NEC

MasterScope Network Manager 9.0
User's Manual

Copyrights

Trademark

Introduction

Thank you for choosing MasterScope Network Manager.

This manual describes the MasterScope Network Manager 9.0 (hereafter referred to as Network Manager) functions and operations.

- Throughout this manual, the installation path is described as *<On the manager, %installfolder%>* .
- If **Change Data Directory** was set to Yes at the installation, one portion of the files will be stored in the path specified as the **Data Directory**. Throughout this manual, the path specified the **Data Directory** is described as *<On the manager, %sharedfolder%>*. If you have not specified the **Data Directory**, *<On the manager, %sharedfolder%>* is the same as *<On the manager, %installfolder%>*.
- In some parts of this manual, "\" is used as the directory symbol, regardless of the type of operating system. This should be read as "/" for the Linux environment.
- To return to the former page after jumping from the hyper link in the PDF manual or the online help, press ALT + Left keys. (In the case of using Adobe Reader or Windows HTML help viewer)
- Due to upgrades, the specifications and design of windows in this manual are subject to change without notice.

Notations and Text Conventions

Document Conventions

In this manual, the following notations are used to indicate items that require special attention and supplementary information.

Notations of Items Requiring Attention and Supplementary Information

Mark	Description
Caution	Indicates important points that the user should observe to configure and use the product properly.
1) **Note**	Describes notes placed in the text.
Tip	Indicates useful information.

Text Conventions

In this manual, the following text conventions are used.

Text Conventions

Notation	Description	Example
uiname	Indicates graphical user interfaces such as dialog boxes, tabs, menus, items, and buttons.	**Alert Detail** dialog, **OK**button
<*userinput*>	Indicates items that change depending on the user environment or items that the user must specify.	<*filepath*>
`configuration file`	Indicates the contents of the configuration file.	Set the following value: `port = 54321`
`command line`	Indicates command line operations.	Run the following script: `> NvPRODBSetup.bat`

Abbreviations

Abbreviations

Formal Name	Abbreviation
MasterScope Network Manager	Network Manager, NetMgr
Configuration management database	Configuration management DB, CMDB
Alert management database	AlertDB
sFlow database	sFlowDB
MasterScope Integrated Management Server	IMS
MasterScope Network Flow Analyzer	NFA

Install Path

Default installation directory: Windows

- 32bit OS: C:\Program Files\NEC\UMF\Operations
- 64bit OS: C:\Program Files (x86)\NEC\UMF\Operations

Contents

Chapter 1. Overview 1

1.1 Product Overview 2
1.1.1 Configuration management 2
1.1.1.1 Map View 2
1.1.1.2 Device panel display (Node Manager function) 3
1.1.1.3 Importing and exporting configuration information 3
1.1.2 Fault management 4
1.1.2.1 State monitoring 4
1.1.2.2 Alert display 4
1.1.2.3 Alert Management window 5
1.1.2.4 Monitoring mode 6
1.1.3 Performance management 7
1.1.3.1 Data Collecting Setting window 7
1.1.3.2 Threshold value monitoring 7
1.1.3.3 Graph display (Checking current data) 7
1.1.3.4 Report creation (Checking historical data) 8
1.1.3.5 Graph display of traffic-flow information by sFlow 10
1.1.4 Resource Manager function 11
1.1.5 Network Provisioning function 12
1.2 Network Manager Licenses 12

Chapter 2. Overview of the Monitoring Window 14

2.1 Structure of the Monitoring Window 15
2.1.1 Network View 16
2.1.2 Map View 17
2.1.2.1 Icon colors 17
2.1.2.2 Zooming in and out in Map View 18
2.1.3 Property View 19
2.2 Web Monitoring View Function 19
2.2.1 Precautions and limitations in the web monitoring view 20
2.2.2 To use the web monitoring view (Manager) 20
2.2.3 Configuring OS settings for the web monitoring view 21
2.2.4 Starting the monitoring view 22
2.3 Web Console 22
2.4 User Access Rights 26
2.5 Operation Modes 27
2.5.1 Changing operation modes 27
2.5.2 Checking the operation mode 27

Chapter 3. Basic Operations (Tutorials) 29

3.1 Before Operating Network Manager 30
3.1.1 Starting the monitoring window 30
3.1.2 Starting the web monitoring view 31
3.2 Configuration: Registering Information for Managed Devices 33

3.2.1 Automatically detecting managed devices....33
3.2.2 Batch registering managed devices....37
3.2.3 Registering information for logging in to managed devices....39
3.2.4 Selecting devices that use the panel display and advanced function....42
3.3 Configuration: Configuring Monitoring Settings....44
3.3.1 Configuring settings for SNMP trap monitoring....44
3.3.2 Configuring settings for alive monitoring and MIB monitoring....46
3.3.3 Configuring settings for syslog monitoring....48
3.3.4 Configuring settings for reporting faults....49
3.3.4.1 Sending fault details by e-mail when specific faults occur....49
3.3.4.2 Activating Patlite when specific faults occur....54
3.3.4.3 Automatically executing commands or programs when specific faults occur....58
3.3.5 Configuring settings for aggregating alert information....62
3.3.6 Automatically collecting device information when an alert is detected....64
3.3.6.1 Executing device commands and collecting information when an SNMP trap is received....65
3.3.7 Configure the setting to manage NEC ESMPRO Agent....67
3.4 Configuration: Collecting Performance Information....68
3.4.1 Configuring settings to collect and store MIB information....68
3.4.2 Configuring settings to collect traffic flow information....72
3.5 Operations: Managing Faults....74
3.5.1 Checking fault locations and details....74
3.5.2 Displaying alerts for specific devices only....76
3.5.3 Checking the detailed status of a device on the front panel display....78
3.5.4 Checking communication and the communication path....79
3.5.4.1 Executing a ping command....79
3.5.4.2 Executing a traceroute command....80
3.6 Operations: Checking Performance Information....81
3.6.1 Checking the load status for each interface....81
3.6.2 Checking network load status from the traffic flow information....84
3.7 Operations: Accessing Managed Devices....86
3.7.1 Logging in to managed devices....86
3.7.2 Controlling the opening and closing of interfaces from the front panel display....88
3.7.3 Using special management tools for specific devices....89
3.8 Operations: Maintaining Managed Devices....91
3.8.1 Stopping monitoring during network maintenance....91
3.8.2 Managing device configurations....95
3.8.3 Upgrading device software....97
Chapter 4. Function Reference (Environment Setup)....100
4.1 Managing Users and Groups....101
4.1.1 Managing user information....101
4.1.1.1 User Management window (**Users** tab)....101
4.1.1.2 Creating a user....102
4.1.1.3 Changing user information....104
4.1.1.4 Deleting a user....107
4.1.1.5 Changing a user password....108

4.1.2 Managing group information 108
4.1.2.1 User Management window (**Groups** tab) 108
4.1.2.2 Adding a group 110
4.1.2.3 Changing a group name 111
4.1.2.4 Deleting a group 111
4.1.2.5 Changing member users 112
4.1.3 Changing group authority 113
4.1.3.1 Group authority settings 113
4.1.3.2 Detailed authority settings of the user management function 115
4.1.3.3 Detailed authority settings of Network View 116
4.1.3.4 Detailed authority settings of the calendar 123
4.1.4 Importing and exporting user information 125
4.1.4.1 Exporting user information 125
4.1.4.2 Importing user information 126
4.2 Creating Network Configuration Map 127
4.2.1 Automatically detecting devices and networks 127
4.2.1.1 Performing autodiscover (TCP/IP Hosts) 127
4.2.1.2 Performing autodiscover (networks and routers) 136
4.2.2 Manually registering devices and networks 138
4.2.2.1 Manual Register dialog box and Properties dialog box 140
4.2.2.2 Icon Type Selection dialog box 146
4.2.3 Registering topology information 147
4.2.3.1 Discovery Protocol 148
4.2.3.2 Automatically detecting topology information 149
4.2.3.3 Manually registering topology information 151
4.2.3.4 Checking topology information 162
4.2.4 Registering ProgrammableFlow physical topology information 164
4.2.4.1 Preparing for autodiscover of ProgrammableFlow physical topology 164
4.2.4.2 Automatically detecting ProgrammableFlow physical topology 166
4.2.4.3 Registering the virtual/physical interface name conversion definition file 167
4.2.5 Registering Nexus 2000 configuration 172
4.2.5.1 Automatically detecting Nexus 2000 information 172
4.2.5.2 Manually registering Nexus 2000 information 175
4.2.6 Changing the background and drawing diagrams 175
4.2.6.1 Changing the background of Map View 175
4.2.6.2 Drawing diagrams in the Map View 176
4.2.7 Updating device information via a network 179
4.2.8 Registering interface information 180
4.2.8.1 Discovering interface information 180
4.2.8.2 Setting default target ports 183
4.2.9 Changing icon properties and locations 184
4.2.9.1 Changing icon properties manually 184
4.2.9.2 Changing topology information manually 185
4.2.9.3 Moving an icon to another map 186
4.2.9.4 Copying an icon 188
4.2.9.5 Deleting topology information 188
4.2.9.6 Deleting an icon 188
4.3 Registering Login Information 189
4.3.1 Login Information Setting window 190
4.3.2 Registering device login information 191

4.3.3 Password Setting dialog box 192
4.3.4 Testing login information 195
4.3.5 Setting external server information 195
4.3.5.1 **File Transfer Protocol** tab 196
4.3.5.2 **TACACS+/RADIUS (login authentication)** tab 197
4.3.5.3 **TACACS+/RADIUS (enable authentication)** tab 197
4.3.5.4 **Port Server** tab 198
4.3.5.5 **File Transfer Server** tab 200
4.4 Managing the Advanced Functions License 201
4.4.1 Manually registering advanced functions licenses 202
4.4.1.1 NetMgr License Manager dialog box 202
4.5 Registering Device-Specific Tools 204
4.5.1 Registering applications launched from icons 204
4.5.2 Registering web URLs launched from icons 205
4.6 Batch Registering or Deleting Configuration Information 206
4.6.1 Preparing the configuration information file 207
4.6.1.1 Configuration information file format 207
4.6.2 Importing a configuration information file 226
4.6.2.1 Importing from the monitoring terminal 228
4.6.2.2 Importing using the manager command 228
4.6.3 Exporting configuration information 229
4.6.3.1 Exporting from the monitoring terminal 229
4.6.3.2 Exporting using the manager command 230
4.6.4 Operation log file 230
4.6.5 Error record file 231
4.7 Registering Routing Information for the Map between Two Nodes 231
4.7.1 Collect Routing Information dialog box 232
4.8 Configuring the Operating Environment for the Fault Management 233
4.9 Error Monitoring 236
4.9.1 Monitoring items 236
4.9.2 About alert severity and priority 237
4.9.2.1 About severity extension 237
4.9.2.2 Changing priority level settings 238
4.9.2.3 Changing severity level settings 239
4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function) 241
4.10.1 State Monitoring window 241
4.10.2 Creating new state monitoring rule entries 243
4.10.2.1 Rule Entry Settings dialog box 244
4.10.2.2 Node List dialog box 246
4.10.2.3 Variable setting dialog box 247
4.10.3 Modifying state monitoring rule entries 249
4.10.4 Copying state monitoring rule entries 250
4.10.5 Deleting state monitoring rule entries 250
4.10.6 Batch registering state monitoring settings 251
4.10.6.1 State monitoring setting file format 251
4.10.6.2 Importing state monitoring rule entries 254
4.10.6.3 Exporting state monitoring rule entries 255

4.10.6.4 Operation log file 257
4.10.6.5 Error record file 257
4.10.7 Embedding rule files 258
4.11 Monitoring SNMP Traps 259
4.11.1 Settings for monitoring SNMP traps/informs 259
4.11.2 Trap definitions 260
4.11.2.1 Trap definition categories 261
4.11.2.2 Trap definition priority levels 262
4.11.3 Referring to trap definitions 265
4.11.3.1 Trap Definition Management window 265
4.11.3.2 Filter Settings dialog box 270
4.11.3.3 Filtering trap definitions to display 274
4.11.4 Searching for trap definitions 275
4.11.4.1 Search Matching Definitions window 276
4.11.4.2 Searching for trap definitions to be applied when SNMP traps are received 281
4.11.5 Adding, editing, or deleting trap definitions 282
4.11.5.1 Add/Edit/Properties of Trap Definition dialog box 282
4.11.5.2 Adding a trap definition 290
4.11.5.3 Editing a trap definition 291
4.11.5.4 Deleting a trap definition 291
4.11.5.5 Adding, updating, or deleting all trap definitions at once 292
4.11.6 Creating a trap definition from an MIB file 292
4.11.6.1 Import dialog box 293
4.11.6.2 Automatically creating a trap definition from an MIB file 295
4.11.6.3 Description of a trap definition automatically created from an MIB file 296
4.11.6.4 Messages output during MIB file analysis 297
4.11.7 Priority order for alert conversion using trap definition files 300
4.12 Monitoring Syslogs 302
4.13 Controlling Alerts (Aggregating, Discarding, and Converting Contents) 302
4.13.1 Controlling alerts 303
4.13.2 Setting controlling conditions 304
4.13.3 Enabling controlling conditions 308
4.13.4 Control condition sample files 308
4.13.5 Important points to consider when massive alerts are rushed 310
4.14 Settings for Sending Alert Reports 310
4.14.1 Alert Notification Setting window 311
4.14.2 Configuring report settings 314
4.14.2.1 Setting example that switches report settings depending on the date and time 316
4.14.3 Defining report settings 318
4.14.3.1 Defining Patlite reports 318
4.14.3.2 Defining e-mail reports 322
4.14.3.3 Defining action reports 326
4.14.3.4 List of substitute strings 329
4.14.4 Linking with other SNMP manager software using SNMP traps 330
4.14.4.1 Configuring settings for sending SNMP traps 330
4.14.4.2 Important points when sending SNMP traps 331
4.14.5 Setting report options 331

4.15 Settings for Executing Device Commands When Alerts Occur 333
4.15.1 Executing commands when SNMP traps are received 333
4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices 334
4.16.1 Data Collecting Setting window 334
4.16.1.1 Port Number Select dialog box 339
4.16.1.2 Interface Number Select dialog box 340
4.16.1.3 Managed Item Selection Dialog dialog box 340
4.16.1.4 MIB Description dialog box 341
4.16.1.5 Rule Setting dialog box 342
4.16.1.6 Instance Select dialog box 342
4.16.2 Configuring threshold monitoring 343
4.16.2.1 Customizing the contents of threshold excess alerts and recovery alerts 348
4.16.3 Configuring MIB expressions 350
4.16.3.1 MIB Expression Creating window 350
4.16.3.2 Creating a new MIB expression 352
4.16.3.3 Editing a MIB expression 354
4.16.3.4 Deleting a MIB expression 355
4.16.3.5 Checking for entries that are using expressions 355
4.16.4 Executing data collection 357
4.16.5 Deleting a data collection entry 358
4.16.6 Batch registering data collection settings 359
4.16.6.1 Data collection settings file format 359
4.16.6.2 Importing data collection settings 364
4.16.6.3 Exporting data collection settings 366
4.16.6.4 Operation log file 367
4.16.6.5 Error record file 368
4.16.7 Maintaining performance data (CSV files, report files) 368
4.16.7.1 Storage folder and format for performance data (CSV files) 368
4.16.7.2 Automatic generation and automatic deletion of reports 369
4.16.8 Filtering function for performance data passed to other MasterScope products 369
4.16.8.1 Filtering performance data passed to other MasterScope products 370
4.16.8.2 Changing the data filter settings 371
4.16.8.3 Confirming status of the data filter function 371
4.16.8.4 Stopping and resuming the data filter function 371
4.16.8.5 File format of the data filter settings 372
4.17 Collecting Traffic Flow (sFlow) Information 373
4.17.1 Registering sFlow agents 373
4.17.1.1 sFlow Agent List window 374
4.17.2 Customizing search conditions 375
4.17.3 Setting duration of flow data retention 376
4.18 Settings for Displaying Device Front Panel 378
4.18.1 Setting for displaying device front panel 379
4.18.2 Customizing a device front panel 380
4.18.2.1 Setting module ports 380
4.18.2.2 Editing a background of the panel window 382
4.18.2.3 Editing port displays 382
4.18.2.4 Editing port positions 385
4.18.2.5 Editing management and statistics menus 385
4.18.2.6 Editing MIBs for port status decision 388

4.18.2.7 Editing a polling interval 388
4.18.2.8 Clearing panel window customizations 389
4.18.3 Using a customized device front panel for multiple icons 389
4.18.4 Using a customized device front panel in other monitoring terminals 390
4.19 Setting for Running Device Commands 391
4.19.1 Defining commands 391
4.19.1.1 Simple scripts 393
4.19.1.2 Precautions in creating commands 395
4.19.1.3 Example of creating a command 397
4.19.2 Scheduling command execution 398
4.20 Setting for Managing Device Configuration (Resource Manager) 399
4.20.1 Registering an FTP or TFTP server 400
4.20.1.1 Using an external FTP or TFTP server 401
4.20.1.2 Configuring the IP for Device 403
4.20.2 Monitoring configuration changes 404
4.20.2.1 Check Configuration window 404
4.20.2.2 Starting config change management 404
4.20.2.3 Stopping config change management 406
4.20.2.4 Batch registration of change management schedule information 406
4.20.3 Changing the limit for the number of config histories 411
4.20.3.1 Changing the number of running-config histories 411
4.20.3.2 Changing the number of startup-config histories 412
4.20.3.3 Changing the number of change management histories 412
4.20.4 Exporting the latest configuration 413
4.20.5 Setting for sending an alert 414
4.21 Linking with NEC SigmaSystemCenter (Network Provisioning) 415
4.21.1 Preparing for linking 415
4.21.2 Coexisting with related applications 416
4.21.3 Precautions during operation 417
4.21.4 Load balancer option settings function 417
4.21.4.1 Option definition file overview 417
4.21.4.2 Option definition file format 417
4.21.5 Uplink Failure Detection (UFD) setup function 422
4.21.5.1 Overview of UFD setup function commands 422
4.21.5.2 UFD setup definition file format 423
4.21.5.3 Configuring UFD setup function 424
4.21.5.4 Changing the VLAN number/FDP number combination 424
4.21.6 Checking configuration status of Network Provisioning 424
4.21.6.1 TSV file format output by NvPRODCImportExportCmd (VLAN) 424
4.21.6.2 TSV file format output by NvPRODCImportExportCmd (LB) 425
4.22 Scheduling 426
4.22.1 Setting a calendar 426
4.22.1.1 Calendar Setting dialog box 427
4.22.1.2 Customizing a calendar 428
4.22.1.3 Customizing calendar rules 433
4.22.2 Setting a time schedule 435
4.22.2.1 Customizing a time schedule 435
4.22.2.2 Customizing time schedule rules 439
4.22.3 Setting a duration schedule 441

4.22.3.1 Customizing a duration schedule 441
4.22.3.2 Customizing duration schedule rules 442
4.23 Settings for Managing Audit Logs 443
4.23.1 Defining report settings for audit logs 444
4.23.2 Customizing the audit log display 444
4.23.3 Setting audit log management options 445
Chapter 5. Function Reference (Operations) 447
5.1 Checking Alert Information 448
5.1.1 Auto recovery and manual recovery type alerts 448
5.1.2 Turning off sound during an alarm 449
5.1.3 Referencing the new alert list 449
5.1.3.1 Alert Detail dialog box 451
5.1.3.2 Node List dialog box 455
5.1.4 Managing alerts 456
5.1.4.1 Filter Settings dialog bar 459
5.1.4.2 Specifying wildcards 460
5.2 Checking Results of Device Commands Executed When Alerts Occurred 461
5.3 Checking Syslog Information from External File 462
5.4 Managing Alert Report Status 463
5.4.1 Referencing report status (list) 463
5.4.2 Referencing report conditions (information) 465
5.4.3 Searching report status 467
5.4.4 Confirming report status (and removing from list) 467
5.4.5 Deleting report histories 467
5.5 Executing Monitoring Commands 468
5.5.1 Executing a ping command 468
5.5.2 Executing a traceroute command 468
5.5.3 Logging in to devices from the monitoring terminal 469
5.6 Launching Device-Specific Management Tools 470
5.6.1 Launching applications from icons 470
5.6.2 Launching web browsers from icons 471
5.7 Displaying Routing Information Map between Two Nodes 471
5.7.1 Displaying a point-to-point map 471
5.7.2 Description of map display 473
5.8 Verifying Interface Properties 475
5.9 Displaying Device Front Panels 475
5.9.1 Opening a device front panel 476
5.9.2 Device front panel menu 477
5.9.3 Displaying configuration information 478
5.9.4 Changing configuration information 479
5.9.5 Displaying statistical information 481
5.10 Executing Device Commands 482
5.10.1 Executing a registered device command 482
5.10.2 Executing a command immediately on the manager 484

5.10.3 Checking command execution results....484
5.10.3.1 Viewing command execution results....484
5.10.3.2 Exporting the list of command execution results....485
5.11 Checking Collected Performance Data (MIB)....485
5.11.1 Displaying a graph....486
5.11.1.1 Graph view window....487
5.11.1.2 Set X axis dialog box....489
5.11.1.3 Set Y axis dialog box....490
5.11.1.4 Select Item dialog box....490
5.11.2 Creating and displaying a report....490
5.11.2.1 View Report window....493
5.11.2.2 Deleting a report....495
5.11.3 Searching for collection entries....496
5.11.4 Setting filters in the Data Collecting Setting window....497
5.11.5 Storage folders for performance data (CSV files, report files)....498
5.12 Checking Analysis of Traffic Flow (sFlow)....500
5.12.1 Graph display of traffic-flow information from sFlow....500
5.12.2 sFlow graph structure....502
5.12.3 CSV file storage folder and format....503
5.13 Starting or Stopping Monitoring by the Monitoring Mode....505
5.13.1 Manually setting monitoring mode....506
5.13.2 Setting and changing a monitoring mode schedule....506
5.13.3 Viewing a monitoring mode schedule....509
5.13.4 Canceling a monitoring mode schedule....510
5.13.5 Deleting a monitoring mode schedule....511
5.14 Managing Device Configuration (Resource Manager)....512
5.14.1 Managing running-config....512
5.14.1.1 Running-config Management window....512
5.14.1.2 Collecting running-config....514
5.14.1.3 Viewing running-config differences....515
5.14.1.4 Managing running-config history....516
5.14.1.5 Uploading running-config....518
5.14.2 Managing startup-config....520
5.14.2.1 Startup-config Management window....520
5.14.2.2 Collecting startup-config....523
5.14.2.3 Viewing startup-config differences....524
5.14.2.4 Managing startup-config history....524
5.14.2.5 Uploading startup-config....526
5.14.3 Checking config differences in change monitoring....528
5.15 Managing Device Software (Resource Manager)....531
5.15.1 Managing software files....531
5.15.1.1 Uploading a software file....539
5.15.1.2 Downloading a software file....541
5.15.1.3 File transfer function dialog box....542
5.15.2 Deploying device software....543
5.15.2.1 Deploying a software file....543
5.15.2.2 Precautions when deploying software....548
5.16 Managing Audit Logs....551

