices assigned to this level of the monitoring hierarchy.</p> <p>Note: The Enable State Polling field must be enabled, too. By default the performance of connected interfaces and addresses is monitored. If you have <i>unconnected</i> interfaces that you want to monitor, expand NNMi monitoring behavior by enabling Poll Unconnected Interfaces.</p>
Enable Component Health Performance Polling	<p><i>NNM iSPI for Performance.</i> Use this attribute to poll Component Health performance. An NNMi administrator can set the threshold for node components related to the following performance metrics: CPU utilization, memory utilization, buffer utilization, buffer miss rate, and buffer failure rate.</p> <p>Note: <i>NNM iSPI for Performance.</i> By default, this feature is enabled for the "Routers" Node Group.</p> <p>Note: Component Health Performance Polling is disabled by default.</p> <p>If <input checked="" type="checkbox"/> enabled, NNMi gathers performance data related to the Component Health performance metrics in devices assigned to this level of the monitoring hierarchy.</p> <p>If <input type="checkbox"/> disabled, NNMi does not extend data collection behavior to include Component Health performance data about devices assigned to this level of the monitoring hierarchy.</p> <p>Note: NNMi uses the same polling interval set for the Performance Polling Interval.</p>
Performance Polling Interval	<p>If you purchase and install the NNM iSPI for Performance, use this field to set the time period that NNMi waits between issuing network traffic to gather performance data.</p>

Default Extend the Scope of Polling Beyond Connected Interfaces




Attribute	Description
Poll Unconnected Interfaces	<p>If <input checked="" type="checkbox"/> enabled, NNMi monitors all interfaces within discovered devices (both connected and unconnected). All interfaces are monitored for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.) Note: The Enable State Polling field must be enabled, and SNMP polling of some type must be enabled (for example, Enable SNMP Fault Monitoring and Enable SNMP Performance Polling).</p> <p>If <input type="checkbox"/> disabled, State Poller polls according to other configuration settings.</p> <p>Tip: Your discovery configuration choices may need to be adjusted to get the results you want. For example, to meet the "connected" criteria for interfaces in switches that do not have an IP address you must add the device to which the interface is connected as a discovery seed. See "Discovery Seeds (as a starting point)" (on page 82).</p>

Attribute	Description
Poll Interfaces Hosting IP Addresses	<p>If <input checked="" type="checkbox"/> enabled, any unconnected interface that has one or more addresses associated with it is monitored for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.) Note: The Enable State Polling field must be enabled, and SNMP polling of some type must be enabled (for example, Enable SNMP Fault Monitoring and Enable SNMP Performance Polling).</p> <p>By monitoring the Interface (in addition to the IP address), NNMi can make more informed decisions about the health of each IP address associated with an unconnected interface.</p> <p>If <input type="checkbox"/> disabled, State Poller polls according to other configuration settings.</p> <p>Tip: The Communication Configuration workspace provides a method of overriding this setting for specific Regions. For this purpose, NNMi provides a predefined Region definition of all possible private addresses (Private IP Addresses). You can also define your own Region to easily turn off ICMP polling to any unreachable addresses in your management domain.</p>

Configure Interface Monitoring



Before you start, you must establish one or more [Interface Group](#) definitions that identify the interface types to which these monitoring settings will apply. NNMi provides nearly 250 interface types to choose from. Interface monitoring applies to matching interfaces and the IP addresses that are hosted on those interfaces. See also, ["Interface Groups Provided by NNMi" \(on page 149\)](#).

To establish monitoring behavior for one or more predefined Interface Groups:

1. Navigate to the **Interface Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Monitoring Configuration**.
 - c. Locate the **Interface Settings** tab.
 - d. Do one of the following:
 - To create an Interface Settings definition, click the  New icon.
 - To edit an Interface Settings definition, select a row, click the  Open icon.
 - To delete an Interface Settings definition, select a row and click the  Delete button
2. Establish the appropriate settings to identify this Interface Setting definition (see [Basics table](#)).
3. *Optional.* Configure the Fault Monitoring behavior for this Interface Setting definition (see [Fault Monitoring table](#)).
4. *NNM iSPI for Performance.* If the NNM iSPI for Performance is installed:
 - Configure the Performance Monitoring behavior for this Interface Setting definition (see [Performance Monitoring table](#)).
 - *Optional.* Navigate to the Threshold Settings tab to configure the NNM iSPI for Performance. See ["Configure Threshold Monitoring for Interfaces \(NNM iSPI for Performance\)" \(on page 162\)](#) for more information.
5. By default, NNMi monitors only interfaces that are connected to other interfaces. When SNMP polling

is enabled, NNMi automatically detects most connections. See ["Add or Delete a Layer 2 Connection" \(on page 124\)](#) for information about manual overrides.

Optional. If you want to expand monitoring behavior for this group to include unconnected Interfaces, indicate your choices in the extend the scope of polling beyond connected Interfaces group box (see the [Extend the Scope of Polling Beyond Connected Interfaces table](#)).

6. Click  **Save and Close** to return to the Monitoring Configuration form.
7. Click  **Save and Close**. NNMi applies your changes. The next regularly scheduled monitoring cycle uses the new settings.

Caution: When you establish monitoring configuration settings, NNMi must recalculate membership in all Node Groups and Interface Groups. This can take some time and slow down your system. Consider making this change during a slow time in your network environment.

Optional. Customize the node monitoring behavior. See ["Configure Node Monitoring" \(on page 168\)](#) .

Basics

Attribute	Description
Ordering	<p>Enter a unique string (any length), characters 0 through 9. Consider using increments of 100 to allow for inserts between existing items over time.</p> <p>NNMi decides which monitoring configurations apply to a node or interface based on the ordering number assigned to the configuration definitions. NNMi monitors the device according to the first match (checked from lowest number to highest number within each category). Categories are read in sequence. Click here for a description of the sequence.</p> <ol style="list-style-type: none"> 1. Interface Settings: NNMi monitors each of the Node's Interfaces and IP Addresses based on the first matching Interface Settings definition. The first match is the Interface Settings definition with the lowest Ordering number. 2. Node Setting: NNMi monitors each Node and each previously unmatched Interface or IP Address based on the first matching Node Settings definition. The first match is the Node Settings definition with the lowest Ordering number. <p>Note: Child node groups are included in the Ordering hierarchy. This means that if the parent node group has a lower Ordering number (for example, parent=10, child=20), then the monitoring configuration specified for the parent node group also applies to the nodes in the child node group. To override a parent node group monitoring configuration, set the Ordering number for the child node group to a number that is lower than the parent (for example, parent=20, child=10).</p> <ol style="list-style-type: none"> 3. Default Settings: If no match is found for a Node, Interface, or IP Address in 1 or 2, NNMi applies the default Monitoring Configuration settings. <p>No duplicate Ordering numbers are allowed. Each Interface Setting ordering number must be unique.</p>
Interface Group	Choose one predefined Interface Group from the list. See "Create Interface Groups" (on page 139) for more information.

Fault Monitoring

Attribute	Description
<p>Enable ICMP Fault Polling</p> <p>Note: This monitoring option is useful for devices that do not support SNMP.</p>	<p>If <input checked="" type="checkbox"/> enabled, State Poller issues ICMP (ping) requests to verify the availability of each managed IP address. Note: In the Global Control section of this form, the Enable State Polling attribute must be enabled, too.</p> <p>If <input type="checkbox"/> disabled, State Poller suspends ICMP polling of all IP addresses:</p> <ul style="list-style-type: none"> IP addresses (both previously discovered and newly discovered) have a State attribute value of "Not Polled" and a Status attribute value of "No Status" with the color of the IP address map-symbol set to beige. See Layer 3 Neighbor View. If both ICMP and SNMP are disabled for a Node, the Node has a Status attribute value of "No Status" and the color of the Node map-symbol background shape is set to beige. <p>Tip: To turn off ICMP polling within a subset of your network environment, use the Communication Configuration workspace Region definitions. For example, you can easily turn off ICMP communication to all private addresses (use the Private IP Addresses region). You can also define your own Regions that identify any unreachable addresses in your management domain.</p>
<p>Enable SNMP Fault Polling</p>	<p>If <input checked="" type="checkbox"/> enabled, State Poller monitors all interfaces by issuing SNMP read-only queries to devices assigned to this level of the monitoring hierarchy.</p> <p>By default, any connected interface is monitored for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.) If you have <i>unconnected</i> interfaces that you want to monitor, expand NNMi monitoring behavior with the Poll Unconnected Interfaces and the Poll Interfaces Hosting IP Addresses attributes.</p> <p>Note: The following attributes must also be enabled:</p> <ul style="list-style-type: none"> In the Global Control section of this form, the Enable State Polling attribute must be enabled, too. See Layer 2 Neighbor View. (See "Set Global Monitoring" (on page 153) for more information.) In the Communication Configuration view, enable State Poller queries with the applicable Enable SNMP Communication attributes (see "Configuring Communication Protocol" (on page 47) for more information). <p>If <input type="checkbox"/> disabled, for devices assigned to this level of the monitoring hierarchy:</p> <ul style="list-style-type: none"> Causal Engine calculates Status based only on IP address State. The following previously discovered objects change to a State attribute value of "Not Polled" and a Status attribute value of "No Status": <ul style="list-style-type: none"> Interfaces (plus any related map-symbol changes to a beige color) Router Redundancy Groups (plus any related map-symbol changes to a beige color) Any fault-related items listed on the Node form, Component Health tab
<p>Fault Polling Interval</p>	<p>The time that State Poller waits between issuing queries to gather information for any of the following that are enabled: ICMP Polling, SNMP Polling, Poll Unconnected Interfaces, and Poll Interfaces Hosting IP addresses.</p> <p>Note: NNMi monitors SNMP agents (Management Addresses) according to this Fault Polling Interval, <i>even if ICMP Polling, SNMP Polling, Poll Unconnected Interfaces, and</i></p>

Attribute	Description
	<i>Poll Interfaces Hosting IP addresses are all disabled.</i> To prevent an SNMP Agent's address from being monitored, one of the following must be true: State Polling is disabled, current Communication Configuration settings turn off SNMP for the SNMP agent's address, or the parent Node is set to Not Managed or Out of Service .

NNM iSPI for Performance. Performance Monitoring

Attribute	Description
Enable SNMP Interface Performance Polling	<p><i>NNM iSPI for Performance.</i> Use this attribute to extend the range of polling data that NNMi collects. NNM iSPI for Performance uses the additional data in a series of performance reports. See "Purchase an HP Smart Plug-in" (on page 319) for more information. When enabled, network traffic increases on your network because NNMi gathers performance data about each member of this group on a regular schedule.</p> <p>If <input checked="" type="checkbox"/> enabled, NNMi gathers performance data from Interfaces, CPU, memory, and buffers in devices assigned to this level of the monitoring hierarchy.</p> <p>If <input type="checkbox"/> disabled, NNMi does not extend data collection behavior to include performance data about devices assigned to this level of the monitoring hierarchy.</p> <p>Note: The Enable State Polling field must be enabled, too. By default the performance of connected interfaces and addresses is monitored. If you have <i>unconnected</i> interfaces that you want to monitor, expand NNMi monitoring behavior by enabling Poll Unconnected Interfaces.</p>
Performance Polling Interval	If you purchase and install the NNM iSPI for Performance, use this field to set the time period that NNMi waits between issuing network traffic to gather performance data.

Extend the Scope of Polling Beyond Connected Interfaces

Attribute	Description
Poll Unconnected Interfaces	<p>If <input checked="" type="checkbox"/> enabled, NNMi monitors all interfaces within discovered devices (both connected and unconnected). All interfaces are monitored for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.) Note: The Enable State Polling field must be enabled, and SNMP polling of some type must be enabled (for example, Enable SNMP Fault Monitoring and Enable SNMP Performance Polling).</p> <p>If <input type="checkbox"/> disabled, State Poller polls according to other configuration settings.</p> <p>Tip: Your discovery configuration choices may need to be adjusted to get the results you want. For example, to meet the "connected" criteria for interfaces in switches that do not have an IP address you must add the device to which the interface is connected as a discovery seed. See "Discovery Seeds (as a starting point)" (on page 82).</p>

Attribute	Description
Poll Interfaces Host- ing IP Addresses	<p>If <input checked="" type="checkbox"/> enabled, any unconnected interface that has one or more addresses associated with it is monitored for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.)</p> <p>Note: The Enable State Polling field must be enabled, and SNMP polling of some type must be enabled (for example, Enable SNMP Fault Monitoring and Enable SNMP Performance Polling).</p> <p>Note: This monitoring option is use- ful for Router interfaces.</p> <p>By monitoring the Interface (in addition to the IP address), NNMi can make more informed decisions about the health of each IP address associated with an unconnected interface.</p> <p>If <input type="checkbox"/> disabled, State Poller polls according to other configuration settings.</p> <p>Tip: The Communication Configuration workspace provides a method of overriding this setting for specific Regions. For this purpose, NNMi provides a predefined Region definition of all possible private addresses (Private IP Addresses). You can also define your own Region to easily turn off ICMP polling to any unreachable addresses in your management domain.</p>

Configure Threshold Monitoring for Interfaces (*NNM iSPI for Performance*)

Use the Threshold Settings form to configure NNMi and the NNM iSPI for Performance to monitor thresholds in your network environment. (See ["Purchase an HP Smart Plug-in" \(on page 319\)](#) for more information about the NNM iSPI for Performance.) If you set thresholds, NNMi can generate an Incident when any threshold is violated. Examples of the types of threshold you can set for an interface include the following: (See [Monitored Attributes](#) in the table below for a complete list.)



- Input and output utilization
- Input and output error rates
- Input and output discard rates







NNM iSPI for Performance provides exceptions reports to track the frequency of threshold breaches. You can open these reports with **Actions** → **Reporting - Report Menu** in the incident, node, or interface views and forms. (See [NNM iSPI for Performance Actions](#).)

To establish threshold monitoring behavior for the NNM iSPI for Performance:

1. *Prerequisite.* After enabling Performance Monitoring for an Interface Group and before setting thresholds, analyze performance data over time to determine wise threshold settings for each group. See ["Determine Reasonable Threshold Settings \(NNM iSPI for Performance\)" \(on page 175\)](#).

Note: When performance polling is enabled, network traffic increases on your network while NNMi gathers performance data.

2. Navigate to the **Thresholds Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Monitoring Configuration**.
 - c. Navigate to the **Interface Settings** tab.
 - d. Do one of the following:
 - To create an Interface Settings definition, click the  New icon.
 - To edit an Interface Settings definition, select a row, click the  Open icon.

3. Verify that Performance Monitoring is enabled for this Interface Settings definition.
4. In the **Interface Settings** form, navigate to the **Threshold Settings** tab.
5. Do one of the following:
 - To create a threshold definition, click the  New icon.
 - To edit a threshold definition, select a row, click the  Open icon.
 - To delete a threshold definition, select a row and click the  Delete icon.
6. Select the attribute you want to monitor and establish the threshold values for that attribute (see [Basic Threshold Settings table](#)). For examples of setting meaningful thresholds, see ["Examples of Threshold Monitoring \(NNM iSPI for Performance\)" \(on page 175\)](#).
7. Click  **Save and Close** to return to the **Interface Settings** form.
8. Click  **Save and Close** to return to the **Monitoring Configuration** form.
9. Click  **Save and Close**. NNMi applies your changes during the next regularly scheduled monitoring cycle.

Note: Threshold Incidents are disabled by default within NNMi to prevent Incident storms. If you are ready to generate Threshold Incidents, see ["Generate Performance Threshold Incidents \(NNM iSPI for Performance\)" \(on page 298\)](#). See also ["Custom Incident Attributes Provided by NNMi" \(on page 214\)](#) for a description of the special custom incident attributes available in Threshold Incidents.

Basic Threshold Settings

Attribute	Description
Monitored Attribute	NNMi gathers data to calculate thresholds for the following values. Click any item in this list for more details about that value.

Note: NNMi also displays the Monitored Attributes that apply to nodes. See ["Configure Threshold Monitoring for Nodes \(NNM iSPI for Performance\)" \(on page 172\)](#) for more information about these attributes.

- **Input Utilization**
The total number of incoming octets traversing the interface as a percentage of the total possible number of octets (based on the ifSpeed value). From Interface to Interface, the exact MIB variables queried vary based on interface speed and whether the system supports the high speed counters for interfaces.

Each interface in an Interface Groups has its utilization calculated by taking the total traffic on all administratively up interfaces in the group and dividing that by the total possible bandwidth.

Tip: To override the ifSpeed value returned by the device's SNMP agent, see the [Interface form](#).

- **Output Utilization**
The total number of outbound octets traversing the interface as a percentage of the total possible number of octets (based on the ifSpeed value). From Interface to Interface, the exact MIB variables queried vary based on interface speed and whether the system supports the high speed counters for interfaces.

Each interface in an Interface Group has its utilization calculated by taking the total traffic on all administratively up interfaces in the group and dividing that by the total possible bandwidth.

Attribute	Description
	<p>sible bandwidth.</p> <p>Tip: To override the ifSpeed value returned by the device's SNMP agent, see the Interface form.</p> <ul style="list-style-type: none"> • Input Error Rate Percentage based on the reported change in the number of input packets on the interface and the packet error count. What constitutes an error is system specific, but likely includes such issues as bad packet checksums, incorrect header information, and runt packets. • Output Error Rate Percentage based on the reported change in the number of incoming packets with errors as a percentage of total incoming packets. What constitutes an error is system specific, but likely includes such issues as collisions and buffer errors. • Input Discard Rate Percentage based on the reported change in the number of input packets on the interface and the discarded packet count. Packets may be discarded because of a variety of issues, including receive buffer overflows, congestion, or system specific issues. • Output Discard Rate Percentage based on the reported change in the number of output packets on the interface and the discarded packet count. Packets may be discarded because of a variety of issues, including transmission buffer overflows, congestion, or system specific issues.
High Value	<p>Designate the percentage above which would indicate a value in the High range. Valid entries are 0.00 through 100.00</p> <p>Note: If you use 100.00 the threshold is disabled because it cannot be crossed.</p>
High Value Rearm	<p>Designate the percentage that when reached would indicate the end of a high threshold situation. Valid entries are 0.00 through 100.00</p> <p>Note: The High Value Rearm must be less than or equal to the High Value and greater than the Low Value Rearm.</p>
High Trigger Count	<p>Designate the number of consecutive polling cycles in which the value must remain in the High range before the threshold state changes to High.</p> <p>Note: The interface performance values are the average value over the entire polling interval, so a trigger count of 1 is usually appropriate.</p>
Low Value	<p>The Low Value must be less than or equal to the High Value.</p> <p>Designate the percentage below which would indicate a value in the low range. Valid entries are 0.00 through 100.00</p> <p>Note: If you use 0.00 the threshold is disabled because it cannot be crossed.</p>
Low Value Rearm	<p>Designate the percentage that when reached would indicate the end of a low threshold situation. Valid entries are 0.00 through 100.00.</p> <p>Note: The Low Value Rearm must be greater than or equal to the Low Value and less than the High Rearm Value.</p>
Low Trigger Count	<p>Designate the number of consecutive polling cycles in which the value must remain in the Low range before the threshold state changes to Low.</p>

Attribute	Description
	Note: The interface performance values are the average value over the entire polling interval, so a trigger count of 1 is usually appropriate.

Determine Reasonable Threshold Settings (*NNM iSPI for Performance*)

You must decide how to define normal behavior for devices in the associated Node Group or Interface Group. You can then set reasonable thresholds for the group, and avoid Threshold Incident storms. See ["Examples of Threshold Monitoring \(NNM iSPI for Performance\)" \(on page 175\)](#).

Create a Node Group or Interface Group filter that includes the devices you want to monitor. Export the Node Group or Interface Group filter to NNM iSPI for Performance. See ["Creating Groups of Nodes or Interfaces" \(on page 126\)](#).

Enable Performance Monitoring for the Node Group or Interface Group. See ["Configure Node Monitoring" \(on page 168\)](#) or ["Configure Interface Monitoring" \(on page 158\)](#). Then wait a minimum of 24 hours before following the steps below.

Access the NNM iSPI for Performance Headline report:

1. In the NNMi console, click **Actions** → **Reporting - Report Menu**.
2. Click the link for **Headline**. The Headline report displays data up until 12 p.m.last night.
3. Click **Show Options**.
4. Expand the **All Nodes/Interfaces** selection.
5. Choose the Node Group or Interface Group filter for which you are setting thresholds.
6. Expand **All Dates/Times**. Select a time period (a day, week, or month).
7. Click **Confirm Selections**.
8. The report for the Node Group or Interface Group you selected appears.
9. Study the Range & Exceptions graphs to guide your decision about what constitutes reasonable threshold settings. See online help for this report for information about how to read this report.

Examples of Threshold Monitoring (*NNM iSPI for Performance*)

You can configure interface threshold monitoring if the NNM iSPI for Performance is installed. See ["Purchase an HP Smart Plug-in" \(on page 319\)](#) for more information.

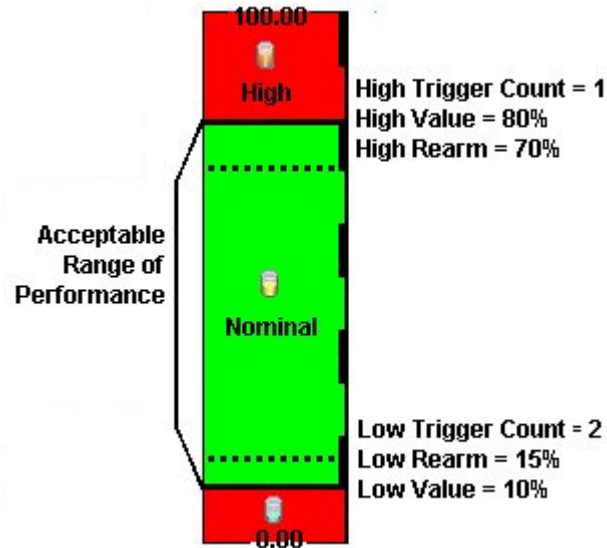
Several examples are presented These examples are not intended to be recommendations. Consider all aspects of your network environment and set performance thresholds that are meaningful in your environment:

- [Thresholds to Monitor Utilization on WAN Connections](#)
- [Thresholds to Monitor Utilization on Important Interfaces](#)
- [Thresholds to Monitor Important Interfaces for Discards](#)
- [Thresholds to Monitor Important Interfaces for Errors](#)

Example 1: Monitor Utilization on WAN Connections

You want to monitor the connections between two sites to verify that your service provider is meeting their guaranteed throughput volume. You pay a fixed cost for a specific bandwidth over this WAN interface.

- Monitor for under-utilization which wastes money (less than 10%).
Tip: If you don't care about under-utilization, set Low Value and Rearm to 0% as shown in Example 2.
- Monitor for over-utilization, which may result in performance bottlenecks or service provider surcharges (greater than 80%).



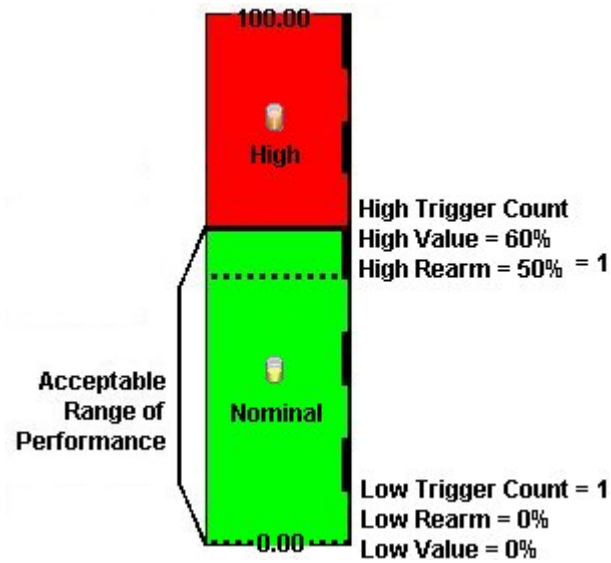
Note: Sometimes an Interface's MIB II ifspeed value is not reported accurately. This may result in threshold calculations outside the 0.00 - 100.00 range. If this happens, the Interface threshold State set to "Unavailable." To correct the problem:

1. Access the **Inventory** workspace
2. Open **Interface** view.
3. Open the form for the Interface that is reporting a threshold state of "Unavailable."
4. Navigate to the **General** tab.
5. Enter a valid entry in **Input Speed** or **Output Speed** (this overrides the value returned by the device's SNMP agent so that NNMi can accurately calculate utilization thresholds).

Example 2: Monitor Utilization on Important Interfaces

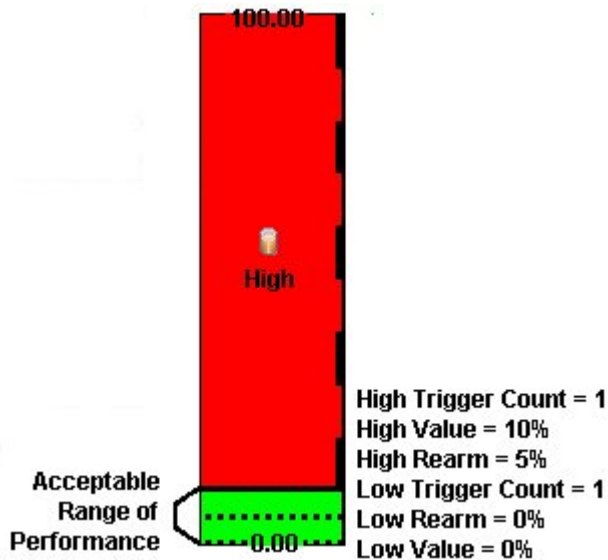
You want to monitor an important Ethernet interface and be notified if it is getting overloaded.

An Ethernet interface configured for full-duplex operation has an acceptable operating range of 0-60%. When average utilization is greater than 60%, NNM generates a High Threshold incident.



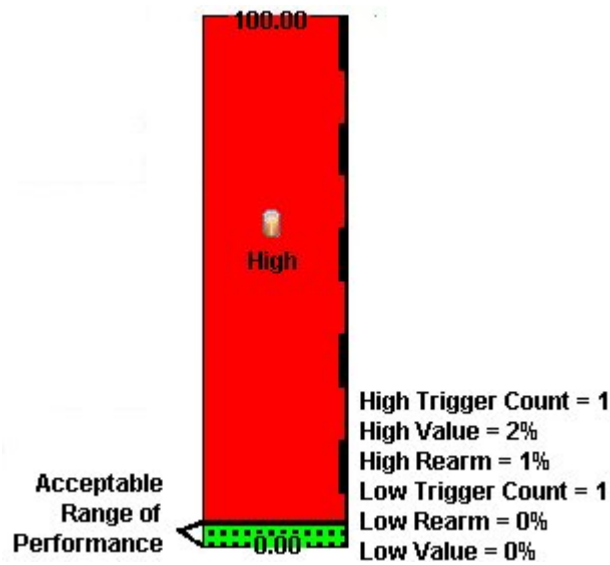
Example 3: Monitor Important Interfaces for Discards

You want to know anytime an interface is dropping data. The acceptable limit for interface discards is 10%. The threshold state is High when the discard rate exceeds 10% and returns to Nominal when the discard rate drops below 5%.



Example 4: Monitor Important Interfaces for Errors



You want to know if packet errors occur. The acceptable limit for packet errors is 2%. The threshold state is High Level (HL) when the error rate exceeds 2% and returns to normal when the error rate drops below 1%.




Configure Node Monitoring

Before you start, you must establish one or more [Node Group](#) definitions that identify the nodes to which these monitoring settings will apply. See also, "[Node Groups Provided by NNMi](#)" (on page 147).

To establish monitoring behavior for a predefined Node Group:

1. Navigate to the **Node Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Monitoring Configuration**.
 - c. Locate the **Node Settings** tab.
 - d. Do one of the following:
 - To create a Node Settings definition, click the  New icon.
 - To edit a Node Settings definition, select a row, click the  Open icon.
2. Establish the appropriate settings to identify this Node Setting definition (see [Basics table](#)).
3. *Optional.* Configure the Fault Monitoring behavior for this Node Setting definition (see [Fault Monitoring table](#)).
4. *NNM iSPI for Performance.* If the NNM iSPI for Performance is installed:
 - Configure the Performance Monitoring behavior for this Node Setting definition (see [Performance Monitoring table](#)).
 - *Optional.* Navigate to the Threshold Settings tab to configure the NNM iSPI for Performance. See "[Configure Threshold Monitoring for Nodes \(NNM iSPI for Performance\)](#)" (on page 172) for more information.
5. By default, NNMi monitors only interfaces that are connected to other interfaces. When SNMP polling is enabled, NNMi automatically detects most connections. See "[Add or Delete a Layer 2 Connection](#)" (on page 124) for information about manual overrides.

Optional. If you want to expand monitoring behavior for this group to include unconnected Interfaces, indicate your choices in the extend the scope of polling beyond connected Interfaces group box (see the [Extend the Scope of Polling Beyond Connected Interfaces table](#)).

6. Click  **Save and Close**. NNMi applies your changes. The next regularly scheduled monitoring cycle uses the new settings.

Caution: When you establish monitoring configuration settings, NNMi must recalculate membership in all Node Groups and Interface Groups. This can take some time and slow down your system. Consider making this change during a slow time in your network environment.

Optional. Customize the interface monitoring behavior. See ["Configure Interface Monitoring" \(on page 158\)](#)

Basics

Attribute	Description
Ordering	<p>Enter a unique string (any length), characters 0 through 9. Consider using increments of 100 to allow for inserts between existing items over time.</p> <p>NNMi decides which monitoring configurations apply to a node or interface based on the ordering number assigned to the configuration definitions. NNMi monitors the device according to the first match (checked from lowest number to highest number within each category). Categories are read in sequence. Click here for a description of the sequence.</p> <ol style="list-style-type: none"> 1. Interface Settings: NNMi monitors each of the Node's Interfaces and IP Addresses based on the first matching Interface Settings definition. The first match is the Interface Settings definition with the lowest Ordering number. 2. Node Setting: NNMi monitors each Node and each previously unmatched Interface or IP Address based on the first matching Node Settings definition. The first match is the Node Settings definition with the lowest Ordering number. <p>Note: Child node groups are included in the Ordering hierarchy. This means that if the parent node group has a lower Ordering number (for example, parent=10, child=20), then the monitoring configuration specified for the parent node group also applies to the nodes in the child node group. To override a parent node group monitoring configuration, set the Ordering number for the child node group to a number that is lower than the parent (for example, parent=20, child=10).</p> <ol style="list-style-type: none"> 3. Default Settings: If no match is found for a Node, Interface, or IP Address in 1 or 2, NNMi applies the default Monitoring Configuration settings. <p>No duplicate Ordering numbers are allowed. Each Node Setting ordering number must be unique.</p>
Node Group	Choose one predefined Node Group from the list. See "Create Node Groups" (on page 126) for more information.

Fault Monitoring

Attribute	Description
<p>Enable ICMP Fault Polling</p> <p>Note: This monitoring option is useful for devices that do not support SNMP. By default, this feature is enabled for the "Non-SNMP Devices" Node Group.</p>	<p>If <input checked="" type="checkbox"/> enabled, State Poller issues ICMP (ping) requests to verify the availability of each managed IP address. Note: In the Global Control section of this form, the Enable State Polling attribute must be enabled, too.</p> <p>If <input type="checkbox"/> disabled, State Poller suspends ICMP polling of all IP addresses:</p> <ul style="list-style-type: none"> IP addresses (both previously discovered and newly discovered) have a State attribute value of "Not Polled" and a Status attribute value of "No Status" with the color of the IP address map-symbol set to beige. See Layer 3 Neighbor View. If both ICMP and SNMP are disabled for a Node, the Node has a Status attribute value of "No Status" and the color of the Node map-symbol background shape is set to beige. <p>Tip: To turn off ICMP polling within a subset of your network environment, use the Communication Configuration workspace Region definitions. For example, you can easily turn off ICMP communication to all private addresses (use the Private IP Addresses region). You can also define your own Regions that identify any unreachable addresses in your management domain.</p>
<p>Enable SNMP Fault Polling</p>	<p>If <input checked="" type="checkbox"/> enabled, State Poller monitors all interfaces by issuing SNMP read-only queries to devices assigned to this level of the monitoring hierarchy.</p> <p>By default, any connected interface is monitored for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.) If you have <i>unconnected</i> interfaces that you want to monitor, expand NNMi monitoring behavior with the Poll Unconnected Interfaces and the Poll Interfaces Hosting IP Addresses attributes.</p> <p>Note: The following attributes must also be enabled:</p> <ul style="list-style-type: none"> In the Global Control section of this form, the Enable State Polling attribute must be enabled, too. See Layer 2 Neighbor View. (See "Set Global Monitoring" (on page 153) for more information.) In the Communication Configuration view, enable State Poller queries with the applicable Enable SNMP Communication attributes (see "Configuring Communication Protocol" (on page 47) for more information). <p>If <input type="checkbox"/> disabled, for devices assigned to this level of the monitoring hierarchy:</p> <ul style="list-style-type: none"> Causal Engine calculates Status based only on IP address State. The following previously discovered objects change to a State attribute value of "Not Polled" and a Status attribute value of "No Status": <ul style="list-style-type: none"> Interfaces (plus any related map-symbol changes to a beige color) Router Redundancy Groups (plus any related map-symbol changes to a beige color) Any fault-related items listed on the Node form, Component Health tab

Attribute	Description
Enable Component Health Fault Polling	<p>Use this attribute to poll Component Health fault metrics. Component Health fault metrics include the following: Fan, Power Supply, Temperature, and Voltage.</p> <p>Note: By default, this feature is enabled for the "Routers" and "Networking Infrastructure Devices" Node Groups.</p> <p>Note: Component Health Fault Polling is disabled by default.</p> <p>If <input checked="" type="checkbox"/> enabled, NNMi gathers fault data related to the Component Health fault metrics in devices assigned to this level of the monitoring hierarchy.</p> <p>If <input type="checkbox"/> disabled, NNMi does not extend data collection behavior to include Component Health fault data about devices assigned to this level of the monitoring hierarchy.</p> <p>Note: NNMi uses the same polling interval set for the Fault Polling Interval.</p>
Fault Polling Interval	<p>The time that State Poller waits between issuing queries to gather information for any of the following that are enabled: ICMP Polling, SNMP Polling, Poll Unconnected Interfaces, and Poll Interfaces Hosting IP addresses.</p> <p>Note: NNMi monitors SNMP agents (Management Addresses) according to this Fault Polling Interval, <i>even if ICMP Polling, SNMP Polling, Poll Unconnected Interfaces, and Poll Interfaces Hosting IP addresses are all disabled</i>. To prevent an SNMP Agent's address from being monitored, one of the following must be true: State Polling is disabled, current Communication Configuration settings turn off SNMP for the SNMP agent's address, or the parent Node is set to Not Managed or Out of Service.</p>

NNM iSPI for Performance. Performance Monitoring

Attribute	Description
Enable SNMP Interface Performance Polling	<p><i>NNM iSPI for Performance</i>. Use this attribute to extend the range of polling data that NNMi collects. NNM iSPI for Performance uses the additional data in a series of performance reports. See "Purchase an HP Smart Plug-in" (on page 319) for more information. When enabled, network traffic increases on your network because NNMi gathers performance data about each member of this group on a regular schedule.</p> <p>If <input checked="" type="checkbox"/> enabled, NNMi gathers performance data from Interfaces, CPU, memory, and buffers in devices assigned to this level of the monitoring hierarchy.</p> <p>If <input type="checkbox"/> disabled, NNMi does not extend data collection behavior to include performance data about devices assigned to this level of the monitoring hierarchy.</p> <p>Note: The Enable State Polling field must be enabled, too. By default the performance of connected interfaces and addresses is monitored. If you have <i>unconnected</i> interfaces that you want to monitor, expand NNMi monitoring behavior by enabling Poll Unconnected Interfaces.</p>
Enable Component Health Performance Polling	<p><i>NNM iSPI for Performance</i>. Use this attribute to poll Component Health performance. An NNMi administrator can set the threshold for node components related to the following performance metrics: CPU utilization, memory utilization, buffer utilization, buffer miss rate, and buffer failure rate.</p> <p>Note: Component Health Performance Polling is disabled by default.</p> <p>If <input checked="" type="checkbox"/> enabled, NNMi gathers performance data related to the Component Health performance metrics in devices assigned to this level of the monitoring hierarchy.</p>

Attribute	Description
<p>Note: <i>NNM iSPI for Performance</i>. By default, this feature is enabled for the "Routers" Node Group.</p>	<p>If <input type="checkbox"/> disabled, NNMi does not extend data collection behavior to include Component Health performance data about devices assigned to this level of the monitoring hierarchy.</p> <p>Note: NNMi uses the same polling interval set for the Performance Polling Interval.</p>
Performance Polling Interval	If you purchase and install the NNM iSPI for Performance, use this field to set the time period that NNMi waits between issuing network traffic to gather performance data.

Extend the Scope of Polling Beyond Connected Interfaces

Attribute	Description
Poll Unconnected Interfaces	<p>If <input checked="" type="checkbox"/> enabled, NNMi monitors all interfaces within discovered devices (both connected and unconnected). All interfaces are monitored for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.) Note: The Enable State Polling field must be enabled, and SNMP polling of some type must be enabled (for example, Enable SNMP Fault Monitoring and Enable SNMP Performance Polling).</p> <p>If <input type="checkbox"/> disabled, State Poller polls according to other configuration settings.</p> <p>Tip: Your discovery configuration choices may need to be adjusted to get the results you want. For example, to meet the "connected" criteria for interfaces in switches that do not have an IP address you must add the device to which the interface is connected as a discovery seed. See "Discovery Seeds (as a starting point)" (on page 82).</p>
<p>Poll Interfaces Hosting IP Addresses</p> <p>Note: This monitoring option is useful for Router interfaces. By default, this feature is enabled for the "Routers" Node Group.</p>	<p>If <input checked="" type="checkbox"/> enabled, any unconnected interface that has one or more addresses associated with it is monitored for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the operational status of interface health.) Note: The Enable State Polling field must be enabled, and SNMP polling of some type must be enabled (for example, Enable SNMP Fault Monitoring and Enable SNMP Performance Polling).</p> <p>By monitoring the Interface (in addition to the IP address), NNMi can make more informed decisions about the health of each IP address associated with an unconnected interface.</p> <p>If <input type="checkbox"/> disabled, State Poller polls according to other configuration settings.</p> <p>Tip: The Communication Configuration workspace provides a method of overriding this setting for specific Regions. For this purpose, NNMi provides a predefined Region definition of all possible private addresses (Private IP Addresses). You can also define your own Region to easily turn off ICMP polling to any unreachable addresses in your management domain.</p>

Configure Threshold Monitoring for Nodes (*NNM iSPI for Performance*)









The Threshold Settings form is used only to configure threshold monitoring when NNM iSPI for Performance is installed. See ["Purchase an HP Smart Plug-in" \(on page 319\)](#) for more information. If you set thresholds, NNMi generates an Incident when any threshold is violated. Examples of the types of threshold

you can set for a node include the following: (See [Monitored Attributes](#) in the table below for a complete list.)

- CPU 5 second utilization
- CPU 1 minute utilization
- CPU 5 minute utilization
- Memory utilization
- Buffer utilization
- Buffer miss rate
- Buffer failure rate

The NNM iSPI for Performance provides exceptions reports to track frequency. When NNMi iSPI for Performance is configured to monitor your network, network traffic increases while NNMi gathers performance data.

To establish threshold monitoring behavior for the NNM iSPI for Performance:

1. After enabling Performance Monitoring for a Node Group and before setting thresholds, analyze performance data over time to determine wise threshold settings for each group. See "[Determine Reasonable Threshold Settings \(NNM iSPI for Performance\)](#)" (on page 175).
2. Navigate to the **Thresholds Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Monitoring Configuration**.
 - c. Navigate to the **Node Settings** tab.
 - d. Do one of the following:
 - To create a Node Settings definition, click the  New icon.
 - To edit a Node Settings definition, select a row, click the  Open icon.
3. *Prerequisite.* Verify that Performance Monitoring is enabled for this Node Settings definition.
4. In the **Node Settings** form, navigate to the **Threshold Settings** tab.
5. Do one of the following:
 - To create a threshold definition, click the  New icon.
 - To edit a threshold definition, select a row, click the  Open icon.
 - To delete a threshold definition, select a row and click the  Delete icon.
6. Select the attribute you want to monitor and establish the threshold values for that attribute (see [Basic Threshold Settings table](#)). For examples of setting meaningful thresholds, see "[Examples of Threshold Monitoring \(NNM iSPI for Performance\)](#)" (on page 175).
7. Click  **Save and Close** to return to the Node Settings form.
8. Click  **Save and Close** to return to the Monitoring Configuration form.
9. Click  **Save and Close**. NNMi applies your changes during the next regularly scheduled monitoring cycle.

Note: Threshold Incidents are disabled by default within NNMi to prevent Incident storms. If you are ready to generate Threshold Incidents, see ["Generate Performance Threshold Incidents \(NNM iSPI for Performance\)" \(on page 298\)](#). And to learn about your incident configuration choices, see ["Custom Incident Attributes Provided by NNMi" \(on page 214\)](#) for a description of the special custom incident attributes available in Threshold Incidents.

Basic Threshold Settings

Attribute	Description
Monitored Attribute	<p>NNMi gathers data to calculate thresholds for the following values. Click any item in this list for more details about that value.</p> <p>Note: NNMi also displays the Monitored Attributes that apply to interfaces. See "Configure Threshold Monitoring for Interfaces (NNM iSPI for Performance)" (on page 162) for more information about these attributes</p> <ul style="list-style-type: none"> • CPU 5Sec Utilization Percentage of CPU usage in relation to the total amount of CPU available. This percentage is measure at 5-second intervals. • CPU 1Min Utilization Percentage of CPU usage in relation to the total amount of CPU available. This percentage is measured at 1-minute intervals. • CPU 5Min Utilization Percentage of CPU usage in relation to the total amount of CPU available. This percentage is measured at 5-minute intervals. • Memory Utilization Percentage of memory usage in relation to the total amount of memory available. • Buffer Utilization Percentage of buffer usage in relation to the total amount of buffer space available. • Buffer Miss Rate Counter indicating that the number of available buffers in the pool has dropped below the minimum level. • Buffer Failure Rate Percentage value based on the number of buffer failures caused by insufficient memory when trying to create additional buffers.
High Value	<p>Designate the percentage above which would indicate a value in the High range. Valid entries are 0.00 through 100.00</p> <p>Note: If you use 100.00 the threshold is disabled because it cannot be crossed.</p>
High Value Rearm	<p>Designate the percentage that when reached would indicate the end of a high threshold situation. Valid entries are 0.00 through 100.00</p> <p>Note: The High Value Rearm must be less than or equal to the High Value and greater than the Low Value Rearm.</p>
High Trigger Count	<p>Designate the number of consecutive polling cycles in which the value must remain in the High range before the threshold state changes to High.</p>
Low Value	<p>The Low Value must be less than or equal to the High Value.</p> <p>Designate the percentage below which would indicate a value in the low range. Valid entries are 0.00 through 100.00</p>

Attribute	Description
	Note: If you use 0.00 the threshold is disabled because it cannot be crossed.
Low Value Rearm	Designate the percentage that when reached would indicate the end of a low threshold situation. Valid entries are 0.00 through 100.00. Note: The Low Value Rearm must be greater than or equal to the Low Value and less than the High Rearm Value.
Low Trigger Count	Designate the number of consecutive polling cycles in which the value must remain in the Low range before the threshold state changes to Low.

Determine Reasonable Threshold Settings (NNM iSPI for Performance)

You must decide how to define normal behavior for devices in the associated Node Group or Interface Group. You can then set reasonable thresholds for the group, and avoid Threshold Incident storms. See ["Examples of Threshold Monitoring \(NNM iSPI for Performance\)" \(on page 175\)](#).

Create a Node Group or Interface Group filter that includes the devices you want to monitor. Export the Node Group or Interface Group filter to NNM iSPI for Performance. See ["Creating Groups of Nodes or Interfaces" \(on page 126\)](#).

Enable Performance Monitoring for the Node Group or Interface Group. See ["Configure Node Monitoring" \(on page 168\)](#) or ["Configure Interface Monitoring" \(on page 158\)](#). Then wait a minimum of 24 hours before following the steps below.

Access the NNM iSPI for Performance Headline report:

1. In the NNMi console, click **Actions** → **Reporting - Report Menu**.
2. Click the link for **Headline**. The Headline report displays data up until 12 p.m.last night.
3. Click **Show Options**.
4. Expand the **All Nodes/Interfaces** selection.
5. Choose the Node Group or Interface Group filter for which you are setting thresholds.
6. Expand **All Dates/Times**. Select a time period (a day, week, or month).
7. Click **Confirm Selections**.
8. The report for the Node Group or Interface Group you selected appears.
9. Study the Range & Exceptions graphs to guide your decision about what constitutes reasonable threshold settings. See online help for this report for information about how to read this report.

Examples of Threshold Monitoring (NNM iSPI for Performance)

You can configure interface threshold monitoring if the NNM iSPI for Performance is installed. See ["Purchase an HP Smart Plug-in" \(on page 319\)](#) for more information.

Several examples are presented These examples are not intended to be recommendations. Consider all aspects of your network environment and set performance thresholds that are meaningful in your environment:

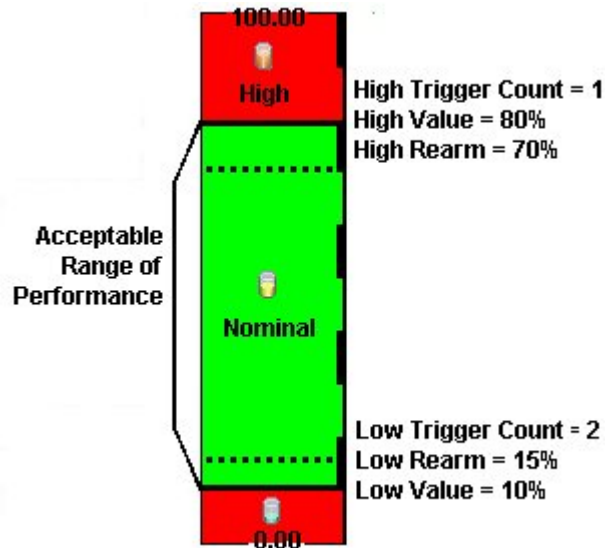
- [Thresholds to Monitor Utilization on WAN Connections](#)
- [Thresholds to Monitor Utilization on Important Interfaces](#)

- [Thresholds to Monitor Important Interfaces for Discards](#)
- [Thresholds to Monitor Important Interfaces for Errors](#)

Example 1: Monitor Utilization on WAN Connections

You want to monitor the connections between two sites to verify that your service provider is meeting their guaranteed throughput volume. You pay a fixed cost for a specific bandwidth over this WAN interface.

- Monitor for under-utilization which wastes money (less than 10%).
Tip: If you don't care about under-utilization, set Low Value and Rearm to 0% as shown in Example 2.
- Monitor for over-utilization, which may result in performance bottlenecks or service provider surcharges (greater than 80%).



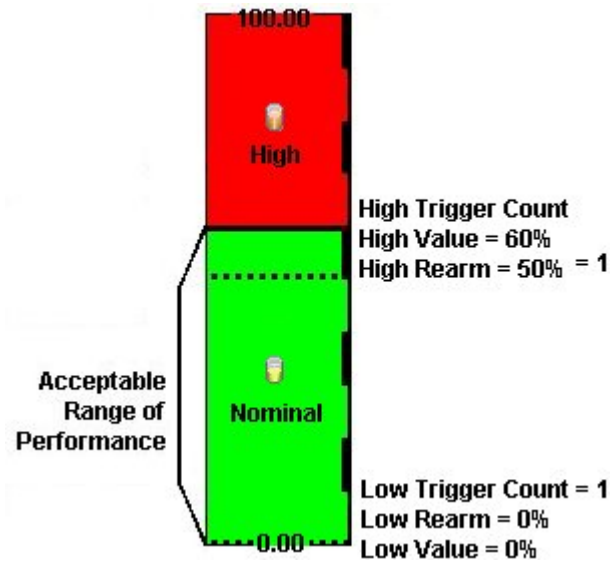
Note: Sometimes an Interface's MIB II ifspeed value is not reported accurately. This may result in threshold calculations outside the 0.00 - 100.00 range. If this happens, the Interface threshold State set to "Unavailable." To correct the problem:

1. Access the **Inventory** workspace
2. Open **Interface** view.
3. Open the form for the Interface that is reporting a threshold state of "Unavailable."
4. Navigate to the **General** tab.
5. Enter a valid entry in **Input Speed** or **Output Speed** (this overrides the value returned by the device's SNMP agent so that NNMi can accurately calculate utilization thresholds).

Example 2: Monitor Utilization on Important Interfaces

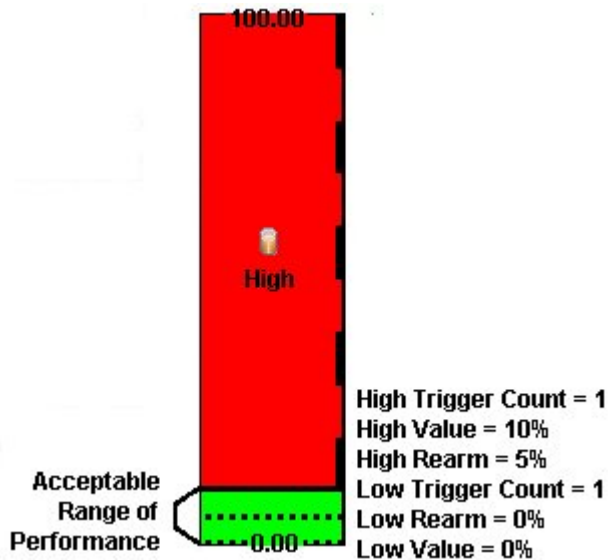
You want to monitor an important Ethernet interface and be notified if it is getting overloaded.

An Ethernet interface configured for full-duplex operation has an acceptable operating range of 0-60%. When average utilization is greater than 60%, NNM generates a High Threshold incident.



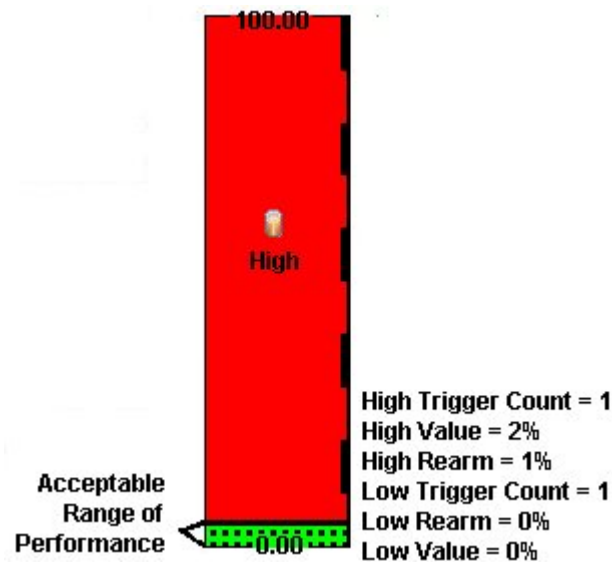
Example 3: Monitor Important Interfaces for Discards

You want to know anytime an interface is dropping data. The acceptable limit for interface discards is 10%. The threshold state is High when the discard rate exceeds 10% and returns to Nominal when the discard rate drops below 5%.



Example 4: Monitor Important Interfaces for Errors

You want to know if packet errors occur. The acceptable limit for packet errors is 2%. The threshold state is High Level (HL) when the error rate exceeds 2% and returns to normal when the error rate drops below 1%.




Configure Node Group Status

NNMi enables an NNMi administrator to configure the Node Group status calculations using either of the following methods:

- Assign the Node Group the most severe status of any Node Group member. This is the default method for obtaining Node Group Status.
- Configure the percentage thresholds for one or more Node Group target statuses. For example, when defining percentage values for a target status of **Critical**, you might change the default so that 30 percent of the nodes in the group must have a status other than Normal, for the Node Group Status to be **Critical**.

To configure Node Group status calculations, do the following:

1. Navigate to the **Status Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Status Configuration**.
2. Make one of the following configuration choices:
 - To assign the Node Group the most severe Status of any Node Group member, in the **Status Configuration** form, under **Global Control**, make sure **Propagate Most Severe Status** is checked:
Propagate Most Severe Status
To configure percentage values for a Node Group Target Status, do the following:
 - In the **Status Configuration** form, under **Global Control**, make sure the **Propagate Most Severe Status** is cleared:
Propagate Most Severe Status
 - [Configure the percentage values for a Node Group Target Status](#)
3. Click  **Save and Close**.




NNMi applies your changes after the configuration is saved.

Configure Percentage Values for the Target Status

NNMi enables you to configure how the status of a Node Group is calculated.

Note: The percentage value that is calculated for a Node Group includes only those nodes whose Management Mode is **Managed**. For example, if a Node Group includes 10 nodes and 3 of the nodes are **Not Managed**, 5 of the nodes have a Status of **Normal**, and 2 have a status of **Critical**, the percentage of **Critical** nodes is $2/7 * 100$.

To configure the percentage values for a Node Group Target Status:

1. Navigate to the **Status Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Status Configuration**.
2. Locate the **Node Group Status Settings** tab.
3. Do one of the following:
 - To create a Node Group Status Settings definition, click the  New icon.
 - To edit a Node Group Status Settings definition, select a row, click the  Open icon.
 - To delete a Node Group Settings definition, select a row and click the  Delete button
4. Establish the appropriate settings to identify this Node Group Status Settings definition. (See the ["Node Group Status Settings Form" \(on page 179\)](#) form)



Note: You can only define one configuration for each Target Status.




Node Group Status Settings Form

The Node Group Status Settings form is used to configure the percentage thresholds for a Node Group Target Status. The percentage thresholds you specify define what percentage of nodes within the group must have a particular Status. When the percentage thresholds are reached, the Node Group is assigned the associated Target Status. For example, when defining percentage thresholds for a target status of **Critical**, you might change the default so that 10 percent of the nodes in the group must have a status of **Critical** for the Node Group Status to be **Critical**.

Note: Use a percentage threshold between 0 (zero) and 1 (for example, .01) to indicate the Target Status to be reached when one node in the Node Group reaches a specified Status. For example, if you want the Node Group Status to be set to **Critical** when the Status of one node in the Group becomes **Critical**, enter a percentage less than one for the **Critical %** value.

To define percentage thresholds for a Target Status:

1. Navigate to the **Node Group Status Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Status Configuration**.
 - c. Navigate to the **Node Group Status Settings** tab.
 - d. Do one of the following:
 - To create a Node Group Status Settings definition, click the  New icon.
 - To edit a Node Group Settings definition, select a row, click the  Open icon.

- To delete a Node Group Settings definition, select a row and click the  Delete icon.
- 2. Set the Target Status and percentages you want (see [Basic Attributes table](#)).
- 3. Click  **Save and Close** to return to the **Status Configuration** form.
- 4. Click  **Save and Close**. NNMi applies your changes after the configuration is saved.

Basics Attributes

Attribute	Description
Target Status	<p>The Status you are configuring. This Status is assigned to the Node Group whenever the specified percentage thresholds are reached.</p> <p>Note the following:</p> <ul style="list-style-type: none"> ● Whether all or one of the percentage thresholds must be reached for a Target Status configuration depends on the Boolean operator you select. The default Boolean operator is OR. (Also see Combine with AND below.) ● If you do not specify any percentages for a Target Status, it does not appear as a Status for a Node Group.
Critical %	Specifies the percentage threshold for the nodes within the group whose Status must be Critical for the Node Group to be assigned the Target Status.
Major %	Specifies the percentage threshold for the nodes within the group whose Status must be Major for the Node Group to be assigned the Target Status.
Minor %	Specifies the percentage threshold for nodes within the group whose Status must be Minor for the Node Group to be assigned the Target Status.
Warning %	Specifies the percentage threshold for nodes within the group whose Status must be Warning for the Node Group to be assigned the Target Status.
Non-Normal %	<p>Specifies the percentage threshold for nodes within the group whose Status must be any of the following for the Node Group to be assigned the Target Status:</p> <ul style="list-style-type: none"> ● Critical ● Major ● Minor ● Warning
Unknown %	Specifies the percentage threshold for nodes within the group whose Status must be Unknown for the Node Group to be assigned the Target Status.
Combine with AND	<p>Specifies that you want NNMi to combine the percentage thresholds you enter using the AND Boolean operator.</p> <p>When using this option, note the following:</p> <ul style="list-style-type: none"> ● All percentage thresholds you enter must be reached for the Node Group to be assigned the Target Status. ● The percentage thresholds you enter must not exceed 100 percent.

Monitor Router Redundancy Groups (NNMi Advanced)

NNMi monitors state and priority information for any discovered HSRP and VRRP objects in the network. These objects include Router Redundancy Members and Tracked Objects. See [Router Redundancy Group View](#) for more information about Router Redundancy Groups and the HSRP or VRRP objects associated with them.

The polling interval used is the Fault Polling Interval that is set for the node associated with the Router Redundancy Member or Tracked Object.

If you do not want these objects polled:

- Set the Management Mode for each node to **Unmanaged** or **Out of Service**. See ["Stop or Start Managing a Node, Interface, or Address"](#) (on page 184) for more information about Management Mode.
- Disable all Router Redundancy Group monitoring. See ["Set Global Monitoring"](#) (on page 153).

NNMi Advanced also uses these HSRP and VRRP objects when calculating a Path View between two nodes that have IPv4 addresses. See [Path View with NNMi Advanced](#) for more information.

Current Health of the State Poller Service

At any time, you can check the current health statistics about the State Poller Service by using the **Help** → **About HP Network Node Manager i-series** menu item.

The State Poller Service contributes towards discovery and ongoing monitoring. See ["About Each NNMi Service"](#) (on page 26).

Verify Monitoring Configuration Settings



After you configure the monitoring settings, you can check the configuration for a particular object to verify that everything is working correctly. Examples of objects on which you can verify monitoring configuration settings include Nodes, Interfaces, IP addresses, Router Redundancy Groups, Tracked Objects, and Node Components. Use the **Actions** → **Monitoring Settings** menu item to display a report.

To verify the monitoring configuration for a Node, Interface, or IP address:




1. Navigate to the view for that object (for example, **Inventory** → **Nodes**).
2. Select the object of interest by selecting the check box that precedes the object information.
3. Select **Actions** → **Monitoring Settings**.

Note: This menu item also is available on any object's form.


To verify the monitoring configuration for a Router Redundancy Member:

1. Navigate to a Router Redundancy Group view (for example, **Inventory** → **Router Redundancy Groups**).
2. Click the  Open icon that precedes the Router Redundancy Group of interest.
3. From the Router Redundancy Members tab, click the  Open icon that precedes the Router Redundancy Group Member of interest.
4. Select **Actions** → **Monitoring Settings**.

To verify the monitoring configuration for a Tracked Object:

1. Navigate to a Router Redundancy view (for example, **Inventory** → **Router Redundancy Groups**).
2. Click the  Open icon that precedes the Router Redundancy Group of interest.
3. From the Router Redundancy Members tab, click the  Open icon that precedes the Router Redundancy Group Member of interest.
4. From the Tracked Objects tab, click the  Open icon that precedes the Tracked Object of interest.
5. Select **Actions** → **Monitoring Settings**.



To verify the monitoring configuration for a Node Component:

1. Navigate to the view for that object (for example, **Inventory** → **Nodes**).
2. Click the  Open icon that precedes the Node of interest.
3. Select the **Component Health** tab.
4. Select the Node Component of interest by selecting the check box that precedes the object information.
5. Select **Actions** → **Monitoring Settings**.

Check status and connectivity of important interfaces.

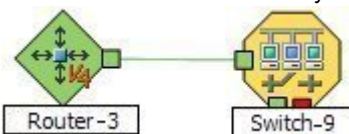
1. Open a Layer 2 Neighbor View map of each important interface's parent device. See [Viewing Maps \(Network Connectivity\)](#).
2. Each connected interface has a little square symbol around the edge of the parent device's map symbol. For example:



3. Hover your mouse over the square to verify the identify of your important interface on the map.
4. Verify that the status color of each important interface is not  Unknown or  Unmanaged (see [About Status Colors](#)). For example:



5. By default, NNMi only monitors the health of connected interfaces. A line appears on the map between interfaces when they are connected. For example:



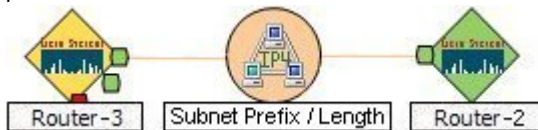
6. If you need to add a connection, see ["Add or Delete a Layer 2 Connection" \(on page 124\)](#).

Check status and connectivity of important addresses.

1. Open a Layer 3 Neighbor View map of each important parent device. See [Viewing Maps \(Network Connectivity\)](#).
2. Each address that is connected to another address in the same subnet has a little hexagon symbol around the edge of the parent device's map symbol. For example:



3. Hover your mouse over the hexagon to verify the identify of your important address on the map.
4. NNMi monitors the health of addresses only if you enable [ICMP Address Monitoring](#). A line appears on the map between addresses when they are connected. The line represents the subnet. For example:



5. If ICMP Address Monitoring is enabled, verify that the status color of each important address is not Unknown or Unmanaged (see [About Status Colors](#)). For example:



6. If you need to add a connection, see ["Add or Delete a Layer 2 Connection" \(on page 124\)](#).

See ["Configure Monitoring Behavior" \(on page 152\)](#) for information about establishing monitoring behavior.

Stop or Start Managing a Node, Interface, or Address

NNMi administrators can specify that a node, interface, or address should no longer be managed or is out of service. To indicate that you want to stop or start managing a node, interface, or address, you use the management mode values.

Reasons you might want to change the management mode include:

- The node is temporarily out of service.
- You have determined that a node, interface, or address should never be managed.

NNMi provides two management modes as described in the following table:

Management Modes

Name	Description
Management Mode	<p>For node, this value is set by the user and is used to help determine the Management Mode value for any associated interface or address.</p> <p>For interfaces and addresses, this value is calculated. The Management Mode for an interface is a computed value based on the Management Mode for the node. The Management Mode value for an address is a calculated value based on the Management Mode for any associated interface. Otherwise, the Management Mode is determined by node on which the address resides. Possible values include:</p> <p>Managed - Used to indicate a node, interface, or address should be managed by NNMi.</p> <p>Not Managed - Used to indicate that you do not plan to manage the node, interface, or address. For example, the object might not be accessible because it is in a private network. NNMi does not discover or monitor these objects.</p> <p>Out of Service - Used to indicate a node, interface, or address is unavailable because it is out of service. NNMi does not discover or monitor these objects.</p>
Direct Management Mode	<p>For interfaces and addresses, this field is set by the user and is used to compute the interface and address Management Mode values. Possible values include:</p> <p>Inherited - For interfaces, this value is used to indicate that the interface should inherit the Management Mode from the node on which it resides. For addresses, this value is used to indicate that the Management Mode should be inherited from the associated interface, if one exists. Otherwise the Management Mode is inherited from the node on which it resides.</p> <p>Not Managed - Used to indicate that you do not plan to manage the interface or address. For example, the object might not be accessible because it is in a private network. NNMi does not discover or monitor these objects.</p> <p>Out of Service - Used to indicate the interface or address is unavailable because it is out of service. Reasons might include the interface being repaired or a known problem with the address. NNMi does not discover or monitor these objects.</p>

Note: You cannot set the Management Mode on an interface or an address, because the value is calculated.

You can change the Management Mode in one of the following ways:

- Change the value of the Management Mode or Direct Management Mode field on the form.

Note: If you are updating the Direct Management Mode for an interface or address, NNMi also updates its Management Mode value after you reopen or refresh the form.

- Use an action from a view or form.
- Use the [nnmmanagementmode.ovpl](#) command.

See [Access Node Details](#) for more information about setting the Management Mode for a node. See [Interface Form](#) for more information about setting the Direct Management Mode for an interface. See [IP Address Form](#) for more information about setting the Direct Management Mode for an address.

["Perform Automated Tasks" \(on page 21\)](#) for more information about setting the Management Mode or Direct Management Mode using actions.

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#) for information about the results of the Management Mode value on these objects.

View the Management Mode for an Object in Your Network

NNMi provides the Management Mode workspace so that you can quickly view the management mode for nodes, interfaces, or addresses in your network. The management mode is calculated using the Management Mode and Direct Management Mode values. NNMi administrators can set the Direct Management Mode. NNMi calculates the current Management Mode based on the combined settings of all the associated objects. For example:

- Node — NNMi administrators can set the Management Mode value, or NNMi can calculate it.
- Interface — The Direct Management Mode (if any) NNMi administrators set for the interface or calculated from the current Management Mode of the associated node and address.
- Address — The Direct Management Mode (if any) NNMi administrators set for the address or calculated from the current Management Mode of the associated node and interface.

The following table describes each possible Management Mode and Direct Management Mode value. As shown in the table, the available Management Mode values depend on the object type (node, interface, or address).

Management Mode Values

Object	Value	Description
Node	Managed	Used to indicate that the node should be managed by NNMi. This means it will be discovered and monitored.
Node	Not Managed	Used to indicate you do not plan to manage the node. For example, the node might not be accessible because it is in a private network. NNMi does not discover or monitor these objects.
Node	Out of Service	Used to indicate the node is unavailable because it is out of service. Reasons might include that the device is being repaired or there is a known problem with the device. NNMi does not discover or monitor these objects.

Direct Management Mode Values

Object	Value	Description
Interface or Address	Not Managed	Used to indicate you do not plan to manage the interface or address. After the interface or address Direct Management Mode is set to Not Managed , NNMi does no longer discovers or monitors the interface or address.

Object	Value	Description
Interface or Address	Out of Service	<p>Used to indicate that the interface or address is out of service. NNMi does not discover or monitor these objects.</p> <p>An interface will not be managed again until the Direct Management Mode is set to Inherited and its associated node is set to Managed.</p> <p>An address will not be managed again until the Management Mode of any associated interface is set to Inherited and the node's Management Mode is set to Managed.</p>
Interface	Inherited	<p>Used to indicate that the interface should assume the Management Mode of the node on which it is hosted.</p> <p>Note: To manage the interface, the Management Mode of the node on which the interface is hosted must be Managed.</p>
Address	Inherited	<p>The address assumes the Management Mode of the interface, if any, with which the address is associated.</p> <p>If the address is not associated with an interface, it assumes the Management Mode of the node on which it is hosted.</p> <p>Note: To manage the address, the Management Mode of the address' interface, if any, must be calculated to be Managed. The Management Mode of the node on which the interface and address are hosted must be set to Managed.</p>

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#) for more information about the effects of using the Not Managed setting.

See the Related Topics list below for information about the views available for checking the Management Mode values for nodes, interfaces, or addresses.

Related Topics:

- ["Using the \(Management Mode\) Nodes View" \(on page 187\)](#)
- ["Using the Managed Interfaces View" \(on page 188\)](#)
- ["Using the \(Management Mode\) IP Addresses View" \(on page 187\)](#)
- ["Using the Not Managed Nodes View" \(on page 189\)](#)
- ["Using the Not Managed Interfaces View" \(on page 190\)](#)
- ["Using the Not Managed Addresses View" \(on page 190\)](#)
- ["Using the Out of Service Nodes View" \(on page 190\)](#)
- ["Using the Out of Service Interfaces View" \(on page 191\)](#)
- ["Using the Out of Service Addresses View" \(on page 191\)](#)
- [Nodes View \(Inventory\)](#)
- [Interfaces View \(Inventory\)](#)
- [IP Addresses View \(Inventory\)](#)

Using the (Management Mode) Nodes View

The Nodes view in the Management Mode workspace identifies the management mode of all of the nodes that are stored in the NNMi database. Sort this view by Management Mode to see which set of nodes are managed, temporarily out of service, and not being managed.

Note: By default, the Node view is sorted by node Name values.

Use this view to select nodes whose management mode should change from their current value.

For each node, you can identify its overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical** and **Unknown**), name, management mode, device profile, the system description, and any notes included for the node.

See ["Using the Nodes View"](#) for more information about uses for nodes views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#)

Using the (Management Mode) Interfaces View

The Interfaces view in the Management Mode workspace identifies the management mode of all of the interfaces that are stored in the NNMi database. This view also shows the management mode of the node associated with an interface so that you can determine how NNMi arrived at the Management Mode value for the interface.

Sort this view by Direct Management Mode to see which interfaces are managed, temporarily out of service, and not being managed.

Note: Check the management mode set for the associated node (**Node Management Mode**) to determine the actual management mode of the interface. For example, if the Direct Management Mode for the interface is **Inherited** and the management mode of the node is **Out of Service**, the management mode for the interface is **Out of Service**. ["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#) for information about how the management mode is calculated for interfaces.

Use this view to select interfaces whose management mode should change from their current value.

For each interface, you can identify the interface's overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical**, and **Unknown**), associated node Name value (Hosted on Node), the interface name, the direct management mode (set by the administrator), the management mode of its associated node, administrative and operational status, type, alias, speed, the date the interface information was last changed, its description, and any notes included for the interface.

See ["Using the \(Inventory\) Interfaces View"](#) for more information about uses for the interfaces views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

Using the (Management Mode) IP Addresses View

The IP Addresses view in the Management Mode workspace identifies the management mode of all of the addresses that are stored in the NNMi database. This view also displays the management mode of the

interface, if any, and the node associated with each address so that you can determine how NNMi arrived at the Management Mode value for the address.

Note: By default, this view is sorted by the IP address values.

Sort this view by Direct Management Mode to see which set of addresses are managed, temporarily out of service, and not being managed.

Note: Check the management mode set for any associated interface (**Interface Management Mode**) and for the node (**Node Management Mode**) to determine the address management mode. For example, if the management mode for the interface is **Inherited** and the management mode of the node is **Out of Service**, the management mode for the address is **Out of Service**. "[Understand the Effects of Setting the Management Mode to Not Managed or Out of Service](#)" (on page 193) for information about how the management mode for addresses is calculated.

Use this view to select addresses whose management mode should change from their current value.

For each IP address, you can identify its state, IP address, its direct management mode (set by the administrator), management mode of any associated interface (calculated by NNMi), management mode of the node on which the address resides, associated node Name value (Hosted on Node), interface name, subnet, and any notes included for the IP address.

See [IP Addresses View \(Inventory\)](#) for more information about uses for addresses views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" \(on page 193\)](#)

Using the Managed Nodes View

The Managed Nodes view identifies all of the discovered nodes that NNMi currently manages.

Use this view to select nodes whose management mode should change to **Not Managed** or **Out of Service**.

For each node, you can identify its overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical** and **Unknown**), its device category (for example, switch), name, system name, system location (the current value of the sysLocation MIB variable), date indicating the last time the node status was modified, the device profile, and any notes included for the node.

Note: Because this view contains only nodes whose Management Mode is set to **Managed**, the Management Mode column is not included.

See ["Using the Nodes View"](#) for more information about uses for nodes views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" \(on page 193\)](#)

Using the Managed Interfaces View

The Managed Interfaces view identifies all of the discovered interfaces NNM currently manages.

Use this view to select interfaces whose management mode should change to **Not Managed** or **Out of Service**.

For each interface, you can identify the interface's overall status (for example, Normal, Warning, Minor, Major, Critical, and Unknown), associated node Name value (Hosted on Node), the interface name, administrative and operational status, type, alias, speed, the date the interface information was last changed, its description, and any notes included for the interface.

Note: Because this view contains only interfaces whose Management Mode is set to **Managed**, the Management Mode column is not included.

See ["Using the \(Inventory\) Interfaces View"](#) for more information about uses for the interfaces views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#)

Using the IP Managed Addresses View

The Managed IP Addresses view identifies all of the addresses NNM currently manages.

Use this view to select addresses whose management mode should change to **Not Managed** or **Out of Service**.

For each IP address, you can identify its state, associated Interface, associated node Name value (**Hosted on Node**), subnet (**In Subnet**) and prefix length (**PL**), and any notes included for the IP address.

Note: Because this view contains only addresses whose Management Mode is set to **Managed**, the Management Mode column is not included.

See [IP Addresses View \(Inventory\)](#) for more information about uses for address views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#)

Using the Not Managed Nodes View

The Not Managed Nodes view identifies all of the nodes whose management mode is **Not Managed**. These are the nodes that are no longer being discovered or monitored.

Use this view to select nodes whose management mode should change to **Managed** or **Out of Service**.

For each node, you can identify its overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical** and **Unknown**), name, system name, system location (the current value of the sysLocation MIB variable), contact name, date indicating the last time the node status was modified, device profile, a device category (for example, switch), the system description, and any notes included for the node.

Note: Because this view contains only nodes whose Management Mode is set to **Not Managed**, the Management Mode column is not included.

See ["Using the Nodes View"](#) for more information about uses for nodes views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#)

Using the Not Managed Interfaces View

The Not Managed Interfaces view identifies all of the interfaces whose management mode is **Not Managed**. These are the interfaces that are no longer being discovered or monitored.

Use this view to select interfaces whose management mode should change to **Managed** or **Out of Service**.

For each interface, you can identify the interface's overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical**, and **Unknown**), associated node Name value (Hosted on Node), the interface name, administrative and operational status, type, alias, speed, the date the interface information was last changed, its description, and any notes included for the interface.

Note: Because this view contains only interfaces whose Management Mode is set to **Not Managed**, the Management Mode column is not included.

See ["Using the \(Inventory\) Interfaces View"](#) for more information about uses for the interfaces views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#)

Using the Not Managed Addresses View

The Not Managed Addresses view identifies all of the addresses whose management mode is **Not Managed**. These are the nodes that are no longer being discovered or monitored.

Use this view to select addresses whose management mode should change to **Managed** or **Out of Service**.

For each IP address, you can identify its state, associated Interface, associated node Name value (**Hosted on Node**), subnet (**In Subnet**) and prefix length (**PL**), and any notes included for the IP address.

Note: Because this view contains only addresses whose Management Mode is set to **Managed**, the Management Mode column is not included.

Note: Because this view contains only addresses whose Management Mode is set to **No Managed**, the Management Mode column is not included.

See [IP Addresses View \(Inventory\)](#) for more information about uses for address views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#)

Using the Out of Service Nodes View

The Out of Service Nodes view identifies all of the nodes whose management mode is **Out of Service**. These are the nodes that are no longer being discovered and monitored.

Use this view to select nodes whose management mode should change to **Managed** or **Not Managed**.

For each node, you can identify its overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical** and **Unknown**), name, system name, system location (the current value of the sysLocation MIB variable), contact name, date indicating the last time the node status was modified, device profile, a device category (for example, switch), the system description, and any notes included for the node.

Note: Because this view contains only nodes whose Management Mode is set to **Out of Service**, the Management Mode column is not included.

See "[Using the Nodes View](#)" for more information about uses for nodes views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#)

Using the Out of Service Interfaces View

The Out of Service Interfaces view identifies all of the interfaces whose management mode is **Out of Service**. These are the interfaces that are no longer being discovered and monitored.

You can also use this view to select nodes whose management mode should change to **Managed** or **Not Managed**

For each interface displayed in the view, you can identify the interface's overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical**, and **Unknown**), associated node Name value (Hosted on Node), the interface name, administrative and operational status, type, alias, speed, the date the interface information was last changed, description, and any notes included for the interface.

Note: Because this view contains only interfaces whose Management Mode is set to **Out of Service**, the Management Mode column is not included.

See "[Using the Interface View](#)" for more information about uses for interface views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#)

Using the Out of Service Addresses View

The Out of Service IP Addresses view identifies all of the addresses whose management mode is **Out of Service**. These are the addresses that are no longer being discovered and monitored.

You can also use this view to select addresses whose management mode should change to **Managed** or **Not Managed**.

For each IP address, you can identify its state, associated Interface, associated node Name value (**Hosted on Node**), subnet (**In Subnet**) and prefix length (**PL**), and any notes included for the IP address.

Note: Because this view contains only addresses whose Management Mode is set to **Managed**, the Management Mode column is not included.

Note: Because this view contains only addresses whose Management Mode is **Out of Service**, the Management Mode column is not included.

See [IP Addresses View \(Inventory\)](#) for more information about uses for address views.

Related Topics

["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#)

["Understand the Effects of Setting the Management Mode to Not Managed or Out of Service " \(on page 193\)](#)

How NNMi Assigns the Management Mode to an Interface or Address

NNMi administrators can instruct NNMi to no longer manage an interface or address by setting the *Direct Management Mode* value. NNMi then calculates the overall Management Mode based on the current Management Mode of all the associated objects.

For example, if you are specifying the Direct Management Mode for an address, NNMi uses the following values to determine the Management Mode value for the address:

- Direct Management Mode you enter for the address
- Management Mode of the associated interface, if any
- Management Mode of the node that contains the address

The following table lists possible values for each object's management mode.

Interface

(Node) Management Mode	(Interface) Direct Management Mode	(Interface) Management Mode
Managed	Inherited	Managed
Not Managed	Inherited	Not Managed
Out of Service	Inherited	Out of Service
Managed	Not Managed	Not Managed
Not Managed	Not Managed	Not Managed
Out of Service	Not Managed	Not Managed
Managed	Out of Service	Out of Service
Not Managed	Out of Service	Out of Service
Out of Service	Out of Service	Out of Service

Address

(Node) Management Mode	(Interface) Direct Management Mode	(Address) Direct Management Mode	(Address) Management Mode
Managed	Inherited	Inherited	Managed
Not Managed	Inherited	Inherited	Not Managed
Out of Service	Inherited	Inherited	Out of Service
Managed	Not applicable*	Inherited	Managed
Not Managed	Not applicable*	Inherited	Not Managed
Out of Service	Not applicable*	Inherited	Out of Service
Managed	Not Managed	Inherited	Not Managed
Not Managed	Not Managed	Inherited	Not Managed
Out of Service	Not Managed	Inherited	Not Managed
Managed	Not Managed	Not Managed	Not Managed
Not Managed	Not Managed	Not Managed	Not Managed
Out of Service	Not Managed	Not Managed	Not Managed
Managed	Not applicable*	Not Managed	Not Managed
Not Managed	Not applicable*	Not Managed	Not Managed
Out of Service	Not applicable*	Not Managed	Not Managed
Managed	Out of Service	Inherited	Out of Service
Not Managed	Out of Service	Inherited	Out of Service
Out of Service	Out of Service	Inherited	Out of Service
Managed	Out of Service	Out of Service	Out of Service
Not Managed	Out of Service	Out of Service	Out of Service
Out of Service	Out of Service	Out of Service	Out of Service
Managed	Not applicable*	Out of Service	Out of Service
Not Managed	Not applicable*	Out of Service	Out of Service
Managed	Not applicable*	Out of Service	Out of Service

* Used to indicate there is no associated interface

Understand the Effects of Setting the Management Mode to Not Managed or Out of Service

The results of setting the management mode to **Not Managed** or **Out of Service** for an object, depends on whether you are setting the value for a node, interface, or address.

Management Mode:

For nodes, setting the Management Mode to **Not Managed** or **Out of Service** has the following effects:

- No incidents are generated for the node
- The node's SNMP Agent is excluded from fault polling.
- The node's interfaces or addresses are excluded from fault and performance polling.
- NNMi quits gathering Component Health data about the node.
- NNMi deletes all Polled Instances associated with the **Not Managed** or **Out of Service** node.
- The Active State for any Custom Poller Nodes associated with the **Not Managed** or **Out of Service** node becomes **Inactive**.
- The node is removed from any associated Router Redundancy Groups.
- Traps related to the node, interface, or address, (for example, coldStart or warmStart) are not stored.
- The node is excluded from discovery.
- **Actions** → **Configuration Poll** is no longer available for this node.
- The status of a node is set to **No Status**.
- **Actions** → **Status Poll** is no longer available for the node, interfaces, or addresses.

Direct Management Mode:

For interfaces, setting the Direct Management Mode to **Not Managed** or **Out of Service** has the following effects:

- No incidents are generated for the interface.
- The interface and any related addresses are excluded from fault and performance polling.
- The Administrative State and Operational State of the interface are set to **Not Polled**.
- The status of the interface is set to **No Status**.
- Traps related to the interface (for example, LinkUp or LinkDown), will not be stored.

For addresses, setting the Direct Management Mode to **Not Managed** or **Out of Service** has the following effects:


- No incidents are generated for the address.
- The state of the address is set to **Not Polled**.
- The address is excluded from fault and performance polling.

Configuring the NNMi User Interface

NNMi enables an NNMi administrator to configure the following user interface features:

- The console time out interval
- The maximum number of nodes to display on a map
- The maximum number of connections to display on a map
- The initial map view to display in the Topology Maps workspace
- Whether NNMi displays unlicensed features that require a special license, such as NNMi Advanced

To configure user interface features do the following:

1. From the workspace navigation panel, select the **User Interface Configuration** workspace.
2. Make your configuration choices (see [table](#)).
3. Click  **Save and Close**.
4. To apply your Console Timeout or Initial View configuration changes, sign out of the NNMi console. After restarting the console, your changes should take effect.

Global Control Attributes for User Interface Configuration

Attribute	Description
Console Timeout	<p>NNMi's default session inactivity timeout value is 18 hours. Use this attribute to change the timeout interval in days, hours, and minutes.</p> <p>Note: The minimum timeout value is 1 minute.</p> <p>After this period, if no mouse movement occurs, the console grays out and the user needs to sign in to the console again.</p> <p>Tip: If your network operation center (NOC) has a large screen where a map of the most important nodes is continuously displayed, use a launched view. See "Launch a Troubleshooting Workspace View" (on page 338). A map session launched with a URL never times out. The map launched automatically updates every 30 seconds. (If you are using Mozilla Firefox, also see Configure Mozilla Firefox Timeout Interval.)</p>
Initial View	<p>Use this attribute to specify the initial view to be automatically displayed in the NNMi console by default.</p> <p>Note the following:</p> <ul style="list-style-type: none">• Use the value None (blank) to specify that you do not want a default view automatically displayed by default.• If the Node Group you select has been removed, NNMi uses None (blank view).

Attribute	Description
	<ul style="list-style-type: none"> • To select a Node Group map you have created: <ul style="list-style-type: none"> ■ <i>Prerequisite.</i> Use the Node Group Map Settings configuration workspace to create a Node Group map and enter a Topology Ordering number that lists the Node Group map as the first or last map in the Topology Maps workspace. See "Configure Basic Settings for a Node Group Map" (on page 200) for more information. ■ For the Initial View attribute: <ul style="list-style-type: none"> ○ If you placed the Node Group map as the first entry in the Topology Maps workspace, select First Node Group in Topology Maps workspace. ○ If you placed the Node Group map as the last entry in the Topology Maps workspace, select Last Node Group in Topology Maps workspace.
Enable URL Redirect	<p>If you are using NNM iSPIs with Single Sign-On, this attribute enables NNMi to redirect URL requests to the official Fully Qualified Domain Name (FQDN). The official FQDN is the hostname used to enable Single Sign-On between NNMi and iSPIs and is determined during NNMi installation.</p> <p>Note: Before enabling URL Redirect, verify that the official FQDN is set correctly and that it is a DNS name that is resolvable from the remote systems that need to access the NNMi management server. If the official FQDN does not meet these requirements, users will view errors when trying to access the NNMi console. To view the official FQDN, select Help → About HP Network Node Manager i-series or use the nmmoficialqdn.ovpl script. To change the official FQDN, use the nmmsetofficialqdn.ovpl script.</p> <p>When URL Redirect is enabled, a user can sign on to the NNMi console using any hostname or IP address that is valid for the NNMi management server.</p>
Show Unlicensed Features	<p>By default, NNMi displays menus, views, and workspaces that require an additional license. If you do not have the required license, NNMi labels these features as (Unlicensed) and displays an error message when you try to use the feature. Examples include NNMi Advanced and NNM iSPI features.</p> <p>Use this checkbox to specify whether you want these unlicensed features to be displayed or removed from the NNMi user interface.</p> <p>Note: Typically, if you do not plan to install a permanent license for these features, it is recommended that you clear this checkbox.</p> <p>To remove unlicensed features from the NNMi user interface, clear the Show Unlicensed Features <input type="checkbox"/> checkbox .</p> <p>To specify that these features should be displayed in the NNMi console, make sure the Show Unlicensed Features <input checked="" type="checkbox"/> checkbox is selected.</p> <p>Note: To determine which NNM iSPIs (HP Smart Plug-ins) are enabled, access Help → About HP Network Node Manager i-series and look under the "Extension Information" section. See "Purchase an HP Smart Plug-in" (on page 319) for more information about possible HP Smart Plug-ins.</p>

Note: You can override Default Map Setting using the **Node Group Map Settings** Configuration workspace. See "[Configure Basic Settings for a Node Group Map](#)" (on page 200) for more information.

Default Map Settings Attributes for User Interface Configuration

Attribute	Description
Map Refresh Interval	Specifies the refresh interval for Status Refresh.
Maximum Number of Displayed Nodes	<p>Use this attribute to change the maximum number of nodes to be displayed on a map.</p> <p>Note the following:</p> <ul style="list-style-type: none"> If you change the default value to display a large number of nodes at one time, you might need to re-adjust this number if maps are taking longer than expected to display. In Layer 2 and Layer 3 Neighbor views, NNMi adds nodes one hop at a time. If NNMi finds a large number of nodes in a single hop, the number of nodes might exceed the maximum number specified.
Maximum Number of Displayed End Points	<p>Use this attribute to change the maximum number of end points to be displayed on a map.</p> <p>Note: If you change the default value to display a large number of end points at one time, you might need to re-adjust this number if maps are taking longer than expected to display.</p>
Indicate Key Incidents	<p>When enabled <input checked="" type="checkbox"/>, NNMi enlarges any objects on a Node Group map that are Source Objects for Key Incidents.</p> <p>When disabled <input type="checkbox"/>, NNMi does not indicate the objects on a Node Group map that are Source Objects for Key Incidents.</p> <p>You can override this setting for a particular Node Group map, when you "Configure Basic Settings for a Node Group Map" (on page 200). When viewing the Node Group map, you can also enable or disable this feature. See Node Group Maps and Key Incident Views for more information.</p>

Registration Attributes for User Interface Configuration

Attribute	Description
Last Modified	Indicates the last date and time that any of the user interface attributes were modified.

NNMi also enables you to configure features specific to Node Group Maps. See ["Define Node Group Map Settings" \(on page 198\)](#) for more information.

Configuring Maps

NNMi enables you to configure the following maps

- Node Group Map views
- Path View Maps

When configuring Node Group maps, you can do the following:

- Include only the nodes that are important to you.
- Specify which Node Group maps appear in the Topology Maps workspace.
- Specify refresh information.
- View node groups in the context of a relevant background image, such as a map illustrating node locations.
- View node groups in a customized arrangement.

When configuring Node Group map views, you can also specify the role level required to save maps in a customized arrangement. See ["Define Node Group Map Settings" \(on page 198\)](#) for more information.

When configuring Path View maps you specify undiscovered regions of your network by creating a `Path-Connections.xml` file that defines the path between the undiscovered nodes. See ["Configure a Path View Map" \(on page 206\)](#) for more information.

You can also specify the maximum number of nodes to display on a map. See ["Configuring the NNMi User Interface" \(on page 195\)](#) for more information.

Related Topics

["Node Group Map Settings Form" \(on page 199\)](#)

[Node Group Map View](#)

[Position Nodes in a Node Group Map](#)

Define Node Group Map Settings

Node Group Map settings specify the node group and background image to be used in a Node Group map. Map settings include the following:

- Node group name
- Topology Maps Workspace ordering
- Minimum role for saving edited locations for each node in the map
- Refresh interval
- The maximum number of map nodes
- Node connectivity information
- Node Group connectivity information
- Background image information

Node Group Map views are used for a variety of purposes in NNMi:

- Viewing groups of only the nodes that are important to you.
- Viewing Node Groups in the context of a relevant background image.
- Viewing Node Groups in a customized arrangement.



To define Node Group Map Settings, use the ["Node Group Map Settings Form" \(on page 199\)](#).

To view a Node Group Map, use the **Actions** menu from the NNMi main toolbar from either a Node Group or Node Group Map Settings. See [Node Group Map](#) for more information.


To view more information about the Node Group from a Node Group map, use the **File** → **Open Node Group for Map** option to open the Node Group form for the selected Node Group.

Node Group Map Settings Form

Use the Node Group Map Settings form to configure maps based on currently defined Node Groups. Items you configure include the background image and type of connectivity (for example, Layer 2) to be displayed on the map.

Note: NNMi displays the list of Node Group Map Settings whose default configuration has been changed. If NNMi does not display a list of Node Group Map Settings, this means that NNMi is using the default settings for each Node Group Map. To change the default settings for a Node Group Map, either reposition the nodes on the map of interest and select  **Save Layout** from the Node Group Map toolbar or use the Node Group Map Settings form to create a Node Group Map Settings configuration as described below. See [Position Nodes on a Node Group Map](#) for more information about using  **Save Layout**.

To configure Node Group Map Settings, do the following:

1. Navigate to the **Node Group Map Settings Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Node Group Map Settings**.
2. Make your configuration choices (see [table](#)).
3. Click  **Save and Close**.

Note: You can also access the Node Group Map Settings form from a Node Group Map using the **File** → **Open Node Group Map Settings** option.

Tasks for Configuring Node Group Map Settings

Task	How
"Configure Basic Settings for a Node Group Map" (on page 200)	Use the Basics Settings pane to configure Node Group, Topology Maps, and Refresh Interval information. Note: To apply your Topology Maps Ordering configuration changes, sign out of the NNMi console. After restarting the console, your changes should take affect. Possible configuration changes include reordering a Node Group map view or adding a new Node Group map view to the workspace.
"Configure the Connectivity to be Displayed for a Node Group Map" (on page 202)	Use the Connectivity tab to configure the level of node connectivity to be displayed on the Node Group Map. Use this tab to also specify the Node Group connectivity to be displayed and maximum connections to be included on the Node Group map.





Task	How
"Configure Background Image Information for a Node Group Map" (on page 203)	Use the Background Image tab to configure information about the Background Image to use on the Node Group map.

Configure Basic Settings for a Node Group Map

The Basic Settings configuration determines general information about the Node Group map, including the following:


- Which Node Group to display
- Availability of the map in the Topology Maps workspace
- Location of the map in the list of views in the Topology Maps workspace
- Minimum role for saving the map layout
- Refresh interval for the Node Group map
- Maximum number of nodes to display on the map
- Whether to indicate Key Incidents

To establish Basic Settings for a Node Group Map:

1. Navigate to the **Node Group Map Settings** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Node Group Map Settings**.
 - c. Do one of the following:
 - To create a Node Group Map Settings definition, click the  New icon.
 - To edit a Node Group Map Settings definition, select a row, click the  Open icon.
 - To delete a Node Group Map Settings definition, select a row and click the  Delete button
2. Establish the appropriate settings to identify Node Group and Refresh Settings information (see [tables](#)).
3. Click  **Save and Close** if you are ready to save your changes.

Basic Attributes





Attribute	Description
Node Group	<p>Specifies which parent node group to display in the Node Group Map view. The contents of the parent node group include any nodes and Child Node Groups associated with it.</p> <p>Note: NNMi displays any Child Node Groups of the selected parent Node Group as a hexagon on the map.</p> <p>The Expand Child in Parent Node Group Map attribute determines how a Child Node Group appears on the Node Group Map. Expand Child in Parent Node Group Map is disabled by default.</p>

Attribute	Description
	<ul style="list-style-type: none"> If the Child Node Group has the Expand Child in Parent Node Group Map attribute <i>disabled</i>, the Child Node Group appears as a hexagon on the map as shown below: <ul style="list-style-type: none">  If any Child Node Group has the Expand Child in Parent Node Group Map attribute <i>enabled</i>, NNMi instead recursively displays each of the nodes in that Child Node Group on the map. <p>See Node Group Form: Child Node Groups Tab for more information about configuring Child Node Groups.</p>
Topology Maps Ordering	<p>Use this attribute to specify the order in which you want the Node Group map to appear in the Topology Maps workspace.</p> <p>Note: If you do not want this Node Group map to appear in the Topology Maps workspace, leave the value blank.</p> <p>See Views Provided by NNMi for more information about the maps provided in the Topology Maps workspace.</p> <p>Note: To apply your Topology Maps Ordering configuration changes, sign out of the NNMi console. After restarting the console, your changes should take affect. Possible configuration changes include reordering a Node Group map view or adding a new Node Group map view to the Topology Maps workspace.</p>
Minimum Role for Saving Map Layout	<p>Controls the minimum user role required to save the layout of repositioned nodes in a Node Group Map. This value also controls the minimum user role for configuring Node Group Map Settings.</p> <p>Note: Only a user with the role of Administrator can set the Minimum Role for Saving Map Layout value.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> Administrator Operator Level 2 Operator Level 1 <p>The default value is <i>Administrator</i>. See "Determine which NNMi Role to Assign" (on page 33) for more information about NNMi roles.</p> <p>Note: A user with any role can initially reposition nodes on a Node Group Map view. However, unless your user name is assigned to the required minimum role, you cannot save the new node locations on the map. After being saved, these node positions are seen by any user opening this Node Group Map.</p>
Map Refresh Interval	<p>Specify the Refresh Interval you want to use in days, hours, minutes, and seconds. By default, the Refresh Interval is 30 seconds. This interval is used to set the Refresh Status interval for this map if it is used.</p>
Indicate Key Incidents	<p>When enabled <input checked="" type="checkbox"/>, NNMi enlarges any objects on a Node Group map that are Source Objects for Key Incidents.</p> <p>When disabled <input type="checkbox"/>, NNMi does not indicate the objects on a Node Group map that are</p>

Attribute	Description
	Source Objects for Key Incidents. When viewing the Node Group map, you can also enable or disable this feature. See Node Group Maps and Key Incident Views for more information.
Maximum Number of Displayed Nodes	Specifies the maximum number of nodes to be displayed on the Node Group map. Note: This number applies to the total number of nodes within the Node Group, including any Child Node Groups displayed on the map.
Maximum Number of Displayed End Points	Specifies the maximum number of end points to be displayed on a map. Note: If maps are taking longer than expected to display, you might need to re-adjust this number.

Configure the Connectivity to be Displayed for a Node Group Map

The Connectivity Tab of the Node Group Map Settings form enables you to specify the level of connectivity to be displayed on the Node Group map. You also specify the connections that you want to display.

- Navigate to the **Connectivity tab** of the **Node Group Map Settings** form.
 - From the workspace navigation panel, select the **Configuration** workspace.
 - Select **Node Group Map Settings**.
 - Do one of the following:
 - To create a Node Group Map Settings definition, click the  New icon.
 - To edit a Node Group Map Settings definition, select a row, click the  Open icon.
 - To delete a Node Group Map Settings definition, select a row and click the  Delete button
 - Select the **Connectivity** tab.
- Configure the connectivity information for this Node Group Map Settings definition (see [table](#)).
- Click  **Save and Close** if you are ready to save your changes.





Connectivity Attributes

Attribute	Description
Connectivity Type	Connectivity Type determines the type of connectivity to display between nodes in the Node Group Map view. By default, NNMi displays the Layer 2 connectivity between nodes when displaying a Node Group Map view. Possible values include: <ul style="list-style-type: none"> • None - Choose this if you do not want any connectivity displayed on the map. • Layer 2 - Uses Layer 2 connectivity when displaying devices in a Node Group Map view. This connectivity is used by default when positioning node locations on a Node Group Map. • Layer 3 - Uses Layer 3 connectivity when displaying devices on a Node Group Map view.

Attribute	Description
	See Position Nodes on a Node Group Map for more information.
Add L2 Subnet Connections	If you specify Layer 3 or None as the Connectivity Type, this option specifies that you want to include any subnet connections determined by Subnet Connections Rules. See " Configure Subnet Connection Rules " (on page 109) for more information.
Add L2 User Connection Edits	If you specify Layer 3 or None as the Connectivity Type, specifies that you want to include any Layer 2 connections added using the NNMi nnmconnect.ovpl command to add or delete connection data. See " Add or Delete a Layer 2 Connection " (on page 124) for more information.
Interface Group	Use this option, if you want to reduce the connectivity endpoints on the Node Group Map. The Interface Group you select defines the Interface Group to which an interface must belong to be used to connect a Node Group to a Node Group or a Node to a Node Group. NNMi displays Layer 2 endpoints that are interfaces in the group. NNMi displays Layer 3 endpoints that are IP addresses associated with interfaces in the group.
Nodes to Node Group	Select this check box if you want Node to Node Group connectivity to appear on the Node Group map. Note: By default, this option is not enabled.
Node Groups to Node Groups	Select this check box if you want Node Group to Node Group connectivity to appear on the Node Group map. Note: By default, this option is not enabled.

Configure Background Image Information for a Node Group Map

Use the Background Image tab of the Node Group Map Settings form to configure information about the Background Image to use on the Node Group map.

- Navigate to the **Background Image** tab of the **Node Group Map Settings** form.
 - From the workspace navigation panel, select the **Configuration** workspace.
 - Select **Node Group Map Settings**.
 - Do one of the following:
 - To create a Node Group Map Settings definition, click the  New icon.
 - To edit a Node Group Map Settings definition, select a row, click the  Open icon.
 - To delete a Node Group Map Settings definition, select a row and click the  Delete button.
- Establish the appropriate settings to identify the Background Image information (see [table](#)).
- Click  **Save and Close** if you are ready to save your changes.

Background Image Attributes

Attribute	Description
Background Image	<p>Enter the URL for the background image you want to use for this Node Group Map. You can use a background image provided by NNMi or add your own.</p> <p>Note: Click Background Image to view the map whose URL you enter.</p> <p>Use a Background Image Provided by NNMi</p> <p>NNMi provides a set of background images that include maps of many countries. If you want to use one of those images, append the location and file name to the URL at which you access the NNMi console. Use the format: <code>/nnmbg/<file name></code>. For example:</p> <pre>/nnmbg/colorado.gif</pre> <p>To see all of the available images provided by NNMi, browse to:</p> <pre>http://<serverName>:<portNumber>/nnmbg/</pre> <p><code><serverName></code> = the fully-qualified domain name of the NNMi management server</p> <p><code><portNumber></code> = the port that the jboss application server uses for communicating with the NNMi console</p> <p>Use a Background Image You Provide</p> <p>You can also provide your own images. See "Background Image Sources in Node Group Maps" (on page 205) for more information about where to load the background images you want to use.</p> <p>To see a list of all the images added to NNMi, access the following URL:</p> <pre>http://<serverName>:<portNumber>/nnmdocs/images/</pre> <p>To use an image that has been added to NNMi, use the following URL:</p> <pre>/nnmdocs/images/<file name></pre> <p>For example: <code>/nnmdocs/images/myimage.gif</code></p> <p>Note the following:</p> <ul style="list-style-type: none">• NNMi accepts images that can be loaded by a Web browser. Common file extensions include: .gif, .png and .jpg.• Image names are case sensitive. All background image file names provided by NNMi are lowercase.• Do not use <code>http://<localhost></code> in your URL. This implies the image is on your local machine and is not available from other clients.• If using full URLs, all client machines must be able to resolve the hostname of the server on which the images reside.• When you pan and zoom around the map, the background image moves in relation with the other objects on the map. <p>If the image does not display, see "Troubleshoot URLs When Specifying a Background Image" (on page 206) for more information.</p>
Background Image Scale	<p>The Background Image Scale attribute applies to the actual background image dimensions when displayed on a Node Group Map.</p> <p>Enter a floating point number greater than zero (0.0) to indicate the ratio at which you</p>

Attribute	Description
	<p>want NNMi to scale the background image. For example, the value 1.0 represents a one-to-one ratio, resulting in a background image displayed at actual size. A value of 2.0 represents a two-to-one ratio, resulting in a background image displayed at twice the actual size.</p> <p>Note: The default ratio value is 1.0. (This means no scaling is applied.) Use this default value initially. You can adjust it as needed based on the relative size between the image and nodes.</p> <p>See "Scale Background Images in Node Group Maps" (on page 206) for guidelines for scaling the background images you specify.</p>

Background Image Sources in Node Group Maps

When specifying background images to include in Node Group Maps, NNMi enables you to use images provided by NNMi or images that you provide.

The images that NNMi provides include maps of many countries.

To see the available images provided by NNMi:

Browse to: `http://<serverName>:<portNumber>/nnmbg/`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

To use your own background images:

Place your user-supplied images in the following directory:

Windows:

`<drive>:/Documents and Settings/All Users/Application Data/HP/HP BTO
Software/shared/nm/www/htdocs/images`

`<drive>` is the drive on which NNMi is installed.

Unix:

`/var/opt/OV/shared/nm/www/htdocs/images`

NNMi accepts images that can be loaded by a Web browser. Common file extensions include: .gif, .png and .jpg.

To see the available images that have been added to NNMi:

Access the following URL: `http://<serverName>:<portNumber>/nmdocs/images`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

See "[Node Group Map Settings Form](#)" (on page 199) for more information about how to configure Node Group Maps to use background images.

Scale Background Images in Node Group Maps

Scale a specified background image for a Node Group Map using the Background Image Scale attribute. See ["Define Node Group Map Settings" \(on page 198\)](#) for more information.

When you use the maps provided by NNMi, it is recommended that you initially use the default value of 1.0 for the Background Image Scale.

When you use your own images for map backgrounds and you are selecting a scale value, consider the following:

- NNMi renders its nodes 50 by 50 pixels. This means if your image is 500 pixels wide, there is room for 10 nodes across the image.
- To display the image at normal resolution, enter a scale value of 1.0. (This means no scaling occurs.)
- After the image displays on the map, look at the relationship between the node size and the background to determine whether you need to rescale the background image:
 - If the nodes look too large compared to the background, enlarge the image using a scale value greater than 1.0.
 - If the nodes look too small compared to the background, make the image smaller using a scale value less than 1.0.

Troubleshoot URLs When Specifying a Background Image

This topic contains troubleshooting steps to use if your background image does not display.

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

If you used a relative URL (beginning with a slash (/) in the Background Image attribute value:

1. Copy and paste the URL to a browser.
2. Insert `http://<serverName>:<portNumber>` in front of the slash (/).

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

If you used an absolute URL (beginning with http://) in the Background Image attribute value:

Copy and paste the URL to a browser.

Configure a Path View Map

Configuring a Path View map is useful when you have two or more areas of your network which are separated by undiscovered devices, such as service provider nodes. NNMi enables you to configure a Path View map that traverses undiscovered regions of your network. To configure this kind of Path View map, create a `PathConnections.xml` file that defines the following:

- **Required.** A Start node for each `<CONNECT>` to be included in the Path View map
- **Optional.** A unique identifier for a `<CONNECT>`

- *Optional.* The outbound interface from each Start node per <CONNECT>
- *Required.* Any number of undiscovered nodes you want to be included in the map between each <CONNECT>
- *Optional.* An End node for a <CONNECT> to be included in the Path View map
- *Optional.* The inbound interface to each End node per <CONNECT> specified.

Each time NNMi determines a node in the Path View, NNMi checks whether the node is specified as a Start node in the `PathConnections.xml` file. If the node is specified as a Start node in `PathConnections.xml`, each <CONNECT> configured in `PathConnections.xml` is inserted in the Path View map.

Note: *NNMi Advanced.* NNMi can use RAMS data to determine router paths. When RAMS data is used to determine the router paths, NNMi ignores the `PathConnections.xml` file. See [Path View with NNMi Advanced](#) for more information.

To configure a Path View map:

Using the required format, create a `PathConnections.xml` file in the following location:

Windows:

```
<drive>:/Documents and Settings/All Users/Application Data/HP/HP BTO Software/shared/ nnm/conf/PathConnections.xml
```

<drive> is the drive on which NNMi is installed

UNIX:

```
/var/opt/OV/shared/nnm/conf/PathConnections.xml
```

The following table describes each of the file elements and its format requirements. (Also see the [sample file](#))

Note: Each segment of the path that you specify using the <CONNECT> element is directional. If you want to view the path between two nodes in both directions, make sure you include the Start and End nodes for each direction. You should also include the inbound interface for the Start node. If you do not limit the possible routers by including the inbound interface for the Start node, Path View might find additional routers in the path.

Elements for the Path View Configuration File

Element Descriptions

<CONNECTIONS>

Required parent element. The file must include only one <CONNECTIONS> element.

<CONNECT>

Specifies a segment of the path. Each <CONNECT> designates a start and stop location for the <CONNECT>.

The file can include more than one <CONNECT> element.

<ID>

C1

</ID>

Optional. Identifies the connection. NNMi uses the ID value you enter when reporting errors for a <CONNECT>.

If you do not provide an ID value for the path between a Start and End node, any error message for the <CONNECT> displays `Not Applicable` rather than the unique identification value.

Element Descriptions

```
<START>
  <IP_OR_DNS>xxx.xx.xxx.x</IP_OR_DNS>
  <OUTBOUND_INTERFACE_IFINDEX>x</OUTBOUND_INTERFACE_IFINDEX>
  <NEXT_HOPS>
    <HOP>xxx.xx.xxx.x</HOP>
    <HOP>xxx.xx.xxx.x</HOP>
  </NEXT_HOPS>
</START>
```

Specifies the node where a segment of the path starts. You provide values for the following elements:

- `<IP_OR_DNS>` provides the name or IPv4 address of a node in your network. See ["Configure the Node Name Strategy" \(on page 99\)](#) for more information about node names.
- *Optional.* `<OUTBOUND_INTERFACE_IFINDEX>` designates which of the Start node's interfaces to use for this segment of the path.
- `<NEXT_HOPS>` designates one or more specific IPv4 addresses or nodes that you want to be included in the path.

```
<END>
  <IP_OR_DNS>xxx.xx.xxx.x</IP_OR_DNS>
  <INBOUND_INTERFACE_IFINDEX>x</INBOUND_INTERFACE_IFINDEX>
</END>
```

Specifies the node where the `<CONNECT>` ends. You provide values for the following elements:

- `<IP_OR_DNS>` provides the name or IPv4 address of a node in your network.
- *Optional.* `<INBOUND_INTERFACE_IFINDEX>` designates which of the End node's interfaces to use for this segment of the path.

```
</CONNECT>
```

Required. Designates the end of the XML code that defines one segment of your path view.

```
</CONNECTIONS>
```

Required parent element. Designates the end of the XML code that defines your path view.

Click here to view a sample file:

```
<?xml version="1.0" encoding="UTF-8"?>
<CONNECTIONS>
  <CONNECT>
    <ID>
      C1
    </ID>
    <START>
      <IP_OR_DNS>StartNode.xx.xxx.x</IP_OR_DNS>
      <OUTBOUND_INTERFACE_IFINDEX>3</OUTBOUND_INTERFACE_IFINDEX>
      <NEXT_HOPS>
        <HOP>hop-1.xxx.xx.xxx</HOP>
        <HOP>hop-2.xxx.xx.xxx</HOP>
      </NEXT_HOPS>
    </START>
  </CONNECT>
</CONNECTIONS>
```



```

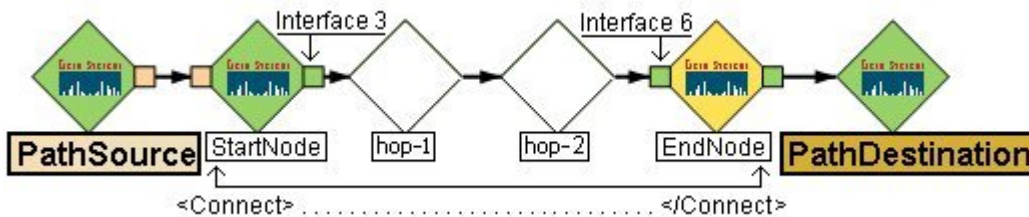
        <IP_OR_DNS>EndNode.xxx.xx.xxx</IP_OR_DNS>
        <INBOUND_INTERFACE_IFINDEX>6</INBOUND_INTERFACE_IFINDEX>
    </END>
</CONNECT>
</CONNECTIONS>

```

When viewing Path View maps that are configured using the `PathConnections.xml` file, note the following:

- If the `<END>` element is not specified, NNMi connects directly to the Destination node to complete the path.
- If the `<END>` element is specified, then the associated `<IP_OR_DNS>` specifies a discovered node as the End node of this segment of your Path View.

Click here to view the sample Path View map generated from the sample file above.



Click here to view a sample file that includes both directions for the sample Path View map above.

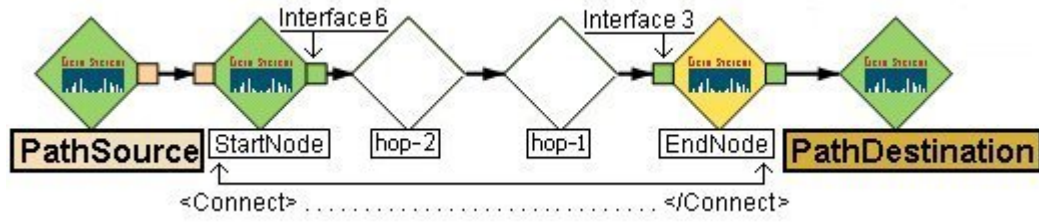
Note: In this example, the path is the same in both directions. In many cases, the path might be different in each direction.

```

<?xml version="1.0" encoding="UTF-8"?>
<CONNECTIONS>
  <CONNECT>
    <ID>
      C1
    </ID>
    <START>
      <IP_OR_DNS>StartNode.xx.xxx.x</IP_OR_DNS>
      <OUTBOUND_INTERFACE_IFINDEX>6</OUTBOUND_INTERFACE_IFINDEX>
      <NEXT_HOPS>
        <HOP>hop-1.xxx.xx.xxx</HOP>
        <HOP>hop-2.xxx.xx.xxx</HOP>
      </NEXT_HOPS>
    </START>
    <END>
      <IP_OR_DNS>EndNode.xxx.xx.xxx</IP_OR_DNS>
      <INBOUND_INTERFACE_IFINDEX>3</INBOUND_INTERFACE_IFINDEX>
    </END>
  </CONNECT>
</CONNECTIONS>

```

Click here to view the sample Path View map generated from the sample file above.



Configuring Incidents

Incidents are information that NNMi considers important to bring to your attention regarding your network. See ["How NNMi Gathers Incidents" \(on page 211\)](#) for more information.

NNMi provides a set of incident configurations for the following:

- Traps generated from an SNMP agent
- Management incidents that are generated by NNMi
- Events generated by NNM 6.x or 7.x management stations

See ["Incident Configurations Provided by NNMi" \(on page 214\)](#) for more information about the configurations provided.

NNMi provides one centralized location, the incident views, where the management events, SNMP traps, and NNM 6.x or 7.x forwarded events are visible to your team. You control which SNMP traps and NNM 6.x or 7.x events are considered important enough to show up as incidents. You can also configure how incidents that are generated by NNMi are displayed. You and your team can easily monitor the incidents and take appropriate action to preserve the health of your network.

You may choose to modify the incident configurations provided by NNMi or create new incident configurations. To do so, see the following topics:

- ["Configure SNMP Trap Forwarding" \(on page 239\)](#)
- ["Configure SNMP Trap Incidents" \(on page 246\)](#)
- ["Configure How Management Events Are Displayed" \(on page 264\)](#)
- ["Configure Remote NNM 6.x/7.x Events" \(on page 261\)](#)
- Using the Incident Configuration form, you can also configure pairwise correlations. See ["About Pairwise Configurations" \(on page 276\)](#) for more information.

Note: If you make changes to an incident configuration provided by NNMi, remember to place your name in the Author attribute. See ["Specify an Author for Your Incident Configuration" \(on page 260\)](#) for more information.

Define relationships between multiple incidents by creating deduplication and rate configurations. See ["Reduce the Number of Incoming Incidents" \(on page 266\)](#), ["Correlate Duplicate Incidents \(Deduplication Configuration\)" \(on page 269\)](#), and ["Track Incident Frequency \(Rate: Time Period and Count\)" \(on page 273\)](#), for more information.

Note: Each time you stop and restart ovjboss, any incidents that have not yet been correlated or persisted are lost. This means that after a restart of ovjboss, an incoming incident might not be correlated as expected. For example, after a restart of ovjboss, a duplicate incident might not be correlated under its original parent incident. Instead, a new parent incident might be generated. See ["Stop or Start an NNMi Process" \(on page 26\)](#) for more information about starting and stopping the ovjboss process.

How NNMi Gathers Incidents

Incidents are information that NNMi considers important to bring to your attention regarding your network. NNMi gathers incident information from the sources described in the following table.

Incidents Collected by NNMi

Information Source	Description
Causal Engine - Management Events	The NNMi Causal Engine analyzes the health of your network and provides the ongoing health status reading for each device. The Causal Engine also extensively evaluates problems and determines the root cause for you, whenever possible, sending incidents to notify you of problems. Any incident generated from a Causal Engine management event has an Origin of Management Software in your incident views. See Using the Incident Form for more information about incident attributes.
SNMP Traps	Traps are unsolicited SNMP notifications that come from your network devices. The NNMi Causal Engine uses this information as symptoms during its analysis. SNMP traps can also appear as incidents if configured to do so, using the NNMi incident configuration feature. See "Configure SNMP Trap Incidents" (on page 246) for more information.
NNM 6.x and 7.x Events	NNMi can display NNM 6.x and 7.x events that are configured to be forwarded to NNMi.