5.16.1 Viewing audit logs....551
5.16.2 Searching audit logs....554
5.16.3 Exporting audit logs to a file....555
5.16.4 Deleting audit logs within a category....555
5.17 Searching for a Node....556
5.18 Changing Window Appearance....557
5.18.1 Changing the method for positioning windows....557
5.18.2 Showing or hiding the toolbar....557
5.18.3 Showing or hiding the status bar....557
5.19 Printing the Map View....557
Chapter 6. Menu Reference....559
6.1 Main Menus....560
6.1.1 List of available main menu commands....560
6.1.2 **File** menu....561
6.1.3 **View** menu....562
6.1.4 **Operation** menu....562
6.1.5 **Setting** menu....563
6.1.6 **Window** menu....563
6.1.7 **Help** menu....564
6.2 Network View Menu....564
6.2.1 **Configuration Management** menu....564
6.2.1.1 List of available **Configuration Management** menu commands....564
6.2.1.2 **Import and Export** menu....566
6.2.1.3 **Autodiscover** menu....566
6.2.1.4 **Update Property** menu....567
6.2.1.5 **Check Topology** menu....568
6.2.1.6 **Collect Routing Information** menu....568
6.2.1.7 **Group List** menu....568
6.2.1.8 **Group Member List** menu....569
6.2.1.9 **Monitoring-mode** menu....569
6.2.1.10 **Monitoring-mode Schedule** menu....569
6.2.1.11 **Login Information Setting** menu....570
6.2.1.12 **FTP/TFTP Server Setting** menu....570
6.2.1.13 **Interface Property** menu....570
6.2.1.14 **Start Application** menu....571
6.2.1.15 **Start Web browser** menu....571
6.2.1.16 **Command Creation** menu....571
6.2.1.17 **Command Execution Result** menu....571
6.2.1.18 **Command Scheduling** menu....571
6.2.2 **Fault Management** menu....572
6.2.2.1 List of available **Fault Management** menu commands....572
6.2.2.2 **State Monitoring** menu....573
6.2.2.3 **Trap Definition Management** menu....573
6.2.2.4 **Alert Notification Setting** menu....573
6.2.2.5 **Show Route of 2 Devices** menu....574
6.2.2.6 **Ping (IPv4)** menu....574
6.2.2.7 **Ping (IPv6)** menu....574
6.2.2.8 **Remote Login** menu....574

6.2.2.9 **Trace Route (IPv4)** menu 574
6.2.2.10 **Trace Route (IPv6)** menu 575
6.2.2.11 **Show Unrecovered Aler** menu....575
6.2.2.12 **Show All Alert** menu 575
6.2.3 **Performance Management** menu....575
6.2.3.1 List of available **Performance Management** menu commands....575
6.2.3.2 **Data Collecting** menu 576
6.2.3.3 **MIB Expression Creating** menu 576
6.2.3.4 **Delete Report Cache on Console** menu 576
6.2.3.5 **Entry Information Import and Export** menu 576
6.2.3.6 **sFlow Setting** menu 576
6.2.4 **Device Config Management** menu....577
6.2.4.1 List of available **Device Config Management** menu commands....577
6.2.4.2 **Alert Sending Setting** menu....578
6.2.4.3 **Export Latest Config** menu 578
6.2.4.4 **Schedule Information Import and Export** menu 578
6.2.4.5 **Running-config Management** menu....578
6.2.4.6 **Startup-config Management** menu 579
6.2.4.7 **Check Configuration** menu 579
6.2.5 **Software Management** menu 579
6.2.5.1 List of available **Software Management** menu commands 580
6.2.5.2 **File Management** menu....580
6.2.5.3 **Software Upgrade** menu 580
6.2.6 **NetMgr License Management** menu....581
6.2.7 **Environment Setting** menu 581
6.2.8 **Device Front Panel** menu 582
6.2.9 **Property** menu 582
6.2.10 **Move** menu 583
6.2.11 **Copy** menu....583
6.2.12 **Update** menu 583
6.2.13 **Delete** menu....583
6.3 Audit Log menu 584
6.3.1 List of available **Audit Log** menu commands 584
6.3.2 **Report Setting** menu 584
6.3.3 **Initialize Category** menu 584
6.3.4 **Swap Category** menu 584
6.4 Common Menus for Background in the Map View 585
6.4.1 List of available Common Background menu commands....585
6.4.2 **Back** menu....585
6.4.3 **Up** menu....585
6.4.4 **Home** menu 585
6.4.5 **Select All** menu....585
6.4.6 **Manual Register** menu 585
6.4.7 **Paste** menu....586
6.4.8 **Port Name** menu....586
6.4.9 **Background Color** menu 586
6.4.10 **Background Bitmap** menu 586
6.4.11 **Grid** menu 586

6.4.12 **Arrange Icon** menu 586
6.5 Common Menus for Objects (Icons) in the Map View 586
6.5.1 **Change Order** menu 587
6.5.1.1 **Move to Front** menu 587
6.5.1.2 **Move to Back** menu 587
6.5.1.3 **Move to Forward** menu 587
6.5.1.4 **Move to Backward** menu 587
6.5.2 **Icon Text** menu 587
6.5.2.1 **Bottom** menu 587
6.5.2.2 **Right** menu 587
6.5.2.3 **Top** menu 587
6.5.2.4 **Left** menu 587
6.6 Common Menus in the Tree View 587
6.6.1 List of available Tree View Common menu commands 587
6.6.2 **Expand** menu 588
6.6.3 **Collapse** menu 588
6.6.4 **Find** menu 588

Chapter 7. Supplemental Explanation for Monitoring Function 589

7.1 State Monitoring Rules 590
7.1.1 Rules for monitoring alive status 590
7.1.1.1 updown:UpDownCheck 590
7.1.1.2 updownv6:ipv6UpDownCheck 591
7.1.1.3 snmpchk:SNMP_Check 592
7.1.2 Rules for monitoring interface status 592
7.1.2.1 ifdown:InterfaceDown 592
7.1.2.2 ifDescr:UpDownCheck 593
7.1.2.3 ifName:UpDownCheck 594
7.1.2.4 ifOper:InterfaceStateCheck 594
7.1.2.5 ifup:InterfaceUp 595
7.1.2.6 nvtp-topchk:InterfaceDownCheck 596
7.1.2.7 nvtp-stpstat:STP_PortStateCheck 597
7.1.3 Rules for monitoring threshold 597
7.1.3.1 ifload64:InterfaceLoad_64bit 597
7.1.3.2 ifload:InterfaceLoad 598
7.1.3.3 nvtp-bandchk:BandTraffic 599
7.1.3.4 thresh:ThresholdValueCheck 601
7.1.4 Rules for host resource monitoring 602
7.1.4.1 host_cpuload:CPU_LoadAvg_1min_HOST 602
7.1.4.2 host_disk_usage:Disk_UsageRate 603
7.1.4.3 host_pmem_usage:PhysicalMemory_UsageRate 604
7.1.4.4 host_vmem_usage:VirtualMemory_UsageRate 605
7.1.4.5 host_process_check:ProcessCheck 605
7.1.5 Rules for specific device models 607
7.1.5.1 PortCheck_for_Catalyst2900:PortStateCheck_C2900PortEntry 607
7.1.5.2 PortCheck_for_Catalyst:PortStateCheck_PortEntry 607
7.1.5.3 AverageBusy5m_for_Catalyst:CPU_avgBusy5_CiscoIOS 608
7.1.6 Other rules 609
7.1.6.1 icmperrv6:ipv6ICMP_OutputErrorPackets 609
7.1.6.2 icmperr:ICMP_OutputErrorPackets 610

7.1.6.3 valchange:ValueChange 610
7.1.7 Creating new rules 611
7.1.7.1 Rule file format 611
7.1.7.2 Initializing (Initialize-section) 611
7.1.7.3 Rule grammar 612
7.1.7.4 Embedding new rule files 619
7.1.7.5 Debugging new rule files 619
7.1.7.6 Customizing fault event message files 620
7.1.7.7 Examples of rule descriptions 621
7.2 Data Collection Rules 622
7.2.1 Traffic of the specific host 622
7.2.2 Traffic of the specific hub port (64bit) 623
7.2.3 Traffic of the specified hub port 625
7.2.4 WAN Traffic (64bit) 627
7.2.5 WAN Traffic 628
7.2.6 Server load 630
7.2.7 Device CPU busy rate for Catalyst series 631
7.2.8 MIB Expression 632
7.2.9 General 634
7.2.10 Built-in MIB Expression rules 636
7.2.10.1 Rules for interfaces 637
7.2.10.2 Rules for QX series 638
7.2.10.3 Rules for IX series 639
7.2.10.4 Rules for IP8800 series and ALAXALA Networks devices 639
7.2.10.5 Rules for PF series 641
7.2.10.6 Rules for SV series 641
7.2.10.7 Rules for BX series and AudioCodes devices 642
7.2.10.8 Rules for Cisco Systems devices 642
7.2.10.9 Rules for Fortinet devices 643
7.2.10.10 Rules for A10 Networks devices 643
7.3 Standard Specification Format 644
7.3.1 Overview of Standard Specification Format 644
7.3.2 Standard Matching Specification Format 644
7.3.3 Standard Component Name Specification Format 645
7.3.4 Standard AMIB Name Specification Format 646
7.3.5 Standard AMIB Value Specification Format 647
7.4 Adding MIBs 648
7.4.1 Procedure for adding an MIB 651
7.4.1.1 Procedure for incorporating an AMIB definition file and type definition file 652
7.4.1.2 Procedure for incorporating an AMIB help file 654
7.4.1.3 Procedure for incorporating an AMIB enumeration 655
7.4.1.4 MIB Definition hexadecimal notation setting procedure 655
7.4.2 Handling errors 656
7.5 Monitoring Devices Using IPv6 662
7.5.1 Using the IPv6 function 662
7.5.2 IPv6-compatible functions 663
7.6 SNMP Trap Identification Method 664
7.7 Notes on Counter-type and Counter64-type MIBs 666

7.8 Notes on Monitoring Nexus 5000 and 2000 Series 667

Chapter 8. Supplemental Explanation for Resource Manager and Device Access 669

8.1 Resource Manager Supplemental Explanation 670
8.1.1 Error Codes in Resource Manager function 670
8.1.2 Supported Devices in Resource Manager function 671

8.2 Supplemental Explanation for Device Access 675
8.2.1 Device-specific operations 675
8.2.1.1 Managing Cisco Nexus 7000 Virtual Device Context (VDC) configuration 675
8.2.1.2 Managing Cisco ASA 5500 redundant/multiple context mode configuration 676
8.2.1.3 Managing Juniper EX4200 Virtual Chassis (VC) configuration 679
8.2.1.4 Managing UNIVERGE WA series 679
8.2.1.5 Managing the PF5459 series, QX-S series 679
8.2.1.6 Managing the BIG-IP series 680
8.2.1.7 Managing the AX series and the Thunder ADC series 681
8.2.1.8 Managing the FortiGate series 682
8.2.1.9 Managing the IP8800/S8300 and IP8800/S8600 series 682
8.2.2 Extended Settings for the Resource Manager Function 682

Chapter 9. Command Reference 685

9.1 Commands for Audit Log (AuditTrailCmd) 686
9.1.1 AuditTrailCmd INIT 686
9.1.2 AuditTrailCmd SWAP 687
9.1.3 AuditTrailCmd CSV 688

9.2 Commands for Alert Report History (ReportCmd) 689
9.2.1 ReportCmd INIT 689
9.2.2 ReportCmd SWAP 690

9.3 Commands for License Registration (LicenseCmd) 690
9.3.1 LicenseCmd ADD 690
9.3.2 LicenseCmd DELETE 691
9.3.3 LicenseCmd LIST 692
9.3.4 LicenseCmd REGISTER 692

9.4 Alert Information Output Command (NvPROAlertPrint) 693

9.5 Definition Files Operation Command 695
9.5.1 NvPROMib2Amib 695
9.5.2 nvpamibcheck 697
9.5.3 NvPROReloadDllMgr 698
9.5.4 NvPROReloadDefFileMgr 699

9.6 Trap Definition Operation Commands 700
9.6.1 Trap definition batch registration command (nvptrapdefconf) 700
9.6.1.1 Trap definition batch registration file format 703
9.6.2 Trap definition auto generation command (nvpmib2trapdef) 710

9.7 SNMP Access Command 712
9.7.1 NvPROAmibGetSvc/NvPROAmibGetMgr 712
9.7.2 NvPROAmibSetMgr 716

9.8 Command for Sending SNMP Traps 717

9.8.1 NvPROTrapSend....717
9.8.2 Sending SNMP trap format....719
9.9 Command for Issuing Alert Events (nvpalertsend)....720
9.10 Configuration Information Operation Command....722
9.10.1 Configuration information batch registration command (nvpnodeconf)....722
9.10.2 Configuration information update command (nvpnodeup)....725
9.10.2.1 Format of files that specify the target devices of `nvpnodeup` command....728
9.10.3 XML file output command (NvPROExportCmd)....729
9.10.4 VLAN/Load Balancer setting information export command (NvPRODCImportExportCmd)....730
9.11 Status Monitoring Config Command (nvpstsmonconf)....731
9.12 Data Collection Config Command....734
9.12.1 Data Collection Config Command (nvpdatacolconf)....734
9.12.2 Data Collection Filter Operation Command (nvpdatacolfilter)....736
9.13 File Code Conversion Command (nvpfileconv)....739
9.14 Command for Executing Device Commands (nvpdevcmdexe)....741
9.15 Backup and Restore Function....744
9.15.1 Backup command....744
9.15.2 Backup list command....746
9.15.3 Backup delete command....747
9.15.4 Restore command (restore procedure)....748
9.15.4.1 Restore procedure for Windows....748
9.15.4.2 Restore procedure for Linux....751

Chapter 10. System Maintenance....755

10.1 Checking Version Information....756
10.1.1 Checking the version of the manager function....756
10.1.2 Checking the version of a monitoring terminal....756
10.2 Starting and Stopping the Manager Function....757
10.3 Registering Licenses....759
10.3.1 License Management window....759
10.3.2 Registering a license key....760
10.3.3 Registering a codeword....762
10.3.4 Deleting a license....763
10.3.5 Checking the number of license....764
10.4 Changing System Environment....764
10.4.1 Changing the IP address for the manager....764
10.4.2 Changing the host name for the manager....765
10.4.3 Changing the destination of a monitoring terminal....766
10.4.4 Changing a port....767
10.4.5 Specifying a source IP address for monitoring packets....768

Chapter 11. Troubleshooting....769

11.1 Errors in Starting the Monitoring Window....770
11.1.1 The error dialog box is displayed when starting the monitoring window....770

11.1.1.1 Failed to connect to Manager.(10061) 770
11.1.1.2 MasterScope Network Manager is not available. Necessary license is insufficient. 770
11.1.1.3 There is no effective License 771
11.1.2 The tree view is not displayed hierarchically 771
11.1.3 Displaying NetMgr License Manager dialog box under condition of license shortage. 771
11.2 Errors in Operations 772
11.2.1 The menu is not accessible (it is dimmed) 772
11.2.2 The error dialog box is displayed when setting device password 772
11.2.3 Monitoring terminal is disconnected from manager after leaving it without operation. 773
11.2.4 The error dialog box is displayed when executing menu with many icons selected 773
11.3 Errors and Precautions for Alert Management 774
11.3.1 No alert display for SNMP traps 774
11.3.2 The system logs are not displayed as alerts 775
11.3.3 Garbled character strings in SNMP traps 775
11.3.4 Precautions when a large number of alerts are received 776
11.4 Coexisting with Other Software 776
11.4.1 Using the Windows SNMP Trap service 776
11.4.2 Sharing the SYSLOG port with other software 778
11.4.3 TFTP server competition with other software 779
Appendix A. Linking with MasterScope SystemManager G 780
A.1 Alert Message Format 780
A.2 Character Limit for Messages 782
A.3 Customizing the Message Text Format 782
A.4 Sending a Message as an SNMP Trap 783
Appendix B. Icons 785
B.1 Map 785
B.2 Node 785
Appendix C. Embedded MIB File List 814

Chapter 1. Overview

Contents

1.1 Product Overview 2
1.2 Network Manager Licenses 12

1.1 Product Overview

Network Manager is an SNMP-based network management system that improves the efficiency of multi-vendor networks and reduces management costs. The following management operations are available using the basic Network Manager functions:

Configuration Management

- Graphical display of network configuration
- Management of information relating to the properties of network configuration elements
- Visualization of the network equipment front panels

Fault Management

- Network state monitoring
- Receipt of fault notifications from devices
- Reporting of faults to the administrator
- Display of alerts from received system logs

Performance Management

- Reports and graphical display of LAN and WAN performance

Advanced Functions of Management Operations:

Advanced functions of management operations:

- Management of device configuration information and software (Resource Manager function)
- Settings for devices linked with NEC SigmaSystemCenter (Network Provisioning function)

Caution

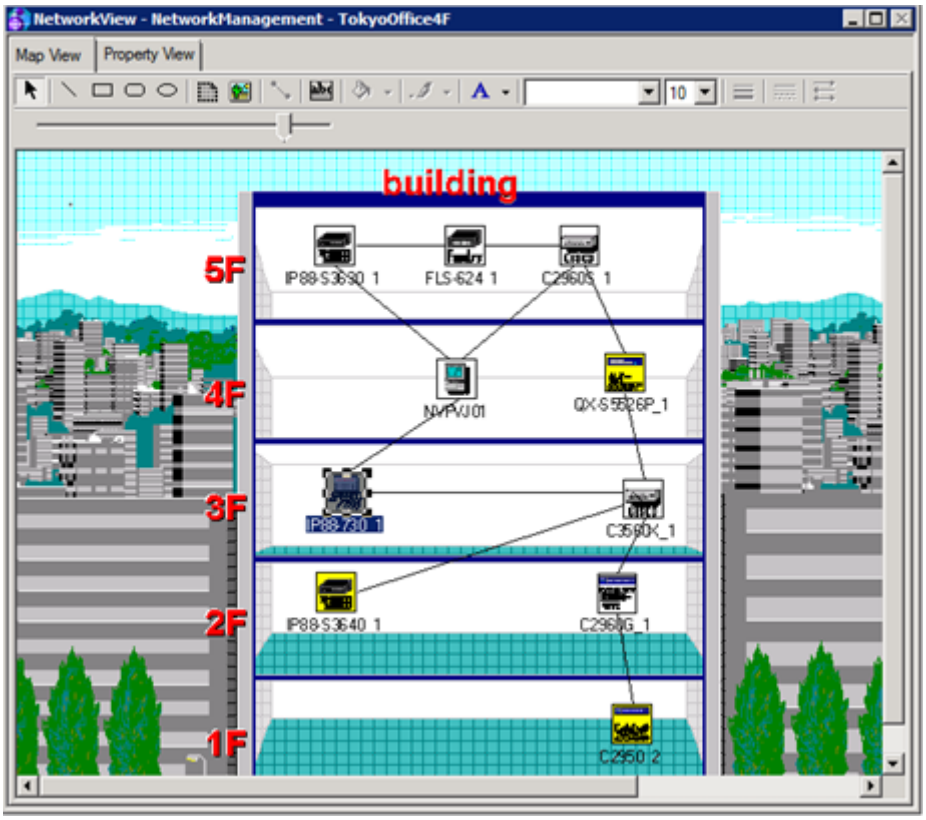
To use advanced functions, an advanced functions license must be purchased. For the license, refer to "1.2 Network Manager Licenses (page 12)".

1.1.1 Configuration management

1.1.1.1 Map View

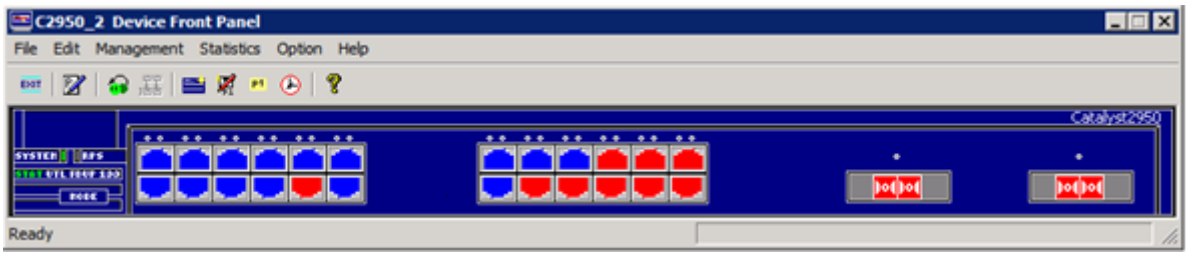
Map View is a basic Network Manager window that graphically displays the following: network configuration diagrams, devices connected to the network, and physical topology. Each of the Network Manager functions starts from this window.

When Network Manager detects a network fault and issues an alert, the color of the device icon in this windows also changes. The color depends on the level of the alert (Normal, Unknown, Warning, MINOR, MAJOR, or Fatal). For details, refer to "2.1 Structure of the Monitoring Window (page 15)".



1.1.1.2 Device panel display (Node Manager function)

By displaying the front panel of a managed device, the up or down status of the ports can be displayed intelligibly. For details, refer to "5.9 Displaying Device Front Panels (page 475)".



1.1.1.3 Importing and exporting configuration information

One method for registering configuration information (device and network information) in Network Manager is importing the information using the import feature.