See ["The NNMi Causal Engine and Incidents" \(on page 212\)](#) for an overview of what the NNMi Causal Engine does with the information collected. See ["About the Event Pipeline" \(on page 213\)](#) for an overview of the event pipeline path each trap or NNMi event takes before NNMi creates an incident. This chronological path guarantees that the data is analyzed in chronological order.

Note: The Causal Engine also sends incident information that it generates through the event pipeline to guarantee the chronological order for determining its root cause incidents.

By default, NNMi includes preconfigured definitions for SNMP traps, NNM 6.x and 7.x events, and the incidents generated by the NNMi Causal Engine. See [Incident Views Provided by NNMi](#) for more information.

Related Topics

["Configure SNMP Trap Incidents" \(on page 246\)](#)

["Configure How Management Events Are Displayed" \(on page 264\)](#)

["Configure Remote NNM 6.x/7.x Events" \(on page 261\)](#)

["Incident Configurations Provided by NNMi" \(on page 214\)](#)

["Reduce the Number of Incoming Incidents" \(on page 266\)](#)

The NNMi Causal Engine and Incidents

The Causal Engine extensively evaluates network issues and determines the root cause for you, whenever possible, sending incidents to notify you of problems.

The NNMi Causal Engine defines root cause in terms of symptoms. To do so, it uses a set of rules to define relationships for fault and performance (thresholding) symptoms and root causes. Sources of symptom information include SNMP traps and the monitoring information from the State Poller. See ["How NNMi Gathers Incidents" \(on page 211\)](#) for more information.

The NNMi Causal Engine communicates through incidents in the following ways:

- The Causal Engine generates notifications about problems.
- The Causal Engine closes incidents that are no longer valid (for example, when a "Cold Start" trap is received a short time after a "Node Down" incident was generated because a device was recently rebooted).
- The Causal Engine creates a parent-child relationship between incidents that are all related to one problem (for example, a "Node Down" incident contains a child "Interface Down" incident for each neighboring interface of the node).

The Causal Engine uses the following three stages to help determine and display root cause incidents and their related conclusions.

NNMi Causal Engine Stages

Causal Engine Stages	Description
Condition Listener	Collects symptoms from NNMi processes and services.
Hypothesis engine	Analyzes these symptoms to determine relationships until a root cause is reached.
Blackboard	Based on the information sent by the hypothesis engine, the blackboard updates a device's status and posts any related incidents.

The NNMi Causal Engine analyzes the health of your network and provides the ongoing health status reading for each node, interface, IP address, SNMP agent, and connection. See ["The NNMi Causal Engine and Monitoring" \(on page 152\)](#) for more information.

About the Event Pipeline

Any incident information that appears in your incident views first travels through the event pipeline. The event pipeline guarantees that the incident data is analyzed in chronological order.

Note: Not all information that travels through the pipeline results in an incident.

If at any time an incident does not meet the criteria for a stage in the event pipeline, it is ignored and passed to the next stage in the pipeline. The following table describes the stages contained in the event pipeline.

NNMi Event Pipeline Stages

Event Pipeline Stages	Description
SNMP Trap and Event Receiver	Accepts all SNMP traps and remote NNM 6.x or 7.x events
Incident Receiver	Accepts all incident information that comes from the NNMi Causal Engine. See "The NNMi Causal Engine and Incidents" (on page 212) NNMi "The NNMi Causal Engine and Incidents" (on page 212)
Type Enforcer	Determines if a configuration exists for this trap, event, or incident. If the incident configuration exists, the type enforcer begins to populate the incident fields according to the configuration. Examples of the incident fields that are populated include Severity , Origin , Category , and Correlation Nature . If an incident con-

Event Pipe- lineStages	Description
	figuration is disabled or does not exist for the incident, NNMi drops the incident.
Resolver	Determines if a record of the problem device or node exists in the NNMi topology database. If available, the resolver populates the incident with the most current Source Node and Source Object attribute values.
Store Bulk	Collects incidents and stores them.
Notification	Notifies other process and services about a new incident.
Pairwise	Checks for any current pairwise configurations for the incident.
Rate	Checks for any current rate configurations for the incident.
Dedup	Checks for any current deduplication configurations for the incident.
Relate	Performs any additional Causal Engine correlations, and cancels the incident when applicable.
Actions	Performs any automatic actions that the NNMi administrator has configured to be run for one or more incidents. See Using Actions to Perform Tasks for more information.

Incident Configurations Provided by NNMi

NNMi provides several incident configurations out-of-the-box. You can review these configurations or modify these configurations to better meet your needs. For example, you might want to customize the message that appears with a particular type of incident, including adding information to the message displayed.

You might also choose to create your own configurations for additional SNMP traps that are important to you.

These out-of-the-box configurations are organized according to the following categories:

["SNMP Trap Incident Configurations Provided by NNMi" \(on page 216\)](#)

["Management Event Configurations Provided by NNMi" \(on page 229\)](#)

["Remote NNM 6.x/7.x Event Configurations Provided by NNMi" \(on page 226\)](#)

["Incident Pair \(Pairwise\) Configurations Provided by NNM" \(on page 276\)](#)

Note: If you make changes to an incident configuration provided by NNMi, remember to place your name in the Author attribute. See ["Specify an Author for Your Incident Configuration" \(on page 260\)](#) for more information.

Custom Incident Attributes Provided by NNMi

NNMi uses custom incident attributes to attach additional information to incidents.

A subset of CIAs are available for any particular incident. Any relevant CIAs are displayed on the [Incident form](#), in the Custom Attributes tab. There are two categories of possible CIAs:

- SNMP trap varbinds identified by the Abstract Syntax Notation value (ASN.1).Varbinds are defined in MIB files that you can load into NNMi. See ["Load SNMP Trap Definitions" \(on page 247\)](#).
- Custom incident attributes provided by NNMi.

The potential custom incident attributes provided by NNMi are described in the table below.

Custom Incident Attributes Provided by NNMi

Name	Description
cia.address	SNMP agent address
cia.snmpoid	SNMP trap object identifier
cia.eventoid	NNM 6.x/7.x object identifier (oid) for the incident
cia.remotemgr	Hostname or IP address of the NNM 6.x or 7.x management station that is forwarding the event
cia.remotetopoid	Topology identifier (topoid) of the NNM 6.x or 7.x event

NNM iSPI for Performance. For network performance monitoring, additional custom incident attributes are provided for your use. Click here for more information.

NNM iSPI for Performance. Custom Incident Attributes Provided for Thresholding

Name	Description
cia.thresholdReason	Configured thresholds have a value of null. Unset thresholds have a value of No threshold settings defined . See " Configure Threshold Monitoring for Interfaces (NNM iSPI for Performance) " (on page 162) for the complete list of possible performance threshold results and for information about how to configure performance thresholds.
cia.thresholdParameter	The monitored attribute that is being measured. For example, Input Utilization . See " Configure Threshold Monitoring for Interfaces (NNM iSPI for Performance) " (on page 162) for the complete list of possible attributes. This value is selected when configuring performance thresholds.
cia.thresholdLowerBound	The configured value for the low performance threshold. See " Configure Threshold Monitoring for Interfaces (NNM iSPI for Performance) " (on page 162) for more information about how to configure performance thresholds.
cia.thresholdUpperBound	The configured value for the high performance threshold. See " Configure Threshold Monitoring for Interfaces (NNM iSPI for Performance) " (on page 162) for more information about how to configure performance thresholds.
cia.thresholdPreviousValue	Results from the previous Performance Polling Interval. For example, the performance threshold results for the Input Error Rate might change from Nominal to High , based on a change in the thresholdMeasuredValue. See Interface Form for a complete list of possible values.
cia.thresholdCurrentValue	Results from the most recent Performance Polling Interval. For example, High . See Interface Form for a complete list of possible values.
cia.thresholdMeasuredValue	The most recent measurement for the performance threshold. NNM iSPI for Performance monitors this measurement for threshold vio-

Name	Description
	lations. This measurement is the average of all measurements taken during the last polling interval (determined by the NNMi State Poller).
cia.thresholdMeasurementTime	The time at which the threshold was reached for a performance threshold. For example, if the threshold for the Input Error Rate is 6.0, and the thresholdMeasuredValue is 6.0, the time at which the thresholdMeasuredValue become equal to 6.0 is stored in this custom incident attribute. The time appears in ISO 8601 format.

These CIAs are used in a variety of ways:

- In SNMP trap configurations. See ["Configure SNMP Trap Incidents" \(on page 246\)](#).
- In remote NNM 6.x/7.x events. See ["Configure Remote NNM 6.x/7.x Events" \(on page 261\)](#).
- In management events. See ["Configure How Management Events Are Displayed" \(on page 264\)](#).
- In automatic actions. See ["Configure an Action for an Incident" \(on page 283\)](#).
- In correlation configurations. See ["Reduce the Number of Incoming Incidents" \(on page 266\)](#).
- In URL Action definitions (accesses through the Actions menu). See ["Control the Actions Menu" \(on page 303\)](#).

SNMP Trap Incident Configurations Provided by NNMi

NNMi provides the SNMP trap incident configurations described in the following table.

You might also choose to create your own configurations for additional SNMP traps that are important to you.

Note: If you make changes to an incident configuration provided by NNMi, remember to place your name in the Author attribute. See ["Specify an Author for Your Incident Configuration" \(on page 260\)](#) for more information.

SNMP Trap Configurations Provided by NNMi

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
BGPBackward Transition	Generated when the BGP Finite State Machine moves from a higher numbered state to a lower numbered state.	Name CIA	
BGPEstablished	Generated when the BGP Finite State Machine enters the ESTABLISHED state.	Name CIA	
CempMemBufferNotify	Signifies that a cempMemBufferPeak object has been updated in the buffer pool.	Name	
CiscoChassisAlarmOff	Signifies that the agent entity has detected the chassisTempAlarm, chassisMinorAlarm, or chassisMajorAlarm object in this MIB has transitioned to the off(1) state.	Name CIA	
CiscoChassisAlarmOn	Signifies that the agent entity has detected the chassisTempAlarm, chassisMinorAlarm,	Name CIA	

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
	or chassisMajorAlarm object in this MIB has transitioned to the on(2) state.		
CiscoChassisChangeNotification	Agent detects any hot-swap component change or changes in the chassis.	Name CIA	
CiscoColdStart	Occurs when a Cisco Agent is powered up.		5 within a time period 5 minutes
CiscoDemand NeighborLayer2Change	Sent to the manager whenever the D-channel of an interface changes state.	Name CIA IF index	
CiscoEnvMonFanNotification	Indicates at least one of the fans in the fan array has failed.		
CiscoEnvMonFanStatusChange Notification	Indicates a state change for a device being monitored by ciscoEnvMonFanState.		
CiscoEnvMonRedundantSupplyNotification	Indicates the redundant power supply failed.		
CiscoEnvMonSuppStatusChangeNotification	Indicates a change in the state of a device being monitored by ciscoEnvMonSupplyState.		
CiscoEnvMonTempStatusChangeNotification	Indicates a change in the state of a device being monitored by ciscoEnvMonTemperatureState.		
CiscoEnvMonTemperatureNotification	Indicates the temperature measured at a given testpoint is outside the normal range for the testpoint, For example, it is at the warning, critical, or shutdown stage.		
CiscoEnvMonVoltStatusChangeNotification	Indicates a change in the state of a device being monitored by ciscoEnvMonVoltageState.		
CiscoEnvMonVoltageNotification	Indicates the voltage measured at a given testpoint is outside the normal range for the testpoint. For example, it is at the warning, critical, or shutdown stage.		
CiscoLinkDown	Occurs when the Cisco agent detects an interface has gone down.	Name CIA IF index	
CiscoLinkUp	Occurs when the Cisco agent detects an interface has come back up.	Name CIA IF index	
CiscoModuleDown	Signifies that the agent entity has detected that a module has gone down.	Name CIA Module Index	
CiscoModuleUp	Signifies that the agent entity has detected that a module has come back up.	Name CIA Module Index	

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
CiscoVlanPortStatusChange	Generated by a device when the value of vlanTrunkPortDynamicStatus object has been changed.	Name CIA	
CiscoWarmStart	Occurs when an Cisco agent is reconfigured.		5 within a time period of 5 minutes
HSRPStateChange	Sent when an HSRP interface transitions to or from an Active or Standby state in a particular HSRP Group.	Name CIA	
lelf_VRRPStateChange	Sent when a standard VRRP interface transitions to or from a Master State in a particular VRRP Group. This trap is used by the standard VRRP protocol. It corresponds to the vrrpTrapNewMaster trap name.	Name CIA	
OSPFIfStateChange	Signifies that there has been a change in the state of a nonvirtual OSPF interface.	Name CIA	
OSPFNbrStateChange	Signifies that there has been a change in the state of a nonvirtual OSPF neighbor.	Name CIA	
OSPFVirtIfStateChange	Signifies that there has been a change in the state of an OSPF virtual interface.	Name CIA	
RMONFallingAlarm	Sent when an RMON device falls below a pre-configured threshold.	Name CIA RMON Alarm Variable	
RMONRiseAlarm	Sent when an RMON device exceeds a pre-configured threshold.	Name CIA RMON Alarm Variable	
Rc2kTemperature	Signifies the SNMPv2c entity acting in an agent role, has detected the chassis is overheating.		
RcAggLinkDown	Signifies the operational state of the Multi-Link Trunk (MLT) Aggregator changed from Up to Down.		
RcAggLinkUp	Signifies the operational state of the Multi-Link Trunk (MLT) Aggregator changed from Down to Up.		
RcChasFanDown	Signifies the SNMPv2c entity, acting in an agent role, has detected that the rcChasFanOperStatus object for one of its power supply units is about to transition to the Down state.		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
RcChasFanUp	Signifies the SNMPv2c entity, acting in an agent role, has detected that the rcChas-FanOperStatus object for one of its power supply units is about to transition to the Up state.		
RcChasPowerSupplyDown	Signifies the rcChasPowerSupplyOperStatus object for one of its power supply units is about to transition to the Down state.		
RcChasPowerSupplyUp	Signifies the SNMPv2c entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply units is about to transition to the Up state.		
RcSmltIsLinkDown	Signifies the operational state of the Split Multi-Link Trunk (SMLT) Aggregator Link is transitioning from Up to Down.		
RcSmltIsLinkUp	Signifies the operational state of the Split Multi-Link Trunk (SMLT) Aggregator Link is transitioning from Down to Up.		
Rc_VrrpStateChange	Sent when a Rapid City (RC) Nortel interface transitions to or from a Master state in a particular VRRP Group. This trap is used by the Rapid City (RC) Nortel propriety VRRP protocol. It corresponds to the rcVrrpTrap-NewMaster trap name.	Name CIA	
Rcn2kTemperature	Signifies that the SNMPv2c entity, acting in an agent role, has detected the chassis is overheating.		
RcnAggLinkDown	Signifies the operational state of the Multi-Link Trunk (MLT) Aggregator Link changed from Up to Down.		
RcnAggLinkUp	Signifies the operational state of the Multi-Link Trunk (MLT) Aggregator Interface has changed from Down to Up.		
RcnChasFanDown	Signifies the SNMPv2c entity, acting in an agent role, has detected that the rcChas-FanOperStatus object for one of its power supply units is about to transition into the Down state.		
RcnChasFanUp	Signifies the SNMPv2c entity, acting in an agent role, has detected that the rcChas-FanOperStatus object for one of its power supply units is about to transition into the Up state.		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
RcnPowerSupplyDown	Signifies the SNMPv2c entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply units is about to transition into the Up state.		
RcnPowerSupplyUp	Signifies the SNMPv2c entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply units is about to transition into the Up state.		
RcnSmltIsLinkDown	Signifies the rcChasPowerSupplyOperStatus object for one of its power supply units is about to transition into the Down state.		
RcnSmltIsLinkUp	Signifies the rcChasPowerSupplyOperStatus object for one of its power supply units is about to transition into the Up state.		
SNMPColdStart	Signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.	Name CIA	5 within a time period of 5 minutes
SNMPLinkDown	Signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.	Name CIA IF index	
SNMPLinkUp	Signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.	Name CIA IF index	
SNMPWarmStart	Signifies that the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.	Name CIA	5 within a time period of 5 minutes
STPNewRoot	Indicates that the sending agent has become the new root of the Spanning Tree.	Name CIA	
STPTopologyChange	Sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state.	Name CIA	

NNMi Advanced. SNMP Trap Incident Configurations for Route Analytics Management Servers (RAMS)

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
RexASPathChange	Signifies the AS path to a route has changed.		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
RexAdjStateDown	Signifies the adjacency went down.		
RexAdjStateFlap	Signifies the adjacency's flap count (rexEventCount) in the duration given by rexCountDuration has become greater than or equal to rexEventThreshold. Both adjacency up and adjacency down count as flaps. For example: An adjacency going down and coming up increments the flap count by two.		
RexAdjStateUp	Signifies the adjacency came up.		
RexBgpRedundChange	Signifies a change in the number of next hops available for reaching a prefix		
RexBgpVpnReachByCustGain	Signifies the routes in the Customer announced by PE that are up and not baselined as compared to the threshold value. The deviation is represented as either of the following: <ul style="list-style-type: none"> • The number of routes in the Customer that are up and not baselined • The percentage of participating routes in the Customer that are up and not baselined 		
RexBgpVpnReachByCustLoss	Signifies the routes in the Customer announced by PE that are down and not baselined as compared to the threshold value. The deviation is represented as either of the following: <ul style="list-style-type: none"> • The number of routes in the Customer that are down and not baselined • The percentage of participating routes in the Customer that are down and not baselined 		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
RexBgpVpnReachByRtGain	Signifies the routes in the Route Target announced by PE that are up and not baselined as compared to the threshold value. The deviation is represented as either of the following: <ul style="list-style-type: none"> The number of routes in the Route Target that are up and not baselined The percentage of participating routes in the Route Target that are up and not baselined 		
RexBgpVpnReachByRtLoss	Signifies the routes in the Route Target announced by PE that are down and not baselined as compared to the threshold value. The deviation is represented as either of the following: <ul style="list-style-type: none"> The number of routes in the Route Target that are down and not baselined The percentage of participating routes in the Route Target that are down and not baselined 		
RexPathChange	Indicates the a path attributes such as metric, number of hops, intermediate hops from a source router to a IP prefix or NSAP address have changed.		
RexPeeringStateDown	Indicates a peering between a router and RAMS has gone down		
RexPeeringStateFlap	Indicates a peering between a router and RAMS has gone down.		
RexPeeringStateUp	Indicates a peering between a router and RAMS has come up.		
RexPrefixDrought	Signifies a particular BGP Peer Rib has decreased significantly from the Baseline Size as a percentage of the baseline		
RexPrefixFlood	Signifies a particular BGP Peer Rib has increased significantly from the Baseline Size as a percentage of the baseline.		
RexPrefixStateDown	Indicates the prefix(<code>rexDstPrfx,rexDstMask</code>) announced by Router(<code>rexSrcRtrSysID, rexSrcRtrIP, rexSrcRtrName</code>) has gone down.		



Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
RexPrefixStateFlap	Indicates the prefix (rexDstPrfx,rex-DstMask) flap count (rexEventCount) in the duration given by rex-CountDuration becomes greater than or equal to rexEventThreshold. Both prefix up and prefix down count as flaps. For example: A prefix going down and coming up increments the flap count by two.		
RexPrefixStateUp	Indicates the prefix (rexDstPrfx,rexDstMask) announced by Router (rexSrcRtrSysID, rexSrcRtrIP, rexSrcRtrName) has come up.		
RexRtrConnected	Indicates the first adjacency of a router becomes full duplex. This means the neighbor sends an LSA and the previously isolated router sends an LSA across that adjacency.		
RexRtrIsolated	Signifies a router has become isolated from the rest of the topology as all of its duplex connections it has to other routers which are not overloaded with respect to a particular routing protocol have gone down.		
RexRtrStateFlap	Signifies the router's flap count (rex-EventCount) in the duration given by rexCountDuration has become greater than or equal to rexEventThreshold. Both router isolation and router connection count as flaps. For example: A router getting isolated and then connected increments the flap count by two.		
RexTest	This trap is sent for test purposes		
RexVpnPEParticipationByCustGain	Signifies the Provider Edges (PEs) participating in the Customer that are up and not baselined as compared to the threshold value. The deviation is represented as either of the following: <ul style="list-style-type: none"> • The number of PEs that are up and not baselined • The percentage of participating PEs that are up and not baselined 		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
RexVpnPEParticipationByCustLoss	<p>Signifies the Provider Edges (PEs) participating in the Customer that are down and not baselined as compared to the threshold value. The deviation is represented as either of the following:</p> <ul style="list-style-type: none"> • The number of PEs that are down and not baselined • The percentage of participating PEs that are down and not baselined 		
RexBgpVpnReachByRtGain	<p>Signifies the routes in the Route Target announced by PE that are up and not baselined as compared to the threshold value. The deviation is represented as either of the following:</p> <ul style="list-style-type: none"> • The number of routes in the Route Target that are up and not baselined • The percentage of participating routes in the Route Target that are up and not baselined 		
RexVpnPEParticipationByRtLoss	<p>Signifies the PEs participating in the Route Target (RT) that are down and not baselined as compared to the threshold value. The deviation is represented as either of the following:</p> <ul style="list-style-type: none"> • The number of PEs that are down and not baselined • The percentage of participating PEs that are down and not baselined 		
RexVpnReachByCustPEGain	<p>Signifies the routes in the Customer announced by PE that are up and not baselined as compared to the threshold value. The deviation is represented as either of the following:</p> <ul style="list-style-type: none"> • The number of routes in the Customer that are up and not baselined • The percentage of participating routes in the Customer that are up and not baselined 		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
RexVpnReachByCustPELoss	<p>Signifies the routes in the Customer announced by PE that are down and not baselined as compared to the threshold value. The deviation is represented as either of the following:</p> <ul style="list-style-type: none"> • The number of routes in the Customer that are down and not baselined • The percentage of participating routes in the Customer that are down and not baselined 		
RexVpnReachByCustPrefixDown	Signifies that the prefix has become unreachable in Customer.		
RexVpnReachByCustPrefixUp	Signifies that the prefix has become reachable in Customer.		
RexVpnReachByRtPEGain	<p>Signifies the routes in the Route Target announced by PE that are up and not baselined as compared to the threshold value. The deviation is represented as either of the following:</p> <ul style="list-style-type: none"> • The number of routes in the Route Target that are up and not baselined • The percentage of participating routes in the Route Target that are up and not baselined 		
RexVpnReachByRtPELoss	<p>Signifies the routes in the Route Target announced by PE that are down and not baselined as compared to the threshold value. The deviation is represented as either of the following:</p> <ul style="list-style-type: none"> • The number of routes in the Route Target that are down and not baselined • The percentage of participating routes in the Route Target that are down and not baselined 		
RexVpnReachByRtPrefixDown	Signifies the prefix has become unreachable in RT.		
RexVpnReachByRtPrefixUp	Signifies that the prefix has become reachable in RT.		
TrafficHighLinkUtilization	Indicates the traffic volume has exceeded a specified threshold on a		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
	link. Specify the threshold as an absolute number in kilobytes per second or in terms of percentage of link capacity.		
TrafficLinkCoSUtilization	Indicates the traffic volume has exceeded a specified threshold for a CoS queue on a link. Specify the threshold as an absolute number in kilobytes per second or in terms of a percentage of link capacity.		
TrafficLowLinkUtilization	Indicates the traffic volume has fallen below a specified threshold on a link. Specify the threshold as an absolute number in kilobytes per second or in terms of percentage of link capacity.		
TrafficQuantityAlert	A generic trap for all non-link related traffic alerts. Specify the threshold as an absolute number in kilobytes per second or in terms of percentage of link capacity.		

To see or modify these SNMP trap incident configurations:

1. Navigate to the Incident Configuration view.
 - a. In the Workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Incident Configuration** view.
2. Select the **SNMP Trap Configuration** tab.
3. Select the configuration you want to see or modify.
4. Click the  Open icon to see or change the configuration.
5. When you are finished, click  **Save and Close**.

Remote NNM 6.x/7.x Event Configurations Provided by NNMi

NNMi provides the remote NNM 6.x or 7.x incident configurations described in the following table.

Note: If you make changes to an incident configuration provided by NNMi, remember to place your name in the Author attribute. See "[Specify an Author for Your Incident Configuration](#)" (on page 260) for more information.

Remote NNMi Out-of-the-Box Incident Configurations



Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
OvStationNormal	Generated when a collection station status is changed to normal/up.		
OvStationCritical	Generated when a remote collection status is changed to down/critical.		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
OvNodeWarning	Generated when NNMi detects the status of a node has become up (some or all interfaces on the node are up).		
OvNodeMajor	Generated when NNMi detects the status of a node has become up (some or all interfaces on the node are up).		
OvNodeMarginal	Generated when NNMi detects the status of a node has become up (some or all interfaces on the node are up).		
OvNodeUp	Generated when NNMi detects the status of a node has become up (some or all interfaces on the node are up).		
OvNodeDown	Generated when NNMi detects the status of a node has become down (all interfaces on the node are down).		
OvIfUp	Generated when NNMi detects the status of an interface has come up, normally by responding to an ICMP Echo (ping) request.		
OvIfDown	Generated when NNMi detects the status of an interface has come up, normally by responding to an ICMP (ping) request.		
OvMessage	Generated by a user to display an event message in the event browser.		
OvIfIntermittent	Generated when NNMi detects the status of an interface has gone down and up multiple times.		
OvApaAddressUp	Generated by the NNMi Causal Engine when it detects that the address is responding to polls.		
OvApaIfUp	Generated by the NNMi Causal Engine when it detects that the interface is responding to polls.		
OvApaNodeUp	Indicates a node's status went from Down to Up.		
OvApaConnUp	Indicates a connection's status went from Down to Up.		
OvApaAggPortUp	Indicates the OperStatus for the logical aggregate port connection is Up.		
OvApaAggPortDown	Indicates the OperStatus for the logical		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
	aggregate port connection is Down.		
OvApaAggPortDegraded	Indicates the OperStatus for one of the physical port connections in the aggregate connection is Down.		
OvApaAggPortConnUp	Indicates that an aggregate port connection between two nodes is responding to polls and no interfaces are down on either side of the connection.		
OvApaAggPortConnDown	Indicates an aggregate port connection between two nodes is not responding to polls and all interfaces may be down on both sides of the connection.		
OvApaAddressDown	Indicates a node's address status went from Up to Down.		
OvApaIfDown	Indicates a node's interface status went from Up to Down.		
OvApaNodeDown	Indicates a node's status went from Up to Down.		
OvApaConnDown	Indicates a connection's status went from Up to Down.		
OvApaIfIntermittent	Indicates an interface's status has gone Down and Up multiple times.		
OvApaAddressIntermittent	Indicates a node's address status has gone Down and Up multiple times.		
OvApaConnIntermittent	Indicates a network's connection status has gone Down and Up multiple times.		
OvApaNodeIntermittent	Indicates a node's status has gone Down and Up multiple times.		
OvApaNodeSNMPNotResponding	Indicates an SNMP agent is not responding to queries.		
OvApaAggPortNotDegraded	Indicates all of the physical port connections in the aggregate connection are Up.		
OvApaIfRemoved	Indicates an interface has been removed.		
OvApaBoardUp	Indicates a node's board status has gone from Down to Up.		
OvApaBoardDown	Indicates a node's board status has gone from Up to Down.		

Incident Configuration Name	Description	Deduplication Configuration	Rate Configuration
OvApaBoardRemoved	Indicates a node's board has been removed.		

To see or modify these Remote NNM 6.x and 7.x trap incident configurations:

1. Navigate to the **Incident Configuration** view.
 - a. In the Workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Incident Configuration** view.
2. Select the **Remote NNM 6.x and 7.x Event Configuration** tab.
3. Select the configuration you want to see or modify.
4. Click the  Open icon to see or change the configuration.
5. When you are finished, click  **Save and Close**.

Management Event Configurations Provided by NNMi

Note: If you make changes to an incident configuration provided by NNMi, remember to place your name in the Author attribute. See ["Specify an Author for Your Incident Configuration" \(on page 260\)](#) for more information.

Deduplication is not configured for out-of-the-box management events. See ["Correlate Duplicate Incidents \(Deduplication Configuration\)" \(on page 269\)](#) for information about how to configure deduplication.

Note: The Interface Disabled incident configuration is Disabled by default. See ["Generate Interface Disabled Incidents" \(on page 298\)](#) for more information.

NNMi provides the incident configurations for management events. Click here for more information

Management Event Configurations Provided by NNMi

Incident Configuration Name	Description	Rate Configuration
AddressNotResponding	Indicate an address is not responding to ICMP. Reasons an address might not respond include: <ul style="list-style-type: none"> • Its node is down • A device, such as a router, has been mis-configured so that some addresses cannot be reached 	5 events in 5 minutes
AggregatorDegraded	Indicates one or more (but not all) physical interfaces that are part of the Aggregator Interface are not operational.	
AggregatorDown	Indicates the operational status of the Aggregator Interface is down (if monitored), or all of	

Incident Configuration Name	Description	Rate Configuration
	the corresponding physical interfaces are Down.	
AggregatorLinkDegraded	Indicates any Aggregator Interface is operationally down on either node, when there is a connection between two Aggregator Interfaces.	
AggregatorLinkDown	Indicates the Aggregator Interface on either side of an Aggregator Link connection is down.	
BufferOutOfRangeOrMalfunctioning	Indicates the buffer pool is exhausted or cannot meet demand.	
ConnectionDown	Indicate that both (or all) ends of a connection are not responding to SNMP queries.	5 events in 5 minutes
ConnectionPartiallyUnresponsive	Indicates that a connection is partially unresponsive. Reasons for this include that an undiscovered device in the connection is down.	
CpuOutOfRangeOrMalfunctioning	Indicates any of 5 second, 1 minute, or 5 minute utilization averages is too high.	
CustomPollCritical	Indicates that a Polling Instance associated with the Custom Poller Collection is in a Critical State.	
CustomPollMajor	Indicates that a Polling Instance associated with the Custom Poller Collection is in a Major State.	
CustomPollMinor	Indicates that a Polling Instance associated with the Custom Poller Collection is in a Minor State.	
CustomPollWarning	Indicates that a Polling Instance associated with the Custom Poller Collection is in a Warning State.	
DuplicateCorrelation	Provided as a template for configuring deduplication for an incident to specify which attribute values NNMi must match to verify that an incident is a duplicate.	
FanOutOfRangeOrMalfunctioning	Indicates the specified fan is not operating correctly.	
ImportantNodeorConnectionDown	Indicates a node is not responding to an ICMP or SNMP query. It also indicates that only one neighbor is down so that the NNMi Causal Engine cannot determine whether the node or the connection is down.	

Incident Configuration Name	Description	Rate Configuration
ImportantNodeUnmanageable	Indicates a nodes is not responding to an SNMP query.	
InterfaceDisabled	Indicates the interface has been explicitly disabled by the device administrator.	5 events in 5 minutes
InterfaceDown	Indicates that the interface is not responding to polls.	5 events in 5 minutes
IslandGroupDown	<p>Indicates all nodes in a group of Layer 2 connected nodes do not respond to monitoring polls (for example, ICMP or SNMP).</p> <p>These groups are automatically discovered and contain all of the nodes that can be connected through NNMi topology. Typically, these are groups on one side of a WAN (wide area network) connection.</p>	
LicenseExpired	Indicates the NNMi license has reached its expiration date and the license capacity is below the current level required to manage the discovered nodes.	
LicenseMismatch	<p>Indicates the Network Node Manager license capacity does not match the license capacity of one of the following additional software licenses in your network environment:</p> <ul style="list-style-type: none"> • An Integration Enablement • An NNM iSPI 	
LicenseNodeCountExceeded	Indicates the number of discovered nodes exceeds the licensed managed node count.	
MemoryOutOfRangeOrMalfunctioning	Indicates the Source Node's memory pool is exhausted or cannot meet the demand for use.	
ModifiedConnectionDown	Indicates a connection has been disconnected, moved, or both and is not responding to SNMP queries.	
NnmClusterFailover	Indicates the NNMi cluster detected a failure of the active server. NNMi services were started on the standby server.	
NnmClusterLostStandby	Indicates the NNMi cluster active server lost its communication to the standby server.	

Incident Configuration Name	Description	Rate Configuration
NnmClusterStartUp	Indicates the NNMi cluster was started in a state where no active server was already present. Therefore the server was started in the active state.	
NnmClusterTransfer	Indicates the system administrator moved the active state from one server to another. The NNMi services will then start on the new active server.	
NodeDown	<p>Indicates that the NNMi Causal Engine has determined the node is down based on the following analysis:</p> <p>100% of the addresses assigned to this node are unreachable</p> <p>The SNMP agent installed on this machine is not responding</p> <p>NNMi is communicating with at least two of the neighboring devices. And at least two neighboring devices report problems with connectivity to this node.</p>	5 events in 5 minutes
NodeOrConnectionDown	Indicate a node is not responding to an ICMP or SNMP query. It also indicates that only one neighbor is down so that the NNMi Causal Engine cannot determine whether the node or the connection is down.	
Node Up	<p>Note: When configuring Incident Actions or Diagnostic Selections, use the Node Down incident configuration and the Closed Lifecycle State. See "Configure an Action for an Incident" (on page 283) and "Configure Diagnostics for an Incident (NNM iSPI NET)" (on page 291) for more information.</p> <p>Indicates the node is up based on the following analysis:</p> <ul style="list-style-type: none"> • All of the addresses assigned to this node are reachable. • The SNMP agent installed on this node is responding. • At least two of the neighboring devices can be reached and are not reporting problems with connectivity to this node. 	
NonSNMPNodeUnresponsive	Indicates that a Non-SNMP node is unresponsive. Reasons for this include: 1) The	

Incident Configuration Name	Description	Rate Configuration
	node is down, or 2) An undiscovered device between the node and the management station is down.	
PowerSupplyOutOfRangeOrMalfunctioning	Indicates a power supply for the Source Node is not operating correctly.	
RateCorrelation	Provided as a template to measure the number of incoming incidents within a defined time period.	
RrgDegraded	<p>Note: This incident occurs only in Router Redundancy Groups using the HSRP protocol and larger than two members.</p> <p>Indicates the following:</p> <ul style="list-style-type: none"> • The Router Redundancy Group has a primary and secondary device. • The remaining devices in the group are not in an expected protocol-specific state. For example, in HSRP other devices may be expected to be in the "Listen" state. <p>Typically, the protocol-specific communication between routers is malfunctioning. However, the group is routing packets properly.</p>	
RrgFailover	<p>Indicates a primary role (for example, HSRP Active or VRRP Master) moved from one device to another in a Router Redundancy Group.</p> <p>Reasons for this incident include one or more of the following:</p> <ul style="list-style-type: none"> • A router or interface in the Router Redundancy Group has gone down. • A tracked object (interface or IP address) in the Router Redundancy Group has gone down. <p>The group is routing packets properly.</p>	
RrgMultiplePrimary	<p>Indicates that multiple primary devices (for example, HSRP Active or VRRP Master) are identified in a Router Redundancy Group.</p> <p>Typically, the protocol-specific communication between routers in the group is malfunctioning.</p>	

Incident Configuration Name	Description	Rate Configuration
RrgMultipleSecondary	<p>Indicates that more than one secondary device (HSRP Standby) is identified in a Router Redundancy Group. Note: This incident applies only to Router Redundancy Groups using the HSRP protocol. VRRP allows more than one secondary role (VRRP Standby State) . Typically, the protocol-specific communication between routers in the group is malfunctioning.</p>	
RrgNoPrimary	<p>Indicates that no primary device (for example, HSRP Active or VRRP Master) is identified in a Router Redundancy group.</p> <p>This incident typically indicates one of the following:</p> <ul style="list-style-type: none"> • Too many routers are down. • Protocol-specific communication between routers in the group is malfunctioning. 	
RrgNoSecondary	<p>Indicates that no secondary device (for example, HSRP Standby or VRRP Backup) is identified in a Router Redundancy Group.</p> <p>This incident typically indicates the following:</p> <ul style="list-style-type: none"> • Protocol-specific communication between routers in the group is malfunctioning. • The group is routing packets properly because a single primary device has been identified. 	
RrgSecondaryChanged	<p>Indicates that a secondary role (for example, HSRP Standby or VRRP Backup) moved from one device to another in a Router Redundancy Group.</p> <p>This incident typically indicates the following:</p> <ul style="list-style-type: none"> • An router or interface in the Router Redundancy Group has gone down. • A tracked object (interface or address) has gone down. • The group is routing packets properly. 	
SNMPTrapLimitCritical	<p>Indicates the number of SNMP traps persisted in the NNMi database is approaching the maximum allowed limit. After the maximum allowed limit is reached, NNM no</p>	

Incident Configuration Name	Description	Rate Configuration
	longer accepts SNMP traps until the number of SNMP traps within the database is reduced using the nnmtrimincidents.ovpl command.	
SNMPTrapLimitMajor	Indicates the number of SNMP traps persisted in the NNMi database has reached or exceeded 95% of the maximum limit. After the maximum limit is reached, NNMi only accepts traps required for Causal Engine analysis until the number of SNMP traps within the database has been reduced using the nnmtrimincidents.ovpl command.	
SNMPTrapLimitWarning	Indicates the number of SNMP traps persisted in the NNMi database has reached or exceeded 90% of the maximum limit. After the maximum limit is reached, NNMi no longer accepts SNMP traps until the number of SNMP traps within the database is reduced using the nnmtrimincidents.ovpl command.	
TemperatureOutOfRangeOrMalfunctioning	Indicates the specified temperature sensor on the Source Node is too hot or too cold.	
TrapStorm	Indicates a trap storm has occurred.	
VoltageOutOfRangeOrMalfunctioning	Indicates the specified voltage on one of the Source Node's power supplies is out of range.	

NNM iSPI for Performance. For network performance monitoring, NNM iSPI for Performance provides additional management event configurations. Click here for more information.



Each of these configurations has a Category value of **Performance**, a Family value of **Interface**, and a Nature of **Root Cause**.

***NNM iSPI for Performance.* Additional Management Event Configurations**

Incident Configuration Name	Description	Rate Configuration
InterfaceInputDiscardRateHigh	Indicates a high input discard rate on the interface. This percentage is based on the reported change in the number of input packets on the interface and the discarded packet count.	
InterfaceInputErrorRateHigh	Indicates a high input error rate on the interface. This percentage is based on the reported change in the number of input packets on the interface and the packet error count.	
InterfaceInputUtilizationHigh	Indicates a high input utilization on the interface. This	

Incident Configuration Name	Description	Rate Configuration
	percentage is based on the interface speed and the reported change in the number of input bytes on the interface.	
InterfaceInputUtilizationLow	Indicates a low input utilization on the interface. This percentage is based on the interface speed and the reported change in the number of input bytes on the interface.	
InterfaceInputUtilizationNone	Indicates there is no input utilization on the interface. This value is based on the interface speed and the reported change in the number of input bytes on the interface.	
InterfaceOutputDiscardRateHigh	Indicates a high output discard rate on the interface. This percentage is based on the reported change in the number of input packets on the interface and the discarded packet count.	
InterfaceOutputErrorRateHigh	Indicates a high output error rate on the interface. This percentage is based on the reported change in the number of output packets on the interface and the packet error count.	
InterfaceOutputUtilizationHigh	Indicates a high output utilization on the interface. This percentage is based on the interface speed and the reported change in the number of output bytes on the interface.	
InterfaceOutputUtilizationLow	Indicates a low output utilization on the interface. This percentage is based on the interface speed and the reported change in the number of output bytes on the interface.	
InterfaceOutputUtilizationNone	Indicates there is no output utilization on the interface. This value is based on the interface speed and the reported change in the number of output bytes on the interface.	

To see or modify these management event incident configurations:

1. Navigate to the **Incident Configuration** view.
 - a. In the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Incident Configuration** view.
2. Select the **Management Event Configuration** tab.
3. Select the configuration you want to see or modify.
4. Click the  Open to see or change the configuration.
5. When you are finished, click  **Save and Close**.

Incident Pair (Pairwise) Configurations Provided by NNM


NNM provides the pairwise configurations described in the following table.



Pairwise Configurations Provided by NNM

Name	Description
CiscoLinkDownUpPair	Cancels a CiscoLinkDown incident with a CiscoLinkUp incident on the same interface for the same SNMP agent address. This configuration is used for known Cisco devices.
NodeDownUpPair	Cancels a NodeDown incident with a NodeUp incident from the same node.
OvApaAddressDownUpPair	Cancels an NNM 6.x or 7.x Node Down event with a NNM 6.x or 7.x Node Up event from the same SNMP agent address.
OvApaAggPortConnDownUpPair	Cancels an NNM 6.x or 7.x APA Aggregate Port Connection Down event with an NNM 6.x or 7.x APA Aggregate Port Connection Up event.
OvApaAggPortDegradeNotDegradePair	Cancels an NNM 6.x or 7.x APA Aggregate Port Degraded event with an NNM 6.x or 7.x APA Aggregate Port Not Degraded event on the same interface for the same SNMP agent address.
OvApaAggPortDownUpPair	Cancels of an NNM 6.x or 7.x APA Aggregate Port Down event with an NNM 6.x or 7.x APA Aggregate Port Up event on the same interface for the same SNMP agent address.
OvApaBoardDownUpPair	Cancels an NNM 6.x or 7.x APA Board Down event with an NNM 6.x or 7.x APA Board Up event from the same SNMP agent address.
OvApaConnDownUpPair	Cancels an NNM 6.x or 7. x APA Address Down event with an NNM 6.x or 7.x APA Address Up event on the same address for the same SNMP agent address.
OvApalfDownUpPair	Cancels an NNM 6.x or 7.x APA If Down event with an NNM 6.x or 7.x APA If Up event on the same interface for the same SNMP agent address.
OvApaNodeDownUpPair	Cancels an NNM 6.x or 7.x APA Node Down event with an NNM 6.x or 7.x APA Node Up event from the same SNMP agent address.
OvIfDownUpPair	Cancels an NNM 6.x or 7.x If Down event with an NNM 6.x or 7.x If Up event on the same interface for the same SNMP agent address.
OvNodeDownUpPair	Cancels an NNM 6.x or 7.x Node Down event with an NNM 6.x or 7.x Node Up event from the same SNMP agent address.
RcAggLinkDownUpPair	Cancels an RcAggLinkDown incident with an RcAggLinkUp incident from the same Multi-Link Trunk (MLT) Aggregator ID (from the MIB) and SNMP agent address.

Name	Description
RcChasFanDownUpPair	Cancels an RcChasFanDown incident with an RcChasFanUp incident from the same fan ID (from the MIB) and SNMP agent address.
RcChasPowerSupplyDownUpPair	Cancels an RcChasPowerSupplyDown incident with an RcChasPowerSupplyUp incident from the same power supply ID (from the MIB) and SNMP agent address.
RcSmltIsLinkDownUpPair	Cancels an RcSmltIsLinkDown incident with an RcSmltIsLinkUp incident from the same SNMP agent address.
RcnAggLinkDownUpPair	Cancels an RcnAggLinkDown incident with an RcnAggLinkUp incident from the same Multi-Link Trunk (MLT) Aggregator Link ID (from the MIB) and SNMP agent address.
RcnChasFanDownUpPair	Cancels an RcnChasFanDown incident with an RcnChasFanUp incident from the same fan ID (from the MIB) and SNMP agent address.
RcnChasPowerSupplyDownUpPair	Cancels an RcnChasPowerSupplyDown incident with an RcnChasPowerSupplyUp incident from the same power supply ID (from the MIB) and SNMP agent address.
RcnSmltIsLinkDownUpPair	Cancels an RcnSmltIsLinkDown incident with an RcnSmltIsLinkUp incident from the same SNMP agent address.
SnmplinkDownUpPair	Cancels an SNMPLinkDown incident with an SNMPLinkUp incident on the same interface for the same SNMP agent address.

To see or modify these incident pair configurations:

1. Navigate to the **Incident Configuration** view.
 - a. In the Workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Incident Configuration** view.
2. Select the **Pairwise Configuration** tab.
3. Select the configuration you want to see or modify, and click  Open to see or change the configuration.

In the **Pairwise Configuration** form, click **Help** → **Using the Pairwise Configuration form** for more information.
4. When you are finished, click  **Save and Close** to return to the Incident Configuration form.
5. Click  **Save and Close**. NNM saves your changes.

Configure Network Devices to Send SNMP Notifications to NNMi

An SNMP notification is a message sent from an SNMP agent on a network device to notify a network management system of an event on the network device. For example, an error occurred on the network device and its SNMP agent sent a notification. The notification may either be an acknowledged inform (SNMPv2c InformRequest) or an unacknowledged trap (SNMPv1 TrapResponse or SNMPv2cTrap).

An inform is an acknowledged notification sent from one SNMP agent to another with the expectation of a reply from the recipient. If no reply is received, the inform message is resent. A trap is a notification sent from one SNMP agent to another without any expectation of a reply.

Configure SNMP agents in your network environment to send traps to the NNMi management server. Sometimes SNMP agents are configured with a recheck interval, so the trap might be sent to the NNMi management server over and over again until the problem is corrected.

The NNMi Causal Engine analyzes these traps and gathers additional information to determine the root cause. It also provides useful troubleshooting information each time an important SNMP notification is received, including the following information:

- The name or address of the node from which the notification came (Source Node)
- The notification identification (SNMP Object ID)
- Notification-specific variables (varbinds)

When configuring the SNMP agent on each network device, configure the agent's trap-forwarding list (or trap-destination list) to include the NNMi management server's fully-qualified hostname or IP address. Refer to the agent's documentation for information about how to do this. If the NNMi management server is included on the trap-forwarding list, NNMi receives notice from the agent when something goes wrong (even if the device does not show up on your NNMi maps).

Note: For an SNMP notification to be processed by NNMi, it must be configured using the NNMi incident Configuration workspace. Many common SNMP notifications are configured in NNMi by default. See ["Configure SNMP Trap Incidents" \(on page 246\)](#) and ["SNMP Trap Incident Configurations Provided by NNMi" \(on page 216\)](#) for more information.

Configure SNMP Trap Forwarding

NNMi enables you to configure SNMP trap forwarding using the Incident Configuration workspace. This feature is useful when you want to forward traps to a specified destination. For example, you might want to forward certain kinds of traps to one server and forward another set of traps to a different server so they can be managed separately.

When configuring SNMP trap forwarding you perform the following tasks:

- ["Configure NNMi Security Settings for SNMPv3 Trap Forwarding" \(on page 239\)](#)
- ["Configure Trap Forwarding Filters" \(on page 241\)](#)
- ["Configure Trap Forwarding Destinations" \(on page 243\)](#)

Configure NNMi Security Settings for SNMPv3 Trap Forwarding

Note: If your network environment uses SNMPv2c or SNMPv1 and does not use SNMPv3, skip this task.


If your network environment uses SNMPv3, specify which user-based security model (USM) settings the NNMi management server uses when NNMi acts as an authoritative entity in the following situations:

- Forwarding SNMPv3 traps to other devices in your network environment
- Sending responses to SNMPv3 Inform-Requests

The settings in this form grant permission for NNMi to use the specified SNMPv3 engine.

Note: When receiving SNMPv3 data, NNMi must decrypt the data received based on your settings in the Communication Configuration workspace. See ["Configure Default SNMPv3 Settings" \(on page 54\)](#).

To configure the NNMi management station as an authoritative entity for SNMPv3:

1. Navigate to the **Incident Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Navigate to the **NNMi SNMPv3 Trap Forwarding Security Settings** group.
3. NNMi displays the ID of the SNMPv3 engine assigned to NNMi. See the attribute value for [NNMi SNMPv3 Engine Id](#).
4. Provide the USM information that NNMi uses for authentication and privacy when using SNMPv3 protocol for sending traps or responses to Inform-Requests to other devices in your network environment (see [table](#)).
5. Click  **Save and Close** to save your changes.

SNMPv3 Engine Assigned to NNMi management server

Attribute	Description
NNM SNMPv3 Engine Id	Remote devices must use this SNMPv3 engine ID when sending traps to NNMi.

SNMPv3 Settings of the NNMi management server's User-Based Security Model (USM)






Attribute	Description
User Name	The SNMPv3 user name text string used by the NNMi management server.
Authentication Protocol	The SNMPv3 authentication protocol. Determines whether authentication is required and indicates the type of authentication protocol used. NNMi supports the following protocols: <ul style="list-style-type: none"> • HMAC-MD5-96 authentication protocol • HMAC-SHA-1 authentication protocol
Authentication Passphrase	The SNMPv3 USM authentication passphrase used by the NNMi management server. If required for authentication, provide the appropriate authentication passphrase for the authentication protocol. The length limitations of the authentication passphrase depend on the authentication protocol.
Privacy Protocol	Specify the SNMPv3 USM privacy protocol used by the NNMi management server. This determines whether encryption is required and indicates the type of privacy protocol used. NNMi supports the DES-CBC Symmetric Encryption Protocol.
Privacy Passphrase	Specify the SNMPv3 USM privacy passphrase used by the NNMi management server. If required for privacy, provide the appropriate encryption passphrase for use with the privacy protocol. The length limitations of the privacy passphrase depend on the privacy protocol.

Configure Trap Forwarding Filters

Pre-requisite: Make sure you have used the NNMi [nnmincidentcfg.ovpl](#) command line utility to automatically create or update the incident configurations for the SNMP traps you want to include. See ["Load SNMP Trap Definitions" \(on page 247\)](#) for more information.

Use the Incident Configuration: Trap Forwarding Filters tab to configure a filter expression to specify the SNMP trap Object Identifier (OID) pattern you want to use to determine which SNMP traps NNMi forwards. The traps which pass the filter you specify can then be forwarded to a specified destination using the Trap Forwarding Destinations tab. See ["Configure Trap Forwarding Destinations" \(on page 243\)](#) for more information.

To configure SNMP Trap Forwarding Filters:

1. Navigate to the **Incident Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Select the **Trap Forwarding Filters** tab.
3. Do one of the following:
 - To create an SNMP Trap Forwarding Filter configuration, click the  New icon, and continue.
 - To edit an SNMP Trap Forwarding Filter configuration, click the  Open icon, and continue.
 - To delete an SNMP Trap Forwarding Filters configuration, click the  Delete icon.
4. In the [SNMP Trap Configuration form](#), provide the required information.
5. Click  **Save and Close** to return to the **Incident Configuration** form.
6. Click  **Save and Close** to save your changes.

The next time that a trap of this type arrives, NNMi uses the filter you specify to determine whether to forward the trap to a specified destination.






Trap Forwarding Filters Form

Pre-requisite: Make sure you have used the NNMi [nnmincidentcfg.ovpl](#) command line utility to automatically create or update the incident configurations for the SNMP traps you want to include. See ["Load SNMP Trap Definitions" \(on page 247\)](#) for more information.

The Trap Forwarding Filters Form enables you to specify the SNMP trap Object Identifier (OID) pattern you want to use to determine which SNMP traps NNMi forwards. The traps which pass the filter you specify can then be forwarded to a specified destination using the Trap Forwarding Destinations tab. See ["Configure Trap Forwarding Destinations" \(on page 243\)](#) for more information.

To configure SNMP Trap Forwarding Filters:

1. Navigate to the **Incident Configuration** form:
 - a. From the workspace navigation pane, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Select the **SNMP Trap Forwarding Filters** tab.

3. Make your configuration choices (see [table](#)).
 - To add an SNMP Trap Forwarding Filter configuration, click the  New icon, and continue.
 - To edit an SNMP Trap Forwarding Filter configuration, click the  Open icon, and continue.
 - To delete an SNMP Trap Forwarding Filter configuration, click the  Delete icon.
4. Click  **Save and Close** to return to the **Incident Configuration** form.
5. Click  **Save and Close** to save your changes.

SNMP Trap Forwarding Filters Configuration



Attribute	Description
Name	Enter the name you want to use for this SNMP Trap Forwarding Filter configuration. Alpha-numeric and special characters (~ ! @ # \$ % ^ & * () _ +) are allowed. No spaces are allowed.
"Trap Forwarding Filter Expression Form" (on page 242)	Access the Trap Forwarding Filter Expression form to specify the valid SNMP Object Identifier (OID) pattern to be used for the SNMP trap filter.





Trap Forwarding Filter Expression Form

Pre-requisite: Make sure you have used the NNMi [nmmincidentcfg.ovpl](#) command line utility to automatically create or update the incident configurations for the SNMP traps you want to include. See ["Load SNMP Trap Definitions" \(on page 247\)](#) for more information.

The Trap Forwarding Filter Expression Form enables you to specify the SNMP trap Object Identifier (OID) pattern you want to use to filter incoming SNMP traps. The traps which pass the filter you specify can then be forwarded to a specified destination using the Trap Forwarding Destinations tab. See ["Configure Trap Forwarding Destinations" \(on page 243\)](#) for more information.

To configure an SNMP Trap Forwarding Filter Expression:

1. Navigate to the Trap Forwarding **Filter Expressions** form:
 - a. From the workspace navigation pane, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Select the SNMP Trap **Forwarding Filters** tab.
 - d. Do one of the following:
 - To create a new configuration, click the  New icon.
 - To edit an existing configuration, select a row, and click the  Open icon.
 - e. On the form that opens, navigate to the **Filter Expressions** tab.
 - f. Locate the **Filter Expressions List** table.
 - g. Do one of the following:

- To add a Trap Forwarding **Filter Expression**, click the  New icon.
 - To edit an existing Trap Forwarding **Filter Expression**, select a row, and click the  Open icon.
2. Make your configuration choices (see [table](#)).
 3. Click  **Save and Close** to return to the **Incident Configuration** form.
 4. Click  **Save and Close** to save your changes.

SNMP Trap Forwarding Filter Expression Configuration





Attribute	Description
Object identifier (OID) Pattern	<p>Enter the SNMP Object Identifier (OID) pattern you want to use for the SNMP trap filter. Valid values include:</p> <ul style="list-style-type: none"> • The entire SNMP trap OID value. For example: <code>.1.3.6.1.6.5.66.7.1225</code> • The SNMP trap OID value that includes a wildcard as a placeholder for the missing values. For example, to specify only the SNMP trap OID matching prefix: <code>.1.3.6.1.6.5.66.7.*</code> • The SNMP trap OID valid range. For example: <code>.1.3.6.1.6.5.66.7.1225 - 1235</code>

Configure Trap Forwarding Destinations

Pre-requisite: Make sure you have used the NNMi [nnmincidentcfg.ovpl](#) command line utility to automatically create or update the incident configurations for the SNMP traps you want to include. See ["Load SNMP Trap Definitions" \(on page 247\)](#) for more information. You must also create the Trap Forwarding Filters for the SNMP traps you want to forward. See ["Configure Trap Forwarding Filters" \(on page 241\)](#) for more information.

The Trap Forwarding Destinations tab enables you to specify the servers to which you want to forward SNMP traps. Use this tab to also specify the Trap Forwarding Filters to be used for this destination.

To configure SNMP Trap Forwarding Destinations:

1. Navigate to the **Incident Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Select the **SNMP Trap Forwarding Destinations** tab.
3. Do one of the following:
 - To create an SNMP Trap Forwarding Destination configuration, click the  New icon, and continue.
 - To edit an SNMP Trap Forwarding Destination configuration, click the  Open icon, and continue.
 - To delete an SNMP Trap Forwarding Destination configuration, click the  Delete icon.
2. In the ["Trap Forwarding Filter Association Form" \(on page 245\)](#), provide the required information.
3. Click  **Save and Close** to return to the **Incident Configuration** form.

4. Click  **Save and Close** to save your changes.






The next time a trap that passes the Trap Forwarding Filter arrives, NNMi forwards the trap to the specified Trap Forwarding Destination.

Trap Forwarding Destination Form

Pre-requisite: Make sure you have used the NNMi [nnmincidentcfg.ovpl](#) command line utility to automatically create or update the incident configurations for the SNMP traps you want to include. See ["Load SNMP Trap Definitions" \(on page 247\)](#) for more information. You must also create the Trap Forwarding Filters for the SNMP traps you want NNMi to forward. See ["Configure Trap Forwarding Filters" \(on page 241\)](#) for more information.

The Trap Forwarding Destinations form enables you to specify the servers to which you want NNMi to forward SNMP traps.

To configure an SNMP Trap Forwarding Destination:

1. Navigate to the **Incident Configuration** form:
 - a. From the workspace navigation pane, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Select the **SNMP Trap Forwarding Destinations** tab.
3. Make your configuration choices (see [table](#)).
 - To add an SNMP Trap Forwarding Destination configuration, click the  New icon, and continue.
 - To edit an SNMP Trap Forwarding Destination configuration, click the  Open icon, and continue.
 - To delete an SNMP Trap Forwarding Destination configuration, click the  Delete icon.
4. Click  **Save and Close** to return to the **Incident Configuration** form.
5. Click  **Save and Close** to save your changes.

SNMP Trap Forwarding Destination Configuration

Attribute	Description
Name	Enter the name you want to use for this SNMP Trap Forwarding Destination configuration. Alpha-numeric and special characters (~ ! @ # \$ % ^ & * () _ +) are allowed. No spaces are allowed.
IP Address	Enter the IP address for the destination server.
Port	Enter the UDP port number for the destination server.
Forwarding Options	<ul style="list-style-type: none">• Default - NNMi processes the trap prior to forwarding. Click here for more information. NNMi adds two new varbinds to the trap for storing origin address information:<ul style="list-style-type: none">▪ Origin IP Address




Attribute	Description
	<ul style="list-style-type: none"> ■ Origin IP Address type <p>See "SNMP Trap Varbinds Provided by NNMi" (on page 246) for more information.</p> <ul style="list-style-type: none"> ● SNMPv3 to SNMPv2 Conversion - NNMi converts an incoming SNMPv3 trap to SNMPv2. Click here for more information. <p>When converting SNMPv3 traps to SNMPv2c traps, NNMi does the following:</p> <ul style="list-style-type: none"> ■ Includes a Context Name varbind - Contains the <code>contextName</code> from the original SNMPv3 trap. ■ Creates a Community Name - The Context Engine ID and User Name of the original SNMPv3 trap are combined as follows: <code>username@contextEngineID</code>. For example, <code>ciscoAdmin@8000000b7f3cbec5632b47455e97070c</code> <ul style="list-style-type: none"> ● Original Trap (UNIX only) - NNMi forwards the trap without any changes.
Specify the Trap Forwarding Filters to Use	<p>Use the Trap Forwarding Filters form to specify the Trap Forwarding Filters configurations to use. These filters determine which traps NNMi forwards to the destination you specify.</p>



Trap Forwarding Filter Association Form

Pre-requisite: Make sure you have used the NNMi [nnmincidentcfg.ovpl](#) command line utility to automatically create or update the incident configurations for the SNMP traps you want to include. See ["Load SNMP Trap Definitions" \(on page 247\)](#) for more information. You must also create the Trap Forwarding Filters for the SNMP traps you want to forward. See ["Configure Trap Forwarding Filters" \(on page 241\)](#) for more information.


The Trap Forwarding Filter Association Form enables you to specify the Trap Forwarding Filters that you want to apply for the SNMP traps NNMi forwards to the specified Trap Forwarding Destination.

To configure the SNMP Trap Forwarding Filters:

1. Navigate to the **Trap Forwarding Filter Association** form:
 - a. From the workspace navigation pane, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Select the **SNMP Trap Forwarding Destination** tab.
 - d. Do one of the following:
 - To create a new configuration, click the  New icon.
 - To edit an existing configuration, select a row, and click the  Open icon.
 - e. On the form that opens, navigate to the **Trap Forwarding Filter Association** tab.
 - f. Locate the **Trap Forwarding Filter List** table.
 - g. To select a **Trap Forwarding Filter**, click the  New icon.
2. Make your configuration choices (see [table](#)).

3. Click  **Save and Close** to return to the **Incident Configuration** form.
4. Click  **Save and Close** to save your changes.

SNMP Trap Forwarding Filter

Attribute	Description
Trap Forwarding Filter	Click the  Lookup icon, and select Open from the drop-down menu to view and select the Trap Forwarding Filter you want to use for the current Trap Forwarding Destination.

SNMP Trap Varbinds Provided by NNMi

NNMi provides the following varbinds for use when forwarding SNMP traps.

Note: NNMi does not create these varbinds if the Forwarding Options attribute is set to *Original Trap (UNIX only)* when configuring trap forwarding destinations. See "[Trap Forwarding Destination Form](#)" (on [page 244](#)) for more information.




SNMP Trap Varbinds Provided by NNMi



Name	oid	Type	Description
Origin IP address	.1.3.6.1.4.1.11.2.17.2.19.1.1.3	InetAddress	Contains the IP address of the original SNMP notification that generated the trap.
Origin IP Address type	.1.3.6.1.4.1.11.2.17.2.19.1.1.2	InetAddressType	Contains the type of the IP address of the Original IP Address varbind. The value "1" indicates IPv4.
Context Name	.1.3.6.1.4.1.11.2.17.2.19.1.1.1	SnmpAdminString	Contains the contextName present in the original SNMPv3 notification. This varbind is present only when NNMi converts an SNMPv3 notification to an SNMPv2c trap. See " Trap Forwarding Destination Form " (on page 244) for more information.

Configure SNMP Trap Incidents

Configure incidents that originate from an SNMP trap.

To configure incidents originating from SNMP traps:

1. Navigate to the **Incident Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Select the **SNMP Trap Configuration (by OID)** or **SNMP Trap Configuration (by Name)** tab.
3. Do one of the following:
 - To create an SNMP trap configuration, click the  New icon, and continue.
 - To edit an SNMP trap configuration, click the  Open icon, and continue.
 - To delete an SNMP trap configuration, click the  Delete icon.

1. In the [SNMP Trap Configuration form](#), provide the required information.
2. Click  **Save and Close** to return to the **Incident Configuration** form.
3. Click  **Save and Close** to save your changes.

The next time that a trap of this type arrives, NNMi creates an associated incident to display in the appropriate incident views.

Load SNMP Trap Definitions

The NNMi `nnmincidentcfg.ovpl -load` script provides a way for you to automatically create or update an incident configuration for an SNMP trap using a MIB file. To load a MIB file, you can use the following syntax:

```
nnmincidentcfg.ovpl -loadTraps <mib_file> -disableAllTraps true|false -u <NNMi-adminUsername> -p <NNMiadminPassword> | -loadMib <mib_file>
```

Note: See [nnmincidentcfg.ovpl](#) for more information, including a complete list of the valid script arguments.

nnmincidentcfg.ovpl Arguments

Argument	Description
<code>-loadTraps <mib_file></code>	Used to load the MIB file <code><mib_file></code> that you want to use to create or update the incident configuration for an SNMP trap. NNMi uses information from the trap definitions (TRAP-TYPES macro) or notification (NOTIFICATION-TYPES macro) in the MIB file for the required incident configuration.
<code>-disableAllTraps</code>	Specifies whether all trap definitions specified using <code>-loadTraps <mib_file></code> should be loaded as disabled. Note: The default value is <code>false</code> . This means that by default all trap definitions specified in <code><mib_file></code> are loaded as enabled. Set this parameter to <code>true</code> to disable the trap definitions that you are loading.
<code>-u</code>	The NNMi user name. This user must be assigned to at least an NNMi administrator role. Note: The user name might be a Principal object stored in the NNMi database or might be from your environment's directory service database (depending on NNMi configuration). See "Configure Sign-In Access" (on page 32) for more information.
<code>-p</code>	The password associated with the NNMi account. Note: The password might be an attribute in an Account object stored in the NNMi database or might be from your environment's directory service database (depending on NNMi configuration). See "Configure Sign-In Access" (on page 32) for more information.
<code>-loadMIB <mib_file></code>	Used to load a MIB file for the cases in which the <code><mib_file></code> specified with <code>-loadTraps</code> has dependencies.

For example, to load the MIB file CISCO-VTP_MIB, you might enter the following:

```
nnmincidentcfg.ovpl -loadTraps "C:\Cisco Mibs\CISCO-VTP-MIB.my"
```






If the incident is already configured, NNMi performs an update based on the MIB file information. If the incident is not configured, NNMi creates a new incident configuration entry for the SNMP trap. See "[Configure SNMP Trap Incidents](#)" (on page 246) for information about changing an SNMP trap configuration.

SNMP Trap Configuration Form

To configure incidents originating from SNMP traps:

1. Navigate to the **Incident Configuration** form:
 - a. From the workspace navigation pane, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Select the **SNMP Trap Configuration** tab.
3. Make your configuration choices (see [table](#)).

Note: If you want to add or edit an SNMP trap configuration, verify that **Enabled** is selected.

 - To add an SNMP trap configuration, click the  New icon, and continue.
 - To edit an SNMP trap configuration, click the  Open icon, and continue.
 - To delete an SNMP trap configuration, click the  Delete icon.
4. Click  **Save and Close** to return to the **Incident Configuration** form.
5. Click  **Save and Close** to save your changes.

Tasks for SNMP Trap Configuration

Task	How
"Specify the Incident Configuration Name" (on page 249)	Use the Basics pane of the SNMP Trap form. Specify a name that helps you to identify the configuration for subsequent use.
"Specify the SNMP Object ID" (on page 249)	Use the Basics pane of the SNMP Trap form. NNMi supports SNMPv2c and SNMPv1 formats.
Specify whether you want to enable this configuration.	In the Basics group of the SNMP Trap form, verify that Enabled <input checked="" type="checkbox"/> is selected for each configuration you want to use.
"Display an SNMP Trap or NNM 6.x/7.x Events as a Root Cause Incident" (on page 251)	Use the Basics pane of the SNMP Trap form.
"Specify Category and Family Attribute Values for Organizing Your Incidents" (on page 251)	Use the Basics pane of the SNMP Trap form. You can organize your incidents using Category and Family.
"Specify the Incident Severity " (on page 255)	Use the Basics pane of the SNMP Trap form. Possible Severity values include: Normal , Warning , Minor , Major , and Critical .
"Specify Your Incident Message Format" (on page 255)	Use the Basics pane of the SNMP Trap form. The message format determines the message to be displayed for the incident.

Task	How
"Specify a Description for Your Incident Configuration" (on page 260)	Use the Basics pane of the SNMP Trap form. Provide a meaningful description.
"Specify an Author for Your Incident Configuration" (on page 260)	Use the Basics pane of the SNMP Trap form.

After you complete the Basic Configuration for the SNMP trap, you can also choose to configure the information described in the following table.

Additional Configurations

Task	How
"Correlate Duplicate Incidents (Deduplication Configuration)" (on page 269)	Select the Deduplication Configuration tab to specify duplicate incidents that you want to be suppressed.
"Track Incident Frequency (Rate: Time Period and Count)" (on page 273)	Select the Rate Configuration tab to specify a rate for duplicate incidents. After the rate limit is reached, NNMi generates an Incident to notify you of the problem.
"Configure an Action for an Incident" (on page 283)	Select the Action Configuration tab to specify actions that should occur automatically when an incident is either generated or closed.
"Configure Diagnostics for an Incident (NNM iSPI NET)" (on page 291)	Select the Configuration Per Node Group tab to specify diagnostic actions that should occur automatically when an incident is generated for a node that belongs to a particular Node Group.

Specify the Incident Configuration Name

When providing the Name for an incident configuration, use the following guidelines:

Name

The name is used to identify the incident configuration and must be unique. Use a name that will help you to remember the purpose or kind of management event, remote NNM 6.x or 7.x event, or SNMP trap whose incident you are configuring. Name is also used to identify your Pairwise configurations.

Specify the SNMP Object ID

When configuring incidents whose source is an SNMP trap, you are asked to provide the SNMP Object ID values that you want to use to assist you in identifying the trap.

NNMi requires that SNMPv1 trap object identifiers be converted to SNMPv2c format. The SNMP Object IDs must be entered in a format that is recognized by NNMi. Select the type of SNMP trap you want to configure from the list below to learn about the required NNMi format.

Note: In all cases, the value you enter for an SNMP Object ID must be unique.

- ["SNMP Object ID Format for SNMPv2c Traps" \(on page 250\)](#)
- ["SNMP Object ID Format for SNMPv1 Generic Traps" \(on page 250\)](#)

- ["SNMP Object ID Format for a Specific SNMPv1 Trap" \(on page 251\)](#)

SNMPv1 generic traps are standard traps that are commonly used across vendors. The SNMPv1 enterprise specific traps are those traps that are generated by a particular vendor's device. The vendor is also known as the enterprise. Both include a vendor name as part of the set of information stored with each trap.

SNMP Object ID Format for SNMPv2c Traps

NNMi stores all SNMP trap information in SNMPv2c format.

To specify an SNMPv2c trap object ID, use the MIB definition file for the device of interest. The MIB file includes object identifiers for all of the traps that the SNMP agent generates for a particular device.

In the **SNMP Object ID** attribute of the **SNMP Trap Configuration (by OID)**, **SNMP Trap Configuration (by Name)**, or **Remote NNM 6.x/7.x Configuration** form, enter the SNMP object identifier value for the trap that you want to see in the console incident views.

SNMP Object ID Format for SNMPv1 Generic Traps

NNMi requires SNMPv1 trap object IDs to be converted to SNMPv2c format. The object IDs are converted according to the specifications in Request for Comments (RFC) document 2576: *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.

When using SNMPv1 format, you can specify either generic or vendor specific traps. SNMPv1 generic traps are standard traps that are commonly used across vendors. The SNMPv1 enterprise specific traps are those traps that are generated by a particular vendor's device. The vendor is also known as the enterprise. Both include a vendor name as part of the set of information stored with each trap.

The six SNMPv1 generic traps have the following SNMP object identifiers that are recognized by SNMPv2c:

1.3.6.1.6.3.1.1.5.1 (coldStart)

1.3.6.1.6.3.1.1.5.2 (warmStart)

1.3.6.1.6.3.1.1.5.3 (linkDown)

1.3.6.1.6.3.1.1.5.4 (linkUp)

1.3.6.1.6.3.1.1.5.5 (authenticationFailure)

1.3.6.1.6.3.1.1.5.6 (egpNeighborLoss)

To configure an SNMP object identifier (SNMP OID) for a generic SNMPv1 trap, specify the SNMP object ID as described in RFC 2576. You also need to include the object identifier for the vendor name (<VendorEnterprise>) as shown below:

<SNMPv2c generic trap OID>.<VendorEnterprise>

The <vendorEnterprise> is the object identifier for the vendor that is included with the varbind trap information.

For example, the SNMP object identifier for Cisco warmStart trap would be:

.1.3.6.1.6.3.1.1.5.2.1.3.6.1.4.1.9

Note: Cisco's Vendor enterprise object identifier in this example is .1.3.6.1.4.1.9

SNMP Object ID Format for a Specific SNMPv1 Trap

NNMi requires SNMPv1 trap object identifiers to be converted to SNMPv2c format. The object IDs are converted according to the specifications in RFC 2576: *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.

When using SNMPv1 format, you can specify either generic or vendor specific traps. SNMPv1 generic traps are standard traps that are commonly used across vendors. The SNMPv1 enterprise specific traps are those traps that are generated by a particular vendor's device. The vendor is also known as the enterprise. Both include a vendor name as part of the set of information stored with each trap.

When specifying the SNMP object ID for an SNMPv1 specific trap, include the SNMP object ID for the vendor name and for the trap that you want to see in the console incident views.

The value you enter must be in the format:

`<VendorEnterprise>.0.<SpecificTrapNumber>`

The `<VendorEnterprise>` is the object identifier for the vendor that is included in the SNMPv1 trap. The `<SpecificTrapNumber>` is the SNMPv1 specific trap identification number that is provided by the vendor.

For example, for an SNMPv1 vendor object id 1.3.6.1.3.1.12.9 and specific trap number 12234, the SNMP object ID would be:

1.3.6.1.3.1.12.9.0.12234

Display an SNMP Trap or NNM 6.x/7.x Events as a Root Cause Incident

SNMP trap and NNM 6.x/7.x events normally appear as symptoms rather than as root cause incidents. However, there might be times when you want an SNMP or NNM 6.x/7.x event to appear as a root cause incident. For example, you might want an HSRP state change (cHsrpStateChange, 1.3.6.1.4.1.9.9.106.2.0.1) trap to be listed as a root cause. This trap might occur when the hot standby has gone down indicating the system is at risk if there is a failover.

Note: To reduce "noise" associated with duplicate incidents, NNMi changes the incident Correlation Nature to **Symptom** for any user-defined Root Cause incidents that exceed the rate or deduplication threshold. Any Stream Correlation incident associated with the user-defined Root Cause incident is change to a Root Cause incident. See [Stream Correlation Incidents View](#) for more information about Stream Correlations.

To display an SNMP trap or NNM 6.x/7.x Event as a root cause incident:

Select **Root Cause** in the **SNMP Trap** or **Remote NNM 6.x/7.x Event Configuration** form.

The next time the incident occurs, the Correlation Nature attribute value changes to **Root Cause**.

To no longer display an SNMP trap or NNM 6.x/7.x Events as a root cause incident:

Clear **Root Cause** in the **SNMP Trap** or **Remote NNM 6.x/7.x Event Configuration** form.

The next time the incident occurs, the Correlation Nature attribute value changes to **Root Cause**.

Specify Category and Family Attribute Values for Organizing Your Incidents

When configuring incidents, NNMi provides the Category and Family attributes to help you organize your incidents.

Preconfigured Categories

The Category attribute helps you organize your incidents. Select the category that you want to be associated with this type of incident when it appears in an incident view. Each of the possible Category values is described in the following table.

Incident Categories Provided by NNMi

Category	Description
Accounting	Used to indicate problems related to usage statistics and allocation of costs associated with the billing of time and services provided by devices. This category is not used by NNMi with default configurations, but it is available for incidents you define.
Application Status	Indicates there is a problem with the health of the NNMi software. Examples of these kinds of events include license expiration or that a certain NNMi process lost connection to the Process Status Manager.
Configuration	Indicates there is a problem with the configuration of a managed device. For example, there is a physical address mismatch
Fault	Indicates a problem with the network, for example Node Down.
Performance	Indicates a threshold has been exceeded. For example, a utility has exceeded 90 percent
Security	Indicates there is a problem related to authentication. For example, an SNMP authentication failure
Status	Indicates some kind of status message. Examples of these kinds of incidents include "SNMP Link Up" or an "HSRP Group status Normal" message.

Note: You can add your own Category entries to NNMi. See ["Create an Incident Category" \(on page 253\)](#) for more information.

Preconfigured Families

The Family attribute provides another way to organize and sort your incident views. For example, you might choose to sort by Family to see all of the incidents related to interfaces or to connections.

The following table describes only some of the Family attribute values from which you can select.

Incident Families Provided by NNMi

Family	Description
Address	Indicates the incident is related to an address problem
Aggregated Port	Indicates the incident is related to an aggregated port problem
Board	Indicates the incident is related to an board problem
Connection	Indicates the incident is related to a problem with one or more connections
Correlation	Indicates the incident has been related to another incident. For example, a LinkDown incident might be correlated as a child to a LinkUp incident.
HSRP	Indicates the incident is related to an HSRP problem








Family	Description
Interface	Indicates the incident is related to a problem with one or more interfaces.
Node	Indicates the incident is related to a node problem
OSPF	Indicates the incident is related to an OSPF problem

Note: You can add your own Family entries to NNMi. See ["Create an Incident Family" \(on page 254\)](#) for more information.


Create an Incident Category

The Category attribute helps you organize your incidents. Create any Category that makes sense to you and your team. For a list of the Category codes provided by NNMi, ["Specify Category and Family Attribute Values for Organizing Your Incidents" \(on page 251\)](#).

To create a new incident Category:

1. Navigate to the **Incident Category** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Locate one of the following:
 - The **SNMP Trap Configuration (by OID)** or **SNMP Trap Configuration (by Name)** tab.
 - The **Remote NNM 6.x/7.x Event Configuration** tab.
 - The **Management Event Configuration** tab.
 - Do one of the following:
 - Click the  New icon.
 - Select a row, click the  Open icon.
 - d. In the configuration form, locate the **Category** attribute.
 - e. Click the  Lookup icon, and select  New.
2. Provide the required information (see [table](#)).
3. Click  **Save and Close** to return to the previous form.
4. Click  **Save and Close** to return to the Incident Configuration form.
5. Click  **Save and Close**. NNMi applies your changes.

Category Code Attributes

Name	Description
Label	Incident category name. For example, Hardware Faults, or Cisco Error. Maximum size is 255 characters. Any character type is valid.
Unique Key	Caution: After you click  Save and Close , this value cannot be changed. Used as a unique identifier when exporting and importing configuration definitions. To ensure that the value you enter is unique, it is recommended that you use the Java name space con-

Name	Description
	<p>vention when providing this value. It is also useful to include the label value as part of the unique key as shown in the following examples:</p> <pre>com.<your_company_name>.nnm.trapConf.category.<category_label></pre> <pre>com.<your_company_name>.nnm.eventConf.category.<category_label></pre> <pre>com.<your_company_name>.nnm.inciConf.category.<category_label></pre> <p>The maximum length is 80 alpha-numeric characters, periods allowed, no spaces allowed.</p>








Create an Incident Family

The Family attribute helps you organize your incidents. Create any Family that makes sense to you and your team. For a list of the Family codes provided by NNMi, ["Specify Category and Family Attribute Values for Organizing Your Incidents" \(on page 251\)](#).


To create a new incident Family:

- Navigate to the **Incident Family** form.
 - From the workspace navigation panel, select the **Configuration** workspace.
 - Select **Incident Configuration**.
 - Locate one of the following:
 - The **SNMP Trap Configuration (by OID)** or **SNMP Trap Configuration (by Name)** tab.
 - The **Remote NNM 6.x/7.x Event Configuration** tab.
 - The **Management Event Configuration** tab.

Do one of the following:

 - Click the  New icon.
 - Select a row, click the  Open icon.
 - In the configuration form, locate the **Family** attribute.
 - Click the  Lookup icon, and select  New.
- Provide the required information (see [table](#)).
- Click  **Save and Close** to return to the previous form.
- Click  **Save and Close** to return to the Incident Configuration form.
- Click  **Save and Close**. NNMi applies your changes.

Family Attributes

Name	Description
Label	Family name. For example, Hardware Faults, or Cisco Error. Maximum size is 255 characters. Any character type is valid.
Unique Key	<p>Caution: After you click  Save and Close, this value cannot be changed.</p> <p>Used as a unique identifier when exporting and importing configuration definitions. To ensure</p>

Name	Description
	<p>that the value you enter is unique, it is recommended that you use the Java name space convention when providing this value. It is also useful to include the label value as part of the unique key as shown in the following examples:</p> <pre>com.<your_company_name>.nnm.trapConf.family.<family_label></pre> <pre>com.<your_company_name>.nnm.eventConf.family.<family_label></pre> <pre>com.<your_company_name>.nnm.inciConf.family.<family_label></pre> <p>The maximum length is 80 alpha-numeric characters, periods allowed, no spaces allowed.</p>

Specify the Incident Severity

The incident severity represents the seriousness calculated for the incident. Use the severity attribute to specify the severity that should be assigned to the incident you are configuring. Possible values are described in the following table.

Incident Severity Values

Attribute	Description
Normal	Indicates there are no known problems related to the associated object. This severity is meant to be informational. Generally, no action is needed for these incidents.
Warning	Indicates there may or may not be a problem related to the associated object.
Minor	Indicates NNMi has detected problems related to the associated object that require further investigation.
Major	Indicates NNMi has detected problems related to the associated object to be resolved before they become critical.
Critical	Indicates NNMi has detected problems related to the associated object that require immediate attention.

See ["Monitor Your Network Using Incident Views"](#) for more information about these severity values.

Specify Your Incident Message Format

When configuring an incident, specify how the incident message appears in the incident view. The string you specify in the Message Format attribute is visible in the view.

Note: The incident message limit is 1024 characters. If you exceed this limit, NNMi truncates the value starting from the right.

You can use any combination of default and custom attributes:

["Valid Parameters for Configuring Incident Messages" \(on page 256\)](#)

["Include Custom Incident Attributes in Your Message Format" \(on page 259\)](#)

Valid Parameters for Configuring Incident Messages

When configuring incident messages, you may want to use incident information as part of the message. NNMi provides the following parameter values. Use these parameters as variables when formatting an incident message.

Tip: See the [Using the Incident Form](#) for more information about the parameter values.

Note: NNMi stores varbind values as custom incident attributes (CIAs).

See "[Specify Your Incident Message Format](#)" (on page 255) for more information about configuring messages.

Valid Parameters Visible From an Incident's Form

Parameter Value	Description
\$category, \$cat	Value of the Category attribute in the Incident form.
\$count, \$cnt	Value representing the number of Custom Incident Attributes that appear in the Incident form.
\$family, \$fam	Value from the Family attribute in the Incident form.
\$firstOccurrenceTime, \$fot	Value from the First Occurrence Time attribute in the incident form.
\$lastOccurrenceTime, \$lot	Value from the Last Occurrence Time attribute in the incident form.
\$lifecycleState, \$lcs	Value from the Lifecycle State attribute in the Incident form.
\$name	Value of the Name attribute from the incident configuration.
\$nature, \$nat	Value from the Nature attribute in the Incident form.
\$origin, \$ori	Value from the Origin attribute in the Incident form.
\$originOccurrenceTime, \$oot	Value from the Origin Occurrence Time attribute in the incident form.
\$priority, \$pri	Value from the Priority attribute in the Incident form.
\$sev, \$severity	Value of the Severity attribute of the Incident form.

Valid Parameters Not Visible From an Incident's Form

Parameter Value	Description
\$id	Unique Object Identifier attribute value for the incident (unique across the entire NNMi Database).
\$ifAlias, \$ifa	Value from the IfAlias attribute of the Interface form.
\$firstOccurrenceTimeMS, \$fms	Value from the First Occurrence Time attribute in the incident form, converted to milliseconds (measured since January 1, 1970, 00:00:00 GMT - Greenwich Mean Time).

Parameter Value	Description
\$id	Unique Object Identifier attribute value for the incident (unique across the entire NNMi Database).
\$ifAlias, \$ifa	Value from the IfAlias attribute of the Interface form.
\$lastOccurrenceTimeMS, \$lms	Value from the Last Occurrence Time attribute in the incident form, converted to milliseconds (measured since January 1, 1970, 00:00:00 GMT - Greenwich Mean Time).
\$managementAddress, \$mga	Value from the Management Address attribute of the associated Node form or SNMP Agent form.
\$oid	Value of the unique object identifier (oid) for the incident configuration that originated from either an SNMP trap, Management Event, or Remote NNM 6.x or 7.x event.
\$otherSideOfConnection, \$osc	If the incident's Source Node is part of a Layer 2 connection, this attribute is the following combination of values for the node and one of its interfaces on the other side of the Layer 2 connection: The fully-qualified DNS name of the node appended with the interface Name in the following format: <fully-qualified DNS name>[interface_name]
\$otherSideOfConnectionIfAlias, \$oia	If the incident's Source Node is part of a Layer 2 connection, this attribute is the value of the ifAlias of one of the interfaces on the other side of the Layer 2 connection.
\$otherSideOfConnectionManagementAddress, \$oma	If the selected interface is part of a Layer 2 connection, this attribute is the value of the Management Address of one of the interfaces on the other side of the Layer 2 connection.
\$originOccurrenceTimeMS, \$oms	Value from the Origin Occurrence Time attribute in the incident form, converted to milliseconds (measured since January 1, 1970, 00:00:00 GMT - Greenwich Mean Time).
\$sourceNodeUuid, \$snu	Universally Unique Object Identifier attribute value of the source node object for the incident (unique across all databases). This identifier distinguishes the source node object instance from all other node objects.
\$sourceNodeName, \$snn	Value from the Name attribute of the Node form.
\$sourceNodeLongName, \$sln	The fully-qualified DNS name as displayed in the Host-name attribute of the incident's Source Node's form.

Parameter Value	Description
\$id	Unique Object Identifier attribute value for the incident (unique across the entire NNMi Database).
\$ifAlias, \$ifa	Value from the IfAlias attribute of the Interface form.
\$sourceObjectClass, \$soc	Value of the object class for the object you want to include. Use this parameter when you need to request more details of a class of objects through a web service. Examples of object classes include: <code>com.hp.ov.nms.model.core.Interface</code> and <code>com.hp.ov.nms.model.snmp.SnmpAgent</code> .
\$sourceObjectName, \$son	Value from the Name attribute of the source object. For example, an interface object is named according to the MIB ifName. Each ifName varies according to the vendor's conventions. Using the name 4/1 as an example, 4 represents the board number and 1 represents the port number.
\$sourceObjectUuid, \$sou	Universally Unique Object Identifier attribute value of the source object for the incident (unique across all databases). This identifier distinguishes the source object instance from all other similar object instances.
\$uuid	Universally Unique Object Identifier attribute value of the incident (unique across all databases). This identifier distinguishes the incident object instance from all other incident objects.

Valid Parameters Established in Custom Incident Attributes

Parameter Value	Description
\$<position_number>	Value of the custom incident attribute (CIA) position number for any CIA that originated from a varbind or was added by NNMi. For example, to indicate you want to use the varbind in position 1, enter: \$1 NNMi stores varbind values as Custom Incident Attributes. If you know the varbind position number, use this parameter.
\$<CIA_name>	Value of the name that is used for the custom incident attribute. For example, \$mycompany.mycia. NNMi provides CIA values for configuring Management Events. See Custom Incident Attributes Provided by NNMi for more information about custom incident attributes.
\$<CIA_oid>	Value of the object identifier for any custom incident attribute that originated as a varbind. For example, \$.1.3.6.1.6.3.1.1.5.1. Use this parameter when you are not certain of a custom incident attribute (varbind) position number.
\$*	Used to indicate you want all of the custom incident attribute values originating as varbinds, to be passed to the action configuration. Each varbind is returned in the following format: \$<CIA_name>:<CIA_value> in which the custom incident attribute name appears followed by the custom incident attribute value.

The function described in the following table replaces the specified numeric value with the associated text value stored in the CIA.

Note: The associated MIB must have been loaded using the [nnmloadmib.ovpl](#) command.

Functions to Generate Values Within Incident Messages

Function	Description
\$text(\$<position_ number>)	<p>The <position_number> argument specifies the numeric value of the custom incident attribute (CIA) position number for any CIA that originated from a varbind or was added by NNMi. For example, to indicate you want to use the varbind in position 1, enter: \$1.</p> <p>NNMi replaces the numeric value with the text value stored in the CIA.</p> <p>Note: If a text value is not available, NNMi returns the numeric value.</p>
\$text(\$<CIA_ oid>)	<p>The <CIA_oid> argument specifies the object identifier for any custom incident attribute that originated as a varbind. For example, \$.1.3.6.1.6.3.1.1.5.1. Use this argument to the \$text function when you are not certain of a custom incident attribute (varbind) position number.</p> <p>NNMi replaces the numeric value with the text value stored in the CIA.</p> <p>Note: If a text value is not available, NNMi returns the numeric value.</p>

Include Custom Incident Attributes in Your Message Format

NNMi includes two categories of CIAs:

- SNMP trap varbinds identified by the Abstract Syntax Notation value (ASN.1). NNMi turns varbinds into CIAs and maintains each varbind's position number. See "[Load SNMP Trap Definitions](#)" (on page 247).
- Custom attributes provided by NNMi. See "[Custom Incident Attributes Provided by NNMi](#)" (on page 214).

You can use CIAs in your message format to extend the amount of information presented. To determine which CIAs are available for any particular incident type, open an Incident view, locate the incident and open the [Incident form](#). Navigate to the **Custom Attributes** tab. A complete list of available CIAs (for that incident type) appears in the table.

To include a CIA in your message format, type the dollar-sign character (\$) plus any of the following:

- Varbind position number or asterisk (*) to include all varbind values
- Name of the CIA
- Object identifier (oid) of the CIA (useful when the varbind position number is not consistent among vendors)

Note: A single incident cannot include two CIAs with the same name. However, two incidents can contain CIAs having the same names and values.

The following table presents some example formats with the subsequent output.

Example Incident Message Formats

Example Message Format	Output in Incident View
Possible trouble with \$3	Possible trouble with <varbind 3>

Example Message Format	Output in Incident View
Possible trouble with \$11	Possible trouble with <varbind 11>
Possible trouble with \$77 (where the varbind position 77 does not exist)	Possible trouble with <Invalid or unknown cia> 77
Possible trouble with \$*	Possible trouble with <cia1_name: cia_value>, <cia2_name; cia_value>,< cian_name: cia_value>
Possible trouble with \$3x	Possible trouble with <varbind 3>x
Possible trouble with \$1.2.3.4.5	Possible trouble with <value of the CIA whose oid is 1.2.3.4.5>
Possible trouble with \$mycia.mycompany	Possible trouble with <value of the CIA whose name is mycia.mycompany>

Tip: NNMi provides an error message when a CIA cannot be found. For example, if you enter an unavailable varbind position, name, or object identifier (oid), NNMi returns an "Invalid or unknown cia" error message.

Specify a Description for Your Incident Configuration

NNMi provides the Description attribute to help you further identify the current incident configuration.

Description

Use the description field to provide additional information that you would like to store about the current incident configuration. This description applies only to the configuration entry.

Type a maximum of 2048 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.










Specify an Author for Your Incident Configuration

The Author attribute value indicates who created the incident configuration.


To create a new Author attribute value:

1. Navigate to the **Author** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Open the **Incident Configuration** form.
 - d. Locate one of the following:
 - The **SNMP Trap Configuration (by OID)** or **SNMP Trap Configuration (by Name)** tab.
 - The **Remote NNM 6.x/7.x Event Configuration** tab.
 - The **Management Event Configuration** tab.

Do one of the following:

- o Click the  New icon.
 - o Select a row, click the  Open icon.
- e. Do one of the following:
- o To create a new configuration, click the  New icon.
 - o To edit an existing configuration, select a row, and click the  Open icon.
- f. In the configuration form, locate to the **Author** attribute.
- g. Click the  Lookup icon, and select  New.
2. Type the text string that represents the new author (see [table](#)).
 3. Click  **Save and Close** to return to the previous form.
 4. Click  **Save and Close** to return to the Incident Configuration form.
 5. Click  **Save and Close**. NNMi saves your changes.

Incident Configuration Author

Attribute	Description
Label	<p>Provide a text string that identifies the author of the incident configuration. Any characters are allowed, including spaces and punctuation.</p> <p>Note: All incident configurations provided by NNMi include HP Network Node Manager as the Label value.</p>
Unique Key	<p>Caution: After you click  Save and Close, this value cannot be changed.</p> <p>Used as a unique identifier when exporting and importing configuration definitions. To ensure that the value you enter is unique, it is recommended that you use the Java name space convention when providing this value. It is also useful to include the label value as part of the unique key as shown in the following examples:</p> <pre>com.<your_company_name>.nnm.trapConf.author.<author_label></pre> <pre>com.<your_company_name>.nnm.eventConf.author.<author_label></pre> <pre>com.<your_company_name>.nnm.inciConf.author.<author_label></pre> <p>The maximum length is 80 alpha-numeric characters, periods allowed, no spaces allowed.</p>

Configure Remote NNM 6.x/7.x Events

NNMi can display incidents from Remote NNM 6.x and 7.x management stations. In the NNMi incident browser, you can manage the lifecycle of incidents generated from previous versions of NNMi.

Tip: Gradually migrate from NNM 6.x or 7.x to NNMi while using this feature.

To configure NNMi to handle incidents generated from remote NNM 6.x/7.x events, perform the following tasks:



- [Configure the NNM 6.x/7.x Management Stations](#)
- [Configure the remote NNMi events](#)

Configure Remote NNM 6.x and 7.x Management Stations





There are multiple benefits to configuring NNMi to recognize the NNM 6.x or 7.x management stations in your environment:

- Configure NNMi to receive and display incidents (events) from remote NNM 6.x or 7.x management stations.
- Enable launching NNM 6.x or 7.x Dynamic Views from forwarded NNM 6.x or 7.x events (see [Access NNM 6.x and 7.x Features](#) for more information).
- Filter NNMi view by NNM 6.x or 7.x management station (show only those incidents received from a particular NNM 6.x or 7.x management station).

To display the details of an NNM 6.x or 7.x management station configuration:

1. From the workspace navigation panel, select the **Inventory** workspace.
2. Select the **Management Stations** view.
3. Locate the row representing the management station, click the  Open icon.
4. The [Management Station form](#) displays.
5. When finished, click the  Close icon.

To configure an NNM 6.x or 7.x management station (if your role allows you to do this):

1. Navigate to the **Management Stations** view.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Management Stations** view.
2. Do one of the following:
 - To create an NNM 6.x or 7.x management station configuration, click the  New icon, and continue.
 - To edit an NNM 6.x or 7.x management station configuration, click the  Open icon, and continue.
 - To delete an NNM 6.x or 7.x management station configuration, click the  Delete icon.
3. In the [Management Station form](#), provide the required information:
 - IPv4 address of the remote NNM 6.x or 7.x management station
 - Port number used by the OpenView Application Server (ovas) on the remote management station
 - Port number used by the web server on the remote NNM 6x or 7x management station
4. Click  **Save and Close** to return to the Management Stations view.
5. If this is the first Management Station configuration, you must exit the NNMi console, and start the NNMi console. (You do not need to exit and start the NNMi console when configuring any subsequent NNM 6.x/7.x management stations.)



6. Next, configure which incidents to receive from your NNM 6.x or 7.x management station ("[Configure Remote NNM 6.x/7.x Events](#)" (on page 261)).



Remote NNMi Event Form

Using NNMi, you can display incidents from Remote NNM 6.x and 7.x management stations. . In the NNMi incident browser, you can manage the lifecycle of incidents generated from previous versions of NNMi.

Tip: Gradually migrate from NNM 6.x or 7.x to NNMi while using this feature.

To configure a Remote NNM 6.x/7.x event:

1. Navigate to the **Remote NNM 6.x/7.x Event Configuration** form:
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Select the **Remote NNM 6.x/7.x Event Configuration** tab.
 - d. Do one of the following:
 - To create a Remote NNM 6.x/7.x Event configuration, click the  New icon.
 - To edit a Remote NNM 6.x/7.x Event configuration, click the  Open icon.

Note: In the Remote NNM 6.x/7.x Event Configuration form, verify that **Enable** is selected.
2. Make your configuration choices (see [table](#)).
3. Click  **Save and Close** to return to the **Incident Configuration** form.
4. Click  **Save and Close** to apply your changes.

Tasks for Remote NNM 6.x/7.x Event Configuration

Task	How
"Specify the Incident Configuration Name" (on page 249)	Use the Basics group of the Remote NNM 6.x/7.x Event Configuration form. Specify a name that helps you to identify the configuration for subsequent use.
"Specify the SNMP Object ID" (on page 249)	Use the Basics group of the Remote NNM 6.x/7.x Event Configuration form. NNMi supports SNMPv2c and SNMPv1 formats.
Specify whether you want to enable this configuration.	In the Basics group of the Remote NNM 6.x/7.x Event Configuration form, make sure Enable <input checked="" type="checkbox"/> is checked for each configuration you want to use.
Display the NNMi Remote Incident as a Root Cause Incident	Use the Basics group of the Remote NNM 6.x/7.x Event Configuration form.
"Specify Category and Family Attribute Values for Organizing Your Incidents" (on page 251)	Use the Basics group of the Remote NNM 6.x/7.x Event Configuration form. You can organize your incidents using Category and Family.
"Specify the Incident Severity " (on page 255)	Use the Basics group of the Remote NNM 6.x/7.x Event Configuration form. Possible Severity values include: Normal, Warning, Minor, Major, and Critical .

Task	How
"Specify Your Incident Message Format" (on page 255)	Use the Basics group of the Remote NNM 6.x/7.x Event Configuration form. The message format determines the message to be displayed for the incident.
"Specify a Description for Your Incident Configuration" (on page 260)	Use the Basics group of the Remote NNM 6.x/7.x Event Configuration form. Provide a meaningful description.
Specify an Author for Your Remote NNM 6.x/7.x Event Configuration	Use the Basics group of the Remote NNM 6.x/7.x Event Configuration form

After you complete the Basic Configuration for the remote NNM 6.x or 7.x event, you can also choose to configure the information described in the following table.




Additional Configurations



Task	How
"Correlate Duplicate Incidents (Deduplication Configuration)" (on page 269)	Select the Deduplication Configuration tab to specify duplicate incidents that you want to be suppressed.
"Track Incident Frequency (Rate: Time Period and Count)" (on page 273)	Select the Rate Configuration tab to specify a rate for duplicate incidents. After the rate limit is reached, NNMi generates an Incident to notify you of the problem.
"Configure an Action for an Incident" (on page 283)	Select the Action Configuration tab to specify actions that should occur automatically when an incident is either generated or closed.
"Configure Diagnostics for an Incident (NNMi iSPI NET)" (on page 291)	Select the Configuration Per Node Group tab to specify diagnostic actions that should occur automatically when an incident is generated for a node that belongs to a particular Node Group.

Configure How Management Events Are Displayed

Management events are those events that are generated from the NNMi Causal Engine. You can configure how you want these events to be displayed in the incident views provided by NNMi. The types of things you configure include its name, category, and the format of its message.

To configure a management event:

1. Navigate to the **Management Event Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Select the **Management Event Configuration** tab.
3. Do one of the following:
 - a. To create a management event configuration, click the  New icon.
 - b. To edit a management event configuration, click the  Open icon.
 - c. To delete a management event configuration, click the  Delete icon.
4. In the [Management Event Configuration form](#), provide the required information.

5. Click  **Save and Close** to return to the **Incident Configuration** form.
6. Click  **Save and Close** to save your changes.






The next time that a management event of this type arrives into the database, NNMi creates an associated incident to display in the appropriate console incident views.

Management Event Form

To configure incidents originating from management events:

1. Navigate to the **Incident Configuration** form:
 - a. From the workspace navigation pane, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Select the **Management Event Configuration** tab.
3. Make your configuration choices (see [table](#)).

Note: If you want to add or edit a management event configuration, verify that **Enabled** is selected.

 - a. To add a management event configuration, click the  New icon, and continue.
 - b. To edit a management event configuration, click the  Open icon, and continue.
 - c. To delete a management event configuration, click the  Delete icon.
4. Click  **Save and Close** to return to the **Incident Configuration** form.
5. Click  **Save and Close** to save your changes.

Tasks for Management Event Configuration

Task	How
"Specify the Incident Configuration Name" (on page 249)	Use the Basics group of the Management Event form. Specify a name that helps you to identify the configuration for subsequent use.
Specify whether you want to enable this configuration.	In the Basics group of the Management Event form, verify that Enable <input checked="" type="checkbox"/> is selected for each configuration you want to use.
"Specify Category and Family Attribute Values for Organizing Your Incidents" (on page 251)	Use the Basics group of the Management Event form. You can organize your incidents using Category and Family.
"Specify the Incident Severity " (on page 255)	Use the Basics group of the Management Event form. Possible Severity values include: Normal , Warning , Minor , Major , and Critical .
"Specify Your Incident Message Format" (on page 255)	Use the Basics group of the Management Event form. The message format determines the message to be displayed for the incident.
"Specify a Description for Your Incident Configuration" (on page 260)	Use the Basics group of the Management Event form. Provide a meaningful description.

Task	How
"Specify an Author for Your Incident Configuration" (on page 260)	Use the Basics group of the Management Event form.

After you complete the Basic Configuration for the management event, you can also choose to configure the information described in the following table.

Additional Configurations

Task	How
"Correlate Duplicate Incidents (Deduplication Configuration)" (on page 269)	Select the Deduplication Configuration tab to specify duplicate incidents that you want to be suppressed.
"Track Incident Frequency (Rate: Time Period and Count)" (on page 273)	Select the Rate Configuration tab to specify a rate for duplicate incidents. After the rate limit is reached, NNMi generates an Incident to notify you of the problem.
"Configure an Action for an Incident" (on page 283)	Select the Action Configuration tab to specify actions that should occur automatically when an incident is either generated or closed.
"Configure Diagnostics for an Incident (NNM iSPI NET)" (on page 291)	Select the Configuration Per Node Group tab to specify diagnostic actions that should occur automatically when an incident is generated for a node that belongs to a particular Node Group.

Reduce the Number of Incoming Incidents

NNMi's Causal Engine reduces the number of incidents by extensively evaluating problems and determining the root cause for you, whenever possible.

To help simplify diagnosing network faults, you can also reduce the number of incidents that are displayed. To do so, you identify additional relationships between incoming incidents. After these relationships are identified, NNMi modifies the flow of incidents by recognizing patterns of incoming management events or SNMP traps, and then nests related incidents as correlated children or correlated parent incidents.

These strategies can dramatically reduce the number of incidents and improve the value of the incidents displayed. For example, instead of displaying an entire incident storm typically generated by equipment and link failures, using the deduplication configuration you specify, NNMi displays only the most meaningful incidents, and lists the rest as correlated children or parents, resulting in faster and easier identification of network problems.

Using NNMi, you can reduce the number of incidents displayed in your incident views using any of the incident configurations described in the following table.

Note: NNMi provides configurations for deduplication, rate, and pairwise configurations. You can choose to use them as is, edit them, or create your own configurations.

Correlation Configuration Possibilities

Configuration	Description
Deduplication	Determines what values NNMi should match to detect when an incident is a duplicate. These duplicate incidents are then correlated under a new Duplicate Correlation incident. The relationship between them is indicated in the Correlated Children tab by a Type of De-Dup Correlation . By reducing the quantity of incidents displayed, your net-

Configuration	Description
	<p>work administrators can focus on the important incidents.</p> <p>To help your operators understand the magnitude or significance of the problem, NNMi stores the number of duplicates generated. This value is captured as the Duplicate Count attribute. It is incremented on the Duplicate Correlation incident. This incident appears in the Stream Correlation Incidents view. Its Correlation Nature attribute value is Stream Correlation.</p> <p>NNMi also stores the following information related to duplicate incidents:</p> <p>First Occurrence Time: Indicates the timestamp of the first occurrence of a duplicate incident.</p> <p>Last Occurrence Time: Indicates the timestamp of the latest notification for a set of duplicate incidents</p>
<p>Rate</p>	<p>Used to measure the number of incoming incidents within a defined time period. When a specified number is received within the specified time interval, NNMi lists each occurrence of the incident as a correlated child incident under a new Rate Correlation incident. The relationship between the child and parent is indicated in the Correlated Children tab by a Type of Rate Correlation. The Rate Correlation incident appears in the Stream Correlation Incidents view. The Correlation Nature attribute value is Stream Correlation.</p> <p>By reducing the quantity of incidents displayed, your network administrators can focus on the important incidents. For example, you might want to specify that if a link is intermittently down at least three times within 30 minutes that these incidents be listed and the rate displayed so that you can subsequently identify any potential rerouting problems.</p> <p>NNMi also stores the following information related to rate:</p> <p>Count: Indicates the rate at which the incident must occur within the specified time-frame.</p> <p>Hours, Minutes, and Seconds: Used to measure the time within the rate must occur</p> <p>First Occurrence Time: Indicates the time at which the measured rate was reached.</p> <p>Last Occurrence Time: Indicates the last time which the incident occurred.</p> <p>Note: NNMi updates the Correlation Notes with the number of incidents that have occurred within the specified time period. For example, 5 in 5 minutes.</p>
<p>Pairwise</p>	<p>Used to pair the first occurrence of an incident to another subsequent incident. After the second incident in the pair occurs, the first incident becomes a correlated child under the second (parent) incident. The relationship between the child and parent incident is indicated in the Correlated Children tab by a Type of Pairwise Correlation.</p> <p>Each incident in the pair is then closed, reducing the quantity of open incidents displayed.</p> <p>For example, you might want to configure a pairwise relationship between a LinkDown and a subsequent LinkUp incident. After the LinkUp incident occurs, it cancels the Link-Down incident and updates the Correlation Notes. The LinkDown incident appears as a correlated child under the LinkUp parent.</p>

Each of these incident reduction strategies determines patterns of incidents by monitoring the attributes you specify when configuring incidents. See ["Configuring Incidents" \(on page 211\)](#) for more information. See ["Load SNMP Trap Definitions" \(on page 247\)](#) for more information about how to specify the SNMP traps you want to receive by automatically creating or updating an incident configuration for an SNMP trap using a MIB file.

Note: You can also reduce the number of incidents generated by setting a device's management mode to either Not Managed or Out of Service. See ["Stop or Start Managing a Node, Interface, or Address" \(on page 184\)](#) for more information about setting the management mode and the resulting behavior.

Related Topics

["Configure How Management Events Are Displayed" \(on page 264\)](#)

["Configure SNMP Trap Incidents" \(on page 246\)](#)

Control which Incoming Traps Are Visible in Incident Views

You can configure devices in your network environment to send traps to the NNMi management server. To do so, use the incident configurations provided by NNMi, create your own, or both. See ["Configure SNMP Trap Incidents" \(on page 246\)](#) for information about how to configure SNMP traps as incidents. See ["SNMP Trap Incident Configurations Provided by NNMi" \(on page 216\)](#) for information about the incident configurations provided by NNMi.

Note: To establish this communication flow, the SNMP agent must be intentionally configured by the device administrator to send SNMP traps to your NNMi management server.

After you configure the incidents for each SNMP trap you want to display, NNMi stores your incident configurations for SNMP traps in the `allowedOids.conf` file. NNMi then uses this file as a positive filter to identify the traps that should appear as incidents.


By default, NNMi enables only the following SNMP Trap incident configurations that it provides:

- CiscoWarmStart
- CiscoColdStart
- SNMPWarmStart
- SNMPColdStart
- CiscoLinkDown
- CiscoLinkUp
- HSRPStateChange
- ltfVrrpStateChange
- RcVrrpStateChange
- SNMPLinkDown
- SNMPLinkUp
- RcnAggLinkUp
- RcAggLinkUp
- RcnAggLinkDown
- RcAggLinkDown

- RcnSmltstLinkUp
- RcSmltstLinkUp
- RcnSmltstLinkDown
- RcSmltstLinkDown

See ["SNMP Trap Incident Configurations Provided by NNMi" \(on page 216\)](#) for more information.

To enable or disable an SNMP trap configuration:

1. Navigate to the Incident Configuration view.
 - a. In the Workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Incident Configuration** view.
2. Select the **SNMP Trap Configuration** tab.
3. Click the  Open icon in the row that represents the SNMP Trap Configuration of interest.
4. To enable the incident configuration, click Enable .
5. To disable the incident configuration, clear Enable .

Related Topics

["Reduce the Number of Incoming Incidents" \(on page 266\)](#)

Correlate Duplicate Incidents (Deduplication Configuration)






The deduplication configuration determines what values NNMi should match to detect when an SNMP trap, management event, or remote NNM 6.x/7.x event is a duplicate.

Note the following:

- NNMi applies only one deduplication configuration per incident . If NNMi generates an incident using a specified deuplication configuration, NNMi continues to correlate duplicate incidents using the original configuration. To use a different deduplication configuration for an incident, first delete the current deduplication incident (created using the original deduplication configuration). NNMi generates the next deduplication incident according to the new deduplication configuration settings.
- By default, NNMi updates the **Duplicate Count** every 30 seconds. This interval cannot be changed.
- NNMi continues to update the duplicate count regardless of an incident's lifecycle state. For example, if an incident's **Lifecycle State** is set to **Closed**, the duplicate count continues to be incremented. See [About the Incident Lifecycle](#) for more information. This behavior helps you identify situations in which the incident is not yet fixed. Take note if the Duplicate Count is incremented after a lengthy time period has elapsed, which might indicate there is a new problem with the node, interface, or address.
- Each time you stop and restart ovjboss, any incidents that have not yet been correlated or persisted are lost. This means that after a restart of ovjboss, an incoming incident might not be correlated as expected. For example, after a restart of ovjboss, a duplicate incident might not be correlated under its original parent incident. Instead, a new parent incident might be generated. See ["Stop or Start an NNMi Process" \(on page 26\)](#) for more information about starting and stopping the ovjboss process.

To specify or delete a deduplication configuration:

1. Navigate to the **Incident Configuration** form:
 - a. From the workspace navigation panel, select the **Configuration** workspace.

- b. Select **Incident Configuration**.
- c. Select the type of incident you want to configure: **SNMP Trap Configuration**, **Remote NNM 6.x/7.x Event Configuration**, or **Management Event Configuration**.
- d. Do one of the following:
 - i. To create a deduplication configuration, click the  New icon, and continue.
 - ii. To edit a deduplication configuration, click the  Open icon, and continue.
 - iii. To delete a deduplication configuration, click the  Delete icon.
2. Select the **Deduplication Configuration** tab.
3. Provide the required information (see [table](#))
4. Click  **Save and Close** to return to the Incident Configuration form.
5. Click  **Save and Close** to save your deduplication configuration.

Deduplication Attributes


Name	Description
Enable	<p>Use this attribute to temporarily disable an incident's deduplication configuration.</p> <p>To temporarily disable the deduplication configuration setting, uncheck Enable.</p> <p>To enable the deduplication configuration setting, click Enable.</p> <p>Note: After a deduplication configuration is enabled, NNMi increments the Duplicate Count for an associated incident regardless of the Lifecycle State value. For example, if an incident's Lifecycle State is set to Closed, the duplicate count continues to be incremented. See About the Incident Lifecycle for more information.</p>
Dedup Count	Specifies the number of duplicate incidents for the current configuration that NNMi stores at one time. For example, if the Dedup Count is 10, after NNMi receives 10 duplicate incidents, NNMi deletes the first duplicate incident and keeps the eleventh. (NNMi stores ten maximum.)
Hour Interval	Used with the Minute and Second Intervals to specify the time that must elapse before a new duplicate incident is generated for this incident configuration. For example, if the Hour Interval value is 1, and no Minute or Second Intervals are specified, and the duplicate incident is not generated within one hour, NNMi generates a new duplicate incident the next time it occurs.
Minute Interval	Used with the Hour and Second interval to specify the time that must elapse before a new duplicate incident is generated for this incident configuration. For example, if the Minute Interval is 30 and no Hour or Second Intervals are specified, and the duplicate incident is not generated within 30 minutes, NNMi generates a new duplicate incident the next time it occurs.
Second Interval	Used with the Hour and Minute Intervals to specify the time that must elapse before a new duplicate incident is generated for this incident configuration. For example, if the Second Interval is 120 and no Hour or Minute Intervals are specified, and the duplicate incident is not generated within 120 seconds, NNMi generates a new duplicate incident the next time it occurs.
Correlation Incident Config	<p>Used to access the out-of-the box deduplicaton configuration provided by NNMi.</p> <p>Select the default value Duplicate Correlation.</p>

Name	Description
	<p>Note: You can choose to use this configuration as is or edit it. If you want to create a new deduplication configuration, you must create a new management event configuration. See "Configure How Management Events Are Displayed" (on page 264) for more information. After you have created a new management event configuration, it appears in the Quick Find list of options. See "Lookup Fields" (on page 18) for more informationn about Quick Find.</p>
Comparison Criteria	<p>Specify which group of attributes must match before the incident is identified as a duplicate. The possible groups of attributes consist of the following choices.</p> <p>Name value of the Incident (from the General tab on the Incident form).</p> <p>Source Node value (from the Basics group on the Incident form). Address or name of the node for which the incident was generated.</p> <p>Source Object value (from the Basics group on the Incident form). For example, the Source Object for a LinkDown incident is interface.</p> <p>CIA custom incident attribute values (select from the list displayed on the Custom Attributes tab on the Incident form). If you want to use CIA as part of your comparison criteria, see "Deduplication Comparison Parameters Form " (on page 271).</p>
Comparison Parameter List	<p><i>Optional.</i> If you selected a Comparison Criteria that includes CIA, you must populate one or more rows in this table. See "Deduplication Comparison Parameters Form " (on page 271).</p>

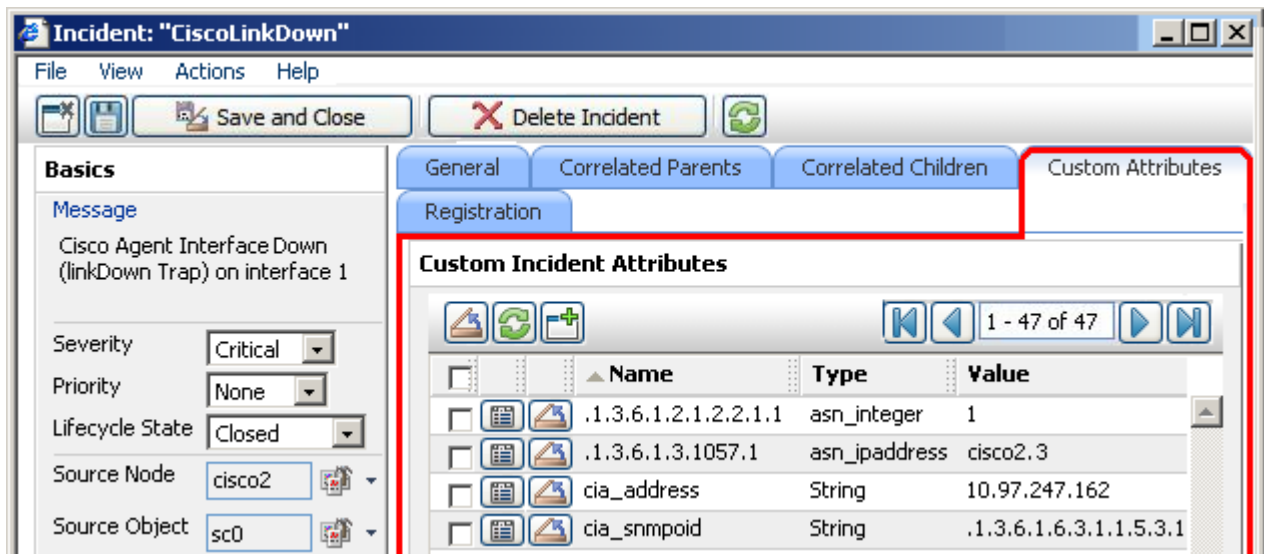
Deduplication Comparison Parameters Form

Custom Incident Attributes (CIAs) are used as parameter values. Parameter values enable accurate identification of duplicate incidents. There are two categories of CIAs:

- SNMP trap varbind values (Name = the MIB varbind identifier, Type = asn_*)
- Custom attributes provided by NNMi (Name = cia.*, Type=String). See ["Custom Incident Attributes Provided by NNMi" \(on page 214\)](#).