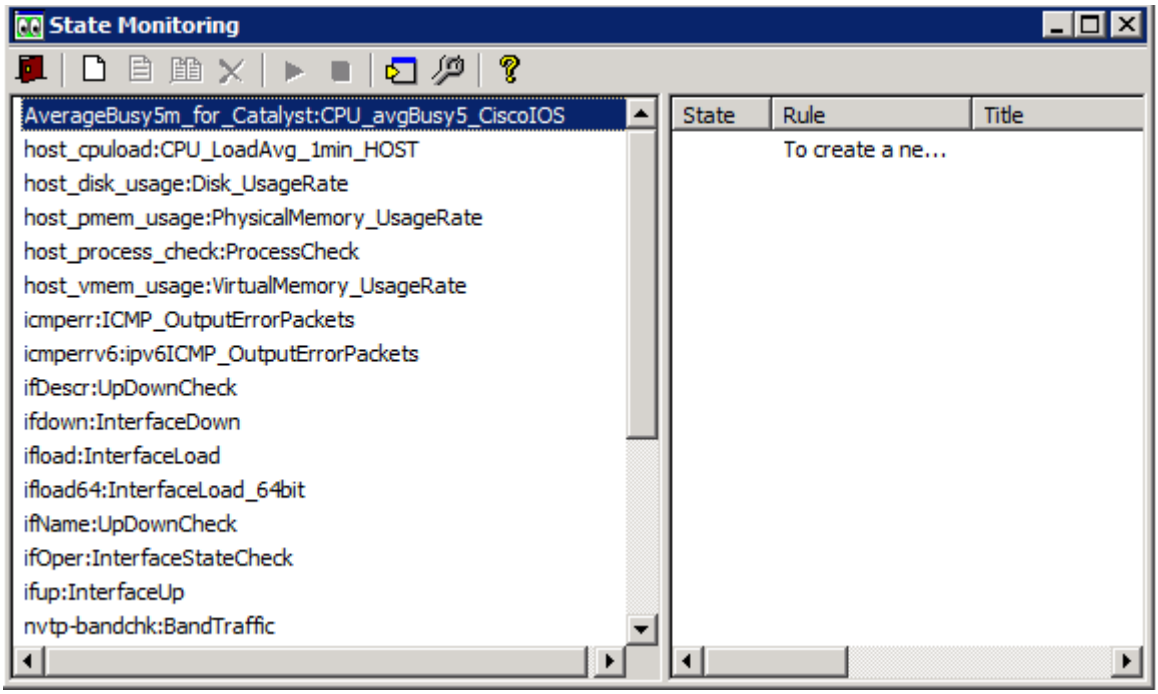
By using the configuration information import feature, many devices in a large-scale environment are registered in a batch. It is also possible to export currently registered configuration information to an external file at the same time. The format of the external file used for importing and exporting is a text (CSV) file. You can edit using a text editor. For details, refer to "4.6 Batch Registering or Deleting Configuration Information (page 206)".

1.1.2 Fault management

1.1.2.1 State monitoring

The state monitoring function monitors the status of devices being managed by Network Manager and detect any changes in their status. For example, it is possible to detect heavily loaded segments and whether a device is up or down.

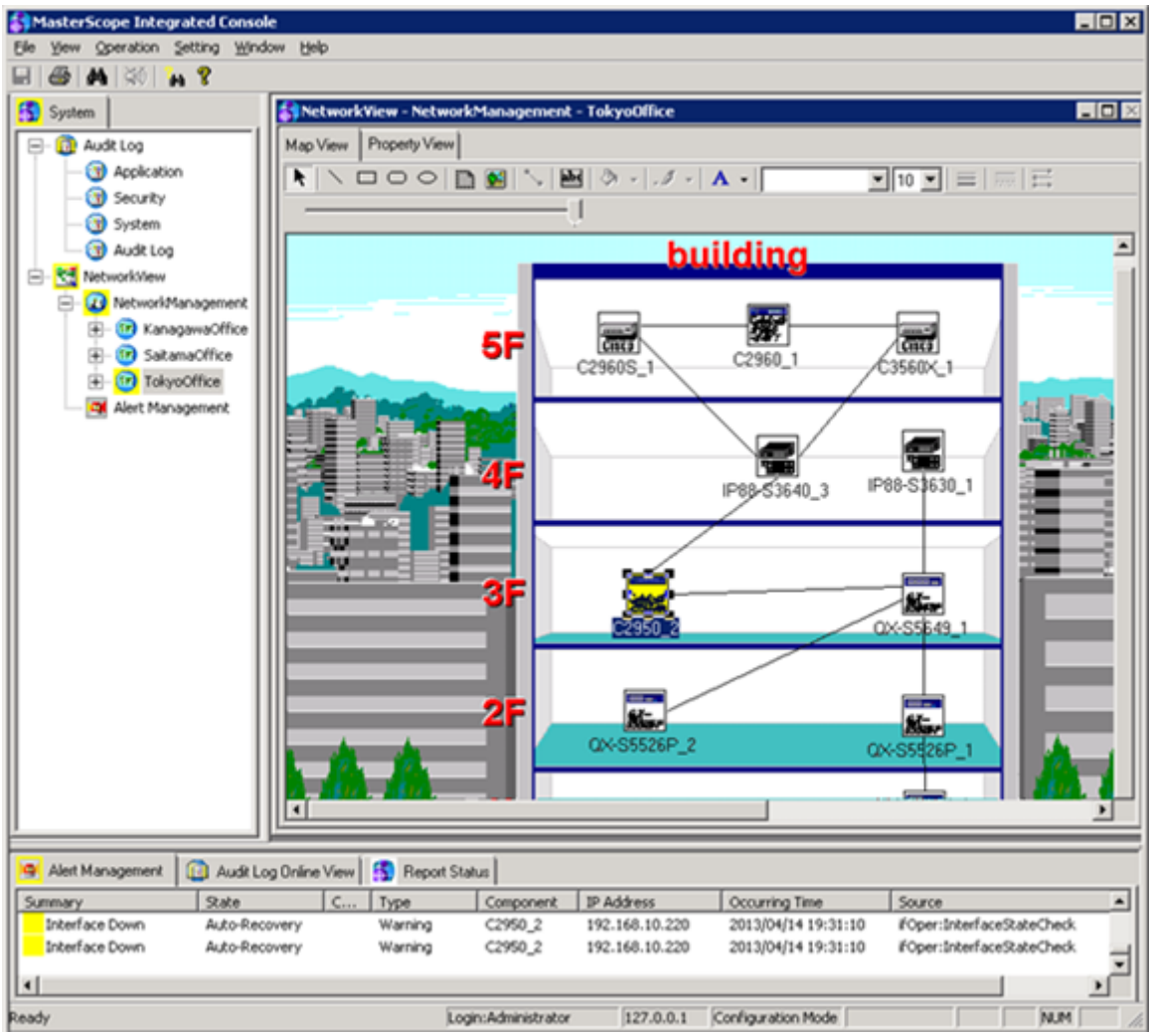
In the State Monitoring window, monitoring rules are set for managed devices as a basis for detecting network faults. For details, refer to "4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function) (page 241)".



1.1.2.2 Alert display

Displays SNMP traps and system logs, sent from managed devices, as alerts. Fault information detected by Network Manager during state monitoring is also displayed as an alert. New alerts are automatically added to the list.

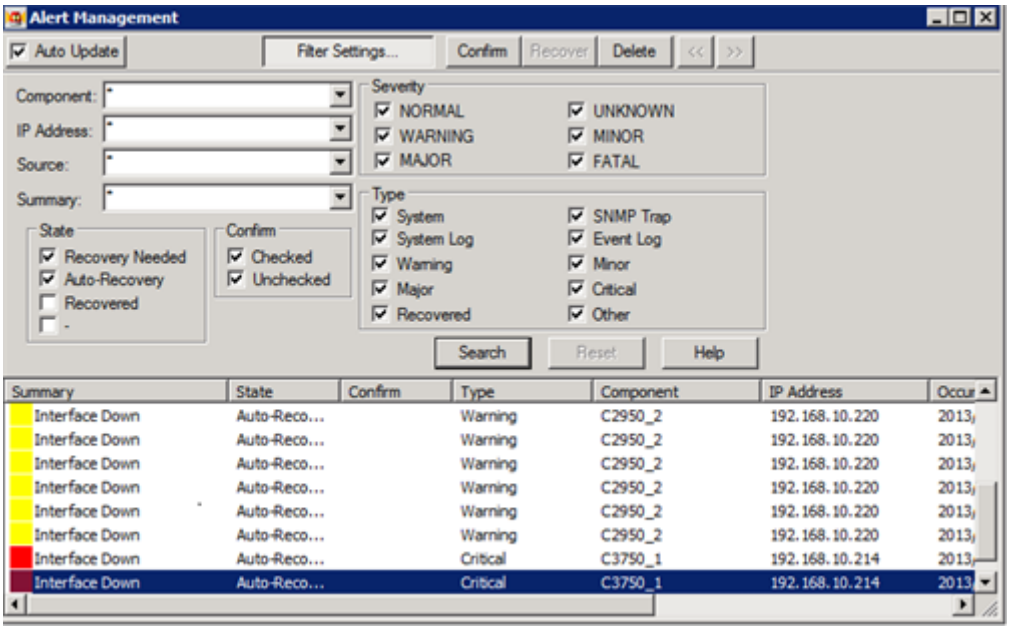
To display detailed information for an alert, double-click in the alert list. For details, refer to "5.1 Checking Alert Information (page 448)".



1.1.2.3 Alert Management window

The Alert Management window displays only those received alerts that require monitoring and resolution.

Detailed information for an alert is displayed by double-clicking the alert in the alert list. Various types of filtered displays are possible. For details, refer to "5.1.4 Managing alerts (page 456)".



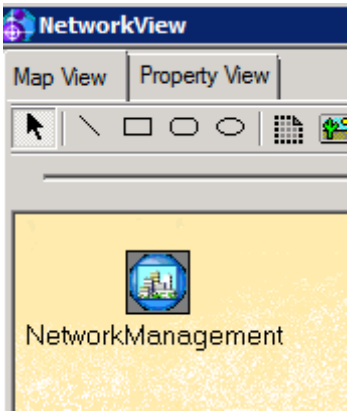
1.1.2.4 Monitoring mode

By switching monitoring mode, stop the monitoring managed devices. The functions listed below stopped when the monitoring-mode is OFF.

- State monitoring function
- SNMP traps and system logs receiving function
- Data collection function
- Configuration change monitoring function

These functions help to turn the monitoring-mode OFF and prevent the unnecessary output of alerts while the network maintenance is being performed.

In this manual, "monitoring-mode ON" indicates that monitoring is being performed and "monitoring-mode OFF" indicates that monitoring has been paused. To verify the status of the monitoring mode, check the color of the network icon. Gray is the default. For details, refer to "5.13 Starting or Stopping Monitoring by the Monitoring Mode (page 505)".

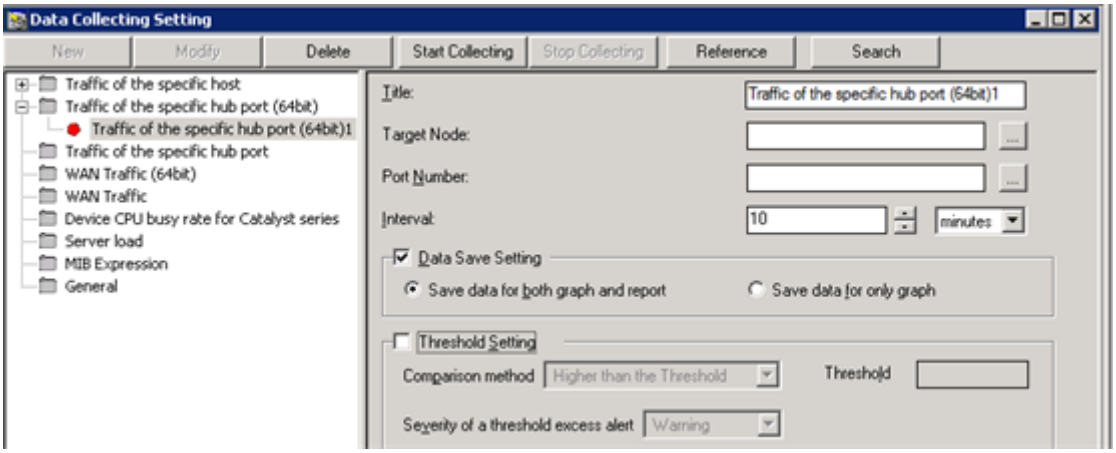


1.1.3 Performance management

1.1.3.1 Data Collecting Setting window

MIB data is periodically collected from devices being managed by Network Manager and stored. When collecting data, Network Manager can check that the data exceeds the preset threshold value. If the data is above the threshold value, an alert will be issued. Graphs can be displayed and reports can be generated on the basis of this stored data.

Collection rules for MIB data collection are set in the Data Collecting Setting. For details, refer to "4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices (page 334)".



1.1.3.2 Threshold value monitoring

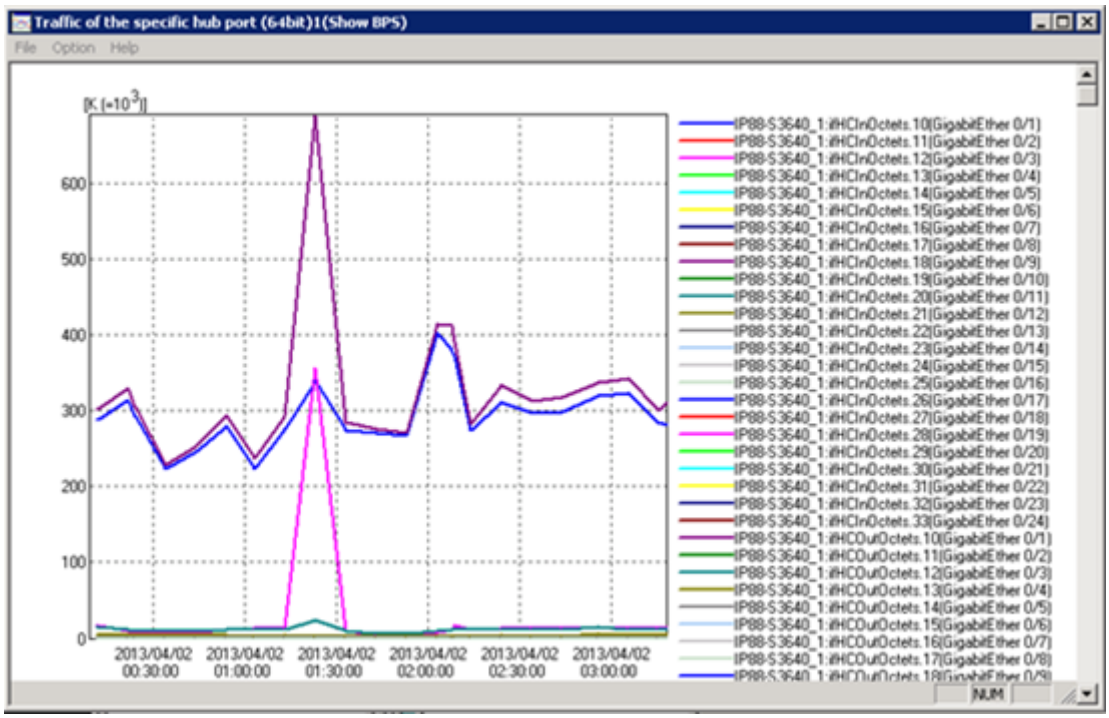
By setting the data collection settings with the monitoring threshold value in advance, the manager can check that the data exceeds the threshold value when collecting data from the managed devices.

If the obtained value is above the threshold value, the manager issues an alert for excess of the threshold value.

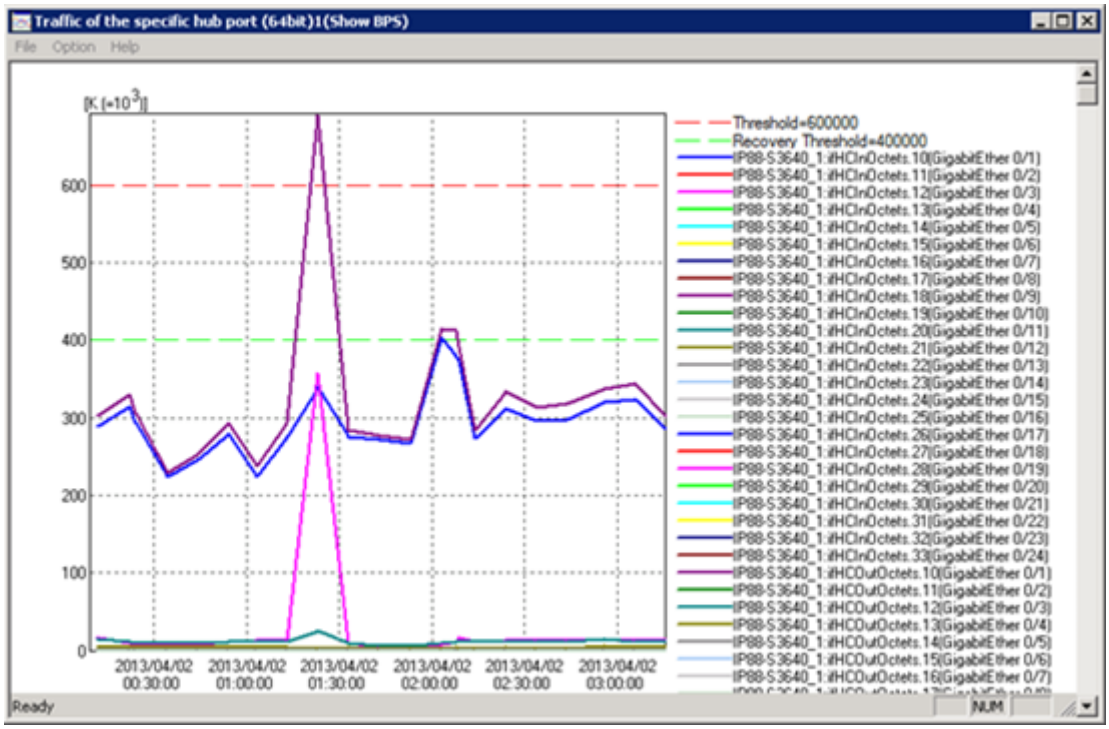
1.1.3.3 Graph display (Checking current data)

By setting the data collection settings in advance, it is possible to display a transition of data on a device on the day. For details, refer to "5.11.1 Displaying a graph (page 486)".

- When the threshold value is not set:



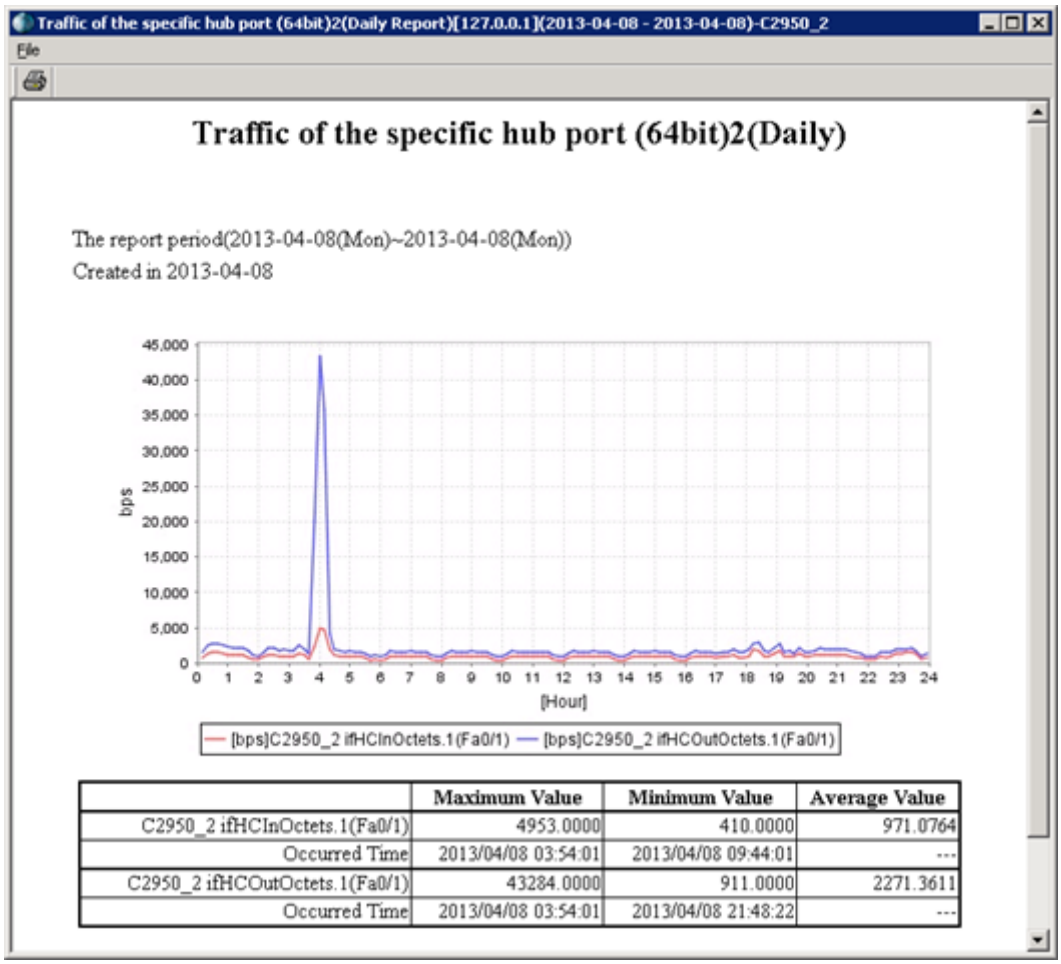
- When the threshold is set:



1.1.3.4 Report creation (Checking historical data)

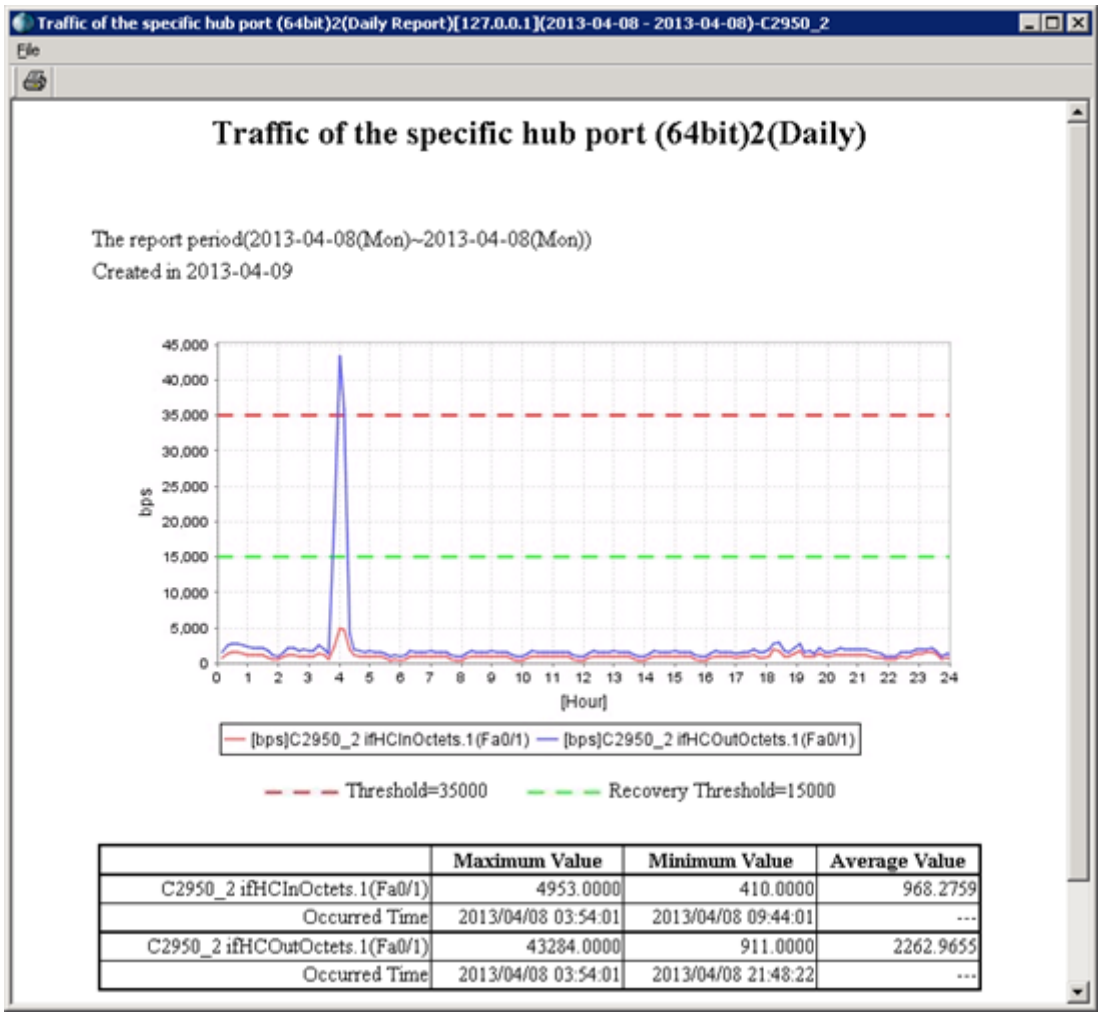
By setting the data collection settings in advance and storing collected data, it is possible to create reports for the day, week, month or year. For details, refer to "5.11.2 Creating and displaying a report (page 490)".