The group of available CIAs depends on which incident you are configuring for this Deduplication (for example, CiscoLinkDown). To see which CIAs are available, navigate to an Incident view, select an instance of that incident-type, click the  Open icon and navigate to the Custom Attributes tab. The items listed in the table are the CIAs for that particular incident-type. For example, all CiscoLinkDown incidents would have the same group of CIAs shown in the illustration below.

Note: You can also use the CIA (varbind) position number.



To specify a CIA to use in the identification criteria for duplicate incidents:

1. Navigate to the **Deduplication Comparison Params** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Navigate to the **SNMP Trap Configuration, Remote NNMi Event Configuration, or Management Event Configuration** tab.
 - d. Do one of the following:
 - To create a new configuration, click the New icon.
 - To edit an existing configuration, select a row, and click the Open icon.
 - e. On the form that opens, navigate to the **Deduplication Configuration** tab.
 - f. Locate the **Comparison Parameter List** table.
 - g. Do one of the following to specify which CIA:
 - To add a Custom Incident Attribute parameter specification, click the New icon.
 - To edit an existing Custom Incident Attribute parameter specification, select a row, and click the Open icon.
2. In the Parameter Value field, type (or copy and paste) the exact text string from the Incident form, Custom Attribute tab, **Name** attribute value:
 - NNMi-provided CIA value (see ["Custom Incident Attributes Provided by NNMi" \(on page 214\)](#)).
 - SNMP trap varbind identified by the Abstract Syntax Notation value (ASN.1).
3. Click **Save and Close** to return to the previous configuration form.
4. Click **Save and Close** to return to the Incident Configuration form.
5. Click **Save and Close**. NNMi saves your changes.

Track Incident Frequency (Rate: Time Period and Count)

Use Rate Configuration to track incident patterns *based on the number of incident reoccurrences within a specified time period*. After the count within the specified time period is reached, NNMi emits a Rate Correlation incident and continues to update the Correlation Notes with the number of occurrences within that rate.

As long as your defined criteria (Count and Hours, Minutes, Seconds) is sustained, the following information is updated in the Correlation Notes of the Rate Correlation incident:

- the actual number of occurrences of incidents for that sustained rate (Count)
- the sustained time interval (Hours, Minutes, Seconds)





For example, you can set a Rate configuration to track when a link is intermittently down at least three times in 30 minutes. NNMi shows the first occurrence of the rate incident in the incident view and uses Correlation Notes to update the number of incidents and time interval to reflect all the incremental incident occurrences and time periods. To continue the example, if the rate of three times in 30 minutes is sustained for 90 minutes, NNMi updates the Correlation Notes to specify that 9 incidents occurred in 90 minutes.

NNMi provides preconfigured Rate correlations. You can add new Rate correlations.



When you open the Incident form of the newest instance:

- On the General tab, two fields notify you that the Rate correlation is working:
 - **Correlation Nature:** Rate
 - **Count:** x
- On the **Correlated Children** tab, each incident is listed in the table.

To establish a rate correlation within an incident configuration:

1. Navigate to the **Rate Configuration** tab.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Open the **Incident Configuration** form.
 - d. Navigate to the **SNMP Trap Configuration, Remote NNM 6.x/7.x Event Configuration, or Management Event Configuration** tab.
 - e. Do one of the following:
 - To create a new configuration, click the  New icon.
 - To edit an existing configuration, select a row, and click the  Open icon.
 - f. On the form that opens, locate the **Rate Configuration** tab.
2. Provide the definition for this Rate Configuration (see [table](#)).
3. *Optional.* If your [Comparison Criteria](#) includes custom incident attributes (CIA) to identify one specific incident, use the Comparison Parameter List table to define each CIA. See "[Rate Comparison Parameters Form](#)" (on page 274).
4. Click  **Save and Close** to return to the Incident Configuration form.
5. Click  **Save and Close**. NNMi saves your changes.


Rate Configuration Definition

Attribute	Description
Enable	If enabled, NNMi actively tracks any reoccurrences of the designated incident within the time period you specify, and generates a Rate incident.
Count	Specify the number of reoccurrences required before your Rate Configuration starts working.
Set the Time Period	Specify a time duration within which the reoccurrences are measured. Fill in one or more of the following attribute fields: Hours Minutes Seconds
Correlation Incident Config	Click the  icon and select  Quick Find. Select RateCorrelation from the list.
Comparison Criteria	Specify which group of attributes must match before the incident is identified as a duplicate. The possible groups of attributes consist of the following choices. Name value of the Incident (from the General tab on the Incident form). Source Node value (from the Basics group on the Incident form). Address or name of the node for which the incident was generated. Source Object value (from the Basics group on the Incident form). For example, the Source Object for a LinkDown incident is interface . CIA custom incident attribute values (select from the list displayed on the Custom Attributes tab on the Incident form). If you want to use CIA as part of your comparison criteria, see " Rate Comparison Parameters Form " (on page 274).
Comparison Parameter List	<i>Optional.</i> If you selected a Comparison Criteria that includes CIA, you must populate one or more rows in this table. See " Rate Comparison Parameters Form " (on page 274).

Rate Comparison Parameters Form

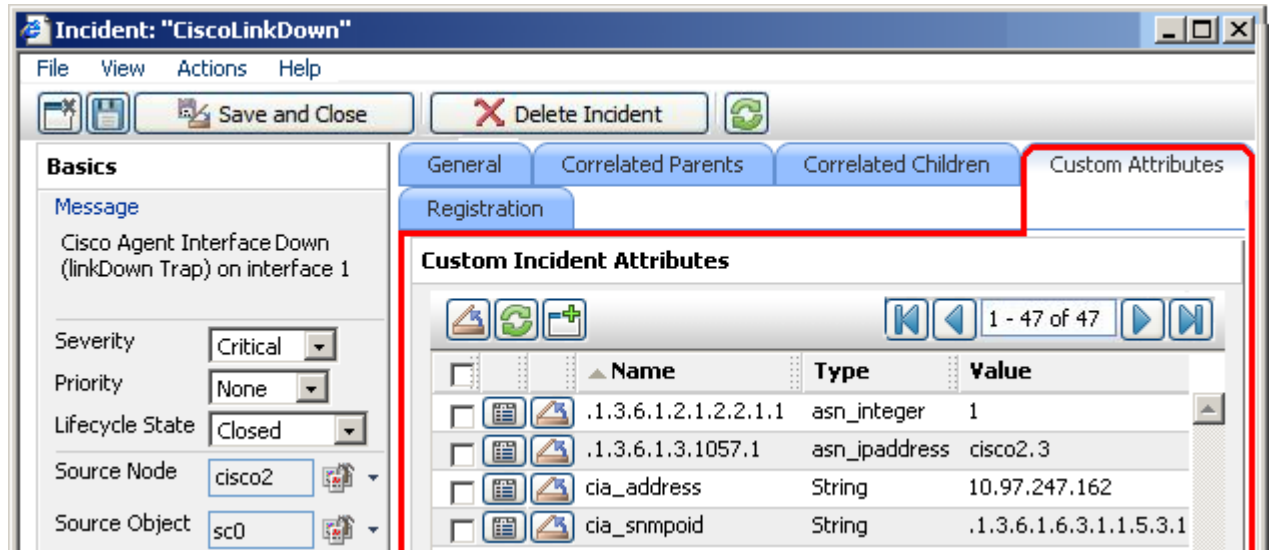
Custom Incident Attributes (CIAs) are used as parameter values. Parameter values enable accurate identification of duplicate incidents. There are two categories of CIAs:

- SNMP trap varbind values (Name = the MIB varbind identifier, Type = asn_*)
- Custom attributes provided by NNMi (Name = cia.*, Type=String). See "[Custom Incident Attributes Provided by NNMi](#)" (on page 214).

The group of available CIAs depends on which incident you are configuring for this Rate (for example, CiscoLinkDown). To see which CIAs are available, navigate to an Incident view, select an instance of that incident-type, click the  Open icon and navigate to the Custom Attributes tab. The items listed in the table



are the CIAs for that particular incident-type. For example, all CiscoLinkDown incidents would have the same group of CIAs shown in the illustration below.

Note: You can also use the CIA (varbind) position number.



To specify a CIA to use in the identification criteria for duplicate incidents:

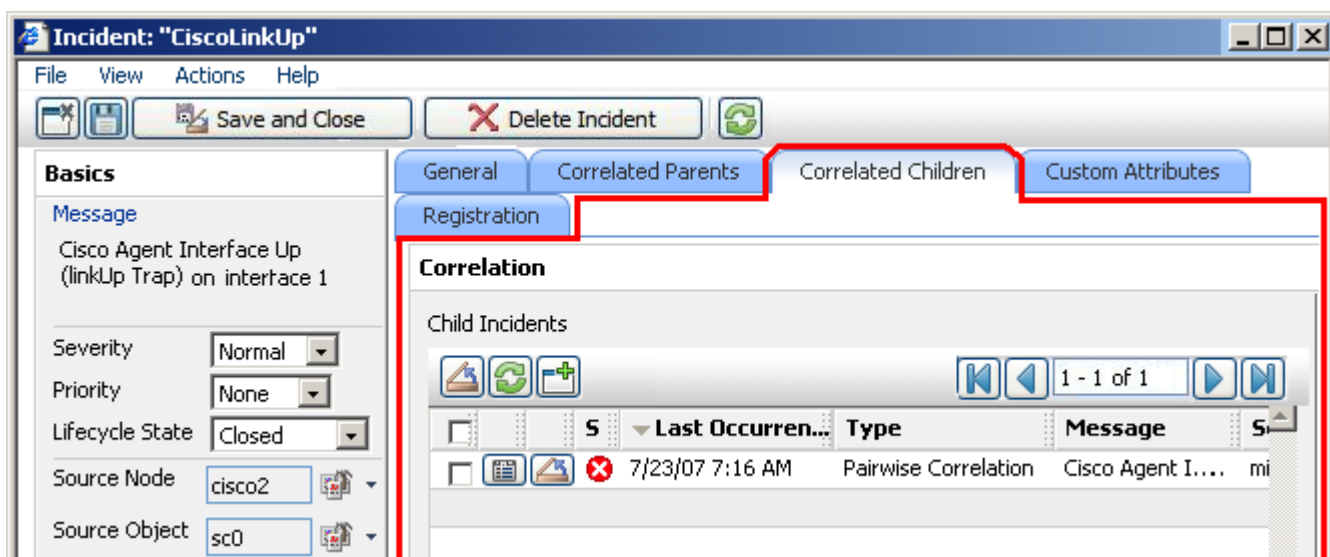
1. Navigate to the **Rate Comparison Params** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Navigate to the **SNMP Trap Configuration**, **Remote NNMi Event Configuration**, or **Management Event Configuration** tab.
 - d. Do one of the following:
 - To create a new configuration, click the New icon.
 - To edit an existing configuration, select a row, and click the Open icon.
 - e. On the form that opens, navigate to the **Rate Configuration** tab.
 - f. Locate the **Comparison Parameter List** table.
 - g. Do one of the following to specify which CIA:
 - To add a Custom Incident Attribute parameter specification, click the New icon.
 - To edit an existing Custom Incident Attribute parameter specification, select a row, and click the Open icon.
2. In the Parameter Value field, type (or copy and paste) the exact text string from the Incident form, Custom Attribute tab, **Name** attribute value:
 - NNMi-provided CIA value (see ["Custom Incident Attributes Provided by NNMi"](#) (on page 214)).
 - SNMP trap varbind identified by the Abstract Syntax Notation value (ASN.1).
3. Click **Save and Close** to return to the previous configuration form.

4. Click  **Save and Close** to return to the Incident Configuration form.
5. Click  **Save and Close**. NNMi saves your changes.

About Pairwise Configurations

Often two incidents have a logical relationship to each other, for example, CiscoLinkDown followed by CiscoLinkUp. There is no need for both incidents to take up room in your Incident view. Nesting the two together helps you do your job quickly and efficiently.

Use the Pairwise Configuration to pair up the occurrence of one incident with another subsequent incident. When the second incident in the pair occurs, the first incident becomes a correlated child incident within the parent incident (see illustration below). See ["Incident Pair \(Pairwise\) Configurations Provided by NNM" \(on page 276\)](#) for ideas.



NNMi automatically ensures that the **Source Node** attribute value is identical in both incidents of your defined pair. Some incident pairs require extensive details to verify an accurate match. If *both sample incidents* have custom incident attributes, you can refine the match criteria beyond Source Node. See ["Pair Item Configuration Form \(Identify Incident Pairs\)" \(on page 281\)](#).

Related Topics:

["Prerequisites for Pairwise Configurations" \(on page 278\)](#)

["Pairwise Configuration Form \(Correlate Pairs of Incidents\)" \(on page 279\)](#)

Incident Pair (Pairwise) Configurations Provided by NNM

NNMi provides the pairwise configurations described in the following table.


Pairwise Configurations Provided by NNM



Name	Description
CiscoLinkDownUpPair	<p>Cancels a CiscoLinkDown incident with a CiscoLinkUp incident on the same interface for the same SNMP agent address.</p> <p>This configuration is used for known Cisco devices.</p>

Name	Description
NodeDownUpPair	Cancels a NodeDown incident with a NodeUp incident from the same node.
OvApaAddressDownUpPair	Cancels an NNM 6.x or 7.x Node Down event with a NNM 6.x or 7.x Node Up event from the same SNMP agent address.
OvApaAggPortConnDownUpPair	Cancels an NNM 6.x or 7.x APA Aggregate Port Connection Down event with an NNM 6.x or 7.x APA Aggregate Port Connection Up event.
OvApaAggPortDegradeNotDegradePair	Cancels an NNM 6.x or 7.x APA Aggregate Port Degraded event with an NNM 6.x or 7.x APA Aggregate Port Not Degraded event on the same interface for the same SNMP agent address.
OvApaAggPortDownUpPair	Cancels of an NNM 6.x or 7.x APA Aggregate Port Down event with an NNM 6.x or 7.x APA Aggregate Port Up event on the same interface for the same SNMP agent address.
OvApaBoardDownUpPair	Cancels an NNM 6.x or 7.x APA Board Down event with an NNM 6.x or 7.x APA Board Up event from the same SNMP agent address.
OvApaConnDownUpPair	Cancels an NNM 6.x or 7.x APA Address Down event with an NNM 6.x or 7.x APA Address Up event on the same address for the same SNMP agent address.
OvApalfDownUpPair	Cancels an NNM 6.x or 7.x APA If Down event with an NNM 6.x or 7.x APA If Up event on the same interface for the same SNMP agent address.
OvApaNodeDownUpPair	Cancels an NNM 6.x or 7.x APA Node Down event with an NNM 6.x or 7.x APA Node Up event from the same SNMP agent address.
OvIfDownUpPair	Cancels an NNM 6.x or 7.x If Down event with an NNM 6.x or 7.x If Up event on the same interface for the same SNMP agent address.
OvNodeDownUpPair	Cancels an NNM 6.x or 7.x Node Down event with an NNM 6.x or 7.x Node Up event from the same SNMP agent address.
RcAggLinkDownUpPair	Cancels an RcAggLinkDown incident with an RcAggLinkUp incident from the same Multi-Link Trunk (MLT) Aggregator ID (from the MIB) and SNMP agent address.
RcChasFanDownUpPair	Cancels an RcChasFanDown incident with an RcChasFanUp incident from the same fan ID (from the MIB) and SNMP agent address.
RcChasPowerSupplyDownUpPair	Cancels an RcChasPowerSupplyDown incident with an RcChasPowerSupplyUp incident from the same power supply ID (from the MIB) and SNMP agent address.
RcSmltIsLinkDownUpPair	Cancels an RcSmltIsLinkDown incident with an RcSmltIsLinkUp incident from the same SNMP agent address.

Name	Description
RcnAggLinkDownUpPair	Cancels an RcnAggLinkDown incident with an RcnAggLinkUp incident from the same Multi-Link Trunk (MLT) Aggregator Link ID (from the MIB) and SNMP agent address.
RcnChasFanDownUpPair	Cancels an RcnChasFanDown incident with an RcnChasFanUp incident from the same fan ID (from the MIB) and SNMP agent address.
RcnChasPowerSupplyDownUpPair	Cancels an RcnChasPowerSupplyDown incident with an RcnChasPowerSupplyUp incident from the same power supply ID (from the MIB) and SNMP agent address.
RcnSmltIsLinkDownUpPair	Cancels an RcnSmltIsLinkDown incident with an RcnSmltIsLinkUp incident from the same SNMP agent address.
SnmpLinkDownUpPair	Cancels an SNMPLinkDown incident with an SNMPLinkUp incident on the same interface for the same SNMP agent address.

To see or modify these incident pair configurations:

1. Navigate to the **Incident Configuration** view.
 - a. In the Workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Incident Configuration** view.
2. Select the **Pairwise Configuration** tab.
3. Select the configuration you want to see or modify, and click  **Open** to see or change the configuration.

In the **Pairwise Configuration** form, click **Help** → **Using the Pairwise Configuration form** for more information.
4. When you are finished, click  **Save and Close** to return to the Incident Configuration form.
5. Click  **Save and Close**. NNM saves your changes.


Prerequisites for Pairwise Configurations

NNMi automatically ensures that the **Source Node** attribute value is identical in both incidents of your defined pair.

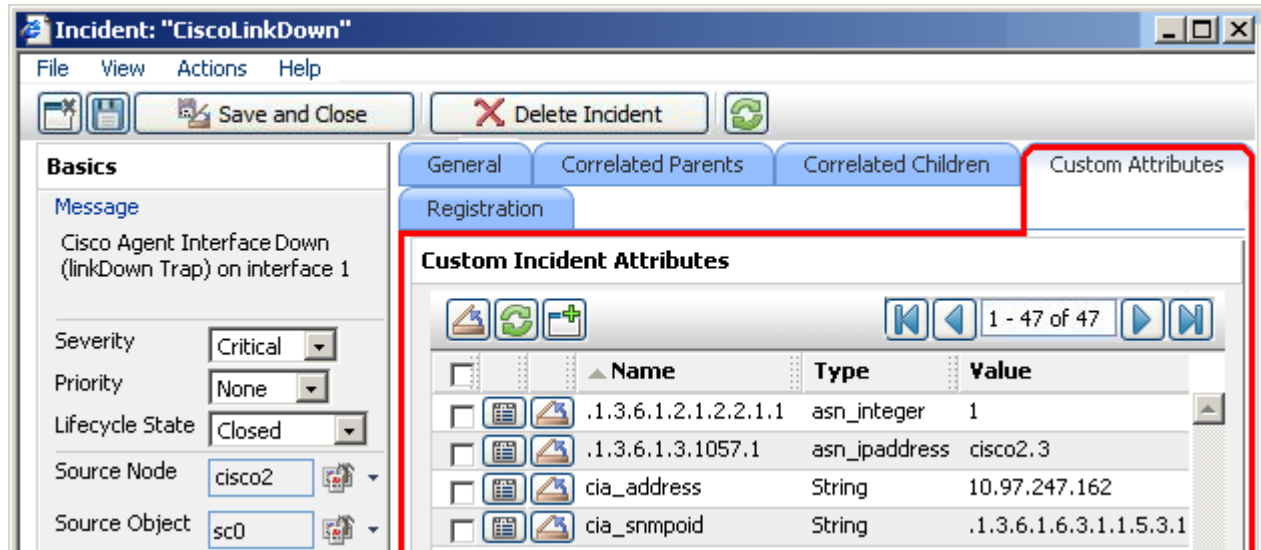
If you need to provide more details to accurately identify the logical pair of incidents (from among all possible incidents related to that source node), complete the Optional step 6 below.

Complete the following steps before attempting to set up a Pairwise Configuration:

1. Identify the two incidents or SNMP traps that consist of the logical relationship that makes the pair.
2. Configure those two incidents or traps within NNMi, if they are not already configured:
 - See ["Incident Configurations Provided by NNMi" \(on page 214\)](#).
 - See ["Configure SNMP Trap Incidents" \(on page 246\)](#).
 - See ["Configure Remote NNM 6.x/7.x Events" \(on page 261\)](#).

3. Generate one of each of the two incidents or SNMP traps so you can see an example of each in one of the NNMi Incident views. See "[Views Provided by NNMi](#)".
4. Select the first sample incident for the pair, and click  Open to display the Incident form.

Navigate to the Custom Attributes tab. These are the custom incident attributes available to use in step 6, below. See "[Custom Incident Attributes Provided by NNMi](#)" (on page 214) for more information about Custom Attributes.






5. Repeat the previous step with the second sample incident for the pair.
6. *Optional.* If both sample incidents have custom attributes, you can refine the match criteria beyond Source Node. Some incident pairs require extensive details to verify an accurate match. See "[Pairwise Configuration Form \(Correlate Pairs of Incidents\)](#)" (on page 279).


Pairwise Configuration Form (Correlate Pairs of Incidents)

Use the Pairwise Configuration to pair the occurrence of one incident with another subsequent incident. See "[About Pairwise Configurations](#)" (on page 276) for more information.



To configure incident pairs:

1. Complete the steps in "[Prerequisites for Pairwise Configurations](#)" (on page 278) so you know exactly which two incidents or traps belong to this logical pair.
2. Navigate to the **Pairwise Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Incident Configuration** view.
 - c. Navigate to the **Pairwise Configuration** tab.
 - d. Do one of the following:
 - To create a new pair configuration, click the  New icon, and continue.





- To edit an existing pair configuration, select a row, and click the  Open icon, and continue.
 - To delete a pair configuration, select a row and click the  Delete icon.
3. Provide the basic definition of the pair of incidents for this correlation (see [table](#)).
 4. NNM automatically ensures that the **Source Node** attribute value is identical in both incidents of your defined pair. Some incident pairs require extensive details to verify an accurate match. If *both sample incidents* have custom incident attributes, you can refine the match criteria beyond Source Node.

Optional. Navigate to the **Pair Items** tab, and provide one or more custom incident attribute sets whose values must match to identify the valid pair of incidents. See "[Pair Item Configuration Form \(Identify Incident Pairs\)](#)" (on page 281). Then, click  **Save and Close** to return to the Pairwise Configuration form.

For example:

 - If you specify a First In Pair and Second In Pair of .1.3.6.1.2.1.2.2.1.1, the first incident's varbind value for the specified OID must match the second incident's varbind value for the specified OID to confirm a match.
 - If you specify two custom attribute sets (one with both First In Pair and Second In Pair set to position 7, and one with both First In Pair and Second In Pair set to position 25), then the values for both custom attributes (varbind position 7 and varbind position 25) in both Incidents must match to confirm the logical pair.
 5. Click  **Save and Close** to return to the Incident Configuration form.
 6. Click  **Save and Close**. NNM saves your changes. The next time the two incidents in this pair are generated, the first one becomes a Child Incident of the second one. See "[About Pairwise Configurations](#)" (on page 276) for an example.

Pairwise Configuration Definition

Attribute	Description
Name	The name is used to identify the pairwise configuration and must be unique. Use a name that will help you to remember the purpose for this pairwise configuration. Maximum length 64 alpha-numeric characters. Periods allowed. No spaces allowed.
Enable	In the Basics group, verify that Enable <input checked="" type="checkbox"/> is selected.
First Incident Configuration	Identify the incident in the pair that would occur first in the logical sequence. Click the  Lookup icon and select  Quick Find . Choose the name of one of the predefined incident configurations. If you cannot find it, see: <ul style="list-style-type: none"> • See "Incident Configurations Provided by NNMi" (on page 214). • See "Configure SNMP Trap Incidents" (on page 246). • See "Configure Remote NNM 6.x/7.x Events" (on page 261).
Second Incident Configuration	Identify the incident in the pair that would occur second in the logical sequence. Click the  Lookup icon and select  Quick Find . Choose the name of one of the predefined incident configurations. If you cannot find it, see: <ul style="list-style-type: none"> • See "Incident Configurations Provided by NNMi" (on page 214). • See "Configure SNMP Trap Incidents" (on page 246).

Attribute	Description
	<ul style="list-style-type: none"> See "Configure Remote NNM 6.x/7.x Events" (on page 261).
Description	<p><i>Optional.</i> Explain the purpose of your pairwise configuration for future reference.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p>


Pair Item Configuration Form (Identify Incident Pairs)

NNMi automatically ensures that the **Source Node** attribute value is identical in both incidents in your defined pair. Some incident pairs require extensive details to verify an accurate match. If *both sample incidents* have custom incident attributes, you can use the Pair Item Configuration form to refine the match criteria beyond Source Node.

Specify *attributes whose values must match* before the identity of the incident pair is confirmed.

You can use any Custom Incident Attributes (CIAs) displayed on the [Incident form](#) of the two incidents you are associating into a logical pair. The group of available CIAs depends on which incidents you select. There are two categories of possible CIAs:








- SNMP trap varbinds identified by the Abstract Syntax Notation value (ASN.1) or position. For example, a varbind OID of .1.3.6.1.2.1.2.2.1.1 or a position number of 25.
- Custom attributes provided by NNMi (Name = cia_*). See ["Custom Incident Attributes Provided by NNMi"](#) (on page 214).

The group of available CIAs depends on which incident you are configuring (for example, CiscoLinkDown). To see which CIAs are available, navigate to an Incident view, select an instance of that incident-type, click the  Open icon and navigate to the Custom Attributes tab. The items listed in the table are the CIAs for that particular incident-type. For example, all CiscoLinkDown incidents would have the same group of CIAs shown in the illustration below.

The screenshot shows the 'Incident: "CiscoLinkDown"' window. The 'Custom Attributes' tab is active, displaying a table of Custom Incident Attributes (CIAs). The table has columns for Name, Type, and Value. The attributes listed are:

Name	Type	Value
.1.3.6.1.2.1.2.2.1.1	asn_integer	1
.1.3.6.1.3.1057.1	asn_ipaddress	cisco2.3
cia_address	String	10.97.247.162
cia_snmpoid	String	.1.3.6.1.6.3.1.1.5.3.1

To configure which attributes NNMi uses to verify incident identity:

1. Complete the steps in "[Prerequisites for Pairwise Configurations](#)" (on page 278) so your choices for this Item Pair configuration are displayed in the NNMi console. (Two Incident forms should be open before you proceed to step 2.)
2. Navigate to the **Pair Item Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Incident Configuration** view.
 - c. Navigate to the **Pairwise Configuration** tab.
 - d. Do one of the following:
 - To create a new pair configuration, click the  New icon.
 - To edit an existing pair configuration, select a row, and click the  Open icon.
 - e. On the **Pairwise Configuration** form, locate the **Pair Items** tab.
 - f. Do one of the following:
 - To create a new pair item configuration, click the  New icon.
 - To edit an existing pair item configuration, select a row, and click the  Open icon.
3. Specify the attributes you want NNMi to use to confirm the identity of the pair of incidents (see [table](#)).
4. Click  **Save and Close** to return to the Pairwise form.
5. Repeat steps 1-3 any number of times. The incidents must pass all Pair Item criteria, plus have identical Source Node attribute values.
6. Click  **Save and Close** to return to the Incident Configuration form.
7. Click  **Save and Close**. NNMi saves your changes.

Pair Item Configuration

Attribute	Description
First In Pair	<p>Type the specification required to confirm the identify of the first incident in this logical pair of incidents. Provide one of the following:</p> <ul style="list-style-type: none"> • The SNMP trap varbind Abstract Syntax Notation value - ASN.1 (OID) • The SNMP trap varbind position number <p>Caution: varbind position numbers are not visible in the table on the Incident form's Custom Attributes tab. And the rows in that table are sorted by the visible column headings and are not in varbind position order. You must access the vendor-supplied information in the underlying MIB file to determine the appropriate position number for any particular varbind.</p> <ul style="list-style-type: none"> • The Custom Attribute Name value (see "Custom Incident Attributes Provided by NNMi" (on page 214) or the Name column in the table on the Incident Form: Custom Attributes Tab of the Incident you are configuring as a member of this logical pair).
Second In Pair	<p>Type the specification required to confirm the identify of the second incident in this logical pair of incidents. Provide one of the following:</p> <ul style="list-style-type: none"> • The SNMP trap varbind Abstract Syntax Notation value - ASN.1 (OID) • The SNMP trap varbind position number

Attribute	Description
	<p>Caution: varbind position numbers are not visible in the table on the Incident form's Custom Attributes tab. And the rows in that table are sorted by the visible column headings and are not in varbind position order. You must access the vendor-supplied information in the underlying MIB file to determine the appropriate position number for any particular varbind.</p> <ul style="list-style-type: none">The Custom Attribute Name value (see "Custom Incident Attributes Provided by NNMi" (on page 214)) or the Name column in the table on the Incident Form: Custom Attributes Tab of the Incident you are configuring as a member of this logical pair).

Related Topics

["Incident Pair \(Pairwise\) Configurations Provided by NNM" \(on page 276\)](#)

Configure an Action for an Incident

You can configure actions to automatically run at any point in the incident lifecycle. For example, you can configure an action to occur when an incident of the type you are configuring is generated (**Registered**). When an incident is generated, you might want to automatically open a trouble ticket or send email or page your network operator. After the incident is **Closed**, you might want to automatically close the trouble ticket.



You can configure actions for incidents generated from SNMP traps, NNM 6.x or 7.x events, and the NNMi management events. Any time an incident configuration changes, the action directory is re-scanned and any Jython files are reloaded to the NNMi database. See ["Lifecycle Transition Action Form" \(on page 284\)](#) for more information about the actions directory.





Tip: Copy any required Jython files to the NNMi actions directory before you configure an incident action. New or updated actions are loaded into NNMi only when an incident configuration is updated or created. See ["Lifecycle Transition Action Form" \(on page 284\)](#) for the location of the NNMi action directory.

When the action runs, output is logged to the `eventActions.*.*.log` file. See ["Verify that NNMi Services Are Running" \(on page 28\)](#) for more information about log files and where they are located.

Note: Do not use the Node Up Incident configuration to configure incident actions. Use the Node Down incident configuration and the Closed Lifecycle State. See ["Management Event Configurations Provided by NNMi" \(on page 229\)](#) for more information about the Node Up and Node Down incident configurations.

To configure an automatic action for an incident:

- Navigate to the **Action Configuration** tab.
 - From the workspace navigation panel, select the **Configuration** workspace.
 - Select **Incident Configuration**.
 - Select the **SNMP Trap Configuration, Remote NNM 6.x/7.x Event Configuration, or Management Event Configuration** tab.
 - Select the **Action Configuration** tab.
- From the **Lifecycle Actions** table toolbar, do one of the following:
 - To create an Action configuration, click the  New icon, and continue.
 - To edit an Action configuration, click the  Open icon, and continue.







- To delete an Action configuration, click the  Delete icon.
- 3. In the "[Lifecycle Transition Action Form](#)" (on page 284), provide the required information.
- 4. Click  **Save and Close** to return to the **SNMP Trap, Remote 6.x/7.x, or Management Event Configuration** form.
- 5. Click  **Save and Close** to return to the **Incident Configuration** form.
- 6. Click  **Save and Close** to save your changes.

The next time the lifecycle changes, NNMi launches the action associated with the lifecycle for the incident of that type .

Lifecycle Transition Action Form

Use this form to enter the command you want to run when an incident of the type you are configuring is at a particular lifecycle state. For example, when an incident is generated (**Registered**), you might want to automatically open a trouble ticket or email or page your network operator.

To configure an action for an incidents:

1. Navigate to the **Lifecycle Transition Actions** form:
 - a. From the workspace navigation pane, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Select the **SNMP Trap Configuration, Remote NNM 6.x/7.x Event Configuration, or Management Event Configuration** tab.
 - d. Select the **Action Configuration** tab.
 - e. From the **Lifecycle Transition Action** table toolbar, do one of the following:
 - To create an Action configuration, click the  New icon, and continue.
 - To edit an Action configuration, click the  Open icon, and continue.
 - To delete an Action configuration, click the  Delete icon.
 2. Make your configuration choices (see [table](#)).
- Note:** NNMi reloads the configuration information anytime the incident configuration is changed.
3. Click  **Save and Close** to return to the **SNMP Trap, Remote 6.x/7.x, or Management Event Configuration** form.
 4. Click  **Save and Close** to return to the **Incident Configuration** form.
 5. Click  **Save and Close** to save your changes.

Create Action Attributes

Attribute	Description
Lifecycle State	Select a lifecycle state from the drop-down menu. Possible values are: Registered, In Progress, Completed, and Closed .
Command Type	If you provided a Jython command, select Jython from the drop-down list. If you are using an executable or bat file, select ScriptOrExecutable from the drop-down list.

Attribute	Description
Command	<p>Enter one of the following:</p> <ul style="list-style-type: none"> • A Jython method with the required parameters • Executable command for the current operating system with the required parameters. <p>When entering a command value, note the following:</p> <ul style="list-style-type: none"> • Verify that you do not have two Jython methods with the same name. Otherwise, NNMi is not able to tell which is the correct method to load. • You can use the same Jython method for more than one incident configuration. • Python files or other executable scripts need to reside in the following directory: <p>Windows:</p> <pre><drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\actions</pre> <p><drive> is the drive on which NNMi is installed.</p> <p>UNIX:</p> <pre>/var/opt/OV/shared/nnm/actions</pre> <p>Note: Use absolute paths to executables instead of relying on the PATH variable as it might not be set correctly.</p> <ul style="list-style-type: none"> • NNMi provides a set of parameters that can pass attribute values from an incident configuration. See "Valid Parameters for Configuring Incident Actions" (on page 285) for more information. <p>See "Example Jython Methods Provided by NNMi" (on page 290) for a description of example Jython methods provided by NNMi.</p>

Valid Parameters for Configuring Incident Actions

When configuring incident actions, you may want to use incident information as part of the action. NNMi provides the following parameter values. Use these parameters as variables in your Jython methods or executable files.

Tip: See the [Using the Incident Form](#) for more information about the parameter values.

Note: NNMi stores varbind values as custom incident attributes (CIAs).

See "[Lifecycle Transition Action Form](#)" (on page 284) for more information about configuring incident actions.

Valid Parameters Visible From an Incident's Form

Parameter Value	Description
\$category, \$cat	Value of the Category attribute in the Incident form.
\$count, \$cnt	Value representing the number of Custom Incident Attributes that appear in the Incident form.
\$family, \$fam	Value from the Family attribute in the Incident form.

Parameter Value	Description
\$firstOccurrenceTime, \$fot	Value from the First Occurrence Time attribute in the incident form.
\$lastOccurrenceTime, \$lot	Value from the Last Occurrence Time attribute in the incident form.
\$lifecycleState, \$lcs	Value from the Lifecycle State attribute in the Incident form.
\$name	Value of the Name attribute from the incident configuration.
\$nature, \$nat	Value from the Nature attribute in the Incident form.
\$origin, \$ori	Value from the Origin attribute in the Incident form.
\$originOccurrenceTime, \$oot	Value from the Origin Occurrence Time attribute in the incident form.
\$priority, \$pri	Value from the Priority attribute in the Incident form.
\$severity, \$sev	Value of the Severity attribute of the Incident form.

Valid Parameters Not Visible From an Incident's Form

Parameter Value	Description
\$id	Unique Object Identifier attribute value for the incident (unique across the entire NNMi Database).
\$ifAlias, \$ifa	Value from the IfAlias attribute of the Interface form.
\$firstOccurrenceTimeMS, \$fms	Value from the First Occurrence Time attribute in the incident form, converted to milliseconds (measured since January 1, 1970, 00:00:00 GMT - Greenwich Mean Time).
\$lastOccurrenceTimeMS, \$lms	Value from the Last Occurrence Time attribute in the incident form, converted to milliseconds (measured since January 1, 1970, 00:00:00 GMT - Greenwich Mean Time).
\$managementAddress, \$mga	Value from the Management Address attribute of the associated Node form or SNMP Agent form.
\$oid	Value of the unique object identifier (oid) for the incident configuration that originated from either an SNMP trap, Management Event, or Remote NNM 6.x or 7.x event.
\$otherSideOfConnection, \$osc	<p>If the incident's Source Node is part of a Layer 2 connection, this attribute is the following combination of values for the node and one of its interfaces on the other side of the Layer 2 connection:</p> <p>The fully-qualified DNS name of the node appended with the interface Name in the following format: <i><fully-qualified DNS name>[interface_name]</i></p>

Parameter Value	Description
\$otherSideOfConnectionIfAlias, \$oia	If the incident's Source Node is part of a Layer 2 connection, this attribute is the value of the ifAlias of one of the interfaces on the other side of the Layer 2 connection.
\$otherSideOfConnectionManagementAddress, \$oma	If the incident's Source Node is part of a Layer 2 connection, this attribute is the value of the Management Address of a node on the other side of the Layer 2 connection.
\$originOccurrenceTimeMS, \$oms	Value from the Origin Occurrence Time attribute in the incident form, converted to milliseconds (measured since January 1, 1970, 00:00:00 GMT - Greenwich Mean Time).
\$sourceNodeUuid, \$snu	Universally Unique Object Identifier attribute value of the source node object for the incident (unique across all databases). This identifier distinguishes the source node object instance from all other node objects.
\$sourceNodeName, \$snn	Value from the Name attribute of the source Node form.
\$sourceNodeLongName, \$sln	The fully-qualified DNS name as displayed in the Host-name attribute of the incident's Source Node's form.
\$sourceObjectClass, \$soc	Value of the object class for the object you want to include. Use this parameter when you need to request more details of a class of objects through a web service. Examples of object classes include: <code>com.hp.ov.nms.model.core.Interface</code> and <code>com.hp.ov.nms.model.snmp.SnmpAgent</code> .
\$sourceObjectName, \$son	Value from the Name attribute of the source object. For example, an interface object is named according to the MIB ifName. Each ifName varies according to the vendor's conventions. Using the name 4/1 as an example, 4 represents the board number and 1 represents the port number.
\$sourceObjectUuid, \$sou	Universally Unique Object Identifier attribute value of the source object for the incident (unique across all databases). This identifier distinguishes the source object instance from all other similar object instances..
\$uuid	Universally Unique Object Identifier attribute value of the incident (unique across all databases). This identifier distinguishes the incident object instance from all other incident objects.

Valid Parameters Established in Custom Incident Attributes

Parameter Value	Description
\$<position_number>	Value of the custom incident attribute (CIA) position number for any CIA that originated from a varbind or was added by NNMi. For example, to indicate you want to use the varbind in position 1, enter: \$1 NNMi stores varbind values as Custom Incident Attributes. If you know the varbind position number, use this parameter.
\$<CIA_name>	Value of the name that is used for the custom incident attribute. For example, \$mycompany.mycia. NNMi provides CIA values for configuring Management Events. See Custom Incident Attributes Provided by NNMi for more information about custom incident attributes.
\$<CIA_oid>	Value of the object identifier for any custom incident attribute that originated as a varbind. For example, \$.1.3.6.1.6.3.1.1.5.1. Use this parameter when you are not certain of a custom incident attribute (varbind) position number.
\$*	Used to indicate you want all of the custom incident attribute values originating as varbinds, to be passed to the action configuration. Each varbind is returned in the following format: \$<CIA_name>:<CIA_value> in which the custom incident attribute name appears followed by the custom incident attribute value.

The function described in the following table replaces the specified numeric value with the associated text value stored in the CIA.

Note: The associated MIB must have been loaded using the [nnmloadmib.ovpl](#) command.

Functions to Generate Values Within Incident Messages

Function	Description
\$text(\$<position_number>)	The <position_number> argument specifies the numeric value of the custom incident attribute (CIA) position number for any CIA that originated from a varbind or was added by NNMi. For example, to indicate you want to use the varbind in position 1, enter: \$1. After the function runs, NNMi replaces the numeric value with the text value stored in the CIA. Note: If a text value is not available, NNMi returns the numeric value.
\$text(\$<CIA_oid>)	The <CIA_oid> argument specifies the object identifier for any custom incident attribute that originated as a varbind. For example, \$.1.3.6.1.6.3.1.1.5.1. Use this argument to the \$text function when you are not certain of a custom incident attribute (varbind) position number. After the function is run, NNMi replaces the numeric value with the text value stored in the CIA. Note: If a text value is not available, NNMi returns the numeric value.

Handling Special Characters in Action Arguments

In some cases, NNMi requires or inserts double quotes or escape characters in action arguments. The following table describes the circumstances around the valid uses of double quotes.

Handling Special Characters in Action Arguments

Circumstance	Result
<p>If the following special characters are part of a CIA value requested as an argument to an action command: , ; & > < (space) =</p>	<p>Windows:</p> <p>The CIA value (containing the special character) must be wrapped in double quotes. For example, to request the CIA having a <i>name</i> value of Hello;World, the argument must enclose "Hello;World" in quotes.</p>
<p>Request all available CIA name/value pairs for a particular incident</p> <p>\$*</p>	<p>The \$* argument returns a parsed string. For this example, the available CIA name/value pairs are:</p> <ul style="list-style-type: none"> • \$1 = 123 • \$com.mycompany.mycia = 012345 • \$.1.3.6.1.2.1.2.2.1.1 = 1007 <p>Example Command</p> <pre>echoScript.bat \$*</pre> <p>NNMi returns the following string in response to the command:</p> <ul style="list-style-type: none"> • Windows: "1: 123, com.mycompany.mycia:012345, .1.3.6.1.2.1.2.2.1.1:1007" • UNIX: 1: 123, com.mycompany.mycia:012345, .1.3.6.1.2.1.2.2.1.1:1007
<p>Request specific CIA values as an argument to an action command</p> <p>\$<CIA name, position, or OID></p>	<p>To request specific CIA values, use the \$ followed by the CIA name</p> <p>Example Command</p> <pre>echoScript.bat \$1 \$com.mycompany.mycia \$.1.3.6.1.2.1.2.2.1.1</pre> <p>For this example, the CIA name/value pairs are:</p> <ul style="list-style-type: none"> • \$1 = 123 • \$com.mycompany.mycia = 012345 • \$.1.3.6.1.2.1.2.2.1.1 = 1007 <p>NNMi returns the following string in response to the command:</p> <ul style="list-style-type: none"> • Windows: 123 012345 1007 • UNIX: 123 012345 1007

Circumstance	Result
If an invalid CIA name, position, or OID is requested as an argument to an action command	<p>If the trap or event does not contain one or more of the requested CIAs, NNMi passes error messages as arguments.</p> <p>UNIX:</p> <pre>Invalid or unknown cia position 1 Invalid or unknown cia com.mycompany.mycia Invalid or unknown cia .1.3.6.1.2.1.2.2.1.1</pre> <p>Windows: NNMi encloses each CIA value in double quotes.</p> <pre>Invalid or unknown cia "position 1" Invalid or unknown cia "com.mycompany.mycia" Invalid or unknown cia ".1.3.6.1.2.1.2.2.1.1"</pre>
Use \$* in your incident action scripts	<p>UNIX:</p> <p>It is recommended that you do not use \$* (shell variable substitution) in your incident action scripts. If you do use \$* within the shell script, specifying \$* expands into the arguments and are rescanned. This means that blanks in arguments will result in multiple arguments.</p> <p>If you want to use shell variable substitution, use the "\$@" instead so that blanks in arguments are ignored.</p>
Use arguments to Jython methods	<p>Enclose any argument that is not preceded with a "\$" (dollar sign) in double quotes. For example, <code>jythonMethod(\$Severity, "Hello; World")</code>.</p>

Example Jython Methods Provided by NNMi

NNMi provides a set of example Jython methods you can use when configuring actions for incidents. These example files reside in the required directory as described in "[Lifecycle Transition Action Form](#)" (on page 284). Also see "[Lifecycle Transition Action Form](#)" (on page 284) for more information about creating incident actions.

Note: The argument values, such as *arg1*, and *arg2*, can be any valid parameter as described in "[Valid Parameters for Configuring Incident Actions](#)" (on page 285).

Example Jython Methods Provided by NNMi

File Name	Command Attribute Value	Description
testPrint.py	testPrint_Registered()	Displays the incident Lifecycle State specified by the method name.
testPrint.py	testPrint_InProgress()	Displays the incident Lifecycle State specified by the method name.
testPrint.py	testPrint_Completed()	Displays the incident Lifecycle State specified by the method name.
testPrint.py	testPrint_Closed()	Displays the incident Lifecycle State specified by the method name.

File Name	Command Attribute Value	Description
testPrintArgs.py	testPrintArgs(<i>arg1</i> , <i>arg2</i> , ...)	Displays the specified argument values.
testPrintStdoutStderr.py	testPrint_StdoutStderr()	Displays a message generated by the method to standard out and standard error.
testPrintThrowException.py	testPrint_Throw-Exception()	Generates an SQLException.
testPrintWithSyntaxError.py	testPrint_With-SyntaxError(num)	Generates a syntax error.

The output generated from these methods is written to the event action log. You can find the event action log in the following directory:

Windows:

```
<drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\log\nnm
```

UNIX:

```
/var/opt/OV/log/nnm
```

Configure Diagnostics for an Incident (NNM iSPI NET)

*NNM iSPI NET*Only: NNMi provides a set of Diagnostics (Flow Definitions) that can be run on the Source Node each time an incident reaches a specified Lifecycle State (for example, as soon as an incident becomes Registered).

These Diagnostics are sets of automated commands specific to one or more device types, including Cisco routers and switches, Cisco switch/routers, and Nortel switches.









See ["Configure Device Profiles" \(on page 95\)](#) for more information about device types . See ["Diagnostics \(Flows\) Provided by NNMi \(NNM iSPI NET\)" \(on page 295\)](#) for more information about the Diagnostics provided by NNMi.

Note: Do not use the Node Up Incident configuration to configure Diagnostics. Use the Node Down incident configuration and the Closed Lifecycle State. See ["Management Event Configurations Provided by NNMi" \(on page 229\)](#) for more information about the Node Up and Node Down incident configurations.

Configuring NNMi to automatically gather diagnostic information about the Source Node whenever a specified incident reaches a selected Lifecycle State is a two-step process:

1. Specify the Node Group using the ["Configuration Per Node Group Form \(NNM iSPI NET\)" \(on page 292\)](#)
2. Specify the Diagnostics (Flow Definitions) using the ["Diagnostic Selection Form \(NNM iSPI NET\)" \(on page 293\)](#).

Configuration Per Node Group Form (NNM iSPI NET)

1. Navigate to the **Configuration Per Node Group** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
 - c. Select the **SNMP Trap Configuration (by OID)**, **SNMP Trap Configuration (by Name)**, **Remote NNM 6.x/7.x Event Configuration**, or **Management Event Configuration** tab.
 - d. Do one of the following:
 - To create an Incident configuration, click the  New icon, and continue.
 - To edit an Incident configuration, click the  Open icon, and continue.
 - e. Navigate to **Configuration Per Node Group** tab, and do one of the following:
 - To create Configuration per Node Group settings, click the  New icon, and continue.
 - To edit Configuration per Node Group settings, click the  Open icon, and continue.
 - To delete Configuration per Node Group settings, click the  Delete icon.
2. Provide the required information (see [table](#)).
3. Navigate to the **Diagnostics Selections** tab. Provide the required information in the "[Diagnostic Selection Form \(NNM iSPI NET\)](#)" (on page 293).
4. Click  **Save and Close** to return to the **SNMP Trap, Remote 6.x/7.x, or Management Event Configuration** form.
5. Click  **Save and Close** to return to the **Incident Configuration** form.
6. Click  **Save and Close** to save your changes.

After configuring the Diagnostic for the incident and Node Group, the Diagnostic must match the following criteria before it runs:

- The Source Node must be in the specified Node Group.
- The Diagnostic must be valid for the Source Node. (For example, only Nortel switch Diagnostics are run on Nortel switches.)
- The incident's current lifecycle state must match the configured lifecycle state. (For example, configure an Incident to run a specified Diagnostic when the incident is Closed. If the current Incident's Lifecycle State is Closed, NNMi runs that Diagnostic.)






Note: If a Source Node is in more than one Node Group, the Diagnostic is only run on the node the first time NNMi finds a match for that Source Node based on the configuration Ordering field.

If these criteria are met, NNM iSPI NET runs the Diagnostics and generates Diagnostic reports to help you solve the problem on the Source Node.

After you configure Diagnostics for an incident, you can also run Diagnostics and access the Diagnostics reports on demand, using **Actions** → **Run Diagnostics** in the Incident form. The same criteria apply (see the [criteria](#) above). See [Incident Form: Diagnostics Tab](#) for more information.






You can also run and access Diagnostics reports from a Node form. See [Node Form: Diagnostics Tab](#) for more information.








Diagnostic Settings Attributes

Attribute	Description
Node Group	<p>Specifies the Node Group to which the Source Node must belong. Click the  Lookup icon and choose one of the following options:</p> <ul style="list-style-type: none">  Quick View to view summary information for the displayed Node Group name  Quick Find to view the list of possible Node Groups  Open to display the Node Group form  New to create a new Node Group
Ordering	<p>Specifies the priority order NNMi should use when a node is a member of more than one Node Group. NNMi runs diagnostics on the node using the lowest applicable Ordering number.</p> <p>For example, if a node belongs to a Node Group with an Ordering number of 4 and to a Node Group with the Ordering number of 11, NNMi runs the diagnostics using the Node Group with the Ordering number of 4. NNMi does not run Diagnostics on the node when NNMi accesses the Node Group with an Ordering number of 11.</p>
Enable	<p>Specifies whether to enable the Diagnostics configuration.</p> <p>To enable the Diagnostics selection, select the Enable <input checked="" type="checkbox"/> checkbox.</p> <p>To disable the Diagnostics selection, clear the Enable <input type="checkbox"/> checkbox .</p>

Diagnostic Selection Form (NNM iSPI NET)

To configure Diagnostics to run on a Source Node for an incident:

- Navigate to the **Diagnostics Selection** form.
 - From the workspace navigation panel, select the **Configuration** workspace.
 - Select **Incident Configuration**.
 - Select the **SNMP Trap Configuration (by OID)**, **SNMP Trap Configuration (by Name)**, **Remote NNM 6.x/7.x Event Configuration**, or **Management Event Configuration** tab.
 - Do one of the following:
 - To create an Incident configuration, click the  New icon, and continue.
 - To edit an Incident configuration, select the Incident configuration, click the  Open icon, and continue.
 - Navigate to **Configuration Per Node Group** tab, and do one of the following:
 - To create a Configuration per Node Group, click the  New icon, and continue.
 - To edit a Configuration per Node Group, select the Configuration per Node Group setting, click the  Open icon, and continue.
 - To delete a Configuration per Node Group, select the Configuration per Node Group setting and click the  Delete icon.

- f. Navigate to the **Diagnostic Selection** tab, and do one of the following:
 - To create a Diagnostic Selection setting, click the  New icon, and continue.
 - To edit a Diagnostic Selection setting, select the Diagnostic Selection setting, click the  Open icon, and continue.
 - To delete a Diagnostic Selection setting, select the Diagnostic Selection setting and click the  Delete icon.
2. Provide the required information (see [table](#)).
3. Click  **Save and Close** to return to the **Configuration per Node Group** form.
4. Click  **Save and Close** to return to the **SNMP Trap, Remote 6.x/7.x, or Management Event Configuration** form.
5. Click  **Save and Close** to return to the **Incident Configuration** form.
6. Click  **Save and Close** to save your changes.

After you configure the Diagnostic for the incident and Node Group, the Diagnostic must match the following criteria before the Diagnostic runs:

- The Source Node must be in the specified Node Group.
- The Diagnostic must be valid for the Source Node. (For example, only Nortel switch Diagnostics are run on Nortel switches.)
- The incident's current lifecycle state must match a lifecycle state for which it was configured. (For example, if you configure the Incident to run a specified Diagnostic when the incident is Closed, then if the current Incident's Lifecycle State is Closed, NNMi runs that Diagnostic.)




Note: If a Source Node is in more than one Node Group, the Diagnostic is only run on the node the first time NNMi finds a match for that Source Node based on the configuration Ordering field.

If these criteria are met, NNM iSPI NET runs the Diagnostics and generates Diagnostic reports to help you solve the problem on the Source Node.

After you configure Diagnostics for an incident, you can also run Diagnostics and access the Diagnostics reports on demand, using **Actions** → **Run Diagnostics** in the Incident form. The same criteria apply (see the [criteria](#) above). See [Incident Form: Diagnostics Tab](#) for more information.

You can also run and access Diagnostics reports from a Node form. See [Node Form: Diagnostics Tab](#) for more information.

Diagnostic Settings Attributes

Attribute	Description
Flow Definition	Select the Diagnostic (Flow Definition) you want to use for the specified Node Group. Click the  Lookup icon and choose one of the following options: <ul style="list-style-type: none">•  Quick View to view summary information for the Flow Definition name displayed.•  Quick Find to view the list of possible diagnostic Flow Definitions. NNMi provides diagnostics for the following types of devices: <ul style="list-style-type: none">■ Cisco switch■ Cisco router■ Cisco switch/router

Attribute	Description
	<ul style="list-style-type: none"> ■ Nortel switch <p>See "Diagnostics (Flows) Provided by NNMi (NNM iSPI NET)" (on page 295) for more information about the diagnostics provided and the devices to which they apply.</p>
Lifecycle State	<p>Select the Incident's Lifecycle State you want to use. Possible values include:</p> <ul style="list-style-type: none"> • Registered • In Progress • Completed • Closed <p>See About the Incident Lifecycle for more information about Lifecycle State.</p> <p>When the Incident is set to this Lifecycle State, the selected Diagnostics (Flow Definitions) is automatically run on each applicable Source Node in the specified Node Group.</p>

Diagnostics (Flows) Provided by NNMi (NNM iSPI NET)

Diagnostics (Flows) are sets of automated commands specific to one or more device types. You can associate these Diagnostics with specific incident configurations. After you associate a Diagnostic with an incident configuration and specify the Lifecycle State for which the Diagnostic should run, the Diagnostic automatically runs on the Source Node for the incident whenever the specified Lifecycle State is reached. See ["Configure Diagnostics for an Incident \(NNM iSPI NET\)" \(on page 291\)](#) for more information.

NNMi also associates these Diagnostics with each node to which the Diagnostics apply. To view the Diagnostics invoked for each node, open the Node form for any node of interest. See [Node Form: Diagnostics Tab](#) for more information.