- When the threshold is not set:



	Maximum Value	Minimum Value	Average Value
C2950_2 ifHCInOctets.1(Fa0/1)	4953.0000	410.0000	971.0764
Occurred Time	2013/04/08 03:54:01	2013/04/08 09:44:01	---
C2950_2 ifHCOutOctets.1(Fa0/1)	43284.0000	911.0000	2271.3611
Occurred Time	2013/04/08 03:54:01	2013/04/08 21:48:22	---

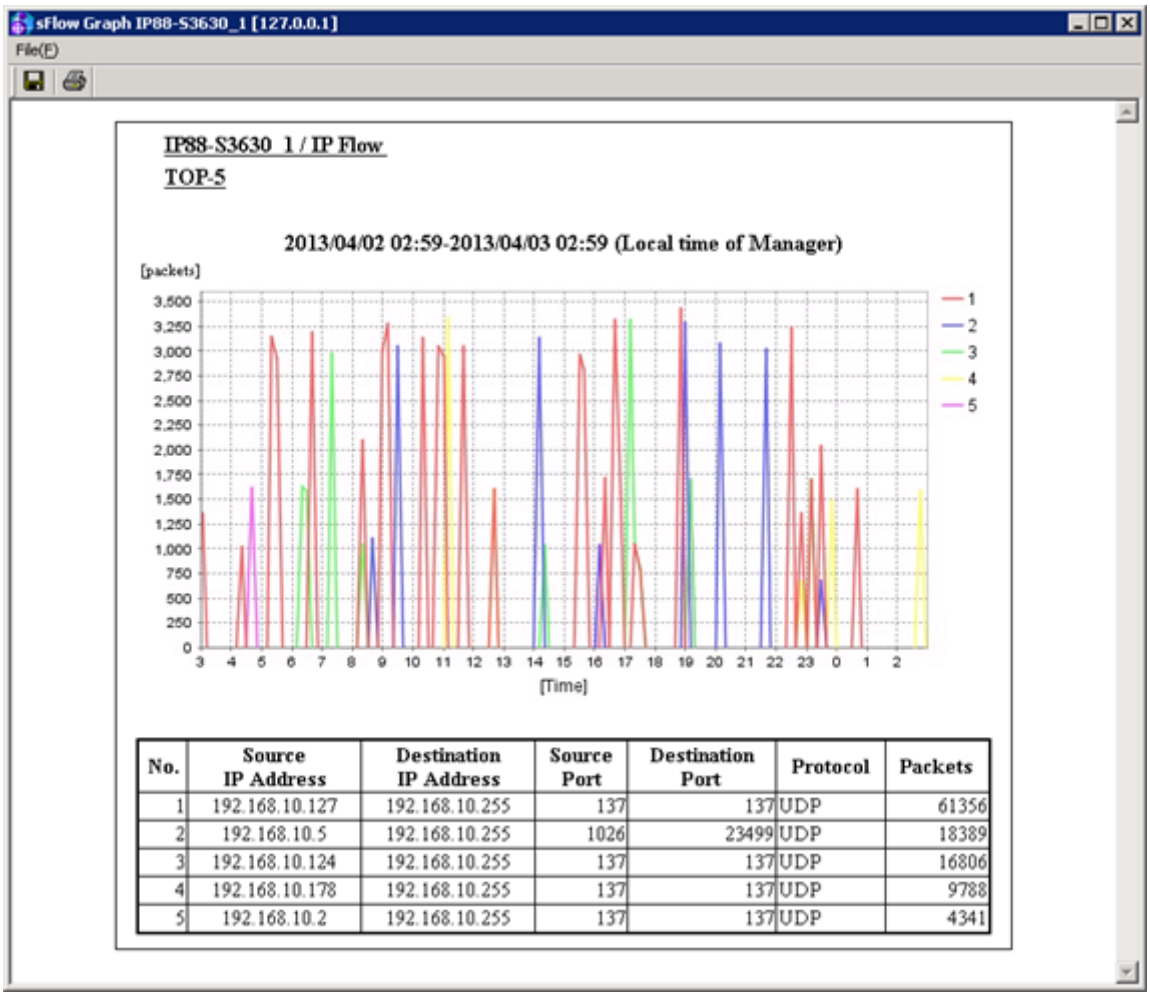
- When the threshold is set:



	Maximum Value	Minimum Value	Average Value
C2950_2 ifHCInOctets.1(Fa0/1)	4953.0000	410.0000	968.2759
Occurred Time	2013/04/08 03:54:01	2013/04/08 09:44:01	---
C2950_2 ifHCOutOctets.1(Fa0/1)	43284.0000	911.0000	2262.9655
Occurred Time	2013/04/08 03:54:01	2013/04/08 21:48:22	---

1.1.3.5 Graph display of traffic-flow information by sFlow

Collect sFlow data received from a network device (an sFlow agent) and use to analyze and graph traffic flow through the network. For details, refer to "5.12.1 Graph display of traffic-flow information from sFlow (page 500)".



No.	Source IP Address	Destination IP Address	Source Port	Destination Port	Protocol	Packets
1	192.168.10.127	192.168.10.255	137	137	UDP	61356
2	192.168.10.5	192.168.10.255	1026	23499	UDP	18389
3	192.168.10.124	192.168.10.255	137	137	UDP	16806
4	192.168.10.178	192.168.10.255	137	137	UDP	9788
5	192.168.10.2	192.168.10.255	137	137	UDP	4341

The graph displays up to 24 hours of analysis data and has many useful applications. For example, when the communication response from the server is slow, refer to the graph to check the IP addresses that are accessing the server and the volume of traffic traveling through it.

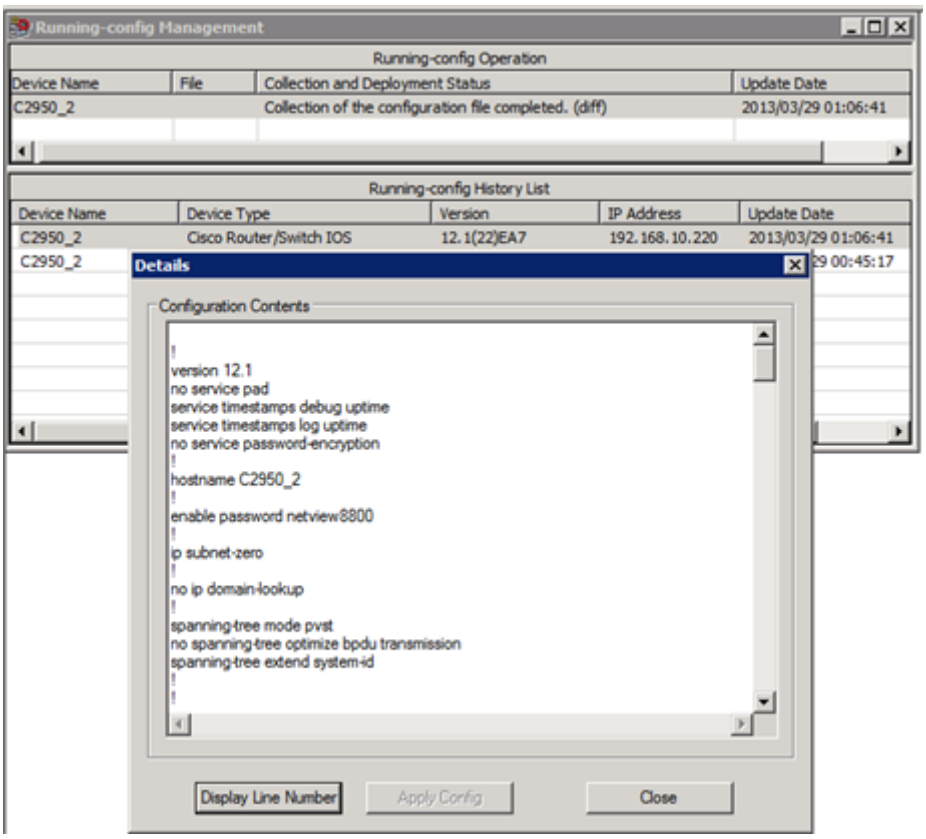
There are multiple versions of sFlow data. Network Manager supports Version 4 and 5.

Make settings on the network-device side for Version 4 or 5.

1.1.4 Resource Manager function

Configuration data and software can be distributed to network devices. For distributed configuration data and software to become effective by restarting a network device, the device can be set to restart at a specified time.

In addition, monitor the changes on configuration data for network devices, and notify the alert when detecting the changes. For details, refer to "5.14 Managing Device Configuration (Resource Manager) (page 512)".



1.1.5 Network Provisioning function

It is possible to link with the System Provisioning function of NEC SigmaSystemCenter and change the VLAN and load balancer distribution settings dynamically for network devices. (Network Provisioning)

For more information on network provisioning using this function, refer to the NEC SigmaSystemCenter manuals.

For setup to use Network Provisioning function, refer to "4.21 Linking with NEC SigmaSystemCenter (Network Provisioning) (page 415)".

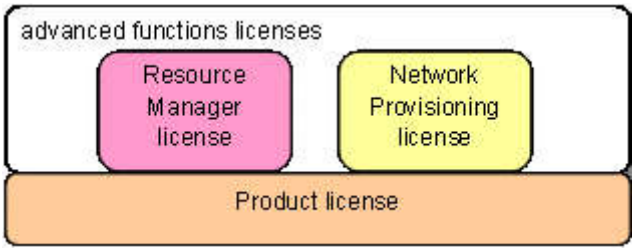
1.2 Network Manager Licenses

There are two types of Network Manager licenses: the basic license and the advanced functions license.

The basic license is required to use the basic Network Manager functions.

The advanced functions license is required to use the advanced Network Manager functions. The following two types of advanced functions licenses are available.

- Resource Manager license
- Network Provisioning license



License type	Functions provided by the license
Basic license	Configuration management (device registration, physical topology display, and panel display [1], etc.) Fault management (state monitoring, SNMP trap/system log reception, and alert display) Performance management (performance data collection, graph display, and report creation)
Resource Manager license	Device configuration collection and distribution and variance checks Device software distribution.
Network Provisioning license	Configuration of VLAN and load distribution settings linked with NEC SigmaSystemCenter.

1) The basic license allows for display of the panels of up to five devices. The Network Manager Node Manager unlimited license is required to display the panels of six or more devices.

Each license is valid after registering in the License Management window. For instructions on how to register, refer to "10.3 Registering Licenses (page 759)".

For each license (excluding the Network Provisioning license), there is a set number of devices available for monitoring. To use the functions included with each license, assign a license to each device in Network Manager.

When registering a monitored device in Network Manager, a "basic license" is automatically assigned. When deleting a device, the license is automatically canceled. For devices that use the panel display, assign a license from the NetMgr License Manager dialog box. This is the same method as the "advanced function licenses".

For the advanced functions license (excluding the Network Provisioning License), it is necessary to clearly specify which license type should be assigned (or canceled) for which device in the NetMgr License Manager dialog box. Functions provided by the advanced functions license can only be used for a device if an advanced functions license has been assigned to that device. For assigning the advanced functions licenses, refer to "4.4 Managing the Advanced Functions License (page 201)".

There is no need to assign a Network Provisioning license to each device.

In this manual, the license required for panel display (Node Manager function) is referred to as the "NM license", the Resource Manager License is referred to as the "RM license", and the Network Provisioning license is referred to as the "NP license".

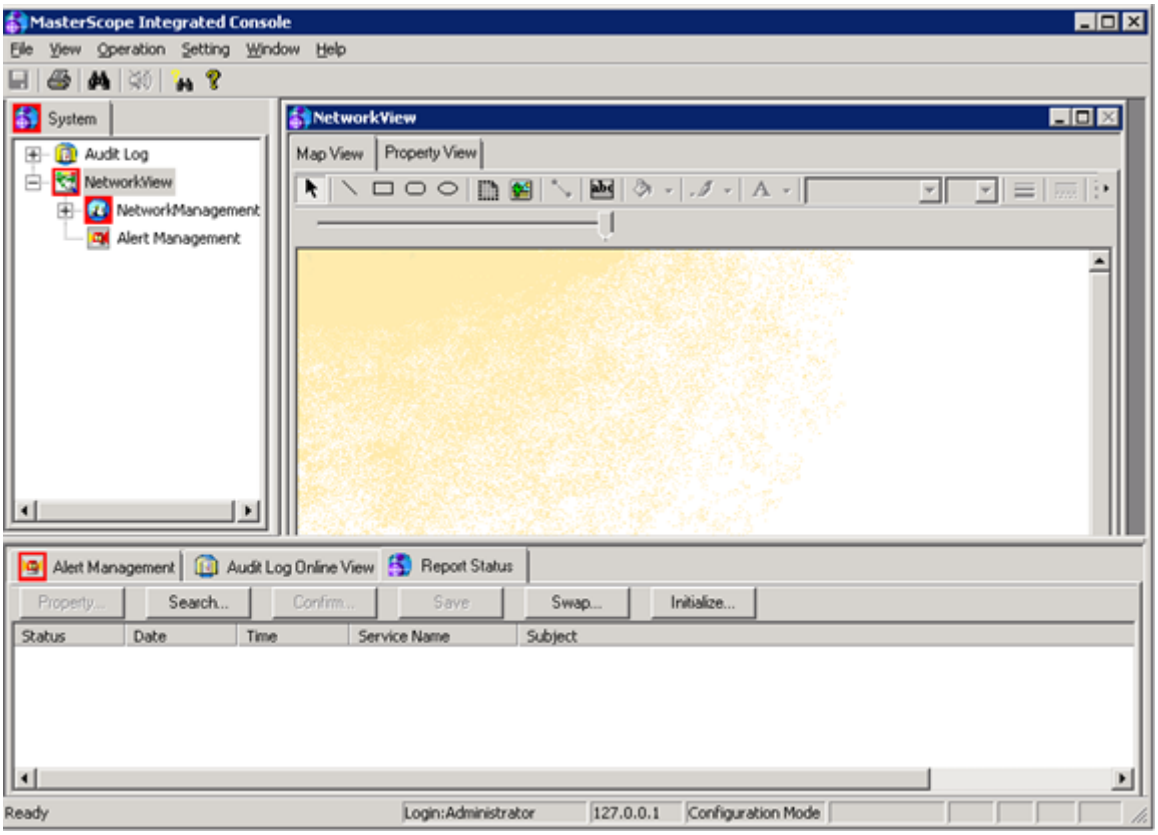
Chapter 2.
Overview of the Monitoring Window

Contents

2.1 Structure of the Monitoring Window 15
2.2 Web Monitoring View Function 19
2.3 Web Console 22
2.4 User Access Rights 26
2.5 Operation Modes 27

2.1 Structure of the Monitoring Window

The following section describes the monitoring window.



- Tree View
  - **NetworkView** icon

    Displays alerts and the network devices being managed by NetworkView window. For details, refer to "2.1.1 Network View (page 16)".
  - **Audit Log** icon

    Displays the Network Manager operations log by Audit Log window.

    Directly below the **Audit Log** icon, four operation categories are displayed: Applications, Security, System, and Audit Log. For details, refer to "5.16 Managing Audit Logs (page 551)".

    The Audit Log window is displayed only if the user that is logged on belongs to a group with "Audit trail reference authority". For details, refer to "4.1.3.1 Group authority settings (page 113)".
- NetworkView window
  - Map View

    Displays the registered device icons, map icons, connection lines and diagrams for the icons selected in the tree view. For details, refer to "2.1.2 Map View (page 17)".
  - Property View

    Displays the properties of registered device icons and map icons for icons selected in the tree view.

- Pane below the monitoring window
  - Alert Management tab

    Displays a list of alerts that occur after the monitoring window is opened. For details, refer to "5.1.3 Referencing the new alert list (page 449)".
  - Audit Log Online View tab

    Displays a list of operation details and results for operations and automated processes performed in the monitoring window or manager functions. For details, refer to "5.16 Managing Audit Logs (page 551)".

    The Audit Log Online View tab is displayed only if the user that is logged on belongs to a group with "Audit trail reference authority". For details, refer to "4.1.3.1 Group authority settings (page 113)".
  - Report Status tab

    After opening the monitoring window, if alerts occur that have a report specification, a list is displayed that shows the status of report processing. For details of the report function, refer to "5.4 Managing Alert Report Status (page 463)".

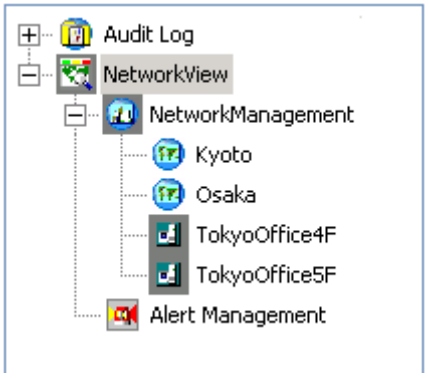
Tip

If an access key is displayed for a menu or button, you can access these controls (menu, button) by pressing ALT + access key.

For example, you can open the **File** menu by pressing ALT + F key.

The shortcut access to the controls using CTRL key is not supported.

2.1.1 Network View



- **NetworkView** icon

  Network Manager root icon.

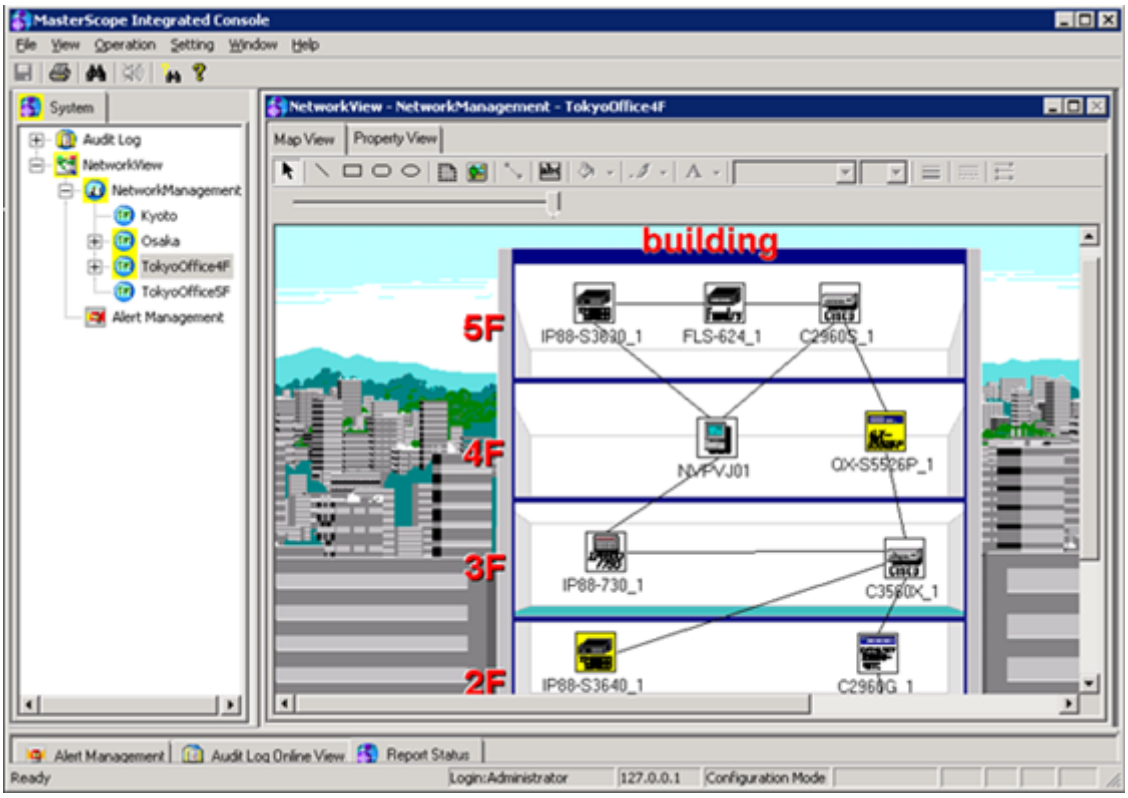
  The **Alert Management** icon and **NetworkManagement** icon are displayed below the **NetworkView** icon.
  - **NetworkManagement** icon

    Device and map icons are displayed below this icon. To access functions, right-click on each icon and select a function from the menu.

- **Alert Management** icon

  By double-clicking the icon, the Alert Management window which manages an alert will appear. For details of the Alert Management window, refer to "5.1.4 Managing alerts (page 456)".