NNMi provides Diagnostics (Flows) for the following device types:

- [Cisco router](#)
- [Cisco switch](#)
- Cisco switch/router (see [Cisco router](#) and [Cisco switch](#))
- [Nortel switch](#)

Cisco Router Diagnostics (Flow Definitions) Provided by NNMi

Name	Description
Cisco Router Baseline Information	<p>Uses a series of show commands to determine the current configuration of a Cisco router. It first displays the router's and NNMi management server's current times. Next, it invokes a series of commands on the router and formats these results on the summary page. Click here for a list of the commands included in this Diagnostic.</p> <pre>show version show protocol show interface summary show ip route</pre>

Name	Description
	<pre>show ip protocol show ip traffic show vlans show cdp show cdp entry show cdp neighbors show log show stacks</pre>
Cisco Show IP Route	Obtains routing information using the <code>show ip route</code> command.
Cisco Route To Node Diagnostic	<p>Note: This Diagnostic Flow is not associated with an NNMi incident or node object and can only be run from Operations Orchestration Central's Flow Library. Before the Diagnostic runs, you are prompted for access information for the source router and target device node.</p> <p>Determines failures of either ping or traceroute to a target node. Uses the router to perform a ping and a traceroute to a target node.</p> <p>Click here for a list of commands included in this Diagnostic</p> <pre>ping target traceroute target</pre>
Cisco Interface Diagnostic	<p>Performs a number of diagnostic checks on a specified interface on the Cisco router. Diagnostics performed include whether the link is Down while the interface is Up. The following error counts are checked:</p> <ul style="list-style-type: none"> • Input errors • CRC errors • Frame errors • Overrun errors • Ignored errors

Cisco Switch Diagnostics (Flow Definitions) Provided by NNMi

Name	Description
Cisco Switch Baseline Information	<p>Uses a series of show commands to determine the current configuration of a Cisco switch. It first displays the switch's and NNMi management server's current times. Next, it invokes a series of commands on the switch and formats these results on the summary page. Click here for a list of the commands included in this Diagnostic.</p> <pre>show version show protocol</pre>

Name	Description
	<pre>show interface summary show vlans show cdp show cdp entry show cdp neighbors show log show stacks</pre>
Cisco Switch Spanning Tree Base-line	<p>Gathers spanning tree protocol and port information from the Cisco switch. The commands run depend on the device's operating system:</p> <p>IOS: show spanning-tree brief</p> <p>CATOS; show spantree</p>

Nortel Switch Diagnostics (Flow Definitions) Provided by NNMi


Name	Description
Nortel Port Diagnostic	<p>Determines statistics, including rate-limit and usage for a specified port on a Nortel switch. This Diagnostic detects rate limit, reception and transmission errors. Similar to Cisco Interface Diagnostic, this flow identifies the following types of errors on the identified port:</p> <ul style="list-style-type: none"> • FCS errors • Undersized packets • Oversized packets • Collisions • Single collisions • Multiple collisions • Excessive collisions • Deferred packets • Late collisions
Nortel Route to Node Diagnostic	<p>Note: This Diagnostic Flow is not associated with an NNMi incident or node object and can only be run from Operations Orchestration Central's Flow Library. Before the Diagnostic runs, you are prompted for access information for the source router and target device node.</p> <p>Determines failures of either ping or traceroute to a target node.</p> <p>Click here for a list of commands included in this Diagnostic</p> <pre>ping target traceroute target</pre>

Name	Description
Nortel Switch Baseline	Determines the configuration of a Nortel switch. It first displays the switch's and NNMi management server's current times. Next, it invokes a series of commands on the switch and formats the results on the summary page. Click here for a list of commands included in this Diagnostic <code>show sys-info</code> <code>show interface</code> <code>show logging config</code> <code>show ssh global</code> <code>show stack-info</code> <code>send show rate-limit</code> <code>send show vlan</code>
Nortel Switch Spanning Tree Baseline	Gathers spanning tree protocol and port information from the Nortel switch. Click here for a list of commands included in this Diagnostic <code>show spanning-tree config</code> <code>show spanning-tree port</code> <code>show spanning-tree vlans</code>

Generate Interface Disabled Incidents

By default, NNMi *does not generate* an incident for interfaces whose **Administrative Status** is set to **Down**. If you want NNMi to generate incidents for these disabled interfaces, use the following procedures.

To enable the Interface Disabled Management Event incident configuration:


1. Navigate to the Incident Configuration view.
 - a. In the Workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **Incident Configuration** view.
2. Select the **Management Event Configuration** tab.
3. Click the  Open icon in the row that represents the Interface Disabled configuration.
4. Click Enable .

Generate Performance Threshold Incidents (NNM iSPI for Performance)

NNMi can generate incidents related to performance thresholds. NNMi does not generate threshold incidents until the NNMi administrator configures the performance thresholds and enables the performance incidents.

To configure NNMi to generate performance threshold incidents:

Prerequisite: Enable performance polling and configure the performance thresholds. See "[Configure Threshold Monitoring for Interfaces \(NNM iSPI for Performance\)](#)" (on page 162) for more information.

1. Navigate to the **Incident Configuration** form:
 - a. From the workspace navigation pane, select the **Configuration** workspace.
 - b. Select **Incident Configuration**.
2. Select the **Management Event Configuration** tab.
3. Click the  Open icon that precedes the performance threshold incident configuration that you want to enable

Select from the following threshold incident configurations:

InterfaceInputErrorRateHigh

InterfaceInputDiscardRateHigh

InterfaceInputUtilizationHigh

InterfaceInputUtilizationLow

InterfaceInputUtilizationNone



InterfaceOutputDiscardRateHigh

InterfaceOutputErrorRateHigh

InterfaceOutputUtilizationHigh

InterfaceOutputUtilizationLow

InterfaceOutputUtilizationNone

4. Enable the threshold incident by checking **Enable** in the **Basics** group of the **Management Event** form.
5. Click  **Save and Close** to return to the **Incident Configuration** form.
6. Click  **Save and Close** to save your changes.
7. Repeat steps 3 through 6 for each configuration you want to use.

The NNM iSPI for Performance now records the number and frequency of threshold related incidents (exceptions). The NNM iSPI for Performance provides reports to help you establish the root cause of network problems. Access the NNM iSPI for Performance reports with **Actions** → **Reporting - Report Menu** in the incident, node, or interface views and forms. (See [NNM iSPI for Performance Actions](#).)

Use HP Route Analytics Management System Data in Path View (NNMi Advanced)

HP Route Analytics Management System (RAMS) is an IP Route Analytics tool that listens to routing protocols and builds a real-time routing topology map. You can use RAMS data to enhance the NNMi ability to trace the route path between the source and destination node when displaying a Path View. Some of the advantages include:

- When accessing RAMS data, NNMi is able to provide a Path View more quickly than when using NNMi alone. This is because RAMS does not use SNMP to learn the routing paths. Therefore, it does not need to handle SNMP timeout issues.
- Because RAMS uses real-time data, rather than data collected from SNMP MIBs, it may also be more accurate than the Path View data collected from NNMi alone.

After you configure RAMS as described in "[Configure One or More Route Analytics Management Systems \(NNMi Advanced\)](#)" (on page 300), Path View provides enhanced information.

Related Topics

[Path Between Two Nodes](#)

[Path Calculation Rules](#)





[Path View Limitations](#)

Configure One or More Route Analytics Management Systems (NNMi Advanced)

HP Route Analytics Management System (RAMS) is an IP Route Analytics tool that listens to routing protocols and builds a real-time routing topology map. You can use RAMS data to enhance the NNMi ability to trace the route path between the source and destination node when displaying a Path View.

To enable NNMi to use RAMS data when calculating a Path View, you must use the RAMS form to configure each Route Analytics Management System you want to use. The RAMS form provides details about the RAMS appliance and the associated RAMS database to be used with NNMi when calculating a Path View.

To configure a Route Analytics Management System:

1. Navigate to the **RAMS Configuration** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **RAMS Configuration**.
2. Do one of the following:
 - To establish a RAMS configuration, click the  New icon, and continue.
 - To edit a RAMS configuration, select a row, click the  Open icon, and continue.
 - To delete a RAMS configuration, select a row and click the  Delete icon.
3. Provide the required information (see [Basic Attributes table](#)).
4. Click  **Save and Close** to save your changes and return to the list of configured RAMS.

Basic Attributes

Attribute	Description
Host	Hostname or IP address used to identify the RAMS appliance that you want NNMi to access.
Query Password	Query password configured for the RAMS appliance.
Database Name	Name of the database that NNMi should access when calculating a Path View. This database must reside on the RAMS appliance that you have identified in the Name attribute.
Priority	Used when you configure more than one RAMS appliance. Determines the order in which NNMi attempts to access the configured RAMS appliances. The lower the number, the higher the priority. For example, the number 1 is the highest priority.

Related Topics

["Use HP Route Analytics Management System Data in Path View \(NNMi Advanced\)" \(on page 300\)](#)

Extending NNMi Capabilities





NNMi enables you to extend its capabilities in the following ways:

- ["Add Custom Attributes to a Node or Interface Object" \(on page 302\)](#)
- You can integrate other programs into the console through the Actions menu. See ["Configure URL Action Basic Behavior" \(on page 303\)](#).
- HP offers extended features, see ["Purchase an HP Smart Plug-in" \(on page 319\)](#).





Add Custom Attributes to a Node or Interface Object

If you determine that you want to keep track of additional information for a node or interface, you can add Custom Attributes to these objects. For example, you might determine that you want to track the owner of your nodes on the network. You might also want to track the serial number for each node.

To add Custom Attributes to a node object:

1. Navigate to the **Custom Attributes** tab:
 - a. From the workspace navigation panel, select a workspace that contains a Node view. For example, the **Inventory** workspace.
 - b. In the Node view, select the check box that precedes the node of interest.
 - c. Click the  Open icon to open the Node Form.
 - d. Select the **Custom Attributes** tab.
2. Click the  New icon to create a Custom Attribute.
3. Enter a Name and Value. See [Node Custom Attributes Form](#) for more information.
4. Click  **Save and Close** to return to the main Node Form.
5. Click  **Save and Close** to save your changes.

To add Custom Attributes to an interface object:

1. Navigate to the **Custom Attributes** tab:
 - a. From the workspace navigation panel, select a workspace that contains an Interfaces view. For example, the **Inventory** workspace.
 - b. In the Interfaces view, select the check box that precedes the interface of interest.
 - c. Click the  Open icon to open the Interface form.
 - d. Select the **Custom Attributes** tab.
2. Click the  New icon to create a Custom Attribute.
3. Enter a Name and Value. See [Interface Custom Attributes Form](#) for more information.
4. Click  **Save and Close** to return to the main Interface Form.
5. Click  **Save and Close** to save your changes.

Control the Actions Menu





Configure additional NNMi Actions menu items that access in-house tools, Web sites, or a variety of other resources. You configure the URL that NNMi associates with each new Actions menu item.

URL Actions are a powerful feature of NNMi. The syntax used to define the URL action includes variables that incorporate real-time data from the NNMi database. Click here for a list of choices:

Configure URL Action Basic Behavior




Configure additional NNMi Actions menu items that access in-house tools, Web sites, or a variety of other resources. You configure the URL that NNMi associates with each new Actions menu item (see ["Control the Actions Menu" \(on page 303\)](#) for more information).

To make changes or additions to the items available in the Actions menu:

1. Navigate to the **URL Action** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **URL Actions** view.
 - c. Do one of the following:
 - To edit an existing Actions menu item, select a row, click the  Open icon, and continue.
 - To create a new Actions menu item, click the  New icon, and continue.
 - To delete an Actions menu item, select a row, and click the  Delete icon.
2. Provide the required information to define the behavior of the URL action (see [basics table](#)).
 If you make changes, remember to place your name in the Author attribute. See ["URL Actions Author" \(on page 304\)](#).
3. Provide the required URL details (see ["Configure URL Action Details" \(on page 305\)](#)).
4. Click  **Save and Close** to return to the URL Actions view.
5. To test your changes to the Actions menu, access a view or form that contains the appropriate object type. Select an object instance and click the Actions menu. Verify your changes are working.

URL Action Basics

Attribute	Description
Menu Label	<p>The text string that appears as the menu link. Ensure that your menu label is unique and accurately reflects the intended use of the URL action.</p> <p>If you add two URL actions with the same menu label string, both show up beneath the Actions menu.</p>
Unique Key	<p>Caution: This value cannot be changed after you click Save.</p> <p>Used as a unique identifier when exporting and importing URL Action definitions. To ensure that the value you enter is unique, it is recommended that you use the Java name space convention when providing this value. It is also useful to include the Menu Label value as part of the unique key as shown in the following example:</p> <pre>com.<company_name>.nnm.urlAction.<url_action_Menu_Label></pre>

Attribute	Description
	Type a maximum of 80 characters. Alpha-numeric and period characters are allowed. No spaces are allowed.
Author	Click the  Lookup icon next to the Author attribute, and do one of the following: <ul style="list-style-type: none"> To select an existing Author value, select a row, click the  Quick Find icon. To create a new Author value, click the  New icon. (See "URL Actions Author" (on page 304).)
Ordering	Valid entries are 1 to 100. This attribute controls where your menu item shows up in the list of available actions (lowest number appears at the top of the group of URL actions).
Browser Width	<i>Optional.</i> When empty, the default browser settings are used. If the value is 1 or more, the browser is launched this number of pixels wide.
Browser Height	<i>Optional.</i> When empty, the default browser settings are used. If the value is 1 or more, the browser is launched this number of pixels high.
Add Browser Decorations	If <input checked="" type="checkbox"/> enabled, the web browser toolbar and menus appear when a user launches your URL. If <input type="checkbox"/> disabled, the web browser has no toolbar or menu when a user launches your URL.
Path View Only	If <input checked="" type="checkbox"/> enabled, your URL action appears <i>only</i> in the Path View window's Actions menu. See "Syntax and Limitations for URL Actions" (on page 306) for additional information about Path View URL configuration choices If <input type="checkbox"/> disabled, your URL action can appear in the menu of multiple views.
Requires Remote Management Station	If <input checked="" type="checkbox"/> enabled, the action appears <i>only</i> when remote NNM 6.x/7.x management stations are configured to communicate with NNMi within your environment. (See "Configure Remote NNM 6.x and 7.x Management Stations" (on page 262) .) If <input type="checkbox"/> disabled, the action always appears.
Description	<i>Optional.</i> Provide a description of your URL action. Your description is visible only within this configuration form. Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.





URL Actions Author

The Author attribute value indicates who created the URL Action definition. For example:


- HP provides predefined actions.
- You can define URL Actions.

To create a new Author attribute value:

1. Navigate to the **Author** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **URL Actions** view.
 - c. Open the **URL Action** form.

- d. In the **URL Action** form, locate the **Author** attribute.
- e. Click the  Lookup icon, and select  New.
2. Type the text that represents the new author (see [table](#)).
3. Click  **Save and Close** to return to the URL Action form.
4. Click  **Save and Close**. NNM saves your changes.





URL Action Author

Attribute	Description
Label	Author name. The maximum length is 255 characters. Any character type is valid.
Unique Key	<p>Caution: After you click  Save and Close, this value cannot be changed.</p> <p>Used as a unique identifier when exporting and importing URL Action definitions. To ensure that the value you enter is unique, it is recommended that you use the Java name space convention when providing this value. It is also useful to include the label value as part of the unique key as shown in the following example:</p> <pre>com.<your_company_name>.nnm.urlAction.author.<author_label></pre> <p>The maximum length is 80 alpha-numeric characters, periods allowed, no spaces allowed.</p>

Configure URL Action Details

Configure additional NNMi Actions menu items that access in-house tools, Web sites, or a variety of other resources. You configure the URL that NNMi associates with each new Actions menu item (see ["Control the Actions Menu" \(on page 303\)](#) for more information).

To make changes or additions to the items available in the Actions menu:

1. Navigate to the URL Action form, **Details** tab.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **URL Actions** view.
 - c. Do one of the following:
 - To edit an existing Actions menu item, select a row, click the  Open icon, and continue.
 - To create a new Actions menu item, click the  New icon, and continue.
 - To delete an Actions menu item, select a row, and click the  Delete icon.
 - d. Provide the required information to define the behavior of the URL action (see ["Configure URL Action Basic Behavior" \(on page 303\)](#)).
 If you make changes, remember to place your name in the Author attribute. See ["URL Actions Author" \(on page 304\)](#).
2. Provide the required URL details (see [URL Action Selection Details](#) and [URL Action Object Types](#)).
3. *Optional.* Provide a filter that controls where this URL action is available (see).
4. Click  **Save and Close** to return to the URL Actions view.

5. To test your changes to the Actions menu, access a view or form that contains the appropriate object type. Select an object instance and click the Actions menu. Verify your changes are working.

URL Action Selection Details

Attribute	Description
Selection Type	<p><i>Optional.</i> Default is Single Selection:</p> <ul style="list-style-type: none">• If you specify any of the following, an error message appears when the user launches the URL action prior to selecting an appropriate object or objects:<ul style="list-style-type: none">▪ Any Selection means zero or more selections required.▪ Single Selection means exactly one selection required.▪ Multiple Selection means one or more selections required.• If you specify No Selection, the user must launch the URL action without selecting any objects. An error message appears if any objects are selected.
Max Selection Count	<p><i>Only valid if Selection Type = Any Selection or Multiple Selection.</i> Zero means unlimited. Specify the maximum number of objects the user can select prior to launching this URL action.</p>
Enable Cumulative Launch	<p>If <input checked="" type="checkbox"/> enabled, any object attribute references in the URL Action definition are populated with values from all selected objects. The multiple values are separated by a comma character. For example, if the attribute is "name", the URL results would be "name1,name2,name3".</p> <p>If <input type="checkbox"/> disabled, the action launches a separate web page instance for each selected object.</p> <p>See "Syntax and Limitations for URL Actions" (on page 306) for details about including object attributes in your URL action.</p>

URL Action Object Types




Attribute	Description
Object Type	<p>Add one or more definitions for the actual URL syntax. See "Syntax and Limitations for URL Actions" (on page 306).</p> <p><i>Optional.</i> Limit the use of the URL by object-type.</p>

Syntax and Limitations for URL Actions

Provide the details of the URL syntax.

To provide the details of a URL action:

1. Navigate to the **URL Action Object Type** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select the **URL Actions** view.
 - c. Open the **URL Action** form.
 - d. Navigate to the **Details** tab.

- e. Locate the **URL Action Object Types** table.
- f. Do one of the following:
 - To add a URL Action, click the  New icon, and continue.
 - To change a URL Action, select a row, click the  Open icon, and continue.
 - To delete a URL Action, select a row and click the  Delete icon.
2. *Optional.* Limit the use of your URL by object type (see [table](#)).
3. Specify the lowest user role allowed to access this Action.
4. Provide the required URL syntax. Use a pattern similar to the following (see [Full URL](#)).

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/<application>?<yourURLparameter1>=${<objectAttribute>}&<yourURLparameter2>=${<objectAttribute>}`



`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

For example: `http://-companyX.com/nodeReport.jsp?node=${hostname}&snmpOid=${systemObjectId}`

Tip: If the application that your URL calls is installed on the NNMi management server, the syntax can be as follows:

`/<application>?<yourURLparameter1>=${<objectAttribute>}&<yourURLparameter2>=${<objectAttribute>}`

5. *Optional.* If your URL Action applies to Nodes, Interfaces, or Incidents, you can provide filters that further refine when the URL action is available in the Actions menu. See "[Specify Optional URL Action Filters](#)" (on page 315) for more information.
6. Click  **Save and Close** to return to the URL Action form.
7. Click  **Save and Close** to return to the URL Actions view.
8. To test your changes to the Actions menu, access a view or form that contains the appropriate object type. Select an object instance and click the Actions menu. Verify your changes are working.

URL Action and Object Types Basics

Attribute	Description
Object Type	<p><i>Optional.</i> If no attribute value is provided, your URL action is visible within the Action menu in all views and forms. If you want your menu item to be available only within a view or form of a particular object type, copy-and-paste one of the following strings into the Object Type attribute.</p> <p>Specific Object-Type Attributes:</p> <p>com.hp.ov.nms.model.core.Interface [parameter list for Interface]</p>

Attribute	Description
	<p> <code>\${capabilities[capability.key=<UniqueKey>].capability.key}</code> <value of one specific Capability, see "Capability Attributes in URL Actions" (on page 312)for more information> <code>\${customAttributes[name=<yourAttrName>].value}</code> <value of the matching Custom Attribute, see "Custom Attributes in URL Actions" (on page 313)for more information> <code>\${ifAlias}</code> <value from the IfAlias attribute> <code>\${ifDescr}</code> <value from the IfDescription attribute> <code>\${ifIndex}</code> <value from the IfIndex attribute> <code>\${ifType.label}</code> <value from the IfType attribute> <code>\${journal.notes}</code> <value from the Notes attribute> <code>\${managementMode}</code> <value from the Management Mode attribute> <code>\${name}</code> <value from the Name attribute> <code>\${overallStatus.lastChange}</code> <value from the Status Last Modified attribute> <code>\${overallStatus.status}</code> <value from the Status attribute> <code>\${physicalAddress}</code> <value from the Physical Address attribute> <code>\${speed}</code> <value from the IfSpeed attribute> Access an attribute on the related Node form: <code>\${hostedOn.hostname}</code> <value from the Hosted On attribute, source Node's Hostname attribute> <code>\${hostedOn.name}</code> <value from the source Node's Name attribute> </p>
	<p>com.hp.ov.nms.model.core.Node [parameter list for Node]</p>
	<p> <code>\${capabilities[capability.key=<UniqueKey>].capability.key}</code> <value of one specific Capability, see "Capability Attributes in URL Actions" (on page 312)for more information> <code>\${customAttributes[name=<yourAttrName>].value}</code> <value of the matching Custom Attribute, see "Custom Attributes in URL Actions" (on page 313)for more information> <code>\${hostname}</code> <value from the Hostname attribute> <code>\${journal.notes}</code> <value from the Notes attribute> <code>\${managementMode}</code> <value from the Management Mode attribute> <code>\${name}</code> <value from the Name attribute> <code>\${overallStatus.lastChange}</code> <value from the Status Last Modified attribute> <code>\${overallStatus.status}</code> <value from the Status attribute> <code>\${snmpSupported}</code> <value from the SNMP Supported attribute> <code>\${systemContact}</code> <value from the System Contact attribute> <code>\${systemDescription}</code> <value from the System Description attribute> <code>\${systemLocation}</code> <value from the System Location attribute, the current value of the sys-Location MIB variable> <code>\${systemName}</code> <value from the System Name attribute> <code>\${systemObjectId}</code> <value from the System Object ID attribute> Access an attribute on the related Device Profile form: <code>\${deviceProfile.deviceModel}</code> <value from the Device Model attribute> <code>\${deviceProfile.SNMPObjectId}</code><value from the SNMP Object ID attribute> Access an attribute on the related SNMP Agent form: <code>\${snmpAgent.agentSettings.managementAddress}</code> <value from the Management Address attribute> </p>
	<p>com.hp.ov.nms.monitoring.groups.model.NodeGroup [parameter list for Node Group]</p>
	<p> <code>\${name}</code> <value from the Name attribute> <code>\${notes}</code> <value from the Notes attribute> <code>\${overallStatus.lastChange}</code> <value from the Status Last Modified attribute> <code>\${overallStatus.status}</code> <value from the Status attribute> </p>
	<p>com.hp.ov.nms.model.incident.Incident [parameter list for Incident]</p>

Attribute	Description
	<p> \${category.label} <value from the Category attribute> \${cias[name=<i>cia.name</i>].value} <value of one specific Custom Incident Attribute, see "Custom Incident Attributes in URL Actions" (on page 311) for more information> \${duplicateCount} <value from the Duplicate Count attribute> \${family.label} <value from the Family attribute> \${formattedMessage} <value from the Message attribute> \${getAttrOrName(<i>attribute</i>)} <value of the specified attribute of the Node associated with the Incident (if the Node exists in the database) or the <i>sourceNodeName</i> attribute of the Incident (if the Node was deleted from the database or never existed in the database). [For example, \${getAttrOrName(hostname)}> \${journal.notes} <value from the Notes attribute> \${lifecycleState.label} <value from the Lifecycle State attribute> \${nature} <value from the Correlation Nature attribute> \${nodeUuid} <value of the uuid for the Source Node, see "Database Object Identifiers for URL Actions" (on page 311)> \${nodeUuid.id} <value of the id for the Source Node, see "Database Object Identifiers for URL Actions" (on page 311)> \${notes} <value from the Correlation Notes attribute> \${origin} <value from the Origin attribute> \${priority.label} <value from the Priority attribute> \${registration.created} <value from Created attribute> \${registration.modified} <value from the Last Modified attribute> \${severity} <value from the Severity attribute> \${sourceName} <value from Name attribute of the source object> \${sourceNodeName} <value from the Name attribute of the source object> \${sourceUuid} <value of the uuid for the Source Object, see "Database Object Identifiers for URL Actions" (on page 311)> \${sourceUuid.id} <value of the source object's id attribute> Access an attribute on the related source object form: \${sourceUuid.name} <value of the source object's Name attribute> Access an attribute on the related Node form: \${nodeUuid.hostname} <value of the fully-qualified DNS name of the Source Node or IP address if no DNS name is available> \${nodeUuid.name} <value of the Name attribute of the Source Node> </p> <p>com.hp.ov.nms.model.layer2.L2Connection [parameter list for Layer 2 Connection]</p> <p> \${journal.notes} <value from the Notes attribute> \${name} <value from the Name attribute of the connection> \${source} <value of the Topology Source attribute, the protocol used to create the connection> </p> <p>com.hp.ov.nms.model.layer3.IPAddress [parameter list for Address]</p> <p> \${journal.notes} <value from the Notes attribute> \${managementMode} <value from the Direct Management Mode attribute> \${name} <value from the Name attribute> \${overallStatus.lastChange} <value from the Status Last Modified attribute> \${overallStatus.status} <value from the Status attribute> \${prefixLength} <value from the Prefix Length attribute> \${value} <value from the Address attribute> </p> <p>com.hp.ov.nms.model.layer3.IPSubnet [parameter list for Subnet]</p> <p>\${journal.notes} <value from the Notes attribute></p>

Attribute	Description
	<p>\${name} <value from the Name attribute> \${prefix} <value from the Prefix attribute> \${prefixLength} <value from the Prefix Length attribute></p>
	<p>Global Object-Type Attributes: Two attributes are valid for all object types. However, the values for these two attributes are not visible anywhere in the console, which makes them harder to use. See "Database Object Identifiers for URL Actions" (on page 311) for more information.</p> <hr/>

Attribute	Description
Role	Specify the lowest level role allowed to access this URL action. All roles above the role you select can also access this URL action. See "Determine which NNMi Role to Assign" (on page 33) .
Full URL	<p>Type the full URL specification. Begin with either http:// or https://. Include any required machine name and port number. Include any required parameters. The list of available parameters changes depending on which object type (if any) you configure as a limiting factor for your URL action (see Object Type).</p> <ul style="list-style-type: none"> You can also use other common URL protocols such as ftp://, mailto://, news://, or telnet://. You can use an object parameter anywhere in the URL string. For example, to specify hostname for an action launched from a Node form: <code>http://\${hostname}:<portNumber>/<application>?attributeName1=\${value}&attributeName2=\${value}</code> You can limit the availability of the action to one specific instance of an object by using the database identifier (see "Database Object Identifiers for URL Actions" (on page 311)). <p>Path View Attributes: If you specified that this action appears only in the Path View menu, additional parameters are available:</p> <p><code>\${pathStartNodeName}</code> <value of the Source attribute> <code>\${pathEndNodeName}</code> <value of the Destination attribute> <code>\${pathList}</code> <list of objects traversed along the path, separated by commas> <code>\${pathCalculationDate}</code> <date and time the path was calculated></p> <p>If the attribute does not exist (for example, you made a mistake when typing the attribute's name), the attribute passes through literally (unresolved). For example:</p> <p>A node named "mynode" is selected, and the URL is:</p> <code>http://companyX.com?name=\${name}&error=\${error}</code> <p>The output would be:</p> <code>http://companyX.com?name=mynode&error=\${error}</code>

Database Object Identifiers for URL Actions

If you need the URL to identify one specific record in the NNMi database, and find that it isn't possible to provide a unique set of attribute values that distinguish that object instance from all other similar object instances, the *database unique identifiers* are a valuable last resort.

- `${uuid}` Universally Unique Object Identifier -Unique across all databases.
- `${id}` Unique Object Identifier - Unique across the Entire NNMi Database.


For example, the user can select an Interface object in the console, and use this URL Action to open the form of the Node in which the Interface resides:

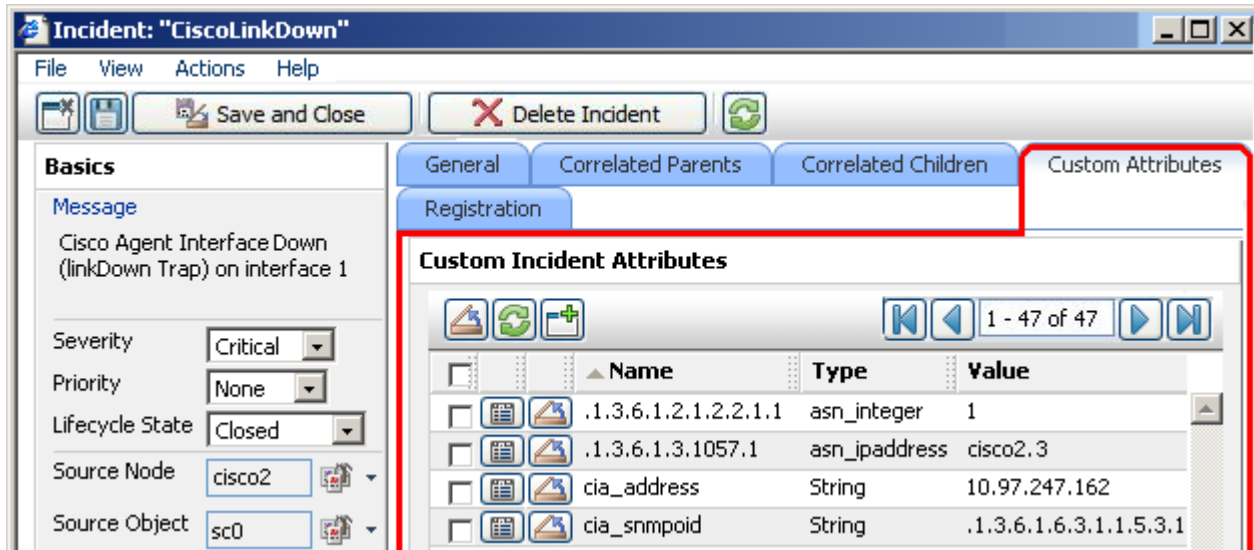
```
/nnm/launch?cmd=showForm&objtype=Node&objid=${hostedOn.id}
```

Custom Incident Attributes in URL Actions

Custom Incident Attributes (CIAs) are used to provide the following types of information within incidents:

- SNMP trap varbinds identified by the Abstract Syntax Notation value, ASN.1 (Name = the MIB varbind identifier, Type = asn_*)
- Custom attributes provided by NNMi (Name = cia.*, Type=String). See ["Custom Incident Attributes Provided by NNMi" \(on page 214\)](#).

To determine which group of CIAs is available for a specific incident-type (for example, CiscoLinkDown), navigate to an Incident view, select an instance of that incident-type, click the  Open icon and navigate to the Custom Attributes tab. The items listed in the table are the CIAs for that particular incident-type. For example, all CiscoLinkDown incidents would have the same group of CIAs shown in the illustration below.



To pass CIA data within your URL Action, type (or copy and paste) the exact text string *from the Incident form, Custom Attribute tab, Name attribute value*:

`#{cias[name=<cia_name>].value}`

Place the CIA into a location in your URL that enables the result you want:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/<application>?<yourURLparameter1>=#{cias[name=<cia_name_1>].value}&<yourURLparameter2>=#{cias[name=<cia_name_2>].value}`

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console


Note: If the CIA that you request in your URL Action does not exist for the selected Incident, the resulting URL passes an empty string.

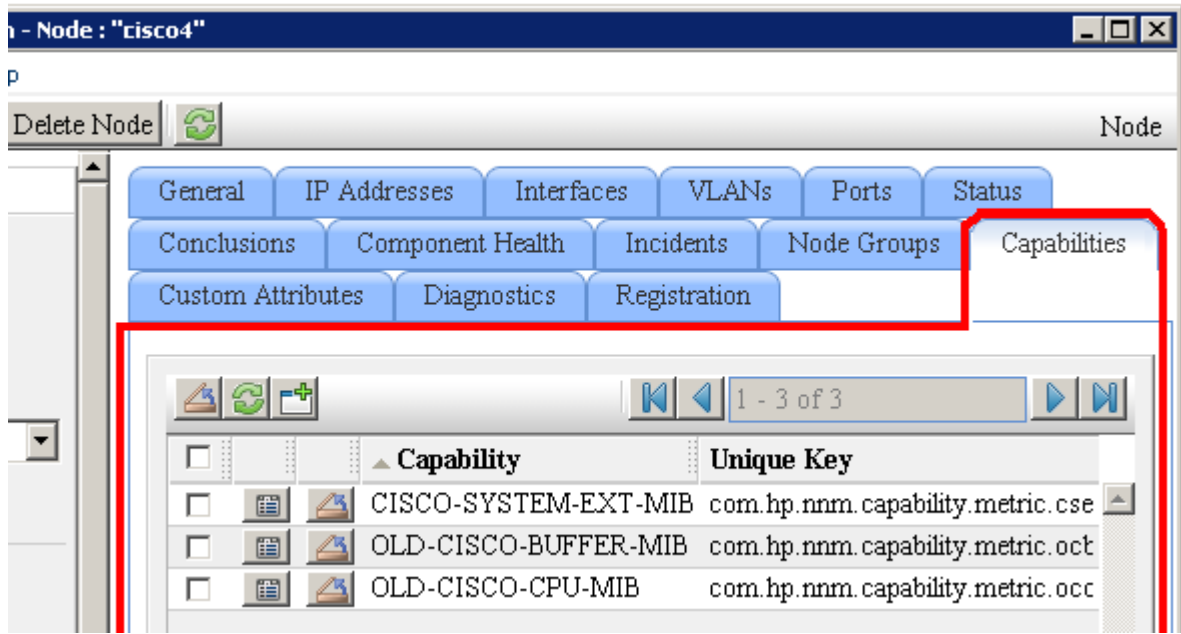
Capability Attributes in URL Actions

Node and Interface objects can have capability attributes:

- [Node Capabilities Provided by NNMi](#)
- [Interface Capabilities Provided by NNMi](#)

- Capabilities can be provided from NNM iSPIs or from integrations with other programs

To determine which group of capabilities are available for a specific Node or Interface, navigate to a Node view or Interface view, select an instance of the object, click the  Open icon and navigate to the Capabilities tab. The items listed in the table are the Capabilities for that particular node or interface. For example, the following illustration shows a Node form with three capability entries.



To pass Capability data within your URL Action, type (or copy and paste) the exact text string *from the Node or Interface form, Capability tab, Unique Key attribute value*:

`${capabilities[capability.key=<UniqueKeyValue>].capability.key}`

Place the Capability into a location in your URL that enables the result you want:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/<application>?<yourURLparameter1>=${capabilities[capability.key=<UniqueKey_1>].capability.key}&<yourURLparameter2>=${capabilities[capability.key=<UniqueKey_2>].capability.key}`

`<serverName>` = the fully-qualified domain name of the NNMi management server


`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

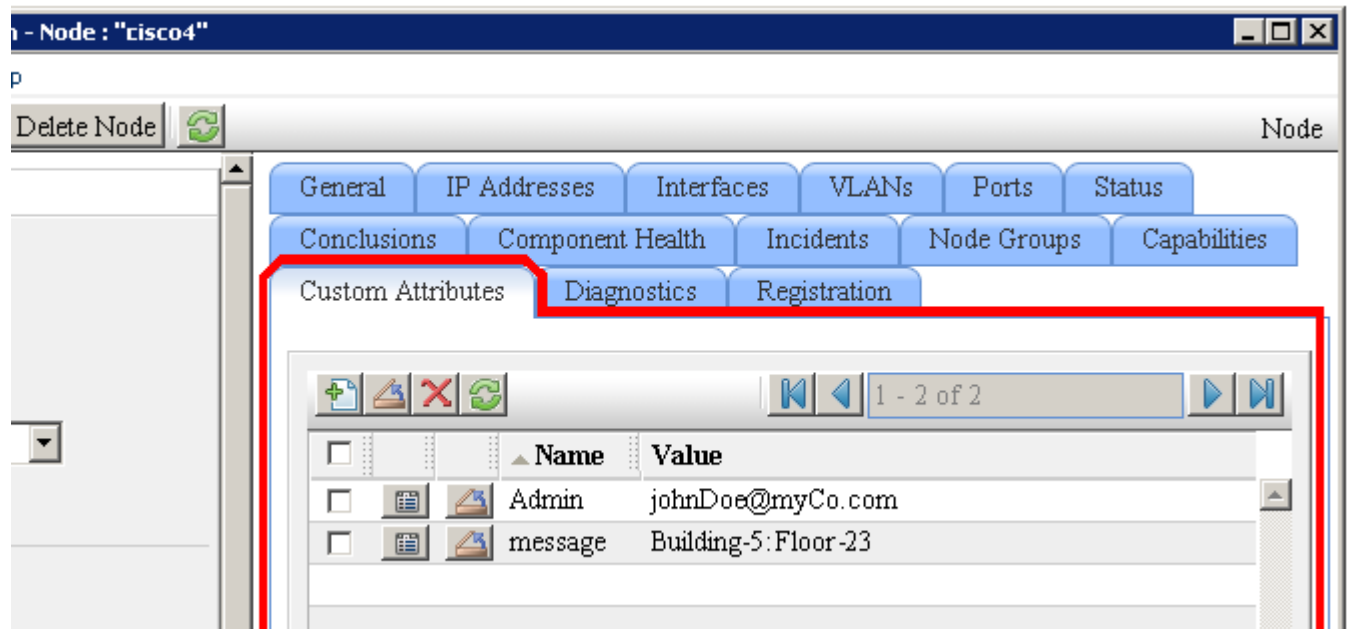
Note: If the Capability that you request in your URL Action does not exist for the selected Node or Interface, the resulting URL passes an empty string.

Custom Attributes in URL Actions

Custom Attributes enable an NNMi administrator to add information to the Node object or Interface object. Custom Attributes can also be set by external applications that have been integrated with NNMi.

The [Node form: Custom Attributes tab](#) and [Incident form: Custom Attributes tab](#) display a table view of any Custom Attributes that have been added to the selected object. See ["Add Custom Attributes to a Node or Interface Object"](#) (on page 302).

To determine which group of Custom Attributes are available for a specific Node or Interface, navigate to a Node view or Interface view, select an instance of the object, click the  Open icon and navigate to the Custom Attributes tab. The items listed in the table are the Custom Attributes for that particular node or interface. For example, the following illustration shows a Node form with two Custom Attribute entries.



To pass Custom Attribute data within your URL Action, type (or copy and paste) the exact text string *from the Node or Interface form, Custom Attributes tab*:

`{customAttributes[name=<yourAttrName>].value}`

Place the Custom Attribute into a location in your URL that enables the result you want:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/<application>?<yourURLparameter1>=${customAttributes[value=<yourAttrValue>].name}&<yourURLparameter2>=${customAttributes[name=<yourAttrName>].value}`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

- Example 1:

`mailto:${customAttributes[name=Admin].value}?subject=URGENT Action Required&body=${customAttributes[name=message].value}&${hostname} router needs attention.`

Resulting URL:

mailto:JohnDoe@myCompany.com?subject=URGENT Action Required&body=Building-5:Floor-23.&cisco4.myCo.com router needs attention.

- Example 2:

```
http://myCo.com/emailAdmin.jsp?name=${hostname}&contact=${customAttributes[name=Admin].value}&body=${customAttributes[name=message].value}
```

Resulting URL:

```
http://myCo.com/emailAdmin.jsp?name=cisco4.myCo.com&contact=johnDoe@myCo.com&body=Building-5:Floor-23
```

Note: If the Custom Attribute that you request in your URL Action does not exist for the selected Node or Interface, the resulting URL passes an empty string.

Environment Attributes in URL Actions

Environment Attributes are session-specific and not stored in the NNMi database. These attributes are received from another application when NNMi is launched from that external application, see "[Launch a View \(showView\)](#)" (on page 324) or "[Launch a Form \(showForm\)](#)" (on page 350) for more information. NNMi stores the environmental attribute name-value pairs and passes them back to that application.

For example, after launching NNMi from your company website, you want to provide an Action menu item within the NNMi console that returns the user to exactly the same place within your company website where they were prior to launching NNMi.

```
${getEnvAttr(<applicationAttrName>)}
```

Place the Environment Attribute into a location in your URL that enables the result you want:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

```
http://<serverName>:<portNumber>/<application>?<yourURLparameter1>= ${getEnvAttr(<applicationAttrName1>)}&<yourURLparameter2>= ${getEnvAttr(<applicationAttrName2>)}
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

For example:

```
http://<myHost>/<myApplication>?com.my.sessionId= ${getEnvAttr(com.my.sessionId)}&com.my.objectName= ${getEnvAttr(com.my.objectName)}
```

Could result in the following URL:

```
http://<myHost>/<myApplication>com.my.sessionId= 123&com.my.objectName= node25
```





Note: If the Environment Attribute that you request in your URL Action does not exist for the selected view or form, the resulting URL passes an empty string.

Specify Optional URL Action Filters

If your URL Action applies to Nodes, Interfaces, or Incidents, you can use the Filters Editor to create expressions that further define the context in which this URL Action is available within NNMi. Design complex

Filters on paper as a Boolean expression first to minimize errors when entering your expressions using this Filters editor.

To create any Filter expressions:

1. Navigate to the **URL Action Object Type** form.
 - a. From the workspace navigation panel, select the **Configuration** workspace.
 - b. Select **URL Actions**.
 - c. Do one of the following:
 - To create an URL Action definition, click the  New icon.
 - To edit an URL Action definition, select a row, click the  Open icon.
 - d. Select the **Details** tab.
 - e. In the **URL Action Object Types** table, do one of the following:
 - To create an URL Action Object Type definition, click the  New icon.
 - To edit an URL Action Object Type definition, select a row, click the  Open icon.
2. Select the **Filters** tab.
3. Establish the appropriate settings for the filter you want to create. (See the [Custom Filter Editor Components](#) table.)

When creating any filters, note the following:



- Each set of expressions associated with a Boolean Operator is treated as if it were enclosed in parentheses and evaluated together. View the expression displayed under **Filter String** to see the logic of the expression as it is created.
- The AND Boolean Operators must contain at least two expressions as shown in the example below.

```
AND
  capability = com.hp.nnm.capability.metric.cse
AND
  customAttrName = ImportantRouters
  customAttrValue = Building5
```

NNMi evaluates the expression above as follows:

```
(capability = com.hp.nnm.capability.metric.cse AND (cus-
tomAttrName=ImportantRouters AND customAttrValue=Building5))
```

- NNMi finds all nodes with a Capability having the Unique Value of **com.hp.nnm-.capability.metric.cse**.
- Of these nodes, NNM then finds all nodes with a Custom Attribute named **ImportantNodes** and having the value of **Building5**.
- The placement of your cursor and the subsequent text that is selected is important when performing operations using the Additional Filters Editor. For example, you append to, replace, or change the indentation of the expression that is selected.
- The placement of your cursor and the subsequent text that is selected is especially important when adding your Boolean operators. See ["Add Boolean Operators in the Additional Filters Editor" \(on page 134\)](#) for more information.

4. Click  **Save and Close** to return to the URL Action form.
5. Click  **Save and Close**.

Custom Filter Editor Components

Attribute	Description
Attribute	<p>The attribute name NNMi should use as the filter criteria. Possible attributes include the following:</p> <p>Interface [click here for a list of attribute vaules]</p> <p>Unique Keys from the Interface Form: Capabilities Tab:</p> <ul style="list-style-type: none"> • capability (Unique Key of the Capability) <p>Values from the Interface Form: Custom Attributes Tab:</p> <ul style="list-style-type: none"> • customAttrName (Custom Attribute Name) • customAttrValue (Custom Attribute Value) <p>Node [click here for a list of attribute values]</p> <p>Unique Keys from the Node Form: Capabilities Tab:</p> <ul style="list-style-type: none"> • capability (Unique Key of the Capability) <p>Values from the Node Form: Custom Attributes Tab:</p> <ul style="list-style-type: none"> • customAttrName (Custom Attribute Name) • customAttrValue (Custom Attribute Value) <p>Incident [click here for a list of attribute values]</p> <p>Values from the Incident Form: Custom Attributes Tab:</p> <ul style="list-style-type: none"> • customAttrName (Custom Attribute Name) • customAttrType (Custom Attribute Type) • customAttrValue (Custom Attribute Value)
Operator	<p>The standard query language (SQL) operations to be used for the search. Valid operators are described below.</p> <p>Note: Only the <code>is null</code> Operator returns null values in its search.</p> <ul style="list-style-type: none"> • <code>=</code> Finds all values equal to the value specified. • <code>!=</code> Finds all values not equal to the value specified. • <code><</code> Finds all values less than the value specified. • <code><=</code> Finds all values less than or equal to the value specified. • <code>></code> Finds all values greater than the value specified. • <code>>=</code> Finds all values greater than or equal to the value specified. • between Finds all values equal to and between the two values specified. • in Searches for a match in at least one of a series of values.

Attribute	Description
Attribute	<p>The attribute name NNMi should use as the filter criteria. Possible attributes include the following:</p> <p>Interface [click here for a list of attribute vaules]</p> <p>Unique Keys from the Interface Form: Capabilities Tab:</p> <ul style="list-style-type: none"> • capability (Unique Key of the Capability) <p>Values from the Interface Form: Custom Attributes Tab:</p> <ul style="list-style-type: none"> • customAttrName (Custom Attribute Name) • customAttrValue (Custom Attribute Value) <p>Node [click here for a list of attribute values]</p> <p>Unique Keys from the Node Form: Capabilities Tab:</p> <ul style="list-style-type: none"> • capability (Unique Key of the Capability) <p>Values from the Node Form: Custom Attributes Tab:</p> <ul style="list-style-type: none"> • customAttrName (Custom Attribute Name) • customAttrValue (Custom Attribute Value) <p>Incident [click here for a list of attribute values]</p> <p>Values from the Incident Form: Custom Attributes Tab:</p> <ul style="list-style-type: none"> • customAttrName (Custom Attribute Name) • customAttrType (Custom Attribute Type) • customAttrValue (Custom Attribute Value)
	<hr/> <ul style="list-style-type: none"> • is not null Searches for all non-blank values. • is null Searches for all blank values. • like Enables you to find matches using the asterisk (*) and question mark (?) as wildcard characters. Question mark character means "any single character of any type at this location". Asterisk character means "any number of characters of any type at this location". • not between Finds all values except those between the two values specified. • not in Finds all values except those included in the list of values. • not like Finds all values except those included in the value specified. The not like operator enables you to use the asterisk (*) and question mark (?) as wildcard characters. <hr/>
Value	<p>The value for which you want NNMi to search.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • The values you enter are case sensitive. • NNMi displays a variable number of value fields depending on the Operator selected. For example, the <code>between</code> Operator causes two value fields to be displayed. • The <code>in</code> and <code>not in</code> operators require that each value be entered on a separate line. <hr/>

Additional Filters Editor Buttons

Button	Description
Append	Appends the current expression (Attribute, Operator, and Value) to the selected expression already included in the filter string.
Replace	Replaces the selected expression with the expression displayed in the Attribute, Operator, and Value fields.
AND	<p>Inserts the AND Boolean Operator in the selected cursor location.</p> <p>Note: View the expression displayed under Filter String to see the logic of the expression as it is created.</p>
OR	<p>Inserts the OR Boolean Operator in the current cursor location.</p> <p>Note: View the expression displayed under Filter String to see the logic of the expression as it is created.</p>
AND < > OR	Switches the selected Boolean Operator to either AND or OR. If the selected Boolean Operator is AND, the value is changed to OR. If the selected Boolean Operator is OR, the value is changed to AND.
Outdent	<p>Moves the indentation of the selected expression one tab to the left. Check the expression displayed under Filter String to determine the new placement of parenthesis.</p> <p>Note: If the expression is located at the leftmost tab, it will not be moved.</p>
Delete	<p>Deletes the selected expression.</p> <p>Note: If the Boolean Operator is selected, the Additional Filters Editor deletes all expressions associated with the Boolean Operator.</p>

Purchase an HP Smart Plug-in

A Smart Plug-in (iSPI) extends NNMi capabilities. For example, each iSPI may or may not:

- Enhance the data that is available.
- Add new workspaces, views, and forms.
- Add tabs to existing NNMi forms.
- Change the features of the NNMi user interface.

Multiple iSPIs are available, enabling you to manage your network in a way that makes sense in your organization:

- NNM iSPI for MPLS
- NNM iSPI for Multicast
- NNM iSPI for Performance
- NNM iSPI for Telephony

See the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>

For information about purchasing HP Smart Plug-ins contact your HP sales representative.

Purchase Integrations with Other HP Products

Multiple HP Software products can be configured to share data with NNMi and receive data from NNMi. See the *HP Network Node Manager i-series Software Deployment Guide*, which is available at:
<http://h20230.www2.hp.com/selfsolve/manuals>

The integration extend NNMi capabilities. For example, each integration may or may not:

- Enhance the data that is available.
- Add new workspaces, views, and forms.
- Add tabs to existing NNMi forms.
- Change the features of the NNMi user interface.

For information about the available integrations, contact your HP sales representative.

Integrating NNMi Elsewhere with URLs

Use URLs to provide access to the console or certain NNMi features. For example:

- Embed views within your company Web portal.
- Launch a map from within other applications, such as from an email.
- Launch a filtered view from a browser window to quickly find the information you need.
- Run a tool without opening the console.

For a quick-reference list of all URLs that launch NNMi, see **Help** → **Documentation Library** → **URL Launch Reference**.

Prerequisite: NNMi requires authentication for access through URLs. See ["Authentication Requirements for launch URLs Access"](#) (on page 321).

Related Topics:

["Launch the Console \(showMain\)"](#) (on page 324)

["Launch a View \(showView\)"](#) (on page 324)

["Launch a Form \(showForm\)"](#) (on page 350)

["Launch Menu Items \(runTool\)"](#) (on page 361)

["Confirm that NNMi Is Running \(cmd=isRunning\)"](#) (on page 370)

Authentication Requirements for launch URLs Access

Log on and authentication are the same as if you log on to the console using `http://<serverName>:<portNumber>/nnm`. Each user must have a preconfigured user name, password, and role assignment. See ["Configure Sign-In Access"](#) (on page 32) for more information.

Caution: There is an inherent vulnerability in passing a plain text password as a Launch URL parameter. Consider configuring the NNMi management server to use https/SSL so that user names/passwords are encrypted between client and server. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

To bypass the log on page, include the following two parameters in your Launch URL string:

- `j_username`
- `j_password`

It is recommended that you only bypass the log on page with the "Guest" role (the Guest role provides "read-only" access to a subset of console features). For example, if you have previously defined an account where both the user Name and Password are "guest", the following brings up a list of example URLs:

Note: If the NNMi Web server uses the https protocol, use `https` instead of `http`. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?j_username=guest&j_password=guest`

`<serverName>` = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

If the user name and password are not valid, the log on page appears with an authentication error message.

Any Launch URL request that contains `j_username` and `j_password` redirects, so the actual user name and password are not visible in the Web browser.

Access to console features is limited by the role assignment. The roles are hierarchical in nature. For more information:

["Access to Forms" \(on page 322\)](#)

["Access to Workspaces" \(on page 322\)](#)

["Access to Commands" \(on page 323\)](#)

Access to Forms

Each role configuration controls what the user can and cannot do within a particular form. These permission settings cannot be changed.

Role Limitations for URL Access to Forms

Forms	Guest Role	Level 1 Operator Role	Level 2 Operator Role	Administrator
Node forms	Read-Only	Read-Write except Management Mode field which is Read-Only	Read-Write	Read-Write
Interface forms	Read-Only	Read-Write except Management Mode field which is Read-Only	Read-Write	Read-Write
IP Address forms	Read-Only	Read-Write except Management Mode field which is Read-Only	Read-Write	Read-Write
IP Subnet forms	Read-Only	Read-Write except Management Mode field which is Read-Only	Read-Write	Read-Write
Incident forms	Read-Only	Read-Write	Read-Write	Read-Write
Node Group forms	Read-Only	Read-Only	Read-Only	Read-Write
Configuration Form				Read-Write

Related Topics

["Determine which NNMi Role to Assign" \(on page 33\)](#)

Access to Workspaces

For integration URLs, the user role determines access each view. The predefined role settings cannot be changed.

Each role configuration controls what the user can and cannot do with particular view. See "[Determine which NNMi Role to Assign](#)" (on page 33).

Role Limitations for URL Access to Workspaces

Workspaces	Guest Role	Level 1 Operator Role	Level 2 Operator Role	Administrator
All views in the Incident workspaces	Yes	Yes	Yes	Yes
All views in the Topology workspaces	Yes	Yes	Yes	Yes
All views in the Monitoring workspace	Yes	Yes	Yes	Yes
All views in the Troubleshooting workspace	Yes	Yes	Yes	Yes
All views in the Inventory workspace	Yes	Yes	Yes	Yes
All views in the Management Mode workspace			Yes	Yes
All views in the Configuration workspace				Yes

Access to Commands

Access to NNMi menus depends on the role assigned to the user. The following table shows the default settings for access to NNMi menu choices.

Tip: NNMi administrators can change the Actions menu settings. See "[Control Menu Access](#)" (on page 34).

Role Limitations to Launch URL Commands

Equivalent Command in the Console	Guest Role	Level 1 Operator Role	Level 2 Operator Role	Administrator
Actions → Ping Command		Yes	Yes	Yes
Actions → Trace Route		Yes	Yes	Yes
Actions → Communications Settings				Yes
Actions → Monitoring Settings		Yes	Yes	Yes
Actions → Status Poll			Yes	Yes
Actions → Configuration Poll			Yes	Yes
Actions → Status Details Command (for Node Groups)		Yes	Yes	Yes
Tools → NNMi Status		Yes	Yes	Yes
Tools → Sign In/Out Audit Log				Yes
File → Sign Out	Yes	Yes	Yes	Yes

Launch the Console (showMain)

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

To launch the entire console, use the following URL:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=showMain
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

To launch the console and bypass login, use the following URL:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=showMain&j_username=<accountName>&j_password=<accountPassword>
```

Caution: Review in the information in ["Authentication Requirements for launch URLs Access"](#) (on page 321) before bypassing the login.

Launch a View (showView)

Tip: A view session launched with a URL never times out. (If you are using Mozilla Firefox, see also [Configure Mozilla Firefox Timeout Interval](#).) To continuously display up-to-date information in your network operation center (NOC), launch a URL view .