2.1.2 Map View



The **NetworkManagement** icon's Map view (including the subordinate maps), is a basic Network Manager window.

In this view, display the network system configuration and manage the state of each device graphically by laying out the "map" icons showing networks and buildings, and "node" icons showing the monitoring of devices.

2.1.2.1 Icon colors

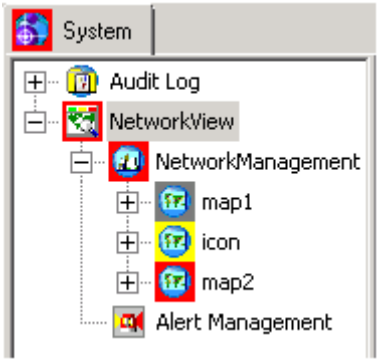
Each icon shows its fault status (degree of importance) in each color. Color of each icon indicates the fault status (degree of importance) and shows which alerts have the highest priority/severity level.

Network Manager shows the degree of importance as described below.

Default Name (Status)	Degree of Importance	Default color	Default priority
FATAL	FATAL	(Red)	Highest
MAJOR	MAJOR	(Yellow)	
MINOR	MINOR	(Yellow)	

Default Name (Status)	Degree of Importance	Default color	Default priority
WARNING	WARNING	(Yellow)	
UNKNOWN	UNKNOWN	(Gray)	
UNMANAGED (Monitoring-mode OFF)	UNMANAGED	(Gray)	
NORMAL	NORMAL	(White)	Lowest

If alerts occur on multiple devices under a map icon, the color of the map icon is same as the color of the highest priority alert in the devices under the map, and the color is also propagated to the parent map.



In the window shown above, for example, the event occurring in the "map2" node (FATAL, color-coded red) has higher priority than the "map1" node (UNMANAGED, monitoring mode OFF, color-coded gray), thus the "NetworkManagement" node, one level higher in the hierarchy, is displayed as FATAL severity level (color-coded red).

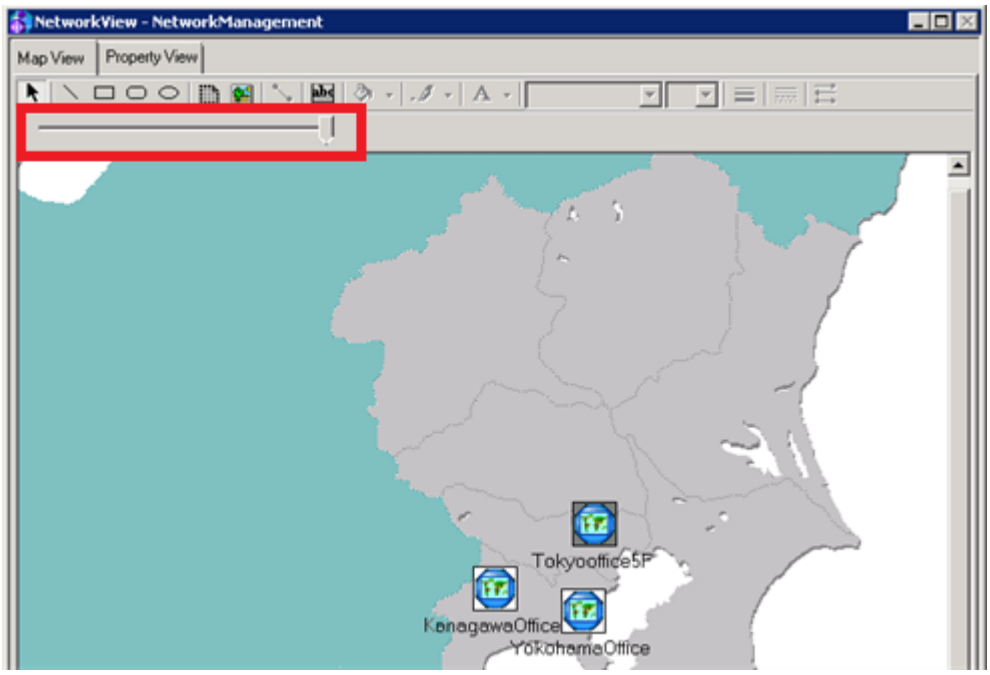
Tip

1. To change the display name, display color, and priority of each severity level. For details, refer to "4.9.2 About alert severity and priority (page 237)".
2. When configuring extended modes, use the "MAJOR" and "MINOR" severity levels. For details, refer to "4.9.2.1 About severity extension (page 237)", "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

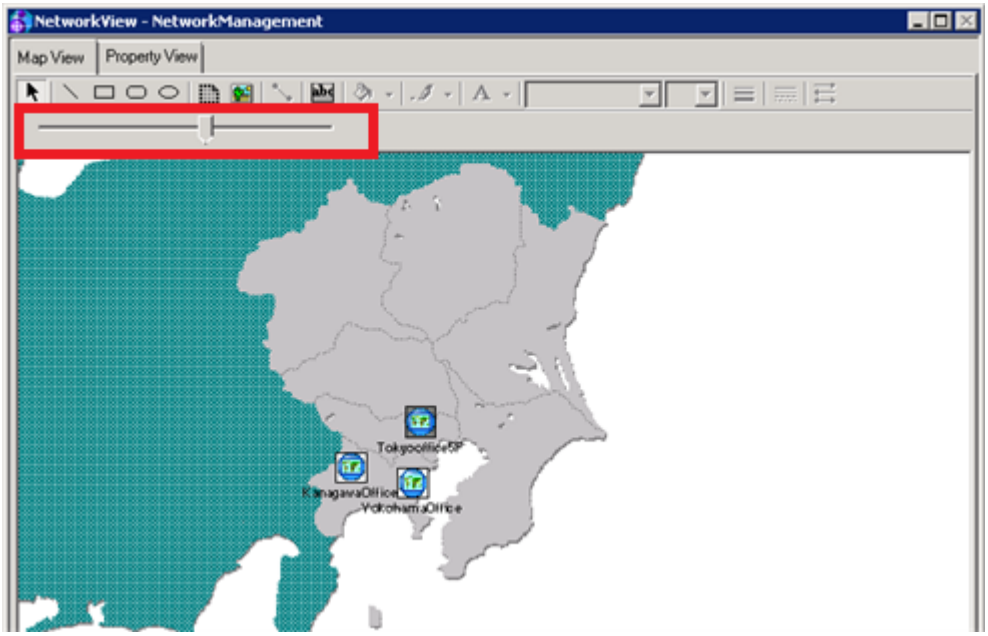
2.1.2.2 Zooming in and out in Map View

In the Map View, zoom out by sliding the slider to the left, and zoom in by sliding to the right.

- Zoom in:



- Zoom out:



2.1.3 Property View

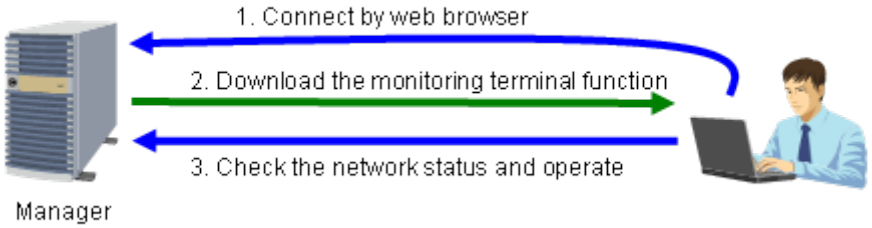
The properties view displays the attributes for the selected node.

To change the attributes of nodes under the **NetworkManagement** icon, select **Properties** menu from each icon and go to the Properties dialog box.

For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

2.2 Web Monitoring View Function

Check the Network Manager monitoring status and change settings from a web browser, in addition to an installed monitoring terminal.



There are some restrictions on the commands that are available in a web browser (web monitoring view). For details regarding web monitoring view restrictions, refer to "2.2.1 Precautions and limitations in the web monitoring view (page 20)".

Tip

This function is provided to ensure compatibility with previous versions. when using Web browser, it is recommend to use Web Console provided by IMS component.

For details of Web Console, refer to "MasterScope Network Management Web Console Reference Manual".

2.2.1 Precautions and limitations in the web monitoring view

The precautions and limitations to consider when using the web monitoring view are shown below.

1. This function is supported in Internet Explorer 11 (32bit version).
2. At least one monitoring terminal used for configuring settings is required to use the web monitoring view.
3. To use the web monitoring view, you must run the Internet Explorer as an administrator.
4. Some Network Manager functions are unavailable in the web monitoring view. For details, refer to "Chapter 6. Menu Reference (page 559)".
5. When you open the web monitoring view at the first time, a message prompting you to restart the computer may be displayed. If a Restart window is displayed, select **Yes** button to restart.
6. Changing the window size of the web monitoring view may freeze up.

   To avoid this problem, configure the following settings.

   Procedure:

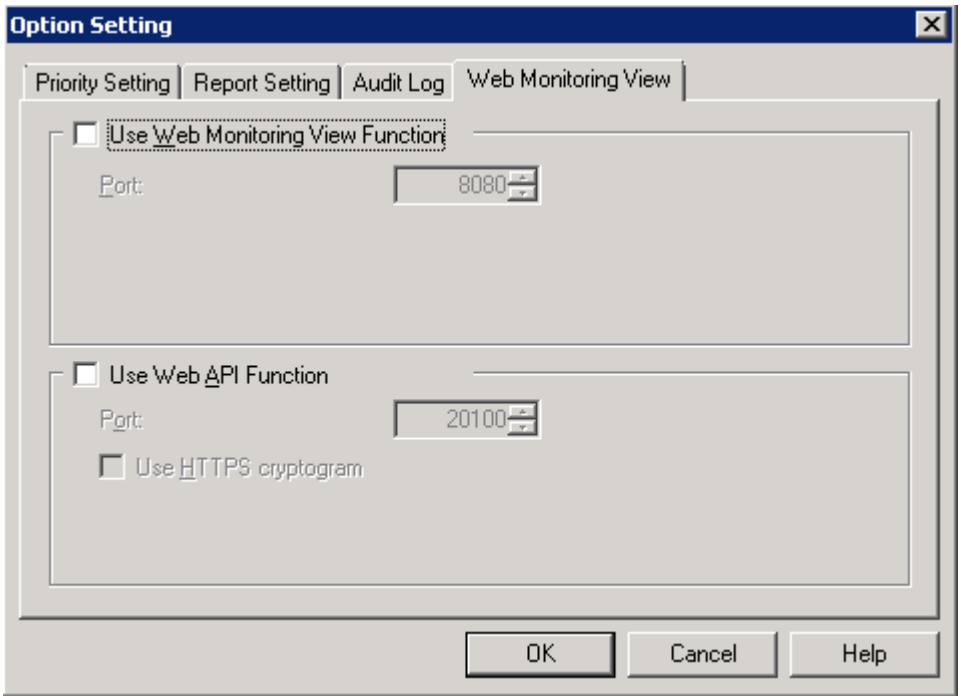
   a. Open the Control Panel window and search "Administrative Tools".
   b. In the Administrative Tools window, open the **Services**.
   c. In the Service window, stop **Themes** service.

2.2.2 To use the web monitoring view (Manager)

WTo use the web monitoring view, configure the following settings in advance, from the monitoring terminal:

1. Open the Option Setting dialog box.

   In the main menu, select **Setting**>**Option**, display the **Web Monitoring View** tab.



2. Check the **Use Web Monitoring View Function** checkbox. By default, this item is not checked.
3. In **Port Number**, specify a port number for the web monitoring view function. The available range is from 1,000 to 32,767.

2.2.3 Configuring OS settings for the web monitoring view

To use the web monitoring view, configure the OS setting of the monitoring terminal machine.

1. Configure the security setting of the Internet Explorer.
   a. From the menu of the Internet Explorer, select **Tools**>**Internet Options**.
   b. Select **Security** tab. Set the Internet Explorer security settings level for the manager machine zone, from the perspective of the monitoring terminal machine, to **Medium-Low**.
   c. In the Internet Options window, click **OK**button.
2. Configure the firewall settings.

   The web monitoring view uses the port to connect to the manager in addition to the ports used by the Windows monitoring terminal. Configure the firewall settings to enable your web browser to communicate with the manager through the port number specified under the options in the **Web Monitoring View** tab.

   For details regarding **Web Monitoring View** tab, refer to "2.2.2 To use the web monitoring view (Manager) (page 20)".
3. Configure your environment settings so that the "Self hostname" value specified during the installation of a manager can be successfully resolved by the terminal that the web monitoring view is being opened on.

   To resolve names, you may use FQDN-based DNS lookup, entries in the Hosts file, or IP address resolution.
4. Configure the Compatibility View settings of the Internet Explorer.

a. From the menu of the Internet Explorer, select **Tools**>**Compatibility View settings**.

b. In the **Compatibility View settings** dialog box, enter a URL of the web monitoring view in the **Add this website**.

For details of a URL of the web monitoring view, refer to "2.2.4 Starting the monitoring view (page 22)".

5. When using a web monitoring view on Windows 8.1 (x64), configure Internet Explorer settings to run it in 32 bit mode.

a. From the menu of the Internet Explorer, select **Tools**>**Internet options**.

b. On the **Advanced** tab under Internet Options, deselect **Enable 64-bit processes for Enhanced Protected Mode**.

c. In the Internet Options window, click **OK** button.

2.2.4 Starting the monitoring view

Start the web monitoring view.

1. Start Internet Explorer as the Administrator user.

- Right-click the Internet Explorer icon, and select **Run as administrator** to start Internet Explorer.

2. Access the following URL from the web browser.

http://*MANAGER*:*PORT*

MANAGER :

The host name or IP address for the manager.

PORT :

Port value set in the **Web Monitoring View** tab of the Option Setting dialog box.

For details, refer to "2.2.2 To use the web monitoring view (Manager) (page 20)".

When connecting to the manager, the same splash screen as the normal monitoring view appears. After preparing view is completed, the web monitoring view starts.

Tip

Since the popup relating to installation of the ActiveX control may appear in starting of the web monitoring view for the first time, in that case, select "Install".

When staring the web monitoring view for the first time, it may take several minutes to download files. You may also be asked to restart OS, depending on the environment setting.

3. Enter **Login name** and **Password** in the Login dialog box.
4. Click **OK** button.

2.3 Web Console

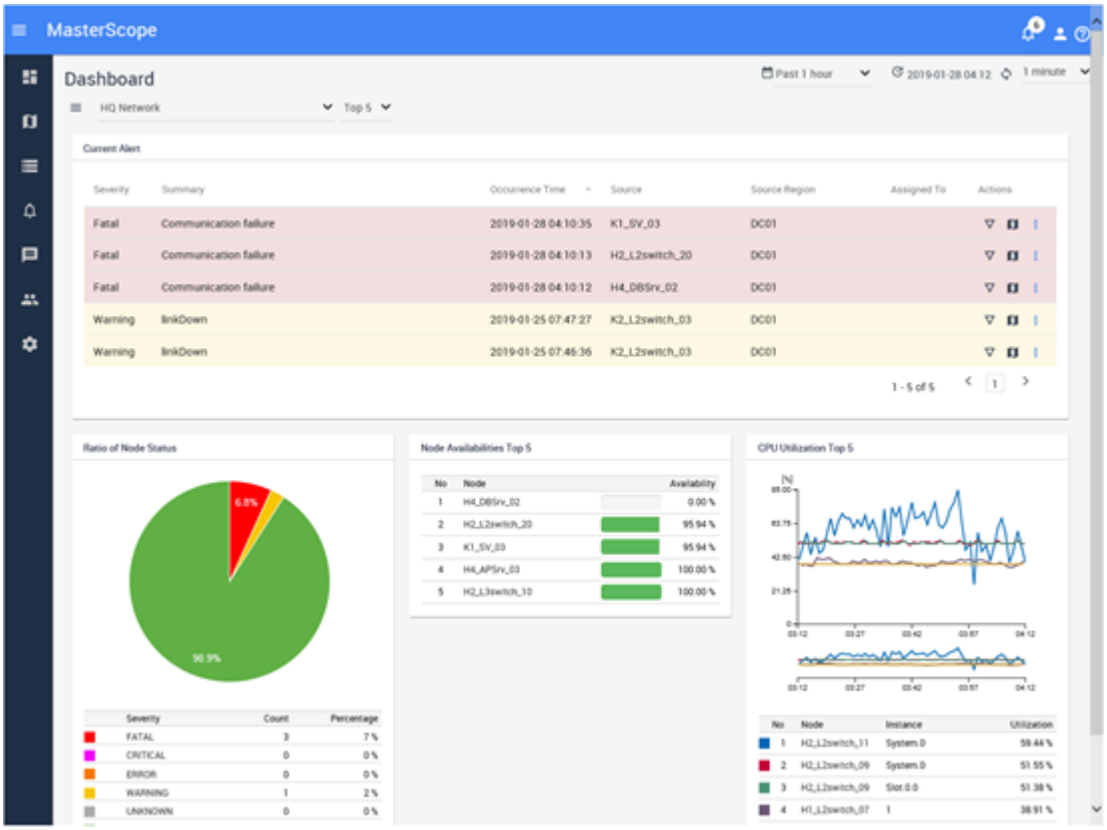
Web Console provided by the IMS component allows users to perform remote operations via a web browser. When a system consists of multiple Network Manager instances, Web Console enables information from Network Manager to be viewed at once.

When NFA is installed, flow information (sFlow, NetFlow, and IPFIX) collected by NFA can also be viewed, enabling the network status to be managed from various viewpoints.

Web Console provides the following operations.

- Dashboard View

  MIB information collected by the data collection function is displayed according to the rank (TopN format) of each item. You can also check the current alerts, the utilization of each node, and the flow information collected by NFA on the dashboard.



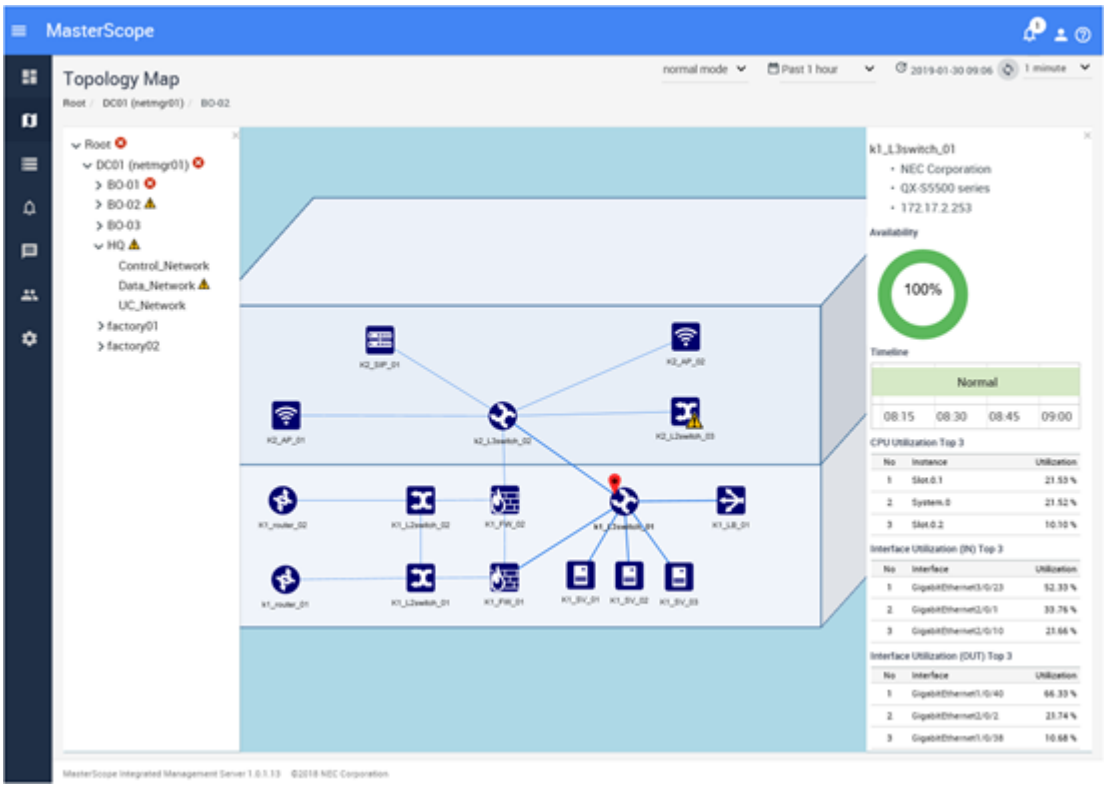
Tip

The dashboard can display the following information collected by the data collection function.

- Bandwidth utilization for input and output interfaces
- Packet loss rate for inbound and outbound packets
- Packet error rate for inbound and outbound packets
- CPU utilization
- Memory utilization

- Displaying a Network Configuration Map (Topology Map)

  Web Console displays a network configuration map based on the map and node information registered under **Map Management**. The network configuration map of Web Console enables users to check the relationship between nodes and the current failure occurrence status.

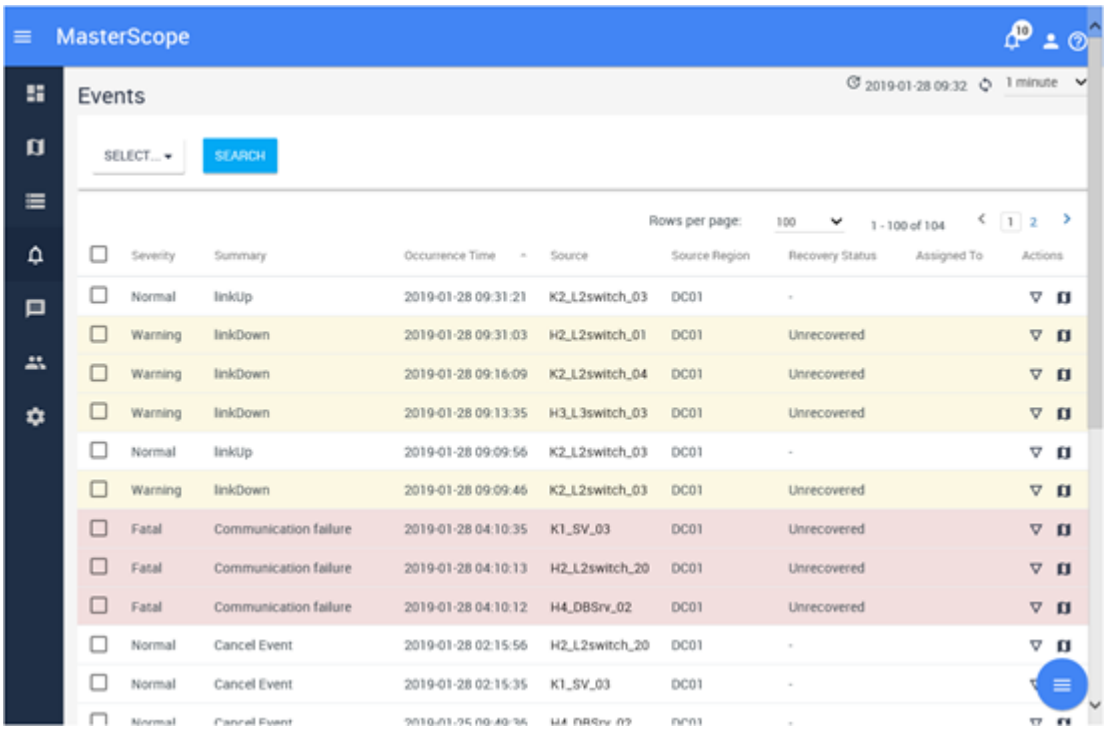


Tip

When displaying a network configuration map, Web Console uses the map configuration, node property information, and connections between nodes under **Map Management**, but does not use the background image and node position. To insert the background image and change the node position, it is necessary to edit the Web Console network map.

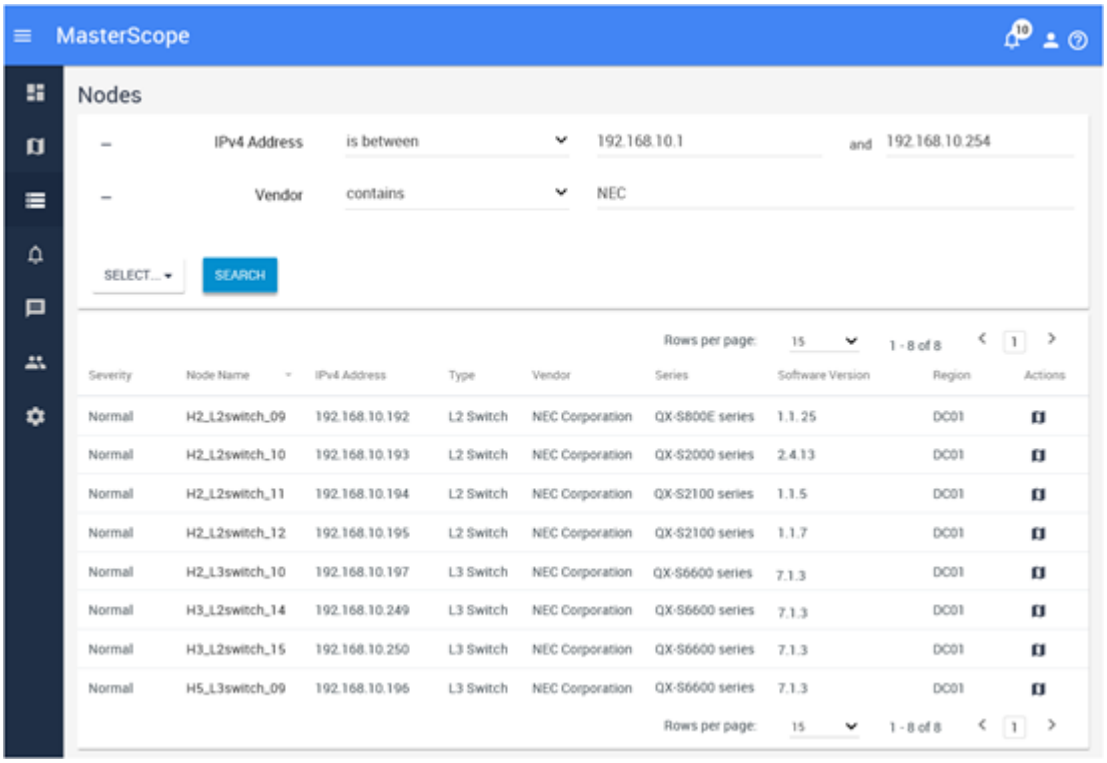
- Displaying Alert (Event) Information

  You can check all alerts detected by Network Manager on Web Console. In addition, you can recover manual recovery alerts.



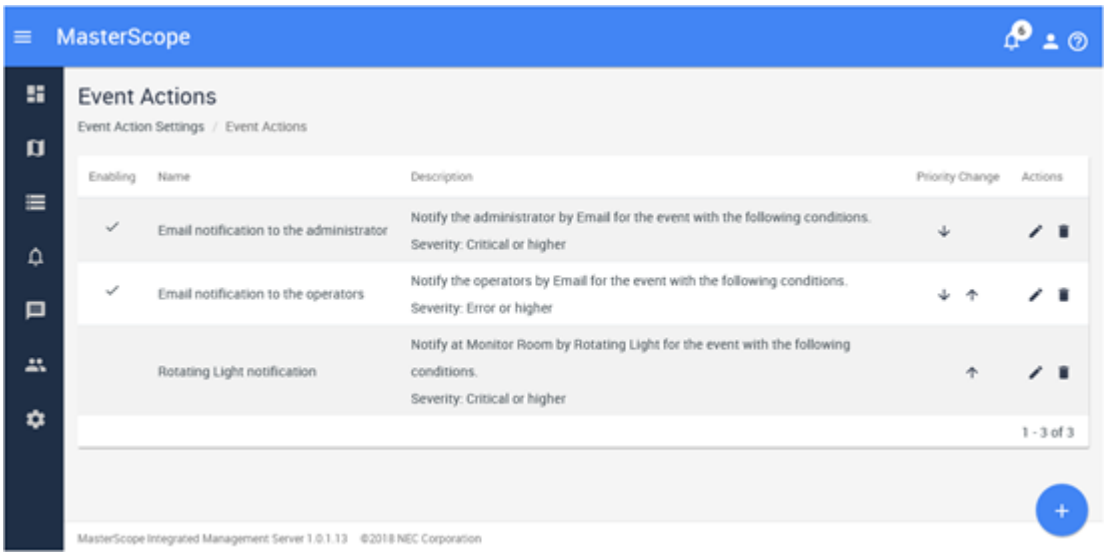
- Displaying the Property Information of nodes and interfaces

  You can search and check property information of all managed nodes and interfaces.



- Alert Notification Settings

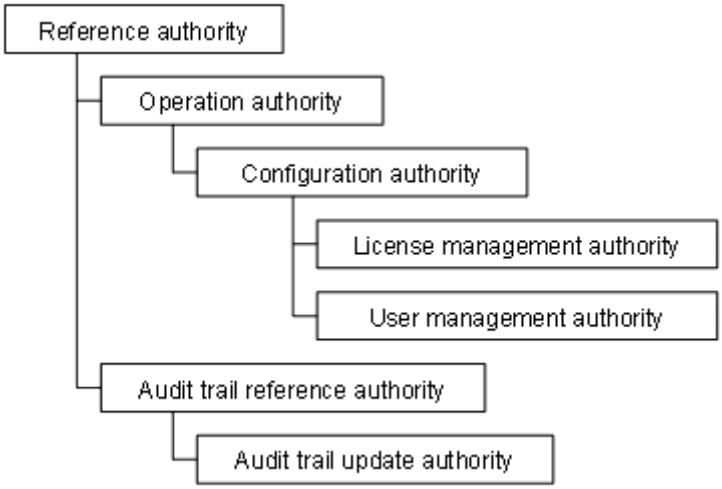
  Alerts detected by Network Manager and NFA can be notified using the same policy.



2.4 User Access Rights

Users of Network Manager belong to a group. Access to the system is based on the access rights assigned to a group. To manage multiple different levels of user access, create multiple groups with different access rights and allocate each user to the appropriate group.

The following displays the relationship between the access rights assigned to a group.



All groups are assigned "reference authority" and are able to view the Map View, Property View, operate the menus, and reference a range of other information, as well as operate the Alert Management window.

If assigned "operation authority", users can operate functions used to access devices, such as **Ping** menu and **Remote Login** menus.

If assigned both "operation authority" and "configuration authority", users can switch to "Configuration Mode" and configure the monitoring environment for Network Manager. Under "configuration authority," you can also assign "license management authority" for registering and deleting licenses, and "user management authority" for registering users and groups. For information regarding "configuration mode," refer to "2.5 Operation Modes (page 27)".

When a user is assigned "audit trail reference authority", the **Audit Log** icon in the tree view and **Audit Log Online View** tab are displayed, and the user can view the audit log. To allow users to

perform management tasks such as audit log maintenance, assign them "audit trail update authority". Before commencing operations, create a plan that outlines the access rights that are assigned to each user (the group to which they will be assigned). For instructions on creating users and groups, refer to "4.1 Managing Users and Groups (page 101)".

Tip

1. For information on the menus to access under each access right, refer to "Chapter 6. Menu Reference (page 559)".
2. When logging in to Network Manager as a user not assigned to a group, the scope of what can be viewed is restricted. You can view Map View, Property View and Alert Management, but you cannot operate the icon menus.

2.5 Operation Modes

The monitoring window has two different modes, normal mode and configuration mode. When the window is opened, it is in normal mode.

- Configuration mode

  This is a special mode for changing the system monitoring definitions. A user can switch to configuration mode in the system if they are in a monitoring window and logged on as a user with "configuration authority". This can only be done in one monitoring window at one time.

- Normal mode

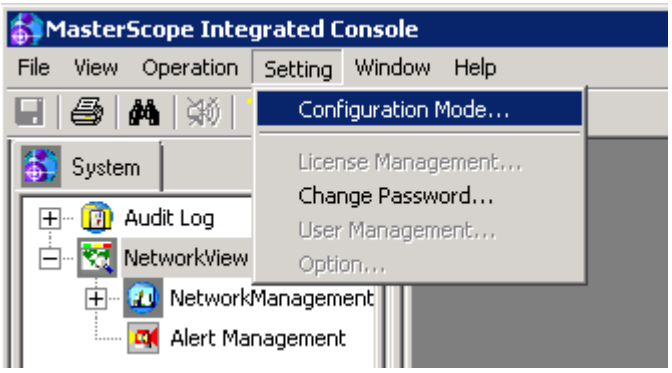
  This is the default operation mode after starting that allows you to view the system status and carry out operating instructions.

To change the operation mode, refer to "2.5.1 Changing operation modes (page 27)".

For "configuration authority", refer to "4.1.3.1 Group authority settings (page 113)".

2.5.1 Changing operation modes

1. On the main menu, select **Setting**>**Configuration Mode**.



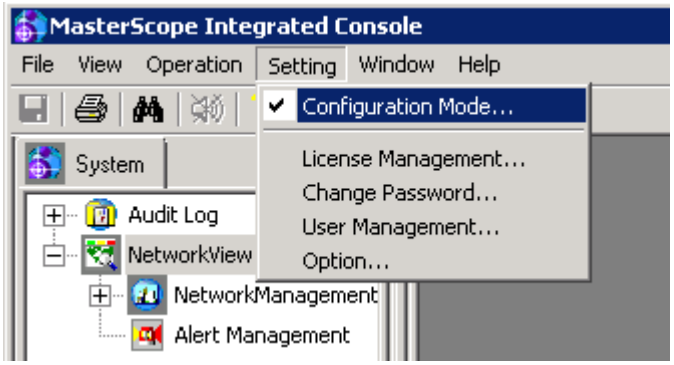
2.5.2 Checking the operation mode

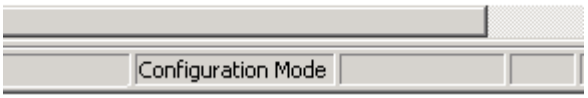
1. Check the main menu **Setting**>**Configuration Mode** and the bottom right corner of the window.
   - In the configuration mode:

A check mark to the left of **Setting**>**Configuration Mode** menu indicates currently operating in the configuration mode. "Configuration Mode" is displayed in the bottom right corner of the window.

- In the normal mode:

  No check mark to the left of **Setting**>**Configuration Mode** menu indicates currently operating in the normal mode. Nothing displayed in the bottom right corner of the window.





Chapter 3. Basic Operations (Tutorials)

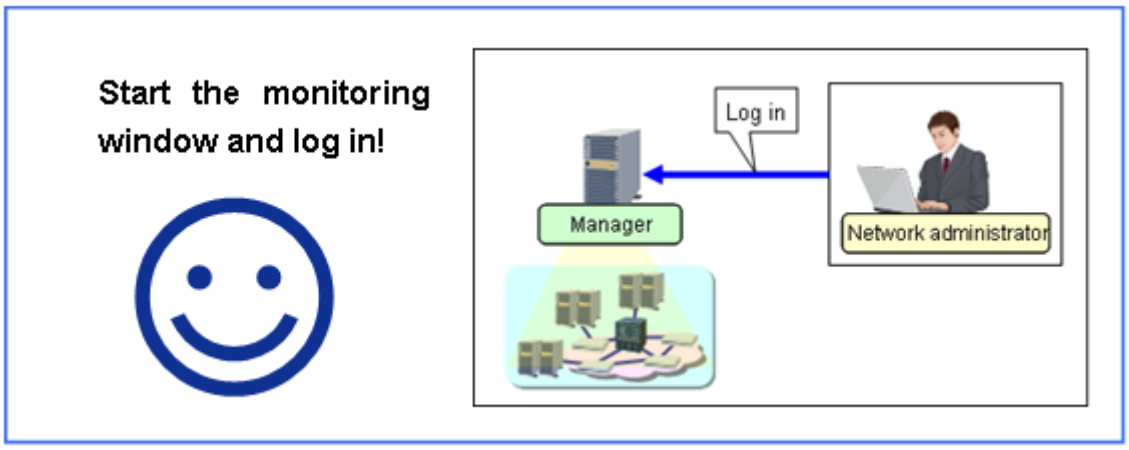
Contents

3.1 Before Operating Network Manager 30
3.2 Configuration: Registering Information for Managed Devices 33
3.3 Configuration: Configuring Monitoring Settings 44
3.4 Configuration: Collecting Performance Information 68
3.5 Operations: Managing Faults 74
3.6 Operations: Checking Performance Information 81
3.7 Operations: Accessing Managed Devices 86
3.8 Operations: Maintaining Managed Devices 91

3.1 Before Operating Network Manager

3.1.1 Starting the monitoring window

In Network Manager, run the monitoring terminal to configure and view the network management information stored on the manager function. This section describes how to start the monitoring terminal and how to log in to the monitoring terminal for the first time.



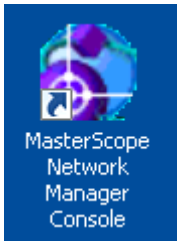
Confirm that the environment you are working in meets the conditions below.

- The monitoring terminal function has been installed.
- The user that has logged in to Windows has administrator privileges.

Tip

If Network Manager will be operated by multiple administrators, create a new user.

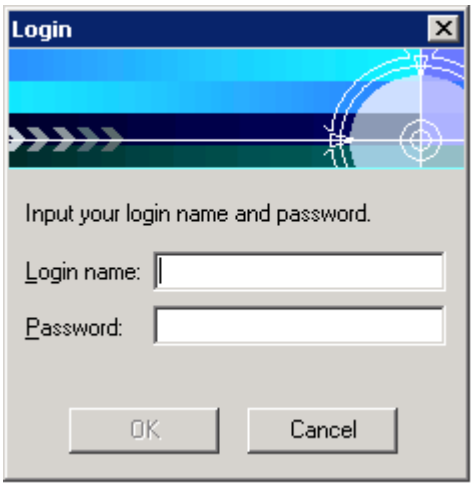
1. Start the monitoring window in one of the following ways.
   - Double-click the **MasterScope Network Manager Console** icon located on the desktop.

   - Start from Windows **Start** menu or Start screen.

     Select **MasterScope Network Manager**>**MasterScope Network Manager Console** menu.

   The Login dialog box is opened.
2. Enter the login information.



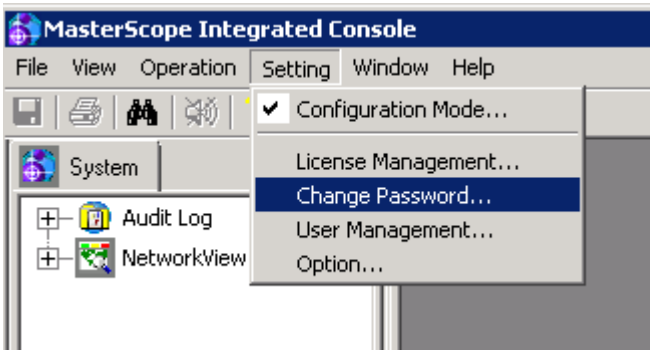
Initial setup is performed for the following user. When you start the console for the first time, enter this information.

- **Login name** : Administrator
- **Password** : websam

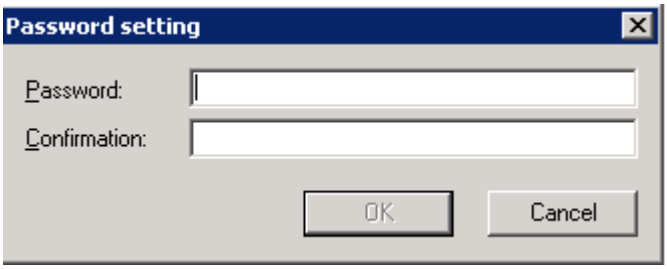
For information regarding the logged in user, refer to "4.1 Managing Users and Groups (page 101)".

When logging in for the first time, always change the user password for the Network Manager administrator.

1. On the main menu, select **Setting**>**Change Password**.



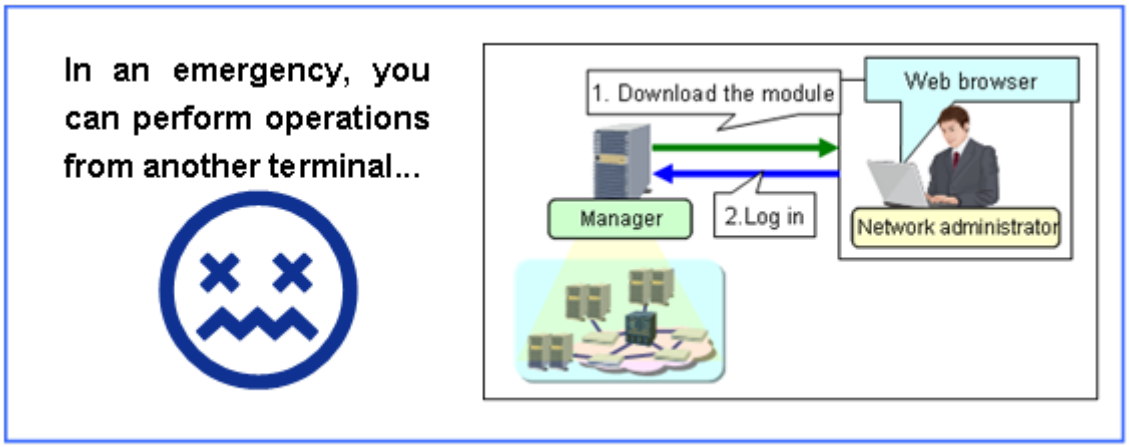
2. Enter a new password.



3. Click **OK** button.

3.1.2 Starting the web monitoring view

In Network Manager, even if you are on a terminal not installed with the monitoring terminal, you can perform operations such as viewing network management information by using a Web browser to download the monitoring terminal function.



Caution

In the web monitoring view, user's operating range is limited. For operational range of the web monitoring view, refer to "Chapter 6. Menu Reference (page 559)".

The **Web Monitoring View** tab needs to be set up from the Option Setting dialog box first. The **Port** value that was set at that time is used when starting the view. For details, refer to "2.2.2 To use the web monitoring view (Manager) (page 20)".

You also need to configure the OS settings before starting the web monitoring view. For instructions, refer to "2.2.3 Configuring OS settings for the web monitoring view (page 21)".

Confirm that the environment that you are starting and operating the web monitoring view in meets the conditions below.

- Internet Explorer 11 (32bit) can be used on the terminal that you are starting the web monitoring view on.
- You must run the Internet Explorer as an administrator.

1. Start Internet Explorer as the Administrator user.
   - Right-click the Internet Explorer icon, and select **Run as administrator** to start Internet Explorer.
2. Specify the following URL.

   http://*MANAGER*:*PORT*

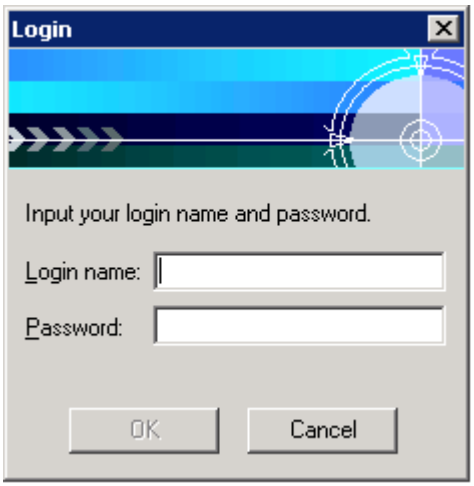
   MANAGER :

   The host name for the manager (or IP address)

   PORT :

   Port value set in the **Web Monitoring View** tab of the Option Setting dialog box.

   For details, refer to "2.2.2 To use the web monitoring view (Manager) (page 20)".
3. Enter **Login name** and **Password** in the Login dialog box.



4. Click **OK** button.

The web monitoring view starts.

3.2 Configuration: Registering Information for Managed Devices

To begin operating the system, you will first need to register information for the devices that are going to be monitored. Use one of the following three procedures to register device information. Select the method that is appropriate for your operating environment from these 3 methods.

Registration method	Usage Conditions	Usage Case
Autodiscover	• The manager is able to communicate with the devices to be monitored. • The operating mode is set to the "configuration mode (page 27)".	• A relatively small number of devices will be registered (less than 100). • The IP addresses of the devices to be registered are consecutive or the address range is clear.
Manual register	• The operating mode is set to the "configuration mode (page 27)".	• A small number of devices will be registered (less than 10). • The devices that you plan to connect to the network are registered in advance.
Batch register	• The operating mode is set to the "configuration mode (page 27)".	• A very large number of devices will be registered (100 or more). • The devices that you plan to connect to the network are registered in advance.

3.2.1 Automatically detecting managed devices

If it is possible to communicate with devices registered in Network Manager and there are a relatively small number of devices, you can register information for monitored devices using Autodiscover. This section describes the basic operations for Autodiscover registration.

Tip

For details, refer to "4.2.1.1 Performing autodiscover (TCP/IP Hosts) (page 127)".