To launch a default table view that displays all instances of a specified object type, use the following URL:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


```
http://<serverName>:<portNumber>/nnm/launch?cmd= showView&objtype= <x>
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

Default View for Each Object Type and Available Filters

x = objtype Value	Default View	Node Filter	Interface Filter
Incident	Incidents workspace, All Incidents table view	Yes	No
Node	Inventory workspace, Nodes table view	Yes	No
Interface	Inventory workspace, Interfaces table view	Yes	Yes
IPAddress	Inventory workspace, IP Addresses table view	Yes	Yes
IPSubnet	Inventory workspace, IP Subnets table view	No	No
NodeGroup	Inventory workspace, Node Groups table view	No	No
InterfaceGroup	Inventory workspace, Interface Groups table view	No	No

The following are optional filter parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&objtype= <x>&nodegroup= <Name>`

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&objtype= <x>&ifgroup= <Name>`

Filter by Node Group (launched Incident, Node, Interface, and IP Address views)

Attribute	Values
nodegroup	<p>The Name attribute value of the Node Group to use as a filter for this view.</p> <p>Note: The Node Group name is translated. If your team shares NNMi within multiple locales, use <code>nodegroupid</code> or <code>nodegroupuuid</code>.</p> <p>If the Name value includes space characters, replace the space character in your URL statement with one of the following:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
nodegroupid	<p>The <code>id</code> is the Unique Object Identifier (unique across the entire NNMi database). Provide the <code>id</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.</p>
nodegroupuuid	<p>The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.</p>



Filter by Interface Group (launched Interface and IP Address views)

Attribute	Values
ifgroup	<p>The Name attribute value of the Interface Group to use as a filter for this view.</p> <p>Note: The Interface Group name is translated. If your team shares NNMi within multiple locales, use ifgroupid or ifgroupuuid.</p> <p>If the Name value includes space characters, replace the space character in your URL statement with one of the following:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
ifgroupid	<p>The id is the Unique Object Identifier (unique across the entire NNMi database). Provide the id of the Interface Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the id attribute value for each object instance.</p>
ifgroupuuid	<p>The uuid is the Universally Unique Object Identifier (unique across all databases). Provide the uuid of the Interface Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the uuid attribute value for each object instance.</p>

The following are optional parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showView&objtype= <x>&menus= <true|false>&newWindow= <true|false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>
envattrs	<p>Use Environment Attributes to store <i><name=value></i> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to the <i>originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p>

Attribute	Values
	<code>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.s- essionId= 123;com.my.objectName= node25</code>

If you want to launch some other view, specify the view rather than the object type:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>`

For more information, see:

["Launch an Incident View" \(on page 327\)](#)

["Launch a Topology Maps Workspace View" \(on page 330\)](#)

["Launch a Monitoring Workspace View" \(on page 335\)](#)

["Launch a Troubleshooting Workspace View" \(on page 338\)](#)

["Launch an Inventory Workspace View" \(on page 343\)](#)

["Launch a Management Mode Workspace Views" \(on page 346\)](#)

["Launch a Configuration Workspace View" \(on page 349\)](#)

Launch an Incident View

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

Potential Incident Workspace Views and Available Filters

View Name	x = View ID	Node Filter	Interface Filter
All Incidents	allIncidentsTableView	Yes	No
All Open Incidents	allOpenIncidentsTableView	Yes	No
Closed Key Incidents	closedKeyIncidentsTableView	Yes	No

View Name	x = View ID	Node Filter	Interface Filter
Closed Root Cause Incidents	closedRCIncidentTableView	Yes	No
Custom Incidents	customIncidentTableView	Yes	No
Incidents by Correlation Nature	incidentsByNatureTableView	Yes	No
Incidents by Family	incidentsByFamilyTableView	Yes	No
Key Incidents by Lifecycle State	keyIncidentsByLifecycleStateTableView	Yes	No
My Open Incidents	myIncidentTableView	Yes	No
NNM 6.x / 7.x Events	nnm6x7xIncidentTableView	Yes	No
NNM 6.x/7.x Event by Category	nnm6x7xIncidentByCategoryTableView	Yes	No
Open Key Incidents	openKeyIncidentsTableView	Yes	No
Open Key Incidents by Category	openKeyIncidentsByCategoryTableView	Yes	No
Open Key Incidents by Family	openKeyIncidentsByFamilyTableView	Yes	No
Open Key Incidents by Priority	openKeyIncidentsByPriorityTableView	Yes	No
Open Key Incidents by Severity	openKeyIncidentsBySeverityTableView	Yes	No
Open Root Cause by Category	openRCIncidentsByCategoryTableView	Yes	No
Open Root Cause by Family	openRCIncidentsByFamilyTableView	Yes	No
Open Root Cause by Priority	openRCIncidentsByPriorityTableView	Yes	No
Open Root Cause by Severity	openRCIncidentsBySeverityTableView	Yes	No
Open Root Cause Incidents	openRCIncidentTableView	Yes	No
Root Cause Incidents	allRCIncidentTableView	Yes	No
Root Cause by Lifecycle State	RCIncidentsByLifecycleStateTableView	Yes	No
Service Impact Incidents	serviceImpactIncidentTableView	Yes	No
SNMP Traps	snmpTrapsIncidentTableView	Yes	No
SNMP Traps by Family	snmpTrapsIncidentByFamilyTableView	Yes	No
Stream Correlation Incidents	streamCorrelationIncidentTableView	Yes	No
Unassigned Open Key Incidents	unassignedKeyIncidentsTableView	Yes	No
Unassigned Root Cause Incidents	unassignedIncidentTableView	Yes	No

The following are optional filter parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&nodegroup= <Name>`



Filter by Node Group (launched Incident, Node, Interface, and IP Address views)

Attribute	Values
nodegroup	<p>The Name attribute value of the Node Group to use as a filter for this view.</p> <p>Note: The Node Group name is translated. If your team shares NNMi within multiple locales, use nodegroupid or nodegroupuuid.</p> <p>If the Name value includes space characters, replace the space character in your URL statement with one of the following:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
nodegroupid	<p>The <code>id</code> is the Unique Object Identifier (unique across the entire NNMi database). Provide the <code>id</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.</p>
nodegroupuuid	<p>The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.</p>

The following are optional parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&menus= <true|false>&newWindow= <true|false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>
envattrs	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to the <i>originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p>

Attribute	Values
	<code>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.s- essionId= 123;com.my.objectName= node25</code>

Launch a Topology Maps Workspace View

The URL required for each one is unique.

Tip: A map session launched with a URL never times out. The view automatically updates every 30 seconds. This is useful if your network operation center (NOC) continuously displays a map of the most important nodes. See ["Configuring Maps" \(on page 198\)](#). (If you use the Mozilla Firefox browser and are prompted to click Continue before the map appears, see [Configure Mozilla Firefox Timeout Interval](#).)

Click here to show the example of a URL that opens the **Node Group Overview** map (`cmd=showNodeGroupOverview`).

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


`http://<serverName>:<portNumber>/nnm/launch?cmd= showNodeGroupOverview`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:



- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

The following are optional parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showNodeGroupOverview&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2= value>`

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>
envattrs	Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an exter-</i>

Attribute	Values
	<p><i>nal application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to the originating external application.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.s- essionId= 123;com.my.objectName= node25</pre>

Click here to show the example of a URL that opens the **Network Overview** map (cmd=showNetworkOverview).

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


http://<serverName>:<portNumber>/nnm/launch?cmd= showNetworkOverview

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:



- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

The following are optional parameters:

http://<serverName>:<portNumber>/nnm/launch?cmd= showNetworkOverview&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2= value>

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>

Attribute	Values
envattrs	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.s- essionId= 123;com.my.objectName= node25</pre>

Click here to show the example of a URL that opens the **Networking Infrastructure Devices** node group map (cmd=showView).

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&objtype= Node&nodegroup= Networking%20Infrastructure%20Devices`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:



- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

The following are optional parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&objtype= Node&nodegroup= Networking%20Infrastructure%20Devices&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2= value>`

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p>

Attribute	Values
	false = Display the view within the current browser window (if not specified, the default is false).
envattrs	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.s- essionId= 123;com.my.objectName= node25</pre>

Click here to show the example of a URL that opens the **Routers** node group map (cmd=showNodeGroup&name=Routers).

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


`http://<serverName>:<portNumber>/nnm/launch?cmd= showNodeGroup&name= Routers`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:



- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

The following are optional parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showNodeGroup&name= Routers
&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2=
value>`

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	true = Display the view in a new browser window. This new window does not display the

Attribute	Values
	<p>browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>
envattrs	<p>Use Environment Attributes to store <i><name=value></i> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</pre>

Click here to show the example of a URL that opens the **Switches** node group map (cmd=showNodeGroup&name=Switches).

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


`http://<serverName>:<portNumber>/nnm/launch?cmd= showNodeGroup&name= Switches`

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:



- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

The following are optional parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showNodeGroup&name= Switches
&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2=
value>
```

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>

Attribute	Values
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>
envattrs	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.s- essionId= 123;com.my.objectName= node25</pre>

Launch a Monitoring Workspace View

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

Monitoring Workspace Views and Available Filters

View Name	x = View ID	Node Filter	Interface Filter
Critical Component Health	criticalComponentHealthTableView	No	No
Critical Interfaces	criticalInterfaceTableView	Yes	Yes

View Name	x = View ID	Node Filter	Interface Filter
Critical Nodes	criticalNodeTableView	Yes	No
Non-Normal Interfaces	nonNormalInterfaceTableView	Yes	Yes
Non-Normal Nodes	nonNormalNodeTableView	Yes	No
Not Responding Addresses	notRespondingIPAddressTableView	Yes	Yes
Nodes by Status	nodesByStatusTableView	Yes	No
Component Health by Status	componentHealthByStatusTableView	No	No
Interfaces by Status	interfacesByStatusTableView	Yes	Yes
Interfaces by Administrative State	interfacesByAdministrativeStateTableView	Yes	Yes
Interfaces by Operational State	interfacesByOperationalStateTableView	Yes	Yes
IP Addresses by State	IPAddressesByStateTableView	Yes	Yes
Interface Performance	interfacePerformanceTableView	Yes	Yes
Router Redundancy Groups	routerRedundancyGroupsTableView	No	No
Node Groups	nodeGroupsStatusTableView	No	No

The following are optional filter parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&nogroup= <Name>`

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&ifgroup= <Name>`

Filter by Node Group (launched Incident, Node, Interface, and IP Address views)

Attribute	Values
nodegroup	<p>The Name attribute value of the Node Group to use as a filter for this view.</p> <p>Note: The Node Group name is translated. If your team shares NNMi within multiple locales, use nodegroupid or nodegroupuuid.</p> <p>If the Name value includes space characters, replace the space character in your URL statement with one of the following:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
nodegroupid	<p>The id is the Unique Object Identifier (unique across the entire NNMi database). Provide the id of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the id attribute value for each object instance.</p>

Attribute	Values
nodegroupuuid	<p>The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.</p>



Filter by Interface Group (launched Interface and IP Address views)

Attribute	Values
ifgroup	<p>The Name attribute value of the Interface Group to use as a filter for this view.</p> <p>Note: The Interface Group name is translated. If your team shares NNMi within multiple locales, use <code>ifgroupid</code> or <code>ifgroupuuid</code>.</p> <p>If the Name value includes space characters, replace the space character in your URL statement with one of the following:</p> <ul style="list-style-type: none"> • <code>%20</code> (W3C URL Encoding Standards) • <code>+</code> (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
ifgroupid	<p>The <code>id</code> is the Unique Object Identifier (unique across the entire NNMi database). Provide the <code>id</code> of the Interface Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.</p>
ifgroupuuid	<p>The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Interface Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.</p>

The following are optional parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&menus= <true|false>&newWindow= <true|false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Views

Attribute	Values
menus	<p><code>true</code> = Show the view menus and the  Close button. If not specified, the default is <code>true</code>.</p> <p><code>false</code> = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	<p><code>true</code> = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p><code>false</code> = Display the view within the current browser window (if not specified, the default is <code>false</code>).</p>

Attribute	Values
envattrs	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.s- essionId= 123;com.my.objectName= node25</pre>

Launch a Troubleshooting Workspace View

There are four types of views in the Troubleshooting workspace. The URL syntax required for each one is unique.

Tip: A map session launched with a URL never times out. The view automatically updates every 30 seconds. This is useful if your network operation center (NOC) continuously displays a map of the most important nodes. See ["Configuring Maps" \(on page 198\)](#). (If you use the Mozilla Firefox browser and are prompted to click Continue before the map appears, see [Configure Mozilla Firefox Timeout Interval](#).)

Click here to show examples of URLs that open a **Layer 2 Neighbor View** (cmd=showLayer2Neighbors).

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showLayer2Neighbors
```


```
http://<serverName>:<portNumber>/nnm/launch?cmd= showLayer2Neighbors&nodename= <x>&hops= <#>
```

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.



Layer 2 Neighbor View Attributes

Attribute	Value
nodename	<p>The source node's DNS hostname or IP address.</p> <p>Provide a full or short DNS name or an IP address.</p> <p>If you use this attribute, NNMi tries to match the string you provide by following this procedure:</p> <ul style="list-style-type: none"> • Check the value in the Hostname field on the Node form. • Check the values in the Address column of the table on the Addresses tab in the Node form. • Check the value of the System Name field on the General tab in the Node form. • Check the value in the Name field on the Node form.
hops	1 - 9

The following are optional parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showLayer2Neighbors&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>
envattrs	<p>Use Environment Attributes to store <i><name=value></i> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to the <i>originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.s- essionId= 123;com.my.objectName= node25</pre>

Click here to show examples of URLs that open a **Layer 3 Neighbor View** (cmd=showLayer3Neighbors).

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https


for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?cmd= showLayer3Neighbors`

`http://<serverName>:<portNumber>/nnm/launch?cmd= showLayer3Neighbors&nodename=<x>&hops= <#>`

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.



Layer 3 Neighbor View Attributes

Attribute	Value
nodename	The source node's DNS hostname or IP address. Provide a full or short DNS name or an IP address. If you use this attribute, NNMi tries to match the string you provide by following this procedure: <ul style="list-style-type: none"> • Check the value in the Hostname field on the Node form. • Check the values in the Address column of the table on the Addresses tab in the Node form. • Check the value of the System Name field on the General tab in the Node form. • Check the value in the Name field on the Node form.
hops	1 - 9
menus	true = Show the menus and window toolbar in the form. If not specified, the default is true. false = Hide the menus and window toolbar in the view.

The following are optional parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showLayer3Neighbors&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2= value>`

Attributes for Launched Views

Attribute	Values
menus	true = Show the view menus and the  Close button. If not specified, the default is true. false = Hide the view menus and the  Close button to save space in the view.
newWindow	true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view. false = Display the view within the current browser window (if not specified, the default is false).

Attribute	Values
envattr	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattr= com.my.sessionId= 123;com.my.objectName= node25</pre>

Click here to show examples of URLs that open a **Path View** (cmd=showPath).


Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?cmd= showPath`

`http://<serverName>:<portNumber>/nnm/launch?cmd= showPath&src= <x>&dest= <y>`

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.



Path View Attributes

Attribute	Value
src	The source node's DNS hostname or IPv4 address.
dest	The destination node's DNS hostname or IPv4 address.

The following are optional parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showPath&menus= <true/false>&newWindow= <true/false>&envattr= <name1= value>;<name2= value>`

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>

Attribute	Values
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>
envattrs	<p>Use Environment Attributes to store <i><name=value></i> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</pre>


Click here to show examples of URLs that open a **Node Group Map View** (cmd=showNodeGroup).

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?cmd= showNodeGroup&name= <x>`

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

Node Group Map View Attributes



Attribute	Value
name	<p>The Name attribute value from the Node Group form.</p> <p>Note: The Node Group name is translated. If your team shares NNMi within multiple locales, use nodegroupid or nodegroupuid.</p> <p>If the Name value includes space characters, replace the space character in your URL statement:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)

Attribute	Value
objid	<p>The <code>id</code> is the Unique Object Identifier (unique across the entire NNMi database). Provide the <code>id</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.</p>
objuuid	<p>The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.</p>

The following are optional parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showNodeGroup&name= <x>&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>
envattrs	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</pre>

Launch an Inventory Workspace View

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>
```

Network Node Manager (NNMi 8.1x Patch 4) Online Help: Information for Administrators


Integrating NNMi Elsewhere with URLs

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

Inventory Workspace Views and Available Filters

View Name	x = View ID	Node Filter	Interface Filter
Nodes	allNodesTableView	Yes	No
Interfaces	allInterfacesTableView	Yes	Yes
IP Addresses	allIPAddressTableView	Yes	Yes
IP Subnets	allIPSubnetsTableView	No	No
VLANs	allVlansTableView	No	No
Layer 2 Connections	allLayer2ConnectionsTableView	No	No
Nodes by Device Category	nodesByDeviceCategoryTableView	Yes	No
Interfaces by IfType	interfacesByIfTypeTableView	Yes	No
Custom Nodes	customNodeTableView	Yes	No
Custom Interfaces	customInterfaceTableView	Yes	Yes
Custom IP Addresses	customIPAddressTableView	Yes	Yes
Router Redundancy Groups	routerRedundancyGroupsTableView	No	No
Node Groups	nodeGroupsTableView	No	No
Interface Groups	interfaceGroupsTableView	No	No
Management Stations	allManagementStationsTableView	No	No

The following are optional filter parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&nodegroup= <Name>`

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&interfacegroup= <Name>`

Filter by Node Group (launched Incident, Node, Interface, and IP Address views)

Attribute	Values
nodegroup	<p>The Name attribute value of the Node Group to use as a filter for this view.</p> <p>Note: The Node Group name is translated. If your team shares NNMi within multiple locales, use nodegroupid or nodegroupuuid.</p> <p>If the Name value includes space characters, replace the space character in your URL statement with one of the following:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
nodegroupid	<p>The <code>id</code> is the Unique Object Identifier (unique across the entire NNMi database). Provide the <code>id</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.</p>
nodegroupuuid	<p>The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.</p>

Filter by Interface Group (launched Interface and IP Address views)

Attribute	Values
ifgroup	<p>The Name attribute value of the Interface Group to use as a filter for this view.</p> <p>Note: The Interface Group name is translated. If your team shares NNMi within multiple locales, use ifgroupid or ifgroupuuid.</p> <p>If the Name value includes space characters, replace the space character in your URL statement with one of the following:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
ifgroupid	<p>The <code>id</code> is the Unique Object Identifier (unique across the entire NNMi database). Provide the <code>id</code> of the Interface Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.</p>
ifgroupuuid	<p>The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Interface Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attrib-</p>

Attribute	Values
-----------	--------

ute value for each object instance.

The following are optional parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Views

Attribute	Values
-----------	--------

menus true = Show the view menus and the  Close button. If not specified, the default is true.
false = Hide the view menus and the  Close button to save space in the view.

newWindow true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.
false = Display the view within the current browser window (if not specified, the default is false).

envattrs Use Environment Attributes to store *<name=value>* pairs that were passed *from an external application* to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).

Note: see ["Environment Attributes in URL Actions" \(on page 315\)](#) for information about how to pass these same environment attribute name-value pairs from NNMi back to *the originating external application*.

For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:

```
http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25
```

Launch a Management Mode Workspace Views

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


```
http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

Management Mode Workspace Views

View Name	x = View ID	Node Filter	Interface Filter
Managed Nodes	managedNodeTableView	Yes	No
Managed Interfaces	managedInterfaceTableView	Yes	Yes
Managed IP Addresses	managedIPAddressTableView	Yes	Yes
Not Managed Nodes	notManagedNodeTableView	Yes	No
Not Managed Interfaces	notManagedInterfaceTableView	Yes	Yes
Not Managed IP Addresses	notManagedIPAddressTableView	Yes	Yes
Out of Service Nodes	outOfServiceNodeTableView	Yes	No
Out of Service Interfaces	outOfServiceInterfaceTableView	Yes	Yes
Out of Service IP Addresses	outOfServiceIPAddressTableView	Yes	Yes
Nodes	managementModeNodeTableView	Yes	No
Interfaces	managementModeInterfaceTableView	No	Yes
IP Addresses	managementModeIPAddressTableView	Yes	Yes

The following are optional filter parameters: The following are optional parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&nodegroup= <Name>`

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&ifgroup= <Name>`

Filter by Node Group (launched Incident, Node, Interface, and IP Address views)

Attribute	Values
nodegroup	<p>The Name attribute value of the Node Group to use as a filter for this view.</p> <p>Note: The Node Group name is translated. If your team shares NNMi within multiple locales, use nodegroupid or nodegroupuuid.</p> <p>If the Name value includes space characters, replace the space character in your URL statement with one of the following:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
nodegroupid	<p>The id is the Unique Object Identifier (unique across the entire NNMi database). Provide the id of the Node Group to use as a filter for this view.</p>



Attribute	Values
	This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.
nodegroupuuid	The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Node Group to use as a filter for this view. This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.

Filter by Interface Group (launched Interface and IP Address views)

Attribute	Values
ifgroup	The Name attribute value of the Interface Group to use as a filter for this view. Note: The Interface Group name is translated. If your team shares NNMi within multiple locales, use <code>ifgroupid</code> or <code>ifgroupuuid</code> . If the Name value includes space characters, replace the space character in your URL statement with one of the following: <ul style="list-style-type: none"> • <code>%20</code> (W3C URL Encoding Standards) • <code>+</code> (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
ifgroupid	The <code>id</code> is the Unique Object Identifier (unique across the entire NNMi database). Provide the <code>id</code> of the Interface Group to use as a filter for this view. This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.
ifgroupuuid	The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Interface Group to use as a filter for this view. This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&menus= <true/false>&newWindow= = <true/false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Views

Attribute	Values
menus	true = Show the view menus and the  Close button. If not specified, the default is true. false = Hide the view menus and the  Close button to save space in the view.
newWindow	true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view. false = Display the view within the current browser window (if not specified, the default is

Attribute	Values
	false).
envattrs	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to pre-serve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.s- essionId= 123;com.my.objectName= node25</pre>

Launch a Configuration Workspace View

Configuration workspaces require that the user be assigned to the **Administrative** role.

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)


`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi view with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.

Use the browser buttons to close the view.

Configuration Workspace Views



View Name	x = View ID
Node Groups	nodeGroupsTableView
Node Group Map Settings	allNodeGroupMapSettingsTableView
Interface Groups	interfaceGroupsTableView
Management Stations	allManagementStationsTableView
RAMS Servers	ramsServerTableView

View Name	x = View ID
URL Actions	allURLActionInfosTableView
User Accounts and Roles	allAccountsTableView
IfTypes	allIfTypesTableView
Device Profiles	allDeviceProfilesTableView

The following are optional parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showView&view= <x>&menus= <true/false>&newWindow= <true/false>&envattrs= <name1= value>;<name2= value>`

Attributes for Launched Views

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
newWindow	<p>true = Display the view in a new browser window. This new window does not display the browser-specific menu bars. The browser-specific menu bars are hidden to provide the maximum amount of room for the requested view.</p> <p>false = Display the view within the current browser window (if not specified, the default is false).</p>
envattrs	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</pre>

Launch a Form (showForm)

To launch a particular form, use the following URL:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?cmd=showForm...`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Launch a form to see information about a particular node, interface, address, subnet, or incident. In the URL string, you must include one or more attributes that enable NNMi to find a specific object. If more than one object meets the criteria, NNMi opens the first one found. When designating more than one attribute, separate each with a semicolon character.

["Launch a Node Form" \(on page 351\)](#)

["Launch an Interface Form" \(on page 353\)](#)

["Launch an IP Address Form" \(on page 355\)](#)

["Launch a Subnet Form" \(on page 356\)](#)

["Launch an Incident Form" \(on page 357\)](#)

["Launch a Node Group Form" \(on page 358\)](#)

["Launch a Configuration Form" \(on page 360\)](#)

Launch a Node Form

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Node&nodename= <x>
```

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Node&objattrs= name= <x>
```

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Node&objattrs= hostname= <x>
```

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Node&objattrs= snmpAgent.agentSettings.managementAddress= <x>
```



```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Node&objattrs= systemName= <x>
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi form with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.
- The  Save and Close button saves data, but does not close the window.
- The File → Save and Close menu item saves data, but does not close the window.

Use the browser buttons to close the form.

Node Form Attributes

Attribute	Values
nodename	<p>Provide a full or short DNS name or an IP address.</p> <p>If you use this attribute, NNM tries to match the string you provide by following this procedure:</p> <ul style="list-style-type: none">• Check the value in the Hostname field on the Node form.• Check the values in the Address column of the table on the Addresses tab in the Node form.• Check the value of the System Name field on the General tab in the Node form.• Check the value in the Name field on the Node form.
name	<p>The Name attribute value from the Node form.</p>
hostname	<p>Caution: The Hostname attribute value on the Node form of the discovered node must match what is entered here (see the Hostname attribute the Node form help topic).</p> <p>If a device has multiple hostnames or no hostname, NNMi follows a set of rules to determine the hostname. Click here for details.</p> <ol style="list-style-type: none">1. If a hostname is available, it must resolve to a valid IP address. NNMi stores the fully-qualifiedhostname in the database as all lowercase characters.2. If more than one address is associated with a node, the loopback address¹ is used with the following exceptions:<ul style="list-style-type: none">■ NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).■ NNMi ignores any address that is virtual (HSRP/VRRP) or an Any-cast Rendezvous Point IP Address².3. If a node has multiple loopback addresses, NNMi uses the loopback address with the lowest number that resolves to a hostname (for example, 10.16.42.197 is a lower number than 10.16.197.42).4. If no loopback address resolves to a hostname and the device supports SNMP, NNMi uses the current value from the Management Address attribute on the Node form.5. If the device does not support SNMP, the IP address or DNS name found during the current rediscovery cycle is used as the hostname.

¹The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.



²Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

Attribute	Values
	This sequence is repeated during each rediscovery cycle. The hostname could change from cycle to cycle (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).
snmpAgent.agentSettings.managementAddress	The Management Address attribute value from the SNMP Agent form of the agent assigned to the specified node. The value is an IP address.
systemName	System Name attribute value (from the Node form, General tab).

The following are optional filter parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Node&nodename=
<x>&menus= <true/false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Forms

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
envattrs	<p>Use Environment Attributes to store <i><name=value></i> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</pre>

Launch an Interface Form

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Inter-
face&objattrs= hostedOn.hostname= <x>;name= <y>
```

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Inter-
face&objattrs= hostedOn.hostname= <x>;ifName= <y>
```

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Inter-
face&objattrs= hostedOn.hostname= <x>;ifAlias= <y>
```



```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Inter-
face&objattrs= hostedOn.hostname= <x>;ifIndex= <y>
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi form with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.
- The  Save and Close button saves data, but does not close the window.
- The File → Save and Close menu item saves data, but does not close the window.

Use the browser buttons to close the form.



Interface Form Attributes

Attribute	Values
hostedOn.hostname	The Hostname of the Node in which the interface resides. This is the Hostname attribute value from the associated Node form .
name	The Name attribute value from the Interface form .
ifName	The IfName attribute value from the Interface form.
ifAlias	The IfAlias attribute value from the Interface form.
ifIndex	The IfIndex attribute value from the Interface form.

The following are optional filter parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Inter-
face&objattrs= hostedOn.hostname= <x>;name= <y>&menus= <true/false>&envattrs= <
name1= value>;<name2= value>
```

Attributes for Launched Forms

Attribute	Values
menus	true = Show the view menus and the  Close button. If not specified, the default is true. false = Hide the view menus and the  Close button to save space in the view.
envattrs	Use Environment Attributes to store <i><name=value></i> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program). Note: see " Environment Attributes in URL Actions " (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i> . For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows: <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</pre>

Launch an IP Address Form

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)



`http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= IPAddress&objattrs= value= <y>`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi form with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.
- The  Save and Close button saves data, but does not close the window.
- The File → Save and Close menu item saves data, but does not close the window.

Use the browser buttons to close the form.



IP Address Form Attributes

Attribute	Values
value	The Address attribute value from the IP Address form .

The following are optional filter parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= IPAddress&objattrs= value= <y>&menus= <true/false>&envattrs= <name1= value>;<name2= value>`

Attributes for Launched Forms

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
envattrs	<p>Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to the <i>originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p>

Attribute	Values
	<code>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</code>

Launch a Subnet Form

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= IPSubnet&objattrs= name= <x>`

`http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= IPSubnet&objattrs= prefix= <x>`



`http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= IPSubnet&objattrs= prefix= <x>;prefixLength= <y>`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi form with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.
- The  Save and Close button saves data, but does not close the window.
- The File → Save and Close menu item saves data, but does not close the window.

Use the browser buttons to close the form.



IP Subnet Form Attributes

Attribute	Values
name	The Name attribute value from the IP Subnet form .
prefix	The Prefix attribute value from the IP Subnet form.
prefixLength	The Prefix Length attribute value from the IP Subnet form.

The following are optional filter parameters:

`http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= IPSubnet&objattrs= name= <x>&menus= <true/false>&envattrs= <name1= value>;<name2= value>`

Attributes for Launched Forms

Attribute	Values
menus	true = Show the view menus and the  Close button. If not specified, the default is true. false = Hide the view menus and the  Close button to save space in the view.
envattrs	Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program). Note: see " Environment Attributes in URL Actions " (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to the <i>originating external application</i> . For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows: <code>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</code>

Launch an Incident Form

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Incident&objid= <x>`



`http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= Incident&objuuid= <x>`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi form with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.
- The  Save and Close button saves data, but does not close the window.
- The File → Save and Close menu item saves data, but does not close the window.

Use the browser buttons to close the form.

Individual incident objects must be identified by their *database unique identifiers*.



Incident Attributes

Attribute	Values
objid	The Unique Object Identifier (unique across the entire NNMi database). This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.
objuuid	The Universally Unique Object Identifier (unique across all databases). This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.

The following are optional filter parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&showForm&objtype= Incident&objid= <x>&menus= <true/false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Forms

Attribute	Values
menus	true = Show the view menus and the  Close button. If not specified, the default is true. false = Hide the view menus and the  Close button to save space in the view.
envattrs	Use Environment Attributes to store <code><name=value></code> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program). Note: see " Environment Attributes in URL Actions " (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to the originating external application. For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows: <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</pre>

Launch a Node Group Form

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= NodeGroup&name= <y>
```

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= NodeGroup&nod- egroupid= <y>
```



```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= NodeGroup&nod- egroupuuid= <y>
```

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi form with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.
- The  Save and Close button saves data, but does not close the window.
- The File → Save and Close menu item saves data, but does not close the window.

Use the browser buttons to close the form.



Node Group Form Attributes

Attribute	Values
name	<p>The Name attribute value from the Node Group form.</p> <p>Note: The Node Group name is translated. If your team shares NNMi within multiple locales, use nodegroupid or nodegroupuuid.</p> <p>If the Name value includes space characters, replace the space character in your URL statement:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
nodegroupid	<p>The <code>id</code> is the Unique Object Identifier (unique across the entire NNMi database). Provide the <code>id</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.</p>
nodegroupuuid	<p>The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.</p>

The following are optional filter parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showForm&objtype= NodeGroup&name=
<y>&menus= <true/false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Forms

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>

Attribute	Values
envattrs	<p>Use Environment Attributes to store <i><name=value></i> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to the <i>originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId=123;com.my.objectName= node25</pre>

Launch a Configuration Form

Configuration forms require that the user be assigned to the **Administrative** role.

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)



`http://<serverName>:<portNumber>/nnm/launch?cmd= showConfigForm&name= <y>`

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Note: If you are using Mozilla Firefox, click here for more information.

Due to the Mozilla Firefox security implementation, launching an NNMi form with a URL has the following limitations:

- The  Close button does not work.
- The File → Close menu item does not work.
- The  Save and Close button saves data, but does not close the window.
- The File → Save and Close menu item saves data, but does not close the window.

Use the browser buttons to close the form.

Configuration Form Attributes



Attribute	Values
name	<p>The name attribute value specifies which form:</p> <ul style="list-style-type: none"> • communication = the Communication Configuration form • custompoller = the Custom Poller Configuration form • discovery = the Discovery Configuration form • monitoring = the Monitoring Configuration form

Attribute	Values
	<ul style="list-style-type: none"> • incident = the Incident Configuration form • status = the Status Configuration form • ui = the User Interface Configuration form

The following are optional filter parameters:

```
http://<serverName>:<portNumber>/nnm/launch?cmd= showConfigForm&name= lt;y>&menus=
<true/false>&envattrs= <name1= value>;<name2= value>
```

Attributes for Launched Forms

Attribute	Values
menus	<p>true = Show the view menus and the  Close button. If not specified, the default is true.</p> <p>false = Hide the view menus and the  Close button to save space in the view.</p>
envattrs	<p>Use Environment Attributes to store <i><name=value></i> pairs that were passed <i>from an external application</i> to NNMi. Environment Attributes are session-specific and stored in memory (not in the NNMi database). The name-value pairs can be any arbitrary string (as required by the external program).</p> <p>Note: see "Environment Attributes in URL Actions" (on page 315) for information about how to pass these same environment attribute name-value pairs from NNMi back to <i>the originating external application</i>.</p> <p>For example, let's assume that NNMi was launched from an application that wants to preserve a session ID (123) and object attribute (node25) as follows:</p> <pre>http://host/nnm?cmd= showView&objtype= Node&envattrs= com.my.sessionId= 123;com.my.objectName= node25</pre>

Launch Menu Items (runTool)

To launch a menu item, use the following URL:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

```
http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=<x>
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Provide quick access to NNMi menu items wherever your team needs them:

["Launch the Actions: Ping Command" \(on page 362\)](#)

["Launch the Actions: Trace Route Command" \(on page 362\)](#)

["Launch the Actions: Communication Configuration Command" \(on page 363\)](#)

["Launch the Actions: Monitoring Settings Command" \(on page 364\)](#)

["Launch the Actions: Status Poll Command" \(on page 367\)](#)

["Launch the Actions: Configuration Poll Command" \(on page 367\)](#)

["Launch the Actions: Status Details Command \(for Node Groups\)" \(on page 368\)](#)

["Launch the Tools: NNMi Status Command" \(on page 369\)](#)

["Launch the Tools: Sign In/Out Audit Log Command" \(on page 370\)](#)

["Launch the File: Sign-Out Command" \(on page 370\)](#)

Launch the Actions: Ping Command

This URL is equivalent to the **Actions** → **Ping (from server)** command in the console.

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

To launch a window that requests you to enter a node name, use the following URL:

`http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=ping`

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

After you specify a node, the real-time results of the ping command appear.

To launch the real-time results of the ping command, use the following URL:

`http://<serverName>:<portNumber>/nnm/launch?cmd=run-
Tool&tool=ping&timeoutSecs=<x>&numPings=<x>&nodename=<x>`

Ping Command Attributes

Attribute	Values
nodename	A DNS resolvable hostname or IP address. The nodename value is passed literally to the underlying command you specify. The nodename value (in this case) is not required to correlate with anything in the NNM database.
timeoutSecs	Amount of time NNMi waits before abandoning a ping request.
numPings	Maximum number of retries.

Related Topics:

[Test Node Access \(Ping\)](#)

Launch the Actions: Trace Route Command

This URL is equivalent to the **Actions** → **Trace Route (from server)** command in the console.

Note: If the NNMi Web server uses the https protocol, use `https` instead of `http`. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

To launch a window that requests you to enter a node name, use the following URL:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=traceroute
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

After you specify a node, the real-time results of the trace route command appear.

To launch the real-time results of the trace route command, use the following URL:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=traceroute&nodename=<x>
```

Trace Route Command Attributes

Attribute	Values
nodename	A DNS resolvable hostname or IP address. The nodename value is passed literally to the underlying command you specify. The nodename value (in this case) is not required to correlate with anything in the NNM database.

Related topics:

[Find the Route \(traceroute\)](#)

Launch the Actions: Communication Configuration Command

This URL is equivalent to the **Actions** → **Communication Settings** command in the console.

Note: If the NNMi Web server uses the https protocol, use `https` instead of `http`. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

To launch a window that reports the current ICMP and SNMP configuration for a node, use the following URL:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=commconf
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

After you specify a node, the real-time results of the ICMP and SNMP configuration report appear.

To launch the real-time results of the ICMP and SNMP configuration report, use the following URL:

`http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=commconf&nodename=<x>`

Communication Configuration Command Attributes

Attribute	Values
nodename	Provide a full or short DNS name or an IP address. If you use this attribute, NNM tries to match the string you provide by following this procedure: <ul style="list-style-type: none">• Check the value in the Hostname field on the Node form.• Check the values in the Address column of the table on the Addresses tab in the Node form.• Check the value of the System Name field on the General tab in the Node form.• Check the value in the Name field on the Node form.

Related Topics:

["Verify Your Communication Settings" \(on page 75\)](#)

Launch the Actions: Monitoring Settings Command

This URL is equivalent to the **Actions** → **Monitoring Settings** command in the console.

Launch the real-time results of the Monitoring configuration report. You must specify the target object.

Note: If the NNMi Web server uses the https protocol, use `https` instead of `http`. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

Click here to show an example URL for requesting a current Monitoring configuration report on a **Node**:

`http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=monitoringconf&objtype=SnmpAgent&nodename=<x>`

Monitoring Configuration Command Node Report Attributes

Attribute	Values
nodename	Provide a full or short DNS name or an IP address. If you use this attribute, NNMi tries to match the string you provide by following this procedure: <ul style="list-style-type: none">• Check the value in the Hostname field on the Node form.• Check the values in the Address column of the table on the IP Addresses tab in the Node form.• Check the value of the System Name field on the General tab in the Node form.• Check the value in the Name field on the Node form.

Click here to show example URLs for requesting a current Monitoring configuration report on an **Interface**:

NNMi displays the report for the first matching Interface found. Provide one or more attributes to ensure a unique match. See "[Launch an Interface Form](#)" (on page 353) for more information about each available attribute.

```
http://<serverName>:<portNumber>/nnm/launch?cmd=run-  
Tool&tool=monitoringconf&objtype=Interface&objattrs=hostedOn.hostname=<x>;name=<x>
```

```
http://<serverName>:<portNumber>/nnm/launch?cmd=  
=runTool&tool=monitoringconf&objtype=Interface&objattrs=host-  
edOn.hostname=<x>;ifName=<x>
```

```
http://<serverName>:<portNumber>/nnm/launch?cmd=  
=runTool&tool=monitoringconf&objtype=Interface&objattrs=host-  
edOn.hostname=<x>;ifAlias=<x>
```

```
http://<serverName>:<portNumber>/nnm/launch?cmd=  
=runTool&tool=monitoringconf&objtype=Interface&objattrs=host-  
edOn.hostname=<x>;ifIndex=<x>
```

Interface Form Attributes

Attribute	Values
hostedOn.hostname	The Hostname of the Node in which the interface resides. This is the Hostname attribute value from the associated Node form .
name	The Name attribute value from the Interface form .
ifName	The IfName attribute value from the Interface form.
ifAlias	The IfAlias attribute value from the Interface form.
ifIndex	The IfIndex attribute value from the Interface form.

Click here to show an example URL for requesting a current Monitoring configuration report on an **IP Address**:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=run-  
Tool&tool=monitoringconf&objtype=IPAddress&objattrs=value=<x>
```

IP Address Form Attributes

Attribute	Values
value	The Address attribute value from the IP Address form .

Click here to show an example URL for requesting a current Monitoring configuration report on an **Router Redundancy Member** (Instance):

```
http://<serverName>:<portNumber>/nnm/launch?cmd=ru-  
nTool&tool=monitoringconf&objtype=RouterRedundancyInstance&objid=<x>
```

Monitoring Configuration Command Router Redundancy Member Report Attributes

Attribute	Values
objid	The Unique Object Identifier (unique across the entire NNMi database).

Attribute	Values
	This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.
objuuid	The Universally Unique Object Identifier (unique across all databases). This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.

Click here to show an example URL for requesting a current Monitoring configuration report on an **Tracked Object**:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=monitoringconf&objtype=TrackedObject&objid=<x>
```

Monitoring Configuration Command Tracked Object Report Attributes

Attribute	Values
objid	The Unique Object Identifier (unique across the entire NNMi database). This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.
objuuid	The Universally Unique Object Identifier (unique across all databases). This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.

Click here to show an example URL for requesting a current Monitoring configuration report on a **Node Component**:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=monitoringconf&objtype=ComponentHealth&objid=<x>
```

Monitoring Configuration Command Node Component Report Attributes

Attribute	Values
objid	The Unique Object Identifier (unique across the entire NNMi database). This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.
objuuid	The Universally Unique Object Identifier (unique across all databases). This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.

Related Topics:

["Verify Monitoring Configuration Settings" \(on page 181\)](#)

Launch the Actions: Status Poll Command

This URL is equivalent to the **Actions** → **Status Poll** command in the console. This command launches a real-time check of the state of the specified device. If the state has changed since the last monitoring cycle, NNMi calculates an updated status reading for the selected device.

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

To launch a window that reports the current status for a node, use the following URL:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=statuspoll
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

After you specify a node, the real-time results of the node's status appear.

To launch the real-time results of a node's status, use the following URL:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=statuspoll&nodename=<x>
```

Status Poll Command Attributes

Attribute	Values
nodename	Provide a full or short DNS name or an IP address. If you use this attribute, NNMi tries to match the string you provide by following this procedure: <ul style="list-style-type: none">• Check the value in the Hostname field on the Node form.• Check the values in the Address column of the table on the IP Addresses tab in the Node form.• Check the value of the System Name field on the General tab in the Node form.• Check the value in the Name field on the Node form.

Related Topics:

[Verify Current Status of a Device](#)

Launch the Actions: Configuration Poll Command

This URL is equivalent to the **Actions** → **Configuration Poll** command in the console.

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

To launch a window that reports the current configuration for a node, use the following URL:

`http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=configurationpoll`

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

After you specify a node, the real-time results of the node's configuration appear.

To launch the real-time results of a node's configuration, use the following URL:

`http://<serverName>:<portNumber>/nnm/launch?cmd=run-
Tool&tool=configurationpoll&nodename=<x>`

Configuration Poll Command Attributes

Attribute	Values
nodename	Provide a full or short DNS name or an IP address. If you use this attribute, NNMi tries to match the string you provide by following this procedure: <ul style="list-style-type: none">• Check the value in the Hostname field on the Node form.• Check the values in the Address column of the table on the Addresses tab in the Node form.• Check the value of the System Name field on the General tab in the Node form.• Check the value in the Name field on the Node form.

Related Topics:

[Verify Device Configuration Details](#)

Launch the Actions: Status Details Command (for Node Groups)

This URL is equivalent to the **Actions** → **Status Details** command in the console.

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

To launch a status poll calculation for a specified Node Group, use the following URL:

`http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=nodegroupstatus`

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

After you specify a node group, the real-time results of the node group's status poll calculations appear.

To launch the real-time results of a node's configuration, use the following URL:

```
http://<serverName>:<portNumber>/nnm/launch?cmd=run-  
Tool&tool=nodegroupstatus&nodegroup=<x>
```

Filter by Node Group (launched Incident, Node, Interface, and IP Address views)

Attribute	Values
nodegroup	<p>The Name attribute value of the Node Group to use as a filter for this view.</p> <p>Note: The Node Group name is translated. If your team shares NNMi within multiple locales, use nodegroupid or nodegroupuuid.</p> <p>If the Name value includes space characters, replace the space character in your URL statement with one of the following:</p> <ul style="list-style-type: none"> • %20 (W3C URL Encoding Standards) • + (works in most browsers, but not guaranteed) • space character (works in some browsers, but not guaranteed)
nodegroupid	<p>The <code>id</code> is the Unique Object Identifier (unique across the entire NNMi database). Provide the <code>id</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>id</code> attribute value for each object instance.</p>
nodegroupuuid	<p>The <code>uuid</code> is the Universally Unique Object Identifier (unique across all databases). Provide the <code>uuid</code> of the Node Group to use as a filter for this view.</p> <p>This attribute value is not visible on any form within the console. To find this value, use the nnmconfigexport.ovpl command-line tool to export an XML file that includes the <code>uuid</code> attribute value for each object instance.</p>

Related Topics:

[Check Status Details for a Node Group](#)

Launch the Tools: NNMi Status Command

This URL is equivalent to the **Tools** → **NNMi Status** command in the console.

To launch a report of the current status of all NNMi processes and services, use the following URL:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

```
http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=nnmstatus
```

<serverName> = the fully-qualified domain name of the NNMi management server

<portNumber> = the port that the jboss application server uses for communicating with the NNMi console

Related Topics:

["Verify that NNMi Processes Are Running" \(on page 26\)](#)

[Check the Status of NNMi](#)

["NNMi Processes and Services" \(on page 25\)](#)

Launch the Tools: Sign In/Out Audit Log Command

This URL is equivalent to the **Tools** → **Sign In/Out Audit Log** command in the console.

To launch a window that reports the current configuration for a node, use the following URL:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?cmd=runTool&tool=signinaudit`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

NNMi logs the history of sign-in and sign-out activity for each user since the NNMi management server was last restarted.

Related Topics:

["Audit NNMi User Activity" \(on page 43\)](#)

Launch the File: Sign-Out Command

This URL is equivalent to the **File** → **Sign Out** command in the console.

To provide a link that issues a sign-out command, use the following URL:

Note: If the NNMi Web server uses the https protocol, use https instead of http. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?cmd=signOut`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

This closes the user session and frees up any memory associated with the session.

Related Topics:

["Sign Out from the Console" \(on page 46\)](#)

Confirm that NNMi Is Running (cmd=isRunning)

To launch a message reporting whether NNMi is currently running, use the following URL:

Note: If the NNMi Web server uses the https protocol, use `https` instead of `http`. (See the "Enabling https for NNMi" chapter in the *HP Network Node Manager i-series Software Deployment Guide*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>)

`http://<serverName>:<portNumber>/nnm/launch?cmd=isRunning`

`<serverName>` = the fully-qualified domain name of the NNMi management server

`<portNumber>` = the port that the jboss application server uses for communicating with the NNMi console

One of the following messages appears:

- NNMi is running.
- A browser error message that the URL is unreachable.

Maintaining NNMi

As an NNMi administrator, you will want to perform the following tasks when maintaining NNMi configurations and data.

["Track Your NNMi Licenses" \(on page 372\)](#)

["Export and Import Configuration Settings" \(on page 373\)](#)

["Back Up and Restore NNMi" \(on page 385\)](#)

["Archive and Delete Incidents" \(on page 387\)](#)

Track Your NNMi Licenses

To assist you in tracking your NNMi licenses, NNMi displays a status message at the bottom of the main console whenever the number of nodes in the database reaches your license limit (based on number of nodes discovered). Install additional licenses (for 50 node increments or more) to extend the limit.

To see a report of the current number of discovered nodes and the current NNMi license limit, access **View Licensing Information** from either of the following locations:

- **Help** → **About HP Network Node Manager i-series**
- The Console Sign-In window

There are four categories of licenses. Each category might have one of three states (instant-on, temporary, or permanent):

- Instant-On or Temporary licenses
- Licenses for NNMi, itself.
- Integration Enablement licenses (for example, required when connecting to an NNMi Smart Plug-in (iSPI) on a remote server or extending the functionality of NNMi in other ways).
- Licenses for developers (SDK licenses).

When tracking license information, note the following:

- NNMi discovers and manages nodes up to the NNMi license limit.
- If the number of discovered nodes reaches or exceeds the licensed limit, NNMi randomly "Unmanages" nodes until the number of "Managed" nodes matches the license limit. No new nodes are discovered until a license extension is installed. If any seeds were "Unmanaged" because of license issues, those seeds are the first nodes changed back to "Managed" after the license extension is installed.

For example: this situation might occur when an Instant-On or Temporary license expires or when an incremental license is intentionally uninstalled from a particular server.

- NNMi generates Incidents under the following circumstances:
 - The number of discovered nodes exceeds the current license limit.
 - An Instant-On or Temporary license expires.
 - An NNMi Smart Plug-in (iSPI) is purchased and installed on the NNMi management server. However, the NNMi license limit does not match the NNM iSPI license limit. See ["Purchase an HP Smart Plug-in"](#) for more information about the NNMi Smart Plug-ins.

- The NNMi license limit does not match the required Integration Enablement license limit (for example, when connecting to an NNMi Smart Plug-in (iSPI) on a remote server or when extending the functionality of NNMi in other ways by using the NNMi SDK).

Export and Import Configuration Settings

Please see the [nnmconfigexport.ovpl](#) and [nnmconfigimport.ovpl](#) Reference Pages for more information, including the complete list of the command line arguments for each command.

The choices that you make when exporting NNMi configuration settings determine how that configuration information can be used.

For example, you might want to make a quick copy of the existing NNMi configuration settings before you try experimenting with a new idea. You can use that exported file to restore your configuration settings if your experiment doesn't work the way you thought it would work.

You might want to copy the NNMi configuration settings to another NNMi management server. For example, import configuration settings when deploying after configuring NNMi in a test environment. Or when establishing remote NNMi management servers, use the central NNMi management server's configuration settings as a starting point.

Carefully review the following topics to make an informed choice:

["Export/Import Behavior and Dependencies" \(on page 373\)](#)

["Export a Snapshot of Your Configuration Settings" \(on page 377\)](#)

["Import Configuration Files to Restore Previous Settings" \(on page 378\)](#)

["Transfer Configuration Settings to Another NNMi Management Server" \(on page 379\)](#)

["Troubleshooting Imports of Configuration Files" \(on page 382\)](#)

Export/Import Behavior and Dependencies

Your configuration settings can be exported to make a copy, and then imported onto the same NNMi management server or another NNMi management server. You need to understand the behavior and dependencies as described in the table below. The locale setting on the NNMi management server at the time of Export must match the locale setting on the NNMi management server at the time of Import.

Replaces all. Export files with this behavior make changes to the NNMi database when Imported (click here for more information).

- NNMi replaces all object instances with matching key identifiers (see ["Troubleshooting Imports of Configuration Files" \(on page 382\)](#) for information about key identifiers).
- NNMi adds all object instances with key identifiers that do not exist in the NNMi database
- **NNMi deletes all existing object instances whose key identifiers do not match any in the exported file.**

Incremental. Export files with this behavior make changes to the NNMi database when Imported (click here for more information).

- NNMi updates all object instances with matching key identifiers (see ["Troubleshooting Imports of Configuration Files" \(on page 382\)](#) for information about key identifiers).

Caution: NNMi also overwrites the values of any codes associated with these object instances (for example, incident family).

- NNMi adds all object instances with key identifiers that do not exist in the NNMi database.
- NNMi does not touch existing object instances whose key identifiers do not match any in the exported file.

Incremental (subset). Export files with this behavior include configuration changes that were made by one Author. Export files with this behavior make changes to the NNMi database when Imported (click here for more information).

- NNMi updates all object instances with matching key identifiers (see "[Troubleshooting Imports of Configuration Files](#)" (on page 382) for information about key identifiers).

Caution: NNMi also overwrites the values of any codes associated with these object instances (for example, incident family).

- NNMi adds all object instances with key identifiers that do not exist in the NNMi database.
- NNMi does not touch existing object instances whose key identifiers do not match any in the exported file.

Export/Import Behavior and Dependencies Among Configuration Areas

Configuration Workspace's View Name	Export Option	Import Behavior	Dependencies
Author *	-c author	Incremental	No dependencies. Import requires one Export file (author.xml). * Not a workspace, but an important data object.
	-c author -a <author>	Incremental (subset)	No dependencies. Import requires one Export file (author.xml).
Communication	-c comm	Replaces all	No dependencies. Import requires one Export file (comm.xml). Caution: SNMPv3 credentials are never imported.
Custom Poller	-c custpoll	Incremental	Import requires four Export files, and they must be imported in this order: (1) author.xml, (2) device.xml, (3) nodegroup.xml, and (4) custpoll.xml Note: When importing Custom Poller configurations, NNMi automatically sets the Active State attribute value for all imported Policies to <i>Suspended</i> .

Configuration Workspace's View Name	Export Option	Import Behavior	Dependencies
Device Profiles	-c device	Incremental	Import requires two Export files, and they must be imported in this order: (1) author.xml and (2) device.xml
	-c device -a <author>	Incremental (subset)	Import requires one Export file (device.xml). The required Author information is embedded in the Export file.
Discovery	-c disco	Replaces all	Import requires three Export files, and they must be imported in this order: (1) comm.xml, (2) discoseed.xml, and (3) disco.xml
Discovery Seeds	-c discoseed	Incremental	Import requires two Export files, and they must be imported in this order: (1) comm.xml and (2) discoseed.xml
Incident	-c incident	Replaces all	Import requires two Export files, and they must be imported in this order: (1) author.xml and (2) incident.xml
	-c incident -a <author>	Incremental (subset)	Import requires one Export file (incident.xml). The required Author information is embedded in the Export file.
Interface Groups	-c ifgroup	Incremental	Import requires five Export files, and they must be imported in this order: (1) iftype.xml, (2) author.xml, (3) device.xml, (4) nodegroup.xml, and (5) ifgroup.xml
IfTypes	-c iftype	Incremental	Interface Types. No dependencies. Import requires one Export file (iftype.xml).
Management Stations (6.x/7.x)	-c station	Incremental	NNM 6.x or 7.x Management Stations. No dependencies. Import requires one Export file (station.xml).
Monitoring	-c monitoring	Replaces all	Import requires six Export files, and they must be imported in this order: (1) author.xml, (2) device.xml, (3) nodegroup.xml,

Configuration Workspace's View Name	Export Option	Import Behavior	Dependencies
			(4) iftype.xml, (5) ifgroup.xml, and (6) monitoring.xml
Node Groups	-c nodegroup	Incremental	<p>Import requires three Export files, and they must be imported in this order:</p> <p>(1) author.xml, (2) device.xml, and (3) nodegroup.xml</p> <p>Caution: Island Nodes Groups are never exported.</p>
Node Group Map Settings	-c ngmap	Incremental	<p>Import requires four Export files, and they must be imported in this order:</p> <p>(1) author.xml, (2) device.xml, (3) nodegroup.xml, and (4) ngmap.xml</p> <p>Note: Any time you save a map layout, NNMi deletes any previous node locations. Therefore, each export contains only the node locations that were last saved.</p>
RAMS Servers	-c rams	Incremental	HP Router Analytics Management Systems. No dependencies. Import requires one Export file (rams.xml).
Status	-c status	Replaces all	<p>No dependencies. Import requires one Export file (status.xml).</p> <p>The imported status applies to all Node Groups in the database.</p>
URL Actions	-c urlaction	Incremental	<p>Import requires two Export files, and they must be imported in this order:</p> <p>(1) author.xml and (2) urlaction.xml</p>
	-c urlaction -a <author>	Incremental (subset)	<p>Import requires one Export file (urlaction.xml).</p> <p>The required Author information is embedded in the Export file.</p>
User Accounts and Roles User Principals	-c account	Incremental	<p>This command gathers data from two Configuration workspace views.</p> <p>Import requires one Export file (account.xml).</p> <p>The data from both User Accounts and Roles User Principals is embedded in the Export file.</p>
User Interface	-c ui	Incremental	No dependencies. Import requires one Export file (ui.xml).

Export a Snapshot of Your Configuration Settings

If you export your configuration settings before you begin making changes, you can easily "undo" your changes if you decide that you do not like the results.

To export a snapshot of your configuration settings:

1. Import behavior is determined when you generate the Export files. Make sure you understand your Import behavior choices before you begin. See ["Export/Import Behavior and Dependencies" \(on page 373\)](#) (consider printing that topic for reference).

Caution: The locale setting on the NNMi management server at the time of Export must match the locale setting on the NNMi management server at the time of Import. Otherwise, you risk losing data. Also, make sure that both NNMi management servers have the same NNMi version/patch number.

2. A user name and password are required with the export command:

```
-u <NNMiadminUserName> -p <NNMiadminPassword>
```

If you do not want to enter a user name and password at the command line, you can use the [`nnmsetcmduserpw.ovpl`](#) command to specify the valid user name and password (instead of `-u` and `-p`). The credentials set using the `nnmsetcmduserpw.ovpl` command are valid for command execution by the same user.

3. Check whether the configuration settings you want to export have dependencies, see ["Export/Import Behavior and Dependencies" \(on page 373\)](#).

- If no dependencies, export only the configuration settings you are planning to change.
- If yes, decide if you need a copy of the dependencies (only if you plan to make changes to those configuration settings, as well). Then export all the required files.

4. At the command line of the NNMi management server, type the command to generate the required export files.

- To export all configuration settings, use the following command:

```
nnmconfigexport.ovpl -c -all -f <directory>
```

You can use `-x <file_prefix>` to provide a unique prefix to the set of exported files. For example, use today's date or a clue about the reason you needed the files:

```
nnmconfigexport.ovpl -c -all -f <directory> -x <file_prefix>
```

- To export specific configuration settings `<X>` from multiple configuration workspace views, separate each with a comma (see ["Export/Import Behavior and Dependencies" \(on page 373\)](#) or the [`nnmconfigexport.ovpl`](#) Reference Pages for the list of choices):

```
nnmconfigexport.ovpl -c <X>, <X>, <X> -f <directory>
```

You can use `-x <file_prefix>` to provide a unique prefix to the set of exported files. For example, use today's date or a clue about the reason you needed the files:

```
nnmconfigexport.ovpl -c <X>, <X>, <X> -f <directory> -x <file_prefix>
```

- To export configuration settings that were created by a particular author (for Author, Device Profiles, Incident, or URL Actions), add the `-a <author>` attribute to the command and provide the Unique Key.

Note: Only one author per `-a <author>` export command is allowed.

Find the Unique Keys for all authors by exporting an author.xml file, then open the file in a text editor and locate the Key attribute values.

Find the Unique Key for a particular Author, in the NNMi console:

- i. Open one of these Configuration workspaces in the NNMi console: Device Profiles Configuration, Incident Configuration, or URL Actions.
 - ii. Select an object created by the Author of interest.
 - iii. Display the Author form, and copy the value of the Unique Key attribute.
5. Verify that the required xml files are in the specified directory.

You are now ready to make configuration changes.

If you need to undo your configuration setting changes, see ["Import Configuration Files to Restore Previous Settings" \(on page 378\)](#).

Import Configuration Files to Restore Previous Settings

If you have a set of export files, you can change the Configuration settings on your NNMi management server to match the settings in the exported files.

Note: You can change the names of the exported files before importing. The import still works the same.

To import a previous snapshot of your configuration settings:

1. Import behavior is determined when you generate the Export files. Make sure your exported files were generated in a manner that meets your current needs. See ["Export/Import Behavior and Dependencies" \(on page 373\)](#) (consider printing that topic for reference).

Caution: The locale setting on the NNMi management server at the time of Export must match the locale setting on the NNMi management server at the time of Import. Otherwise, you risk losing data. Also, make sure that both NNMi management servers have the same NNMi version/patch number.

2. A user name and password are required with the import command:

```
-u <NNMiadminUserName> -p <NNMiadminPassword>
```

If you do not want to enter a user name and password at the command line, you can use the [nmmsetcmduserpw.ovpl](#) command to specify the valid user name and password (instead of `-u` and `-p`). The credentials set using the `nmmsetcmduserpw.ovpl` command are valid for command execution by the same user.

3. Check whether the configuration settings you want to import have dependencies, see ["Export/Import Behavior and Dependencies" \(on page 373\)](#).

- If no dependencies, import only the configuration settings you are planning to change.
- If yes, decide if you need a copy of the dependencies (only if you made changes to those configuration settings, as well). Then import all the required files.

4. At the command line of the NNMi management server, type the command to import a file:

```
nmmconfigimport.ovpl -f <filename>
```

When importing multiple XML files at once using `-f <directory>`, the NNMi `nmmconfigimport.ovpl` command takes care of ordering issues.

- To import all configuration settings, use the following command:

```
nnmconfigimport.ovpl -f <directory>
```

You can use `-x <file_prefix>` to specify a unique prefix for a set of files:

```
nnmconfigimport.ovpl -f <directory> -x <file_prefix>
```

- To import specific configuration settings from multiple configuration areas, create a directory that contains the set of files you want to import.

At the command line of the NNMi management server, type the appropriate command to import files:

```
nnmconfigimport.ovpl -f <directory>
```

You can use `-x <file_prefix>` to specify a unique prefix for a set of files:

```
nnmconfigimport.ovpl -f <directory> -x <filePrefix>
```

- To import configuration settings that were created by specific authors (for Author, Device Profiles, Incident, or URL Actions), create a directory that contains the set of files you want to import.

At the command line of the NNMi management server, type the appropriate command to import the files:

```
nnmconfigimport.ovpl -f <file>
```

```
nnmconfigimport.ovpl -f <directory>
```

You can use `-x <file_prefix>` to provide a unique prefix for a set of exported files:

```
nnmconfigimport.ovpl -f <directory> -x <filePrefix>
```

5. If you encounter problems, see "[Troubleshooting Imports of Configuration Files](#)" (on page 382).

Additional import options for timeout or memory issues:

You can append the following options to any import command if you encounter problems:

Option	Description	Default Setting
<code>-timeout</code> <seconds>	For larger data imports, you may encounter timeout issues. To increase the number of seconds that NNMi waits (per file) during an import, append the <code>-timeout</code> option to the end of your command line.	1800 seconds (minimum)
<code>-memory</code> <megabytes>	For larger data imports, you may encounter memory issues. To increase the number of megabytes allotted to memory during an import, append the <code>-memory</code> option to the end of your command line.	512 megabytes

6. After completing the import, open NNMi and verify your configuration settings.

Transfer Configuration Settings to Another NNMi Management Server

You can export configuration settings and import them onto another NNMi management server to save time.

To move configuration settings to another NNMi management server:

1. Import behavior is determined when you generate the Export files. Make sure you understand your Import behavior choices before you begin. See ["Export/Import Behavior and Dependencies" \(on page 373\)](#) (consider printing that topic for reference).

Caution: The locale setting on the NNMi management server at the time of Export must match the locale setting on the NNMi management server at the time of Import. Otherwise, you risk losing data. Also, make sure that both NNMi management servers have the same NNMi version/patch number.

2. A user name and password are required with the export command:

```
-u <NNMiadminUserName> -p <NNMiadminPassword>
```

If you do not want to enter a user name and password at the command line, you can use the [nmmsetcmduserpw.ovpl](#) command to specify the valid user name and password (instead of `-u` and `-p`). The credentials set using the `nmmsetcmduserpw.ovpl` command are valid for command execution by the same user.

3. Check whether the configuration settings you want to export have dependencies, see ["Export/Import Behavior and Dependencies" \(on page 373\)](#).
 - If no dependencies, export only the configuration settings you are planning to change.
 - If yes, decide if you need a copy of the dependencies (only if you plan to make changes to those configuration settings, as well). Then export all the required files.

4. At the command line of the NNMi management server export all configuration settings, type the appropriate command:

```
nmmconfigexport.ovpl -c -all -f <directory>
```

You can use `-x <file_prefix>` to provide a unique prefix to the set of exported files. For example, use today's date or a clue about the reason you needed the files:

```
nmmconfigexport.ovpl -c -all -f <directory> -x <file_prefix>
```

Note: You can change the names of the exported files before importing. The import still works the same.

5. Delete any files that you do not need.
6. To export configuration settings that were created by a particular author (for Author, Device Profiles, Incident, or URL Actions), repeat the export command for each configuration item modified by that author. Add the `-a <author>` attribute to the command and provide the Unique Key.

Note: Only one author per `-a <author>` export command is allowed.