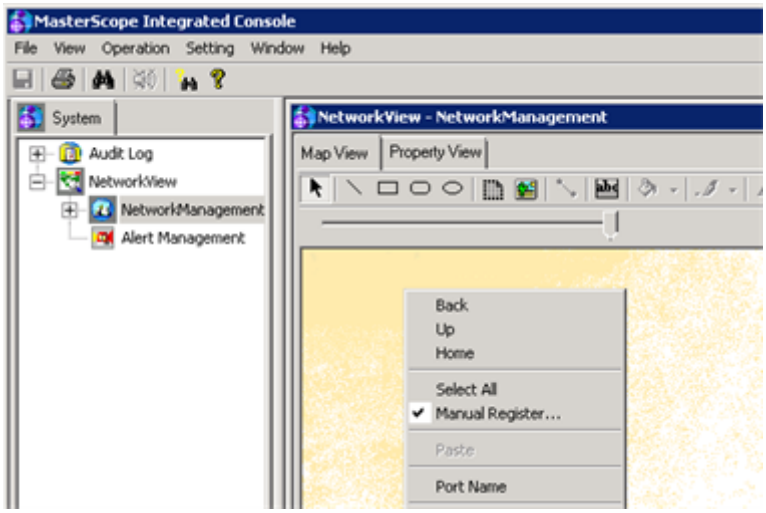
Confirm that the environment you are working in meets the conditions below.

- You can connect the manager to the network and establish communication with the devices to be monitored.

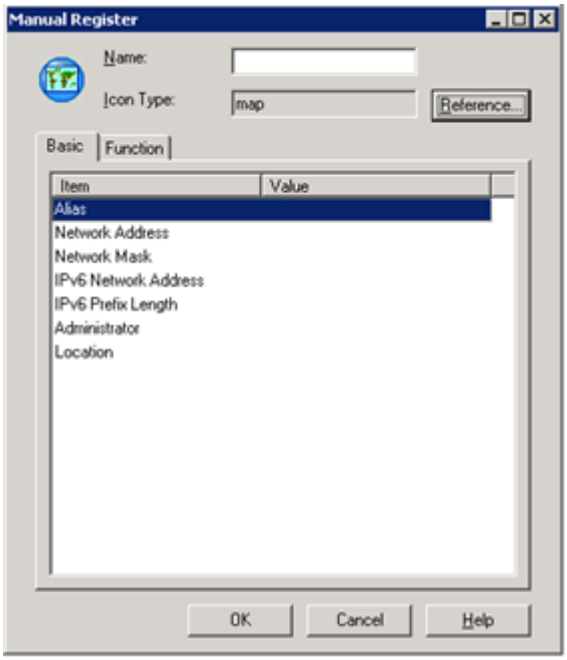
You must first change to the "configuration mode (page 27)".

1. Under **Network Management**, add a map icon.

   In the **Map View** of the NetworkManagement, right-click and select **Manual Register**.



2. Enter information to the Manual Register dialog box.

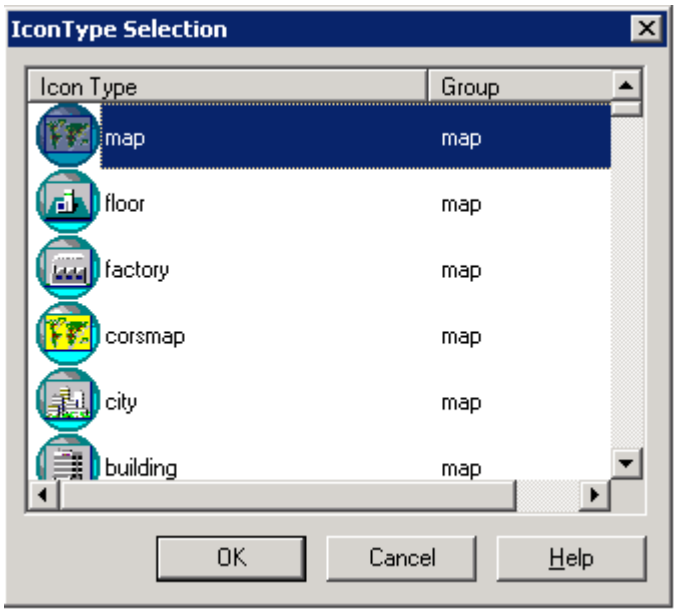


- **Name**

  Enter the map name.

- **Icon Type**

  Click **Reference** button. The Icon Type Selection dialog box is displayed. Select an icon type that belongs to the map group.



- **Network Address**

  Specify IPv4 network address of the map.

- **Network Mask**

  Specify IPv4 network mask of the map.

If necessary, enter other information to the **Basic** tab.

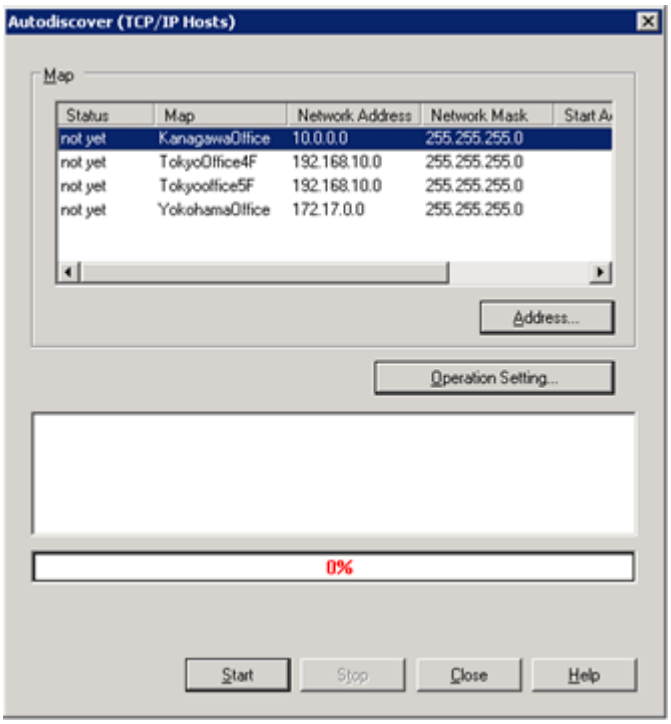
For details, refer to "4.2.2 Manually registering devices and networks (page 138)".

3. Open the Autodiscover (TCP/IP Hosts) dialog box.

   Right-click the **NetworkView**, **NetworkManagement** icon, or the map icon. Select **Configuration Management**>**Autodiscover**>**TCP/IP Hosts**.

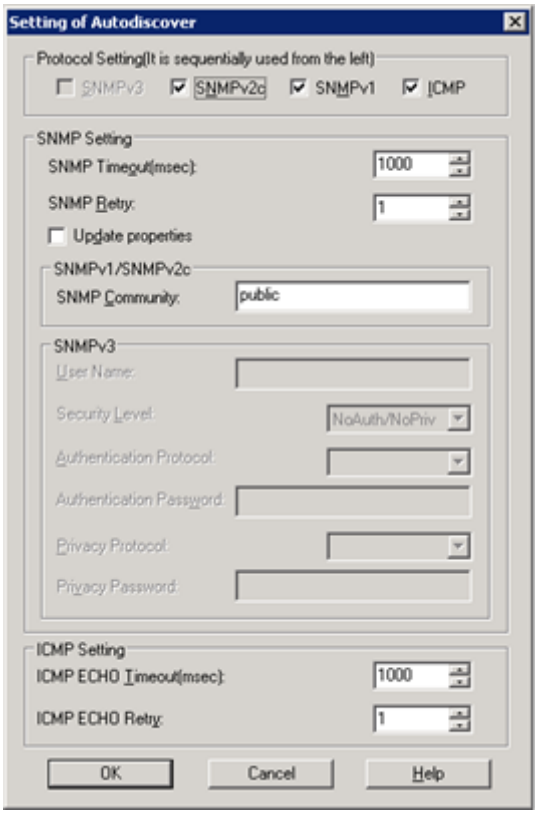
   The information for the registered map icon is displayed in **Map**.

4. Select the maps that you want to autodiscover and click **Start** button.



Tip

To change the SNMP community name that is used for discovery, or perform the discovery operation using SNMPv3, click the **Operation Setting** button in the Autodiscover (TCP/IP Hosts) to open the Setting of Autodiscover dialog box and change the parameters.



- **Protocol Setting**

  Select the protocol to be used in the Autodiscover.

- **SNMPv1/SNMPv2c**

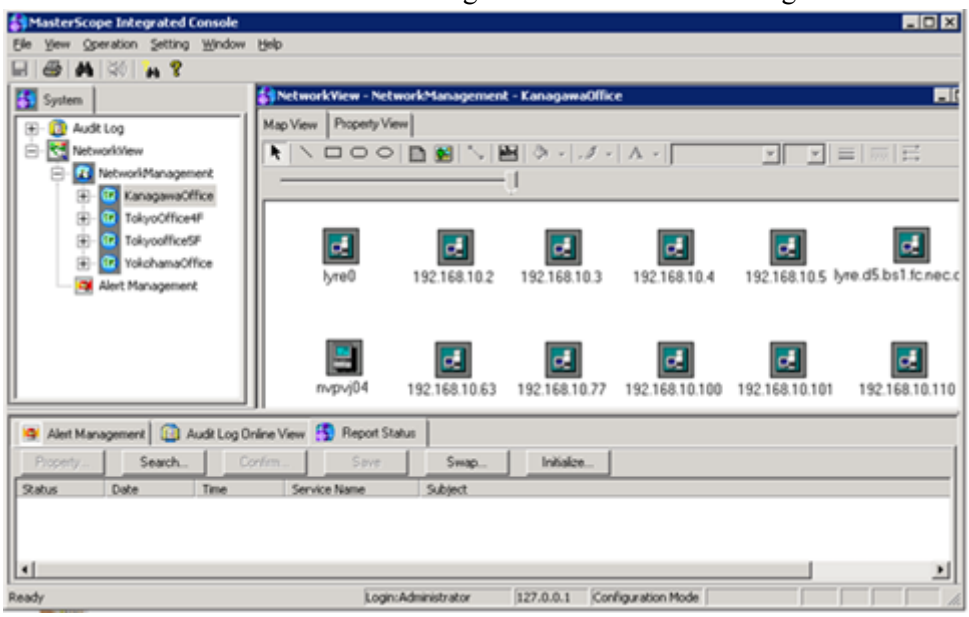
Specify the SNMP community name to be used when using SNMPv1 or v2c.

- **SNMPv3**

  Specify the parameters to be used when using SNMPv3.

5. Confirm that discovered devices have been registered in the map.

   The icons for discovered devices are registered with the monitoring mode off.



Tip

You can customize maps to make them more intuitive by inserting a bitmap in the background of the Map View, or showing the status of connections between device icons.

For information regarding customizing the map configuration, refer to the following:

- "4.2.3 Registering topology information (page 147)"
- "4.2.6 Changing the background and drawing diagrams (page 175)"

3.2.2 Batch registering managed devices

If there are a large number of devices to register in Network Manager, or if you want to register devices that are not connected to the network in the configuration stage, you can register the devices for monitoring in a batch using a file.

This section describes how to register basic information for maps and devices.

Tip

For details, refer to "4.6 Batch Registering or Deleting Configuration Information (page 206)".

You must first change to the "configuration mode (page 27)".

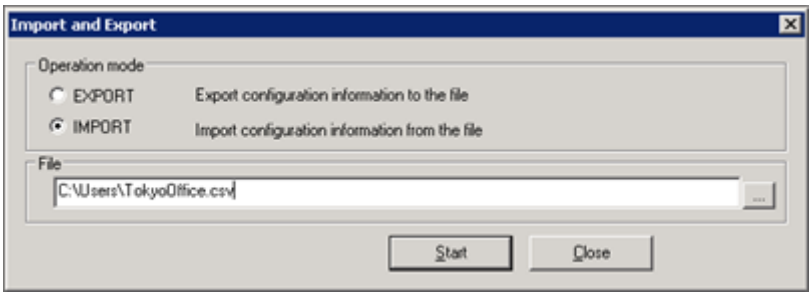
1. Prepare a CSV file that contains the information for the maps and devices to be registered.

   A sample image of the CSV file is provided below.

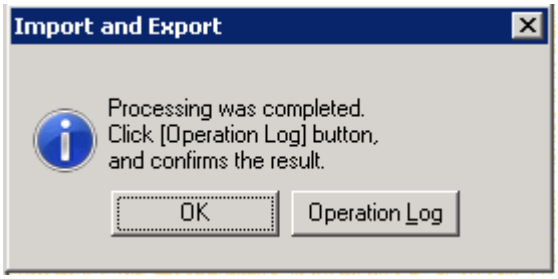
Map Registration	Device Registration	Device Name	Icon Type	Map Name	Map Path
1				Branches	/ NetworkManagement /
1				TokyoBranch	/ NetworkManagement /Branches/
	1	EastSwitch01	IP8800_720	TokyoBranch	
	1	WestSwitch01	CiscoDevice	TokyoBranch	

2. Open the Import and Export dialog box.

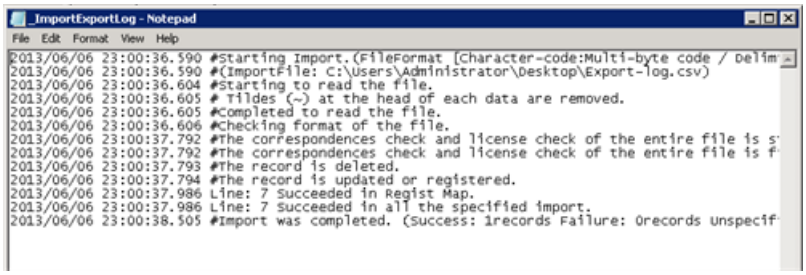
   Right-click **NetworkView** icon, **NetworkManagement** icon, or device icon, and select **Configuration Management**>**Import and Export**.



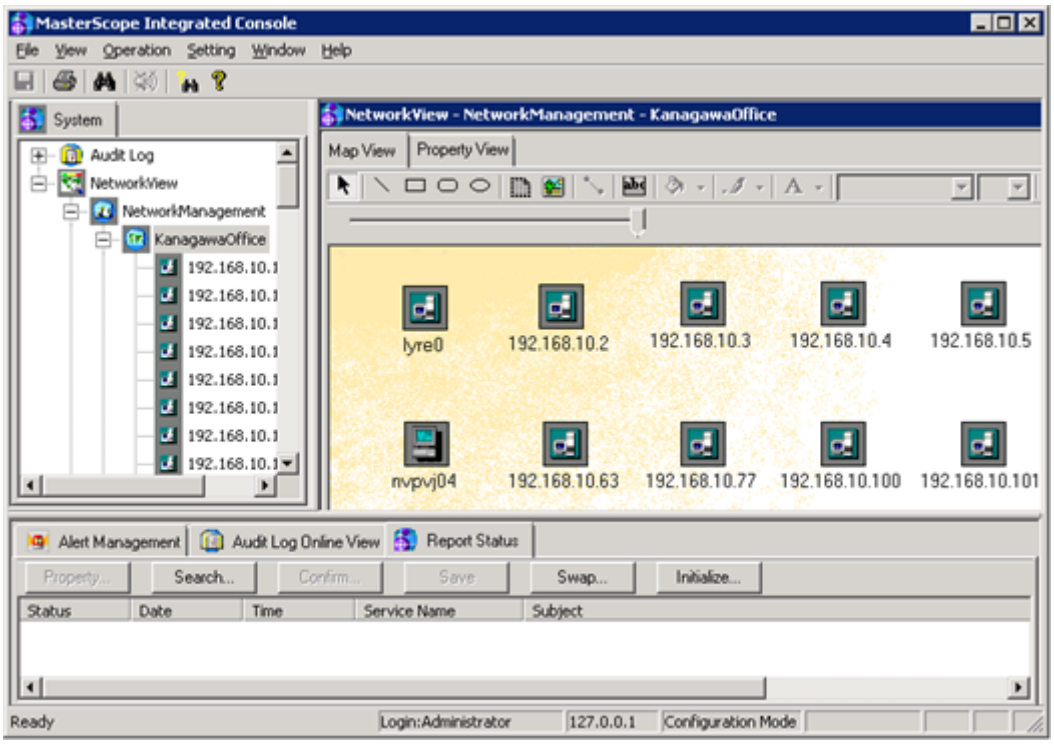
3. Select **IMPORT** in the **Operation mode**.
4. Specify the absolute path name of the import file in the **File**.
5. Click **Start** button.
6. When the import finishes, verify the results.



   Click the **Operation Log** button, and confirm that the log contents have no problem.



7. Confirm that registered devices and maps have been registered under the **NetworkManagement** icon.



When devices registered in a batch are connected to the network, it is recommend to update device information. By performing a device information update, you can update the device information registered in Network Manager, with the information obtained from devices connected to the network. To update the device information, right-click **NetworkManagement** icon, map icon, or device icon, and select **Configuration Management**>**Update Property**>**Update Required Property**.

Tip

You can customize maps to make them more intuitive by inserting a bitmap in the background of the Map View, or showing the status of connections between device icons.

For customization of the map configuration, refer to the following.

- "4.2.3 Registering topology information (page 147)"
- "4.2.6 Changing the background and drawing diagrams (page 175)"

3.2.3 Registering information for logging in to managed devices

In the following Network Manager functions, devices are logged in to and administered using telnet or ssh.

Remote login:

"5.5.3 Logging in to devices from the monitoring terminal (page 469)"

Device command execution:

"4.19 Setting for Running Device Commands (page 391)"

"5.10 Executing Device Commands (page 482)"

Execution of a command when an alert occurs:

"4.15 Settings for Executing Device Commands When Alerts Occur (page 333)"

Resource Manager function:

"4.20 Setting for Managing Device Configuration (Resource Manager) (page 399)"

"5.14 Managing Device Configuration (Resource Manager) (page 512)"

"5.15 Managing Device Software (Resource Manager) (page 531)"

This section describes how to register the login information that needs to be registered before using the above functions.

Tip

For details, refer to "4.3 Registering Login Information (page 189)".

To register login information, you first need to set the following information in the device icon properties.

- IP address
- Telnet Server : ON

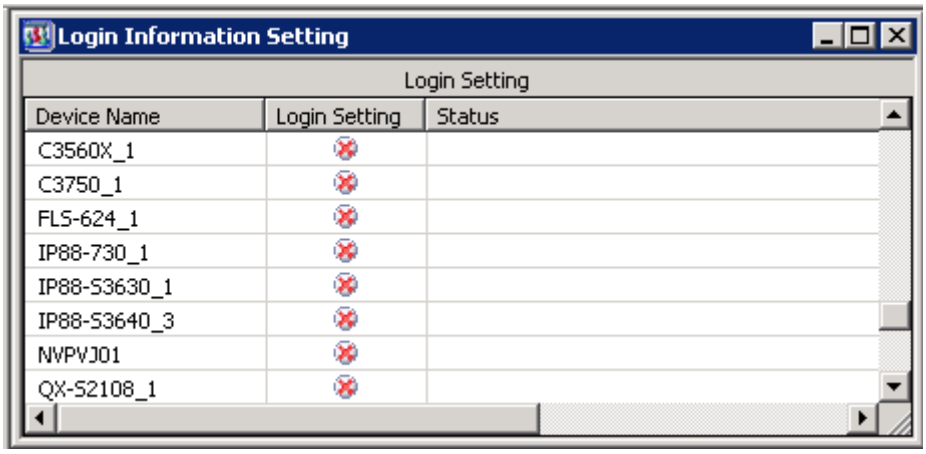
The Telnet or SSH Server function needs to be activated on the target device-side. The SSH server must support protocol version 2 and password authentication.

Prepare the information for performing a telnet or ssh login to the device, in advance.

You must first change to the "configuration mode (page 27)".

1. Open the Login Setting window.

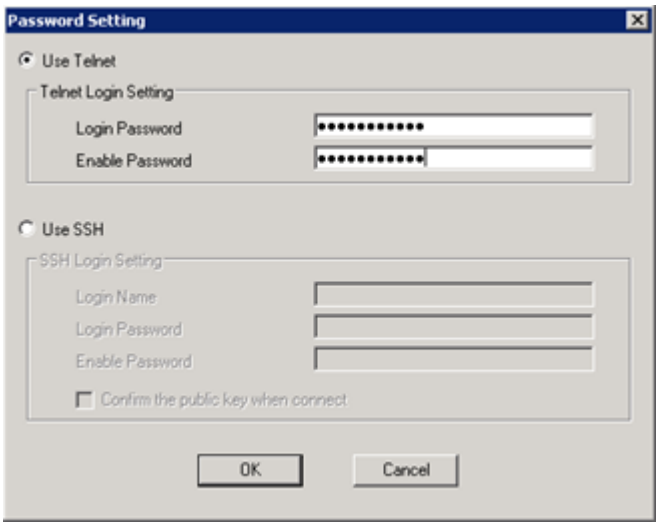
   Right-click the **NetworkView** icon and select **Configuration Management**>**Login Information Setting**.



2. Open the Password Setting dialog box.

   Right-click the target device and select **Login Setting**>**Password Setting**.

3. Enter information necessary for login.



Tip

When the setting is configured using TACACS+/RADIUS authentication, or the device is logged in via the port server, login information can be registered from **Login Setting**>**Server Setting**.

a. Open the Server Setting dialog box.

Right-click the device to which you desire to set the login information and select **Login Setting**>**Server Setting**

b. Select one of the following tabs.