```
nmmconfigimport.ovpl -a <author> -f <directory>
```

You can use `-x <file_prefix>` to provide a unique prefix to the set of exported files. For example, use today's date or a clue about the reason you needed the files:

```
nmmconfigimport.ovpl -a <author> -f <directory> -x <file_prefix>
```

Find the Unique Keys for all authors by exporting an author.xml file, then open the file in a text editor and locate the Key attribute values.

Find the Unique Key for a particular Author, in the NNMi console:

- a. Open one of these Configuration workspaces in the NNMi console: Device Profiles Configuration, Incident Configuration, or URL Actions.
- b. Select an object created by the Author of interest.

- c. Display the Author form, and copy the value of the Unique Key attribute.
- 7. Verify that all required xml files are in the specified directory.

To import the configuration settings onto the other NNMi management server:

1. Import behavior is determined when you generate the Export files. Make sure you understand your Import behavior choices before you begin. See ["Export/Import Behavior and Dependencies" \(on page 373\)](#) (consider printing that topic for reference).

Caution: The locale setting on the NNMi management server at the time of Export must match the locale setting on the NNMi management server at the time of Import. Otherwise, you risk losing data. Also, make sure that both NNMi management servers have the same NNMi version/patch number.

2. A user name and password are required with the export command:

```
-u <NNMiadminUserName> -p <NNMiadminPassword>
```

If you do not want to enter a user name and password at the command line, you can use the [nnmsetcmduserpw.ovpl](#) command to specify the valid user name and password (instead of `-u` and `-p`). The credentials set using the `nnmsetcmduserpw.ovpl` command are valid for command execution by the same user.

3. Verify that all required xml files are in the specified directory.
4. When importing multiple XML files at once using `-f <directory>`, the NNMi `nnmconfigimport.ovpl` command takes care of ordering issues.

At the command line of the NNMi management server, type the appropriate command to import the configuration files that you gathered for transfer:

```
nnmconfigimport.ovpl -f <filename>
```

```
nnmconfigimport.ovpl -f <directory>
```

You can use `-x <file_prefix>` to specify a unique prefix for a set of files:

```
nnmconfigimport.ovpl -f <directory> -x <file_prefix>
```

5. If you encounter problems, see ["Troubleshooting Imports of Configuration Files" \(on page 382\)](#).

Additional import options for timeout or memory issues:

You can append the following options to any import command if you encounter problems:

Option	Description	Default Setting
<code>-timeout <seconds></code>	For larger data imports, you may encounter timeout issues. To increase the number of seconds that NNMi waits (per file) during an import, append the <code>-timeout</code> option to the end of your command line.	1800 seconds (minimum)
<code>-memory <megabytes></code>	For larger data imports, you may encounter memory issues. To increase the number of megabytes allotted to memory during an import, append the <code>-memory</code> option to the end of your command line.	512 megabytes

6. After completing the import, open NNMi and verify your configuration settings.

Troubleshooting Imports of Configuration Files

When importing incremental sets of configuration files, NNMi abandons the import if mis-matched configuration objects are encountered. Each configuration object has a set of Unique Identifiers whose values must match for incremental updates, or must not match any existing data before NNMi adds the configuration object to the database, see tables below.

If you receive an error message while trying to import configuration information, use the information below to figure out how to use the error message to determine what you need to change before creating another export file (thus, solving the problem).

Author Configuration Unique Identifiers

Configuration Item Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
Author = Author form	author = Unique Key attribute value	Yes	

Communication Configuration Unique Identifiers

Attribute Name = NNMi Console Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
DiscoveryConfiguration = Communication Region form	uuid	No	name = Name value ordering = Ordering value
UsmSettings = SNMPv3 Settings form	uuid	No	name = Unique Name value

Custom Poller Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
ComparisonMap = Comparison Map form	uuid	No	ordering = Ordering value
Policy = Custom Poller Policy form	uuid	No	The combination of these two: collection = Collection value ordering = Ordering value

Device Profile Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
DeviceCategory =	key = Unique Key attribute	Yes	

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
Device Category form			
DeviceFamily = Device Family form	key = Unique Key attribute	Yes	
DeviceProfile = Device Profile form	snmpObjectId = SNMP Object ID value	Yes	
DeviceVendor = Device Vendor form	key = Unique Key attribute	Yes	

Discovery Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
AutoDiscoveryRegion = Auto-Discovery Rule form	uuid	No	name = Name value ordering = Ordering value

Discovery Seed Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
DiscoverySeed = Discovery Seed form	host = Host Name/IP value	Yes	

Incident Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
MgmtEventConfig = Management Event Configuration form	uuid	No	name = Name value
SnmpTrapConfig = SNMP Trap Configuration (by OID) form	uuid	No	iod = SNMP Object ID value name = Name value
RemoteNnmEventConfig	uuid	No	iod name = Name value
PairwiseConfig = Pairwise Configuration form	uuid	No	name = Name value The combination of these two: firstIncidentName = First Incident Configuration value secondIncidentName = Second Incident Configuration value

Interface Groups Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
InterfaceGroup = Interface Group form	uuid	No	name = Name value

Interface Type Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
IfType	IfType attribute	Yes	

Monitoring Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
InterfaceSettings = Interface Settings form	uuid	No	ordering = Ordering value
NodeSettings = Node Settings form	uuid	No	ordering = Ordering value

Node Group Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
NodeGroup = Node Group form	uuid	No	name = Name value

URL Actions Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
UrlActionInfo = URL Action form	key = Unique Key	Yes	

User Accounts and Roles Configuration Unique Identifiers

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
Account = User Account form	uuid	No	name = Name value
Principal = User Principal form	uuid	No	Name value
RoleEntry = Account Mapping form	uuid	No	The combination of these two: principal = Account value

Attribute Name	Primary Identifier	Editable Attribute?	Other Key Attributes that must be unique
			role = Role value

Back Up and Restore NNMi

As an NNMi administrator, develop a plan for NNMi backups. You have the following choices:

- Complete backups or backups limited to specific NNMi data and files
- Offline backups (NNMi is stopped) or online backups (NNMi is running)

For example, you might want to back up your configuration data before discovering your network. You might also want to save your configuration, discovered topology, and incident data without stopping NNMi.

The scope of any subsequent NNMi restore is determined by the contents of your backup. Only the data present in the backup is restored. NNMi must be stopped for all restore operations.

Note: You cannot restore NNMi files and data to a system that is different from the one you used to create the backup files. When you back up NNMi files and data, note the NNMi version, operating system, and character set used on the system you back up. The hostname and IP address do not have to be identical.

["Back Up NNMi Data and Files" \(on page 385\)](#)

["Restore NNMi Data and Files" \(on page 386\)](#)

Related Topics

["Archive and Delete Incidents" \(on page 387\)](#)

Back Up NNMi Data and Files

Before you begin a backup, ensure you have adequate storage space in your target directory (for example, verify that you have enough space to store the contents of the directories listed in the following table).

NNMi Directories

Operating System	Default Location
Windows	<drive>:\Program Files (x86)\HP\HP BTO Software <drive> is the drive on which NNMi is installed
Windows	<drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO Software <drive> is the drive on which NNMi is installed.
UNIX	/opt/OV
UNIX	/var/opt/OV

The NNMi backup command performs database level backups for embedded databases. If you installed with the embedded database option, the embedded database data is stored in the following directory:

Windows:

```
<drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO  
Software\shared\nnm\databases\Postgres
```

<drive> is the drive on which NNMi is installed.

UNIX:

```
/var/opt/OV/shared/nnm/databases/Postgres
```

If you chose a different database at install time, your table data is not backed up using this command.

Note: You may compress the files after backup.

When backing up NNMi data and files, you specify online or offline, the scope of the backup, the format of the backup copy (such as a tar file), and the location of the target directory where the backup is stored. These arguments are described in the following table.

Note: See [nnmbackup.ovpl](#) for a complete description, including all command arguments.

nnmbackup.ovpl Parameters

Parameter	Description
-force	Used to start and stop the required processes for the NNMi backup to complete successfully. NNMi uses the backup parameters provided to determine which processes to start or stop. For example, for an offline backup, if NNMi is running, the -force option stops all NNMi processes.
-scope [config topology events all]	Determines the data that is backed up. Note: When performing offline backups it is recommended that do not provide a scope. In such cases, NNMi backs up the entire contents of the NNMi database.
-target <directory>	Specifies the output directory where the backup file is stored. NNMi creates a parent directory named <code>nnm-bak-<i><timestamp></i></code> inside the target directory where all backup files are stored.
-type [online offline]	Determines the type of backup to be performed. If you use the online argument, NNMi must be running when the backup is performed. If you specify offline, NNMi must be completely stopped.
-archive	Creates a tar file that contains the backed up data (uncompressed).

Restore NNMi Data and Files

The NNMi `nnmrestore.ovpl` command restores data from an NNMi backup (created with the `nnmbackup.ovpl` command). The `nnmrestore.ovpl` command restores NNMi to the state stored in the backup files.

Only the data present in the backup is restored.

Note: NNMi must be stopped when restoring any NNMi data and files. Use the -force parameter to stop NNMi automatically as part of the restore operation.

When using `nnmrestore.ovpl`, you need to provide the source directory as described in the parameter table included below.

Note: See the [nnmrestore.ovpl](#) command for a complete description, including all of the command arguments.

Restore Parameters

Parameter	Description
-source <directory>	Specifies the directory to which you want the files restored. Note: When a tar file contains the backup, the tar file extracts into a temporary folder in the current working directory. NNMi removes the temporary folder when the restore finishes.
-force	Stops NNMi prior to running the restore procedure.

Archive and Delete Incidents

NNMi enables you to archive and remove incidents that you no longer want to track. This feature is useful if you want to purge the database of incidents that are older than a specified time period or date. With archiving, you can keep a history of incidents and manage the volume of incidents.

To archive and then delete incidents in NNMi, you use the `nnmtrimincidents.ovpl` command. You can choose to only archive or only delete your incidents as described in the argument table that follows.

When archiving and deleting incidents, note the following:

- For the best performance results, archive and delete your incidents so that no more than 100,000 incidents are stored in the NNMi database at one time. By default, NNMi sets the maximum number of SNMP traps to 100,000.
- After 90 percent of the maximum limit for SNMP traps is reached or exceeded, NNMi generates an incident whose Severity is set to Warning to notify you that NNMi is approaching the maximum limit.
- After 95 percent of the maximum limit for SNMP traps is reached or exceeded, NNMi generates an incident whose Severity is set to Major to notify you that NNMi is approaching the maximum limit. In addition, NNMi only accepts traps required for Causal Engine analysis until the number of SNMP traps within the database has been reduced using the `nnmtrimincidents.ovpl` command.
- After the maximum SNMP trap limit is reached or exceeded, NNMi generates an incident whose Severity is set to Critical. NNMi no longer accepts any SNMP traps until the number of SNMP traps within the database has been reduced using the `nnmtrimincidents.ovpl` command.

Use the `nnmtrimincidents.ovpl` command to archive and delete your incidents based on any of the attributes described in the following table. See the [nnmtrimincidents.ovpl](#) command for more information, including a complete list of arguments for this command.

Archive Incident Arguments

Incident Attribute	Description
-archiveOnly	Used to specify that you want to only archive incidents rather than archive and then delete them.
-trimOnly	Used to specify that you want to only delete incidents rather than archive and then delete them.
-date	The date must be entered in the following ISO 8601 format: <code><yyyy-mm-dd>T<hh>:<mm>:<ss>[Z,-<hh>:<mm>,+<hh>:<mm>]</code> ISO Date Format:

Incident Attribute	Description
	<ul style="list-style-type: none"> • <i>yyyy</i> — Four-digit year • <i>mm</i> — Two-digit month • <i>dd</i> — Two-digit day • <i>hh</i> — Two digits representing the hour (00 through 23) • <i>mm</i> — Two digits representing the minutes (00 through 59) • <i>ss</i> — Two digits representing the seconds (00 through 59) • <i>+<hh>:<mm></i> — Local time zone which is the hours (<hh>) and minutes (<mm>) ahead of Coordinated Universal Time • <i>-<hh>:<mm></i> — Local time zone which is the hours (<hh>) and minutes (<mm>) behind Coordinated Universal Time <p>For example: <code>2007-11-05T08:15:30-5:00</code> corresponds to November 5, 2007, 8:15:30 am, Eastern Standard Time.</p> <p>Note: You must specify either a <code>-age</code> or a <code>-date</code> value.</p>
-age	<p>The age of the incident specified in number of days, weeks, or months.</p> <p>Note: You must specify either an <code>-age</code> or a <code>-date</code> value.</p>
-family	<p>The incident Family. See Incident Form: General Tab for a list of possible Family values.</p>
-incr	<p>The increment value that helps determine the <code>-age</code> value. Supported increments include days, weeks, and months. The default increment value is days.</p>
-path	<p>Specifies the archive file name, including the complete path. The default archive file name is:</p> <p><date> is the date in <i>yyyy-mm-dd</i> format</p> <p><ms> is milliseconds</p> <p>Windows:</p> <p><code>%NnmDataDir%\tmp\incidentArchive.<date>.<ms>.txt.gz</code></p> <p>UNIX:</p> <p><code>/var/opt/OV/tmp/incidentArchive.<date>.<ms>.txt.gz</code></p> <p>Note: NNMi keeps only one backup copy of the default archive file name. Therefore, to ensure you archive all incidents of interest, provide an archive file name each time you want to archive incidents.</p>
-lifecycle	<p>Identifies where the incident is in the incident lifecycle. Possible values are Registered, In Progress, Completed, and Closed.</p> <p>See About the Incident Lifecycle for more information about Lifecycle State.</p> <p>Note: This argument is optional.</p>
-name	<p>Identifies the name of the incident configuration.</p>

Incident Attribute	Description
-nature	<p>Identifies the nature of the incident. Possible values are: Info, None, Root Cause, Secondary Root Cause, Service Impact, and Symptom.</p> <p>See Using the Incident Form for more information.</p> <p>Note: This argument is optional.</p>
-origin	<p>Identifies the Origin of the incident configuration. Possible values are: Management Software, Manually Created, Remotely Generated, and SNMP Trap. See Incident Form: General Tab for more information.</p>
-u	<p>The user name required to run this command. This user name must be a valid NNMi user name with a role of either Administrator or System.</p> <p>Note: The user name might be a Principal object stored in the NNMi database or might be from your environment's directory service database (depending on NNMi configuration). See "Configure Sign-In Access" (on page 32) for more information.</p>
-p	<p>The associated password for the user name specified by the -u attribute value.</p> <p>Note: The password might be an attribute in an Account object stored in the NNMi database or might be from your environment's directory service database (depending on NNMi configuration). See "Configure Sign-In Access" (on page 32) for more information.</p>
-quiet	<p>Use this argument when you want to trim incidents without requiring user prompts and responses. (Status information appears.)</p>
-sysobjectid	<p>The system object identification (system OID) from the incoming SNMP trap or Remote NNM 6.x/7.x event that is assigned to the incident configuration.</p>

For example, archive and delete all incidents with lifecycle equal to Closed and age equal to or greater than 1 month.

```
nnmtrimincidents.ovpl -age 1 -incr months -lifecycle Closed -u <NNMiadminUsername>
-p <NNMiadminPassword>
```

You can also specify a batch size when archiving or deleting incidents. Specify the maximum number of incidents to delete at one time within a single database transaction. This number then determines how often you see a status message that the deletions are complete. Using the default value of 1,000 as an example, NNMi displays a status message after successfully deleting each 1,000 incidents.

Note: The default value of 1,000 was selected to maintain a balance between performance and the frequency of progress messages for the archive and delete operation. This default determines the maximum number of incidents archived and deleted at one time within a single database transaction.

Related Topics

["Back Up and Restore NNMi" \(on page 385\)](#)

Appendix A: Glossary Terms

A

Anycast Rendezvous Point IP Address

Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

L

Layer 2

Refers to the Data Link layer of the multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer moves data across the physical links in the network. The switches and bridges are devices that redirect data messages at the layer 2 level, using the destination Media Access Control (MAC) address to determine where to direct the message.

Layer 3

Refers to the Network layer of the multilayered communication model, Open Systems Interconnection (OSI). The Network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding incoming

messages to local host domains. The router and switch-router are the devices that redirect data messages at the Layer 3 level. Everything in a subnet is connected at the Layer 3 (IP) level.

Link Aggregation

A Link Aggregation is comprised of an Aggregator Link, Aggregator Interface, and the physical interfaces and connections that they represent. An Aggregator Link object represents many-to-many physical connections. For example, two nodes might be connected with four physical connections. These four physical connections are depicted as a single Aggregator Link object using a thick line on the Layer 2 Neighbor View map. The interface depicted at each end of the Aggregator Link object is an Aggregator Interface object. An Aggregator Interface object represents the collection of physical interfaces for one end of an Aggregator Link.

loopback address

The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured

loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

Appendix B: Index

A			
Abstract Syntax Notation	259	launching commands	
access		Communication Configuration	363
command line	42	Configuration Poll	367
configuring sign-in	32, 35, 37, 40	Monitoring Settings	364
controlling	32, 34	ping	362
disabling user	41	Sign In/Out Audit Log	370
read only	321	Sign Out	370
troubleshooting	41	Status Details	368
accessing		Status Poll	367
device details	95	traceroute	362
help	31	out-of-box	22
integration URL		Actions menu	
commands	323	commands	
forms	322	Communication Configuration	363
workspaces	322	Configuration Poll	367
iSPI for Performance Headline report	165, 175	Monitor Settings	364
NNMi from URLs	321	Ping	362
Account Mapping form	36, 39, 41	Status Details	368
accounts, user		Status Poll	367
auditing activity	43	Trace Route	362
changing	32, 35, 37, 40	configuring URL actions	303, 305
determining roles	33	controlling	34, 303
disabling	41	invoking actions	21
editing	36, 39-40	Actions stage	213
Action Configuration tab	283-284	activity, auditing account	43
actions		adding	
arguments	288	Boolean operators	134
configuring incident	283-284	connections	124
incident parameters	285	custom attributes	302
		discovery seeds	113-115
		node	
		group filters	128
		optional filters	315
		SNMP trap configuration	248
		Additional Filters tab	128, 141

Index: address gathering phase – attribute values

address gathering phase		allowedOids.conf file	268
node name decision tree	81	ampersand (&)	
Spiral Discovery	77	character	288
addresses		AND variable	134
assigning management mode	192	applications, launching maps within other	321
configuring		archiving incidents	387
IP	60	arguments, action	288
monitoring	181	ARP cache	83, 96
excluding from discovery	83, 93	ASN	259
IPv4	84	assigning	
managed	189	hostname wildcards	61
monitoring configuration	181	management mode	192
not		node group status	178
managed	190	assignments, importing community string	74
out-of-box actions	22	attribute values	
out of service	191	Author form	260, 304
restarting management	184	communication	
stopping management	184	protocol settings for node	67
adjusting		regions	57
discovery intervals	98	Communication Configuration form	360
administrator		community strings	
backing up NNMi	385	defaults	52
introduction	14	regions	62, 72
overriding default node group status	178	Configuration Per Node Group	292
restoring NNMi	385	Configuration Poll command	367
role permissions	32-35, 37, 40, 192, 322-323	Configuration Workspace view	349
tools	15	Configure User Interface form	195
Advanced, NNMi		connection	124
Enable Router Redundancy Group Monitoring	153	Deduplication form	269
monitoring router redundancy groups	181	Default Device Credentials form	53
RAMS	300	default monitoring	154
agents, SNMP		device	
configuring	238	credentials	73
discovering	90	profile	95
		Diagnostic Selection form	293

Discovery Configuration form	360	Path View	338
Discovery Seeds form	113	RAMS Configuration form	300
Discovery State	117	Rate Configuration	273
excluded addresses	108	Rediscovery Interval	98
Family	251, 254	Routers view	330
Hostname Wildcard	61	SNMP	
Incident Configuration form	360	default settings	47
Incident form	357	trap definitions	247
Incident views	327	SNMPv3	239
incidents	251, 253-255, 387	Status Configuration form	360
Interface form	353	Status Details command	368
Interface Group form	141	Status Poll command	367
Interface Settings form	158	Subnet form	356
Inventory Workspace view	343	Switches view	330
IP Address form	355	system object ID ranges	106
IP address ranges	60	Thresholds Settings form	162, 165, 172, 175
Layer 2 connection	124	Trap Forwarding Destination form	244
Layer 2 Neighbors view	338	Trap Forwarding Filter Association form	245
Lifecycle Transition Action form	284	Trap Forwarding Filters form	241
Management Mode Workspace view	346	Troubleshooting Workspace view	338
Monitoring Configuration form	360	URL Action Object Type form	306, 315
Monitoring Workspace view	335	URL Actions Author	304
Network Overview view	330	URL Actions form	303, 305
Networking Infrastructure Devices view	330	User Interface Configuration form	360
Node Form view	351	attributes	
Node Group form	128, 358	capability	312
Node Group Map Settings form	199-200, 202-203	custom	313, 315
Node Group Overview view	330	Attributes, Custom Incident	214, 255-256, 259, 271, 274, 311
node names	79, 81, 99	audit log files	43
Node Settings form	168	auditing account activity	43
organizing incidents	251	authentication requirements, URL access	321
Pair Item Configuration form	281	Author form	260, 304
Pairwise Configuration form	279	Author, URL Actions	304
pairwise configurations	281		

switches	295	Status Details	368
collecting incidents	211	Status Poll	367
comma (,) character	288	traceroute	295, 362
comma separated values	137	communication	
command line		protocols	47
adding discovery seeds	115	regions	61
granting user access to commands	42	settings	75
setting up access	42	team	44
verifying SNMP/ICMP configuration for IP address		Communication Community String form	62, 72
commands		Communication Configuration	
accessing integration URL	323	command	363
automated	295	form	47, 51, 53, 56, 66, 74, 360
Communication Configuration	363	Communication Default Community String form	52
Configuration Poll	367	Communication Node form	67
get	47	communication protocols, configuring	66-67
Monitoring Settings	364	Communication Region form	57, 61, 64
nnmbackup.ovpl	385	Communication Settings menu item	34, 323
nnmcommload.ovpl	74	community strings	
nnmconfigexport.ovpl	373	configuring default	51
nnmconfigimport.ovpl	373	loading from file	74
nnmconnect.ovpl	124	setting	62, 72
NNMi Status	369	default	52
nnmincidentcfg.ovpl	241, 244-245, 247	nodes	67
nnmloadnodegroups.ovpl	127, 137	regions	57
nnmloadseeds.ovpl	114-115	SNMPv2c	50
nnmmanagementmode.ovpl	184	Community Strings tab	57, 62, 72
nnmrestore.ovpl	386	comparison parameters, deduplications	271
nnmsetcmduserpw.ovpl	42	Comparison Params form	274
nnmtrimincidents.ovpl	387	Component Health	
ovstart	26, 30	monitoring	153
ovstatus	26, 28	components	
ovstop	26, 30	Causal Engine	152, 211-212, 264, 266
ping	47, 295, 362	event pipeline	213
Sign In/Out Audit Log	370	nodes	181
Sign Out	370		

Index: Condition Listener stage – configuring

Condition Listener stage	212	credential settings	
configuration		nodes	73
auto-discovery	88, 90-94	regions	64
creating objects	20	default	
deduplication	266, 269, 271	community strings	51
describing incident configurations	260	protocol settings	47
exporting settings	373	device profiles	95
importing settings	373	discovery	96
management event	229	discovery seeds	113
maps	198	DNS	86
node group map settings	198	excluded addresses	108
pairwise	237, 266, 276, 278	IANA ifType-MIB definitions	140
rate	266, 274	incidents	211, 214, 216, 226, 229, 237, 246, 248-249, 255-256, 261, 265, 268, 276, 279, 281, 283- 284, 291-293
wizard	15	interface monitoring	158
workspaces	16	IP address ranges	60
Configuration Item menu item	34	management	
Configuration Per Node Group form	292	event display	264
Configuration Poll		stations	262
command	367	maps	198
menu item	323	monitoring	
Configuration workspace	33	behavior	152
Configuration Workspace view	349	settings	181
Configure User Interface form	195	network	
configuring		devices	86, 238
access	32	region protocols	56
actions for incidents	284	node	
audit log files	43	connectivity	202
auto-discovery rules	101	monitoring	168
automatic actions	283	name resolution	99
background images	203	node group	
communication protocols	47	map settings	198
devices	66	status calculations	178, 200
nodes	67	node group map settings	199
community strings for regions	62		
console	14		

Path View maps	206	out	46
RAMS	300	contacting devices	50-51
remote events	263	controlling	
security settings for SNMPv3	239	access	32, 34
sign-in access	32, 35, 37, 40	Actions menu	303
SNMP traps	239, 241, 245-246, 268	address discovery	108
subnet connection rules	109	node names	99
target status	179	correlating incidents	
threshold monitoring	162, 165, 172, 175	duplicates	269
URL Actions	303, 305	pairs	276, 279
user interface	195	counts	
USM	54-55, 65	incident frequency	273
connection		creating	
editor file	124	additional group filters	
phase	77	interface	141
connections		nodes	128
adding	124	attributes	
deleting	124	Author	260
subnet rules	84, 109, 111	auto-discovery rules	91
connectivity		configuration objects	20
checking addresses	181	discovery seed file	114
console		incident	
accessing commands	323	categories	253
adding discovery seeds	113-114	families	254
administrator tools	15	interface groups	126
configuring	14, 195	IP ranges	91
defining node groups	127	management	
disabling user access	41	event configuration	264
launching from URLs	324	station configuration	262
opening	44	node group map settings	200
running outside		node groups	126
help	31	credential settings	
tools	321	configuring	64, 73
signing		default	53
in	46	CSV	137

custom attributes		USM settings	54
interface objects	302	views	324
load for nodes	138	defining	
node objects	302	interface groups	139
URL actions	313, 315	node groups	126, 137
Custom Attributes tab	302, 313, 315	target status	179
Custom Incident Attributes	214, 255-256, 259, 271, 274, 311	definitions	
cycle times, discovery	98	flow	295
		SNMP traps	247
		deleting	
		Boolean operators	134
		connections	124
		incidents	387
		management	
		event configuration	264
		station configuration	262
		node group map settings	200
		nodes	122
		SNMP trap configuration	248
		table rows	20
		user accounts	41
		describing incidents	260
		Description attribute	260
		determining	
		node names	81
		user account roles	33
		developer licenses	372
		developing filters	126
		Device Credentials tab	
		Communication Regions form	64
		Specific Node Settings form	73
		Device Profile form	95
		devices	
		adding group filters	128
		communication protocols	66
D			
data			
backing up	385		
RAMS	300		
restoring	386		
database			
auto-discovery	83		
object			
IDs for URL Actions	311		
decision tree, node name	81		
Dedup stage	213		
Deduplication Comparison Params form	271		
deduplication configuration	266, 269, 271		
Deduplication form	269		
Default Community String tab	51		
Default Device Credentials form	53		
defaults			
community strings			
configuring	51		
setting	52		
credential settings	53		
health monitoring	154		
protocols			
settings	47		
traffic control	154		

configuring		excluding	
network	238	addresses	83, 93
node names	99	devices	94
diagnostics	295	intervals	79
discovering		node name choices	79
SNMP	90	prerequisites	86
specific	88	process	77
vendors	92	routers	89
excluding from discovery	94	SNMP devices	90
profiles	85, 95	specific devices	88
retry behavior	50-51	switches	89
timeout behavior	50-51	vender devices	92
types	95	discovery	
Diagnostic Selection form	293	adjusting intervals	98
Diagnostics (Flows)	295	checking	
diagnostics, incident		discovery seed status	118
configuring	291-293	node state	117
out-of-box	295	progress	117
direct management mode	193	configuring	96
directories, NNMi	385	excluded addresses	83
directory service		IP address ranges	104
configuration	32, 37, 40	node name choices	79
disable SNMP trap definitions	247	protocols	83
disabled		seeds	81-82, 88, 112-115, 117-118
incidents	298	SNMP system object ID ranges	106
disabling		verifying	116-117, 120-121
user accounts	41	Discovery Configuration	
discovering networks		form	360
approach	88	Discovery Configuration form	96, 98, 118
auto-discovery regions	83	Discovery Seeds	
description	76	form	113
device profiles	85	tab	112
discovery seeds	82, 112	Discovery System Object ID Range form	106
everything	91	Discovery, Spiral	76
		adjusting discovery interval	98

Index: displaying – families

configuring	88, 95	email, launching maps from	321
discovering		embedding views within Web portals	321
everything	91	Enable Component Health Monitoring	153
routers and switches	89	Enable Router Redundancy Group Monitoring	153
excluding		Enable State Polling	153
SNMP object IDs	94	enabling JavaScript	44
specific IP addresses	94	ENDP	83, 109
fine-tuning	85	Enterasys Discovery Protocol	109
process	77	enterprise-specific traps, SNMP	249
speeding up	86	equals sign (=)	288
displaying		establishing monitoring behavior	154, 158, 168
management		events	
events	264	configurations	226, 264-265
station configurations	262	duplications	269
SNMP traps as root causes	251	management	229
DNS		pipeline	213
names	79	everything, discovering	91
prerequisite	86	examples	
do not discover list	83	adding group filters	
dollar sign (\$)	288	interface	134
Domain Name System	86	nodes	134
down		Jython methods	290
interface	298	threshold monitoring	165, 175
duplicate incidents, correlating	269	excluding from discovery	
		addresses	83, 93-94, 108
E		devices	94
editing		exporting configuration settings	373
management		extending capabilities	
event configuration	264	NNMi	302
station configuration	262	Extreme Discovery Protocol	109
node group map settings	200		
SNMP trap configuration	248	F	
user accounts	36, 39-40	families	
editor, connection	124	creating incident	254
EDP	109		

Family		flow	
attribute	251	definitions	295
FDP	83, 109	form toolbar	20
fields, Lookup	18-19	formats, incident messages	255, 259
files		forms	
allowedOids.conf	268	accessing integration URL	322
backing up	385	Account Mapping	36, 39, 41
creating discovery seed	114	Author	260, 304
hostNoLookup.conf	86	Auto-Discovery Rules	101, 104
ipNoLookup.conf	86	Communication Community String	62, 72
launchsamples.jsp	321	Communication Configuration	47, 51, 53, 56, 66, 74, 360
log	28, 43	Communication Default Community String	52
MIB	247	Communication Node	67
nms-roles.properties	41-42	Communication Region	57, 61, 64
nms-users.properties	41-42	Comparison Params	274
nnm.ports.properties	44	Configuration Per Node Group	292
nnmDocs_en.war	31	Configure User Interface	195
PathConnections.xml	206	Deduplication	269
restoring	386	Deduplication Comparison Params	271
text	137	Default Device Credentials	53
filtering		Device Profile	95
node groups	147	Diagnostic Selection	293
filters		Discovery Configuration	96, 98, 118, 360
developing	126	Discovery Seeds	113
interface		Discovery System Object ID Range	106
groups	139, 141	Hostname Wildcard	61
node groups	126	Incident	313, 315, 357
out-of-box	149	Incident Category	253
SNMP trap forwarding	241	Incident Configuration	211, 241, 248, 260, 269, 273-274, 298, 360
Find Node menu item	34	Incident Family	254
Firefox		Included Address Range	60
launching URL views	324, 327, 330, 335, 338, 343, 346, 349, 351, 353, 355-358, 360	Interface	353
opening console	44	Interface Group	139, 141

Interface Settings	158	forwarding, SNMP trap	239
invoking actions	21	Foundry Discovery Protocol	83, 109
IP Address	355	frequency, tracking incident	273
launching outside NNMi	350		
Lifecycle Transition Action	284	G	
Lifecycle Action	283	gathering incidents	211
Management Event Configuration	264-265	generating incidents	
Monitoring Configuration	152-153, 360	interface disabled	298
Node	117, 313, 315, 351	performance threshold	298
Node Group	128, 358	generic traps, SNMP	249-251
Node Group Map Settings	199-200, 203	get command	47
Node Group Map Settings form	202	global settings, Ping Sweep	98
Node Group Status Settings	179	graphical user interface	
Node Settings	168	configuring	195
opening	18	greater than sign (>)	288
Pair Item Configuration	281	groups	
Pairwise	276	interface filters	141
Pairwise Configuration	279	node filters	126-128, 134, 137, 147, 149, 198
RAMS Configuration	300	node groups	178-179, 200
Region Device Credentials	64	out-of-box	
Remote NNM 6.x/7.x Event Configuration	263	interface	149
SNMP Trap Configuration	248	node groups	147
Specific Node Device Credentials	73	router redundancy	181
Specific Node Settings	73	Guest role	32-35, 321-323
Status Configuration	178-179, 360	GUI	
Subnet	356	configuring	195
Subnet Connection Rules	109		
Thresholds Settings	162, 165, 172, 175	H	
Trap Forwarding Destination	244	Headline report, accessing	165, 175
Trap Forwarding Filter Association	245	health, network	
Trap Forwarding Filters	241	monitoring	151-152, 181
URL Action Object Type	306, 315	help	
URL Actions	303, 305	running outside console	31
User Account	36, 39	Hostname attributes	79, 81
User Interface Configuration	360		

hostname resolution phase	81	important nodes	
Hostname Wildcard form	61	group filter	147
Hostname Wildcards tab	57, 61	Important Nodes group	147
hostnames		importing	
assigning wildcards	61	community string assignments	74
discovery seeds	82	configuration settings	373
hostNoLookup.conf file	86	SNMP assignments	74
HSRP		Incident Category form	253
objects	181	Incident Configuration	
Hypothesis Engine stage	212	form	360
		Incident Configuration form	211, 241, 248, 260, 269, 273-274, 298
I		Incident Family form	254
IANA ifType-MIB definitions	140	Incident form	313, 315, 357
ICMP		incident messages	
enabling nodes	67	valid parameters	256
retries		Incident Receiver stage	213
default	47	Incident views	327
node	67	incidents	
regions	57	accident parameters	285
timeouts		archiving	387
default	47	attributes	214, 229, 237, 276
nodes	67	Causal Engine	212
region	57	configurations	229
traffic control	47	configuring	211, 214, 216, 226, 246, 248- 249, 261, 265, 276, 279, 283- 284, 291, 293
identifying		controlling incoming trap visibility	268
attribute pairs	281	correlating	
IDs, SNMP object	94, 106, 137, 249-251	duplicate	269
IfTypes		pairs	276, 279
view	140	creating	
images, background		categories	253
configuring	203	families	254
out-of box	205	deleting	387
scaling	206	descriptions	260
troubleshooting	206		

Index: Incidents workspace – IP addresses

gathering	211	monitoring	
generating		configuration	181
interface disabled	298	not managed	190
performance threshold	298	out-of-box	
message format	255, 259	actions	22
organizing	251	groups	149
out-of-box actions	22	out of service	191
reducing incoming	266	restarting management	184
root causes	251	reviewing group definitions	139
severity	255	stopping management	184
tracking		utilization	165, 175
frequency	273	viewing	
viewing	298	disabled incidents	298
Incidents workspace	33	Interface form	353
Included Address Range form	60	Interface Group	
Included Address Ranges tab	57	form	139, 141
incoming traps, controlling visibility	268	interface groups	
Instant-On license	372	creating additional filters	141
integrating NNMi with other applications	321	defining	139
integration URLs		filters	139
commands	323	out-of-box	149
forms	322	Interface Settings form	158
workspaces	322	Interface Type Filters tab	139
interface		Interfaces view	187
adding		Internet Control Message Protocol	47
custom attributes	302	Internet Explorer	
management mode	192	opening console	44
capability attributes	312	intervals, discovery	79, 98
configuring		inventory	
ifTypes	140	verifying discovery	120
monitoring	158, 181	Inventory workspace	33
user	195	Inventory Workspace view	343
creating groups	126	IP Address form	355
defining groups	139	IP addresses	
managed	188	configuring ranges	60

discovering		launching from URLs	
discovery seeds	82	authentication requirements	321
excluded from	83	commands	323, 362-364, 367-370
networks	79	console	324
discovery ranges	104	forms	350-351, 353, 355-358, 360
excluding from Spiral Discovery	94	menu items	361
verifying		views	321, 324, 327, 330, 335, 338, 343, 346, 349
monitoring configuration	181	launchsamples.jsp file	321
SNMP configuration	74	Layer 2 connection attributes	124
IP Addresses view	187	Layer 2 Discovery, verifying	120-121
ipNoLookup.conf file	86	Layer 2 Neighbors view	338
IPv4 addresses	84	Layer 2 Rediscovery Interval	79
ISDN Interfaces group	149	Layer 3 Neighbors view	338
Island Node Group	149	LDAP	
iSPIs		configuration	32, 37, 40
NNM iSPI for Performance		less than sign (<)	288
CIAs	214	Level 1 Operator role	32, 35, 322-323
incidents	298	Level 2 Operator role	32, 35, 322-323
interfaces	158	licenses	
management event configurations	229	tracking	372
node groups	126-127	Lifecycle Action form	283
nodes	168	Lifecycle Transition Action form	284
setting default monitoring	154	limits	
State Poller	151	licenses	372
threshold monitoring	162, 165, 172, 175	URL	
purchasing	319-320	actions	306
		commands	323
J		Link Aggregation group	149
JavaScript, enabling	44	Link Layer Discovery Protocol	109
Jython methods	256, 285, 290	listing object instances	19
		LLDP	109
L		loading	
launching		community strings from file	74
Quick Start Configuration wizard	15	SNMP trap definitions	247

log files	28, 43	modifying device symbols	85
logins, bypassing	324	node group map settings	198, 206
Lookup fields	18-19	menu access, controlling	34
M			
maintaining NNMi	372	menu items, launching outside NNMi	361
Managed Addresses view	189	messages, incidents	
Managed Interfaces view	188	formats	255, 259
Managed Nodes view	188	parameters	256
Management Address attributes	81	methods, Jython	290
Management Event Configuration form	264-265	MIB file	247
management event configurations	229	MIB IANA ifType definitions	140
management mode		MIB II sysName Values	79
assigning to interface or address	192	Microsoft Internet Explorer	
IP addresses	187	opening console	44
not managed	193	Microsoft Windows Systems node group	147
out of service	193	modes, management	184
stopping or starting	184	modifying	
views	185	incident pair configurations	237, 276
workspace	187	Monitor Settings menu item	323
Management Mode workspace	33	monitoring	
Management Mode Workspace view	346	configuration settings	181
Management Stations		interface	158
view	262	network	
management stations, configuring		devices	152
remote	262	health	152, 154
SNMPv3	239	nodes	168
map views		router redundance groups	181
configuring Path View	206	suspending all	153
Device Profiles	95	thresholds	162, 165, 172, 175
invoking actions	21	Monitoring Configuration	
navigating	75	form	360
maps		Monitoring Configuration form	152-153
configuring	198	Monitoring Settings command	364
		Monitoring workspace	33
		Monitoring Workspace view	335

Index: NNMi Status command – Node Settings form

incident configurations	226	nnmtrimincidents.ovpl command	387
viewing management stations	262	Node form	117, 313, 315
actions	22	Node Form view	351
Advanced		Node Group	
Enable Router Redundancy Group Monitoring15		form	128, 358
monitoring router redundancy groups	181	Node Group Map menu item	34
RAMS	300	Node Group Map settings	
backing up	385	background images	206
CIAs	214	troubleshoot map background images	206
components	212	Node Group Map Settings form	199-200, 202-203
controlling access	32	Node Group Overview view	330
directories	385	Node Group Status Settings form	179
extending capabilities	302	node groups	
incident configurations	214	actions	22
integrating with other applications	321	configuring	
launching from URLs	324	status	178, 200
maintaining	372	creating	126
processes	25-26	defining	126
properties files	42	filters	126
restoring	385-386	getting status	368
services	25-26	important nodes	147
SNMP trap varbinds	246	maps	203, 205
tracking licenses	372	out-of-box	147
troubleshooting access	41	populate	126
verifying running	370	protocol traffic control	162, 165, 168, 172, 175
NNMi Status command	34, 323, 369	verifying	126
nnmincidentcfg.ovpl command	241, 244-245, 247	Node Groups	
nnmloadnodegroups.ovpl command	127, 137	view	127
nnmloadseeds.ovpl command	114-115	node identification phase	77
nnmmanagementmode.ovpl command	184	node names	
nnmnetloadnodeattrs command	138	decision tree	81
nnmrestore.ovpl command	386	discovery choices	79
nnmsetcmduserpw.ovpl command	42	Node Settings form	168

nodename attribute	367	out-of-box	
nodes		actions	22
adding		out of service	190
custom attributes	302, 313, 315	restarting management	184
filters	128, 134	selecting	75
assigning hostname wildcards	61	status	367
capability attributes	312	stopping management	184
components	181	Nodes view	187
configuration settings	368	Non-SNMP Devices node group	147
configuring		Nortel	
communication protocol settings	67	switches	295
connectivity	202	Not Managed Addresses view	190
credential settings	73	Not Managed Interfaces view	190
diagnostics	292-293	Not Managed mode	193
group status calculations	178, 200	Not Managed Nodes view	189
monitoring	168, 181	Notification stage	213
name resolution	99	notifications, sending SNMP	238
creating groups	126		
defining groups	127, 137	O	
deleting	122	objects	
discovering		adding custom attributes	302, 313, 315
description	76	capability attributes	312
name choices	79	creating	18, 20
specific nodes	112	database IDs for URLActions	311
state check	117	deleting	20
filtering		excluding IDs from discovery	94
groups	147	HSRP	181
group maps	205	listing	19
Island Node Groups	149	management modes	192
load custom attributes	138	SNMP system object ID ranges	106
managed	188	specifying SNMP ID	137, 249-251
monitoring		State Poller	151
configuration	181	tracked	181
not managed	189	URL action	306

viewing			node	
management modes		185	groups	147
VRRP		181	pairwise configurations	237, 276
opening			SNMP trap varbinds	246
console		44	subnet connection rules	111
forms		18	user roles	32, 35
operating systems			view filters	147
audit log files		43	Out of Service Addresses view	191
command-line access		42	Out of Service Interfaces view	191
discovery seeds		115	Out of Service mode	193
help systems		31	Out of Service Nodes view	190
port numbers		44	ovjboss services	26, 28
operator			ovstart command	26, 30
Boolean		134	ovstatus command	26, 28
roles			ovstop command	26, 30
level 1		34		
Level 1		32-33, 35, 322-323	P	
level 2		34	Pair Item Configuration form	281
Level 2		32-33, 35, 322-323	Pair Items tab	281
optional filters, adding		315	Pairwise	
OR variable		134	form	276
organizing incidents		251	stage	213
out-of-box			Pairwise Configuration form	237, 276, 279
actions		22	pairwise configurations	237, 266, 276, 278-279, 281
background images		205	parameters	
CIAs		214	backup	385
diagnostics		295	deduplication	271
incident			incident	
categories		251	actions	256, 285
configurations		214	messages	255
families		254	rate	274
interface			restore	386
groups		149	passwords, changing user	36, 39-41
Jython methods		290		
management event configurations		229		

Path View		verifying running	26
attributes	338	profiles, device	85, 95
configuring maps	206	progress	
RAMS	300	discovery	117
PathConnections.xml file	206	properties files	42
percentage, target status values	179	protocols	
performance		auto-discovery rules	83
generating incidents	298	communication	47
monitoring	158	defaults	47
performing automated tasks	21	devices	66
permanently disabling user accounts	41	configuring network regions	56
permissions, role	33	region	57
ping command	47, 151, 295, 362	SNMP	50
Ping menu item	34, 323	purchasing HP iSPIs	319-320
Ping Sweep, configuring	98		
pipe symbol ()		Q	
character	288	Quick Find	18-19
pipeline, event	213	Quick Start Configuration wizard	15
Point to Point Interfaces group	149	Quick View	18
populate node groups	126		
portals, embedding views within	321	R	
ports		RAMS Configuration form	300
numbers	44	RAMS data and Path View	300
prerequisites		ranges	
discovery	86	IP addresses	60, 104
pairwise configurations	278	SNMP system object ID	106
prerequisites, discovery	86	rate configuration	266, 273-274
problems		Rate Configuration tab	273-274
Causal Engine	212	Rate stage	213
processes		read-only access	321
configuring discovery	96	real-time data	300, 363, 367-368
description	26	Rediscovery Interval	98
NNMi	25	reducing incoming incidents	266
starting	26	redundancy groups, monitoring router	181
stopping	26		

Index: refreshing – routers

refreshing		RFC	250
console window	44	roles	
Region Device Credentials form	64	accessing	
regions		forms	322
assigning hostname wildcards	61	menus	34
configuring		workspaces	322
communication	57, 62, 72	administrator	322-323
credential settings	64	assigning	32
network protocols	56	assigning management modes	192
USM settings	55, 65	Guest	32, 35, 321-323
Regions tab	56-57, 60, 62, 72	launching commands	323
Relate stage	213	operator	
relative URLs	206	Level 1	32, 35, 322-323
remote		Level 2	32, 35, 322-323
event configuration	226, 261, 263	system	41
management stations	262	System	32-33, 35
Remote NNM 6.x/7.x Event Configuration form	263	user	
removing		changing	36, 39-40
incidents	387	deleting	41
reports, audit	43	determining account	33
Request for Comments	250	out-of-box	32, 35
requirements		Web Service Client	32, 35, 323
pairwise configurations	278	root causes	
URL access authentication	321	SNMP traps	251
resolution, node name	99	round-robin DNS	86
Resolver stage	213	Route Analytics Management System	300
restarting management	184	Router Redundancy Group	
restoring		monitoring	153
NNMi	385-386	Router Redundancy Member	
system role	41	form	181
results		routers	
discovery	116, 120-121	Cisco	295
discovery seeds	117-118	discovering networks	89, 112
retry behavior	50-51	Island Node Group	149
reviewing node group definitions	127	monitoring	181

Routers		default settings	54
node group	147	importing SNMPv3 settings	74
Routers view	330	Quick Start Configuration wizard	15
rows		SNMP prerequisite	86
deleting	20	seeds, discovery	81-82, 88, 112-115, 117-118
rules, auto-discovery	83	selecting	
configuring	101	nodes	75
basic settings	102	semicolon (;) character	288
Ping Sweep	98	services	
custom	88	NNMi	25-26
discovery seeds	82	ovjboss	26, 28
everything	91	starting	30
IP addresses	93, 104	State Poller	95, 151, 181
object IDs	94	stopping	30
overview	88	verifying running	28
routers	89	setting up command-line access	42
SNMP devices	90	settings	
switches	89	auto-discovery	
system object IDs	106	basic	102
vendors	92	Ping Sweep	98
rules, subnet connections	84, 109, 111	communication protocols	47
running		community strings	52, 62, 72
help outside console	31	exporting configuration	373
verifying		importing configuration	373
processes	26	node group maps	198, 206
services	28	verifying communication	75
runTool	361	severity, incident	255
		Show All Incidents menu item	34
		Show All Open Incidents menu item	34
		show commands	295
		Show Members menu item	34
		showForm	350
		showMain	324
		showView	324
S			
scaling map background images	206		
SDK licenses	372		
security check	34		
security, user-based model			
configuring	47, 55, 65		
credentials	50-51		

sign-in access, configuring	32, 35, 37, 40, 42	State Poller	151
Sign In/Out Audit Log command	370	system object ID ranges	106
Sign In/Sign Out Audit Log menu item	34, 323	timeouts	
Sign Out		default	47
command	370	nodes	67
menu item	323	regions	57
signing in		traffic control	47
console	46	trap incident configurations	211, 216, 246
URL access	321	trap varbinds	246
signing out from console	46	traps	211, 244, 259
Simple Network Management Protocol	47	verifying configuration	74
Smart Plug-ins, purchasing	319-320	SNMP Trap Configuration	
SNMP		form	248
configuring		tab	246
discovery	96	SNMP Trap Receiver stage	213
traps	239, 241, 245, 268	SNMP traps	
default community strings	51	disable trap definitions	247
discovering		SNMPv1	15, 47, 51, 72, 74, 86, 238, 249-251
devices	90	SNMPv2	15
networks	77	SNMPv2c	47, 50-51, 72, 74, 86, 238, 250-251
displaying traps	251	SNMPv3	50, 74, 86, 239
enabling nodes	67	Software Loopback Interfaces group	149
loading trap definitions	247	SONMP	83, 109
phase	81	space character	288
ports		special characters in action arguments	288
default	47	Specific Node Device Credentials form	73
nodes	67	Specific Node Settings	
regions	57	form	73
protocol version	50	tab	66-67, 74
retries		Spiral Discovery	76
default	47	adjusting discovery interval	98
nodes	67	configuring	88, 95
regions	57	discovering	
sending notifications	238	everything	91
specifying object ID	137, 249-251		

Index: tabs – Tracked Objects

deleting rows	20	remote NNM 6.x/7.x event configuration	261, 263
invoking actions	21	SNMP trap configuration	248
navigating	75	subnet connection rules	109
tabs		verifying discovery	116
Action Configuration	283-284	team communication	44
Additional Filters	128, 141	Telnet menu item	34
Community Strings	57, 62, 72	Temporary license	372
Custom Attributes	302, 313, 315	text files	137
Default Community String	51	threshold	
Default Device Credentials	53	configuring	178
Device Credentials	64	incidents	298
Discovery Seeds	112	monitoring	162, 165, 172, 175
Hostname Wildcards	57, 61	target status	179
Included Address Ranges	57, 60	Thresholds Settings form	162, 165, 172, 175
Interface Type Filters	139	time period	
Management Event Configuration	264-265	incident frequency	273
Pair Items	281	timeout	
Pairwise Configuration	237, 276, 279	behavior	50-51
Rate Configuration	273-274	toolbar	
Regions	56-57, 60, 62, 72	form	20
SNMP Trap Configuration	246, 248	tools menu	34
Specific Node Settings	66-67, 74	tools, console	
target status	179	administrator	14-15
tasks		running outside	321
auto-discovery	89-94, 101	topology maps	
configuring		building	300
communication protocols	47	island node groups	149
management events	264-265	updating	76, 122
node group map settings	199	Topology Maps Workspace view	330
subnet connection rules	109	traceroute command	295, 362
controlling SNMP object ID ranges	106	Traceroute menu item	34, 323
discovery	96	Tracked Objects	
monitoring network health	151-152	monitoring configuration	181
performing			
automated	21		

custom attributes	313, 315		
Custom Incident Attributes	311		
database object IDs	311		
form	303, 305		
limitations	306		
syntax	306		
user-based security model			
configuring	47, 55, 65		
credentials	50-51		
default settings	54		
importing SNMPv3 settings	74		
Quick Start Configuration wizard	15		
SNMP prerequisite	86		
User Account form	36, 39		
User Interface Configuration			
form	360		
users			
auditing activity	43		
changing passwords	41		
determining account roles	33		
disabling accounts	41		
editing accounts	36, 39-40		
out-of-box roles	32, 35		
restoring system role	41		
USM			
configuring	47, 55, 65		
credentials	50-51		
default settings	54		
importing SNMPv3 settings	74		
Quick Start Configuration wizard	15		
SNMP prerequisite	86		
utilization			
WAN and interface	165, 175		
			V
		varbind values	238, 259, 274, 311
		varbinds, out-of-box	246
		vendor devices	
		discovering	92
		vendor specific traps, SNMP	251
		verifying	
		address connectivity	181
		communication settings	75
		configuration for IP addresses	74
		discovery	116
		inventory	120
		Layer 2	120-121
		seeds	117
		nms-roles.properties file	41
		NNMi running	370
		node groups	126
		processes running	26
		services running	28
		user account deletion	41
		version numbers	
		SNMP protocols	50
		viewing	
		incident pair configurations	237, 276
		interface disabled incidents	298
		interface group	
		definitions	139
		management mode for objects	185
		node group	
		definitions	126
		remote management stations	262
		views	
		Configuration Workspace	349
		controlling incoming trap visibility	268

ifTypes	140	Web portals, embedding views within	321
Incidents	327	Web Service Client role	32-33, 35, 323
Interface Group	139	well-configured DNS	86
Interfaces	187	wide area networks	
Inventory Workspace	343	Island Node Group	149
IP Addresses	187	threshold monitoring	165, 175
launching outside NNMi	324	wildcards, assigning hostnames	61
Managed Addresses	189	Windows	
Managed Interfaces	188	background images	205
Managed Nodes	188	DNS prerequisite	86
Management Mode Workspace	346	log files	28, 43
Management Stations	262	nms-roles.properties file	41-42
Monitoring Workspace	335	nms-users.properties file	41-42
Node Groups	127	nnm.ports.properties file	44
Nodes	187	nnmbackup.ovpl command	385
Not Managed Addresses	190	nnmcommload.ovp command	74
Not Managed Interfaces	190	nnmDocs_en.war file	31
Not Managed Nodes	189	nnmloadseeds.ovpl command	114-115
Out of Service Addresses	191	PathConnections.xml file	206
Out of Service Interfaces	191	wizard, Quick Start Configuration	15
Out of Service Nodes	190	workspaces	
predefined view filters	147	accessing	322
Topology Maps Workspace	330	configuration	16
Troubleshooting Workspace	338	views	33
workspaces	33		
visibility, incoming traps	268		
VLAN Interfaces group	149		
Voice Interfaces group	149		
VRRP			
objects	181		
W			
WANs			
Island Node Group	149		
threshold monitoring	165, 175		