- **TACACS+/RADIUS (login authentication)** tab

  Set telnet login to the device using TACACS+/RADIUS authentication

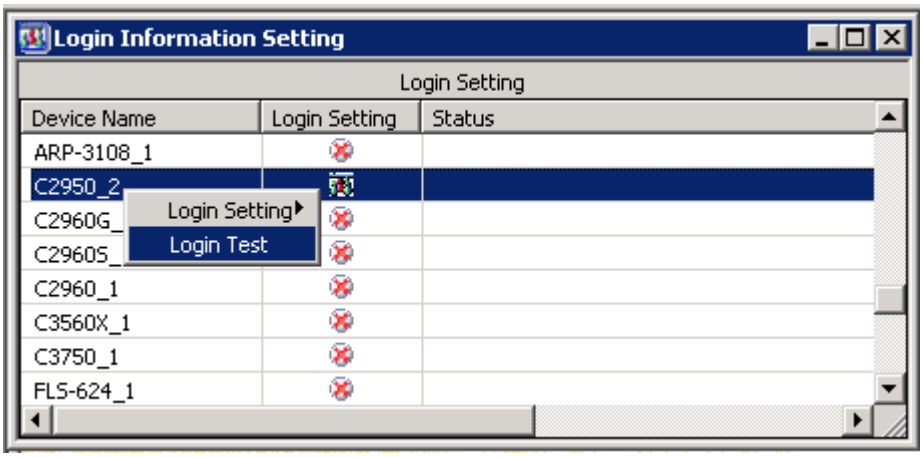
- **Port Server** tab

  Set login to the device via the Port Server

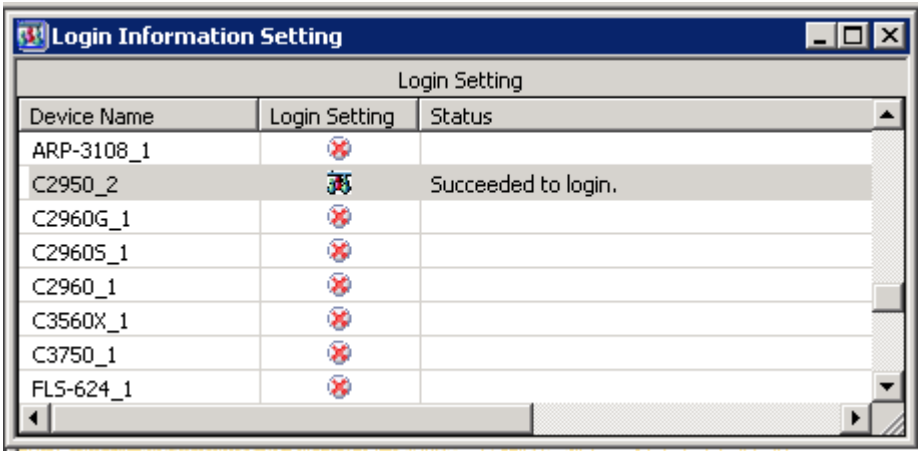
c. Enter the information, and click **OK** button.

4. Confirm that you are actually able to log in using the login information that has been set up in Network Manager.

a. Right-click the target device and select **Login Test**menu.



b. Check the results that are displayed in the **Status** column.



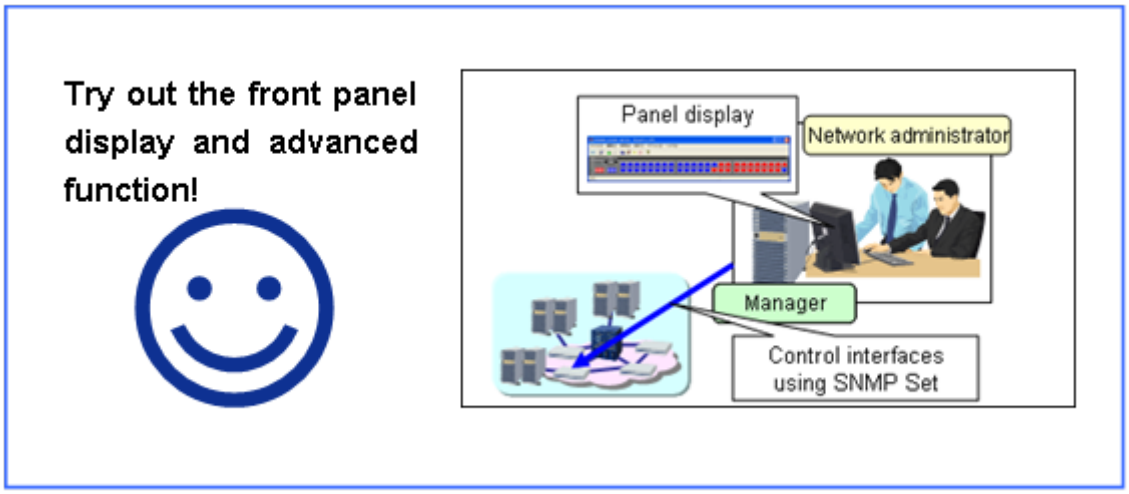
3.2.4 Selecting devices that use the panel display and advanced function

An advanced function license is provided in Network Manager to enhance the efficiency of operations.

When using the device front panel display (Node Manager function) and the Resource Manager function, you need to select the target devices to be used with each function.

Tip

You do not need to assign licenses to devices being used with the Network Provisioning function.



This section describes how to select the target devices to be used with each function.

Tip

For details, refer to "4.4 Managing the Advanced Functions License (page 201)".

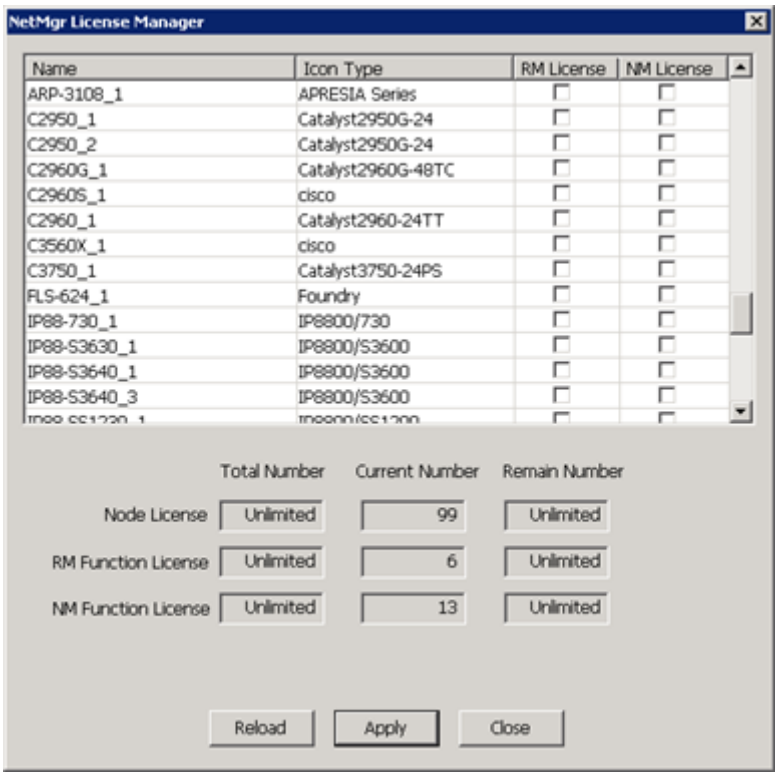
Decide which devices will be used with the front panel display and Resource Manager function.

When using the Resource Manager function, you need to register a codeword for each license.

You must first change to the "configuration mode (page 27)".

1. Open the NetMgr License Manager dialog box.

   Right-click the **NetworkView** icon and select **NetMgr License Management** menu.

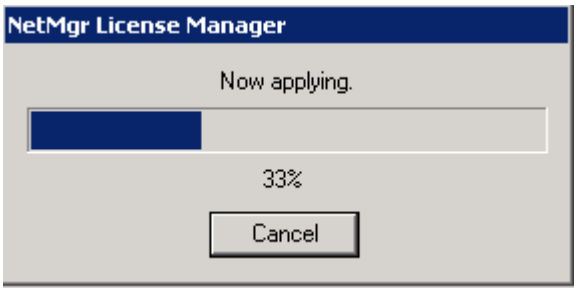


2. Double-click the check box for each target device license and assign a license.

   RM Lisence Resource Manager function

   NM Lisence Front panel display function (Node Manager function)

3. Click **Apply** button to apply settings.



Check the **Remain Number** value and assign a license to the device. The **Total Number** upper limit can be increased by registering a codeword for the additional node license for each advanced function.

Tip

When using each advanced function, you also need to register the information below.

Front panel display:

- Register the IPv4 address or IPv6 address in the properties
- Register the SNMP community name (get) or SNMPv3 information in the properties
- Register the device front panel type in the properties

Resource Manager function:

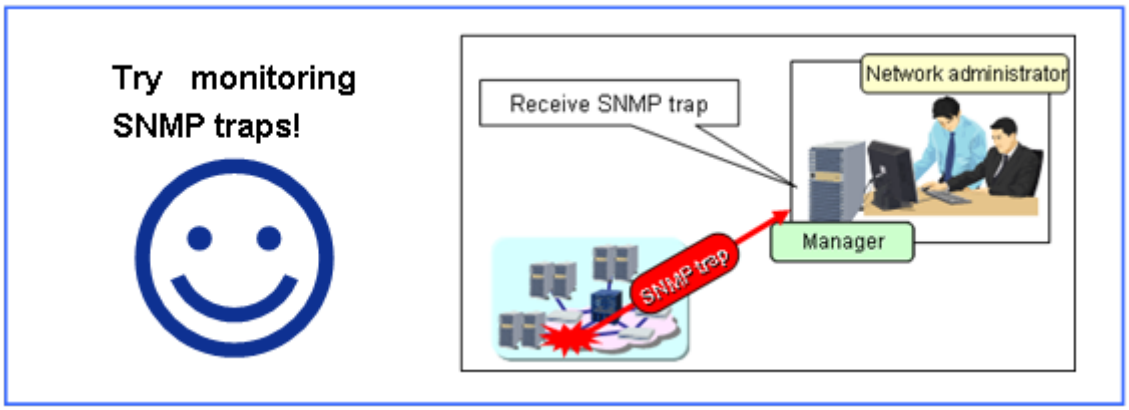
- Register the IPv4 address, OS type and the software version in the properties
- Register login information

3.3 Configuration: Configuring Monitoring Settings

In Network Manager, you can receive SNMP traps and syslogs, perform alive monitoring using an ICMP echo, perform MIB monitoring using SNMP.

3.3.1 Configuring settings for SNMP trap monitoring

Network Manager can receive SNMP traps sent from devices and display as alerts.



If the source address matches the **IP Address** or **IPv6 Address** in the device icon properties, the manager receives and displays it. If it does not match, the system checks whether it corresponds with an address value registered in Interface Properties dialog box. If it does not correspond with any of the values, the manager discards it without receiving.

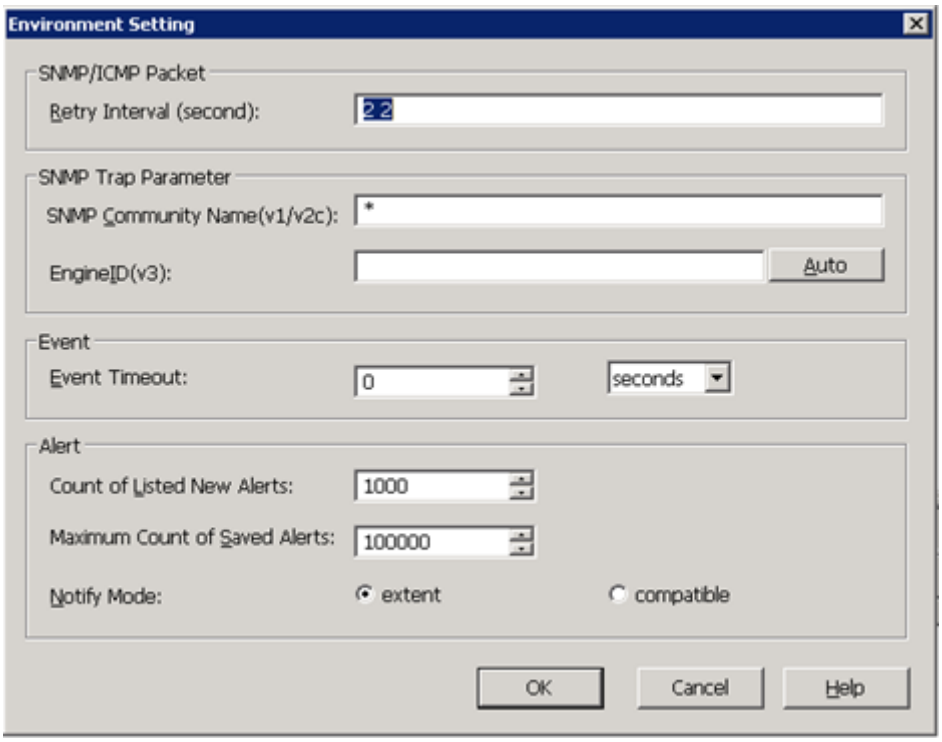
To receive SNMP traps in Network Manager, confirm the following.

- The SNMP trap port (162/udp) on the server installed with the manager of Network Manager does not conflict with another product.

You must first change to the "configuration mode (page 27)".

1. Open the Environment Setting dialog box.

   Right-click the **NetworkView** icon and select **Environment Setting** menu.



For details regarding to the Environment Setting dialog box, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

2. Specify the community name of the SNMPv1/v2c traps or informs to be received in **SNMP Community Name(v1/v2c)** of **SNMP Trap Parameter**.

   SNMP traps with community names that do not match the specified value will be discarded without being received. If you specify an asterisk (*), all community names will be received.

3. To receive SNMPv3 informs, specify the engine ID of the SNMPv3 informs to be received in **EngineID(v3)** of **SNMP Trap Parameter**.

   The specified value must be set to the device as a remote engine ID. For details, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

4. To receive SNMPv3 traps, you need to register the SNMPv3 information in the properties for the target device icon.

   The **EngineID** in the SNMPv3 information might be updated when the device is rebooted or the IP address is changed.

   For details on registering properties of SNMPv3 information, refer to "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)".

5. Set the "monitoring mode (page 505)" for the target device icon to ON.

6. On the monitored device, set the SNMP trap send destination to the manager IP address of Network Manager.

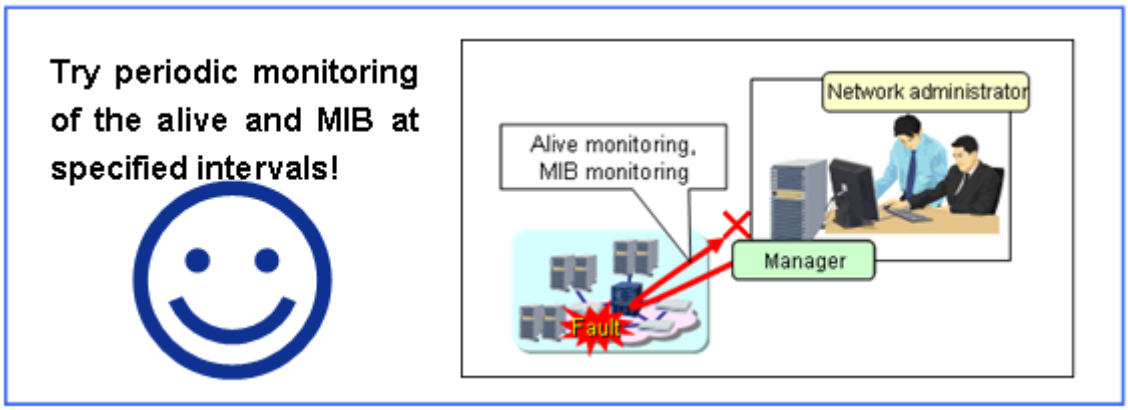
7. Confirm that an SNMP trap, such as a linkDown from the device, has been generated and a notification appears in the **Alert Management** tab.

Tip

You can change the contents of the SNMP trap notification to something that is easier to understand by creating a trap definition file. For details, refer to "4.11.3.1 Trap Definition Management window (page 265)".

3.3.2 Configuring settings for alive monitoring and MIB monitoring

You can perform alive monitoring using an ICMP echo, or MIB monitoring using SNMP at specified intervals.



Tip

For details of the state monitoring setting, refer to the following:

- "4.10.2 Creating new state monitoring rule entries (page 243)"
- "7.1 State Monitoring Rules (page 590)"

The following example shows that alive monitoring on all registered devices is performed at five-minute intervals.

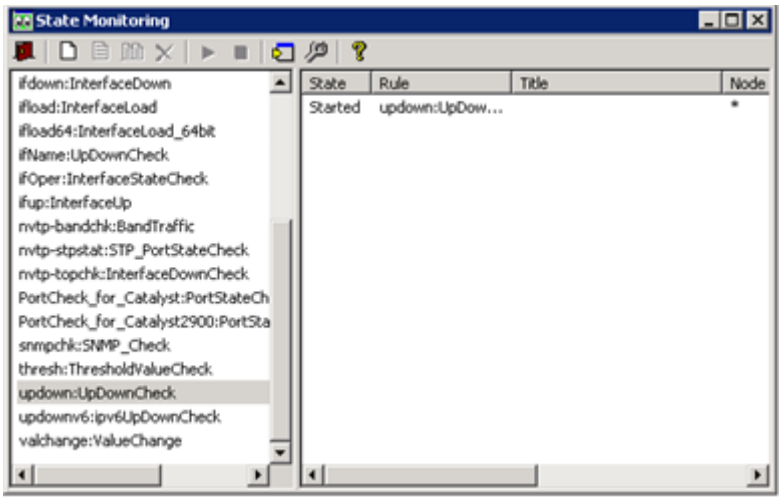
The following information needs to be registered in the properties for the target icons:

- IPv4 address or IPv6 address
- SNMP community name (get) or SNMPv3 information (not required when performing alive monitoring through an ICMP echo)
- Monitoring mode : ON

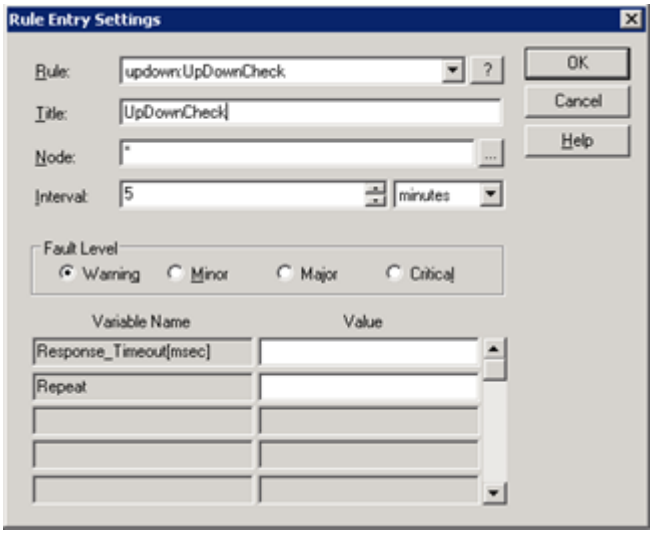
1. Open the State Monitoring window.

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Fault Management**>**State Monitoring**.

2. Select **updown:UpDownCheck** and click the  (Create a new rule entry button).



3. In the Rule Entry Settings dialog box, configure the monitoring parameters.



- **Title** : UpDownCheck
- **Node** : *

  Tip

  You can specify a group name. If you specify a group as the target of the state monitoring rules, when new device icon is added, you make the device belong to the target group in order to start the monitoring. Change of the monitoring setting is not needed.

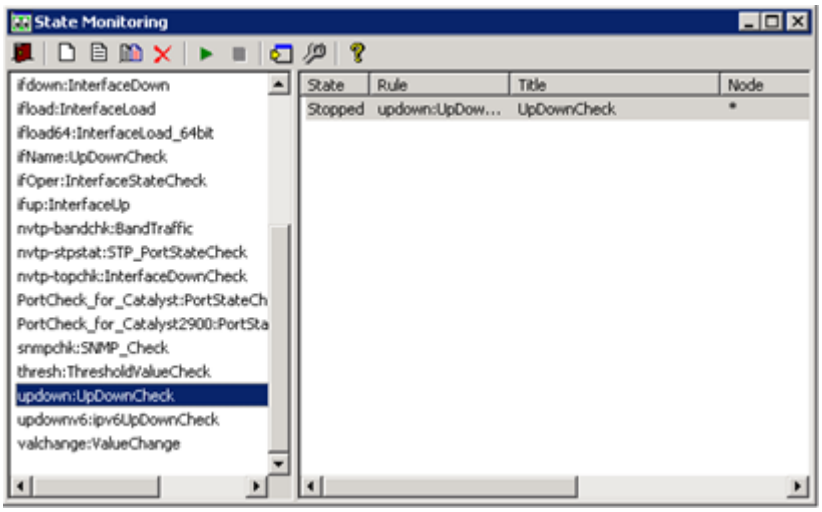
  To make a device belong to a group, specify a group name to the **Group** in the icon property of the device. For details, refer to the following.

  - "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)"
  - "6.2.1.7 **Group List** menu (page 568)"
  - "6.2.1.8 **Group Member List** menu (page 569)"

- **Interval** : 5 minutes
- **Fault Level** : Select the fault level for the alert notification.

4. Select the set monitoring rule, and click  (Start rule entries) button.

   In this example, select the registered "alive monitoring all devices" out of the list.



When the status of a state monitoring rule is set to execute, monitoring is performed for devices that have the monitoring mode set to ON.

Tip

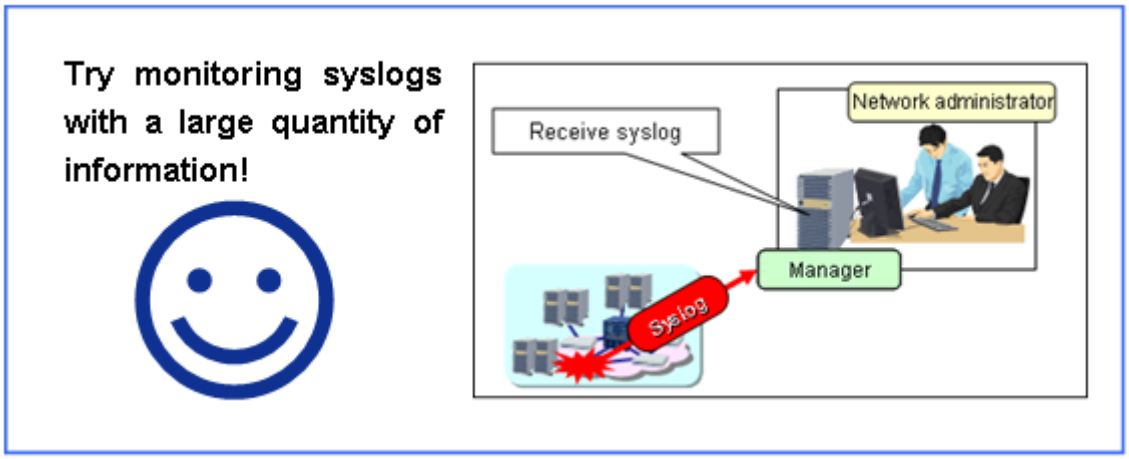
The system waits for a response from monitored devices and performs resends based on the value specified in the **Retry Interval** in Environment Setting dialog box. In some operating environments, it may take longer to get a response from monitored devices. You may therefore need to change the **Retry Interval** value in the Environment Setting dialog box. For details, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

5. Confirm that an alert appears in the **Alert Management** tab.

   Temporarily change the status so that communication cannot be established with the device.

3.3.3 Configuring settings for syslog monitoring

Network Manager can receive syslogs other than SNMP traps sent from devices, and display as alerts.



If the source address matches the **IP Address** in the device icon properties, the manager receives and displays it. If there is no matching address, the manager discards it without receiving.

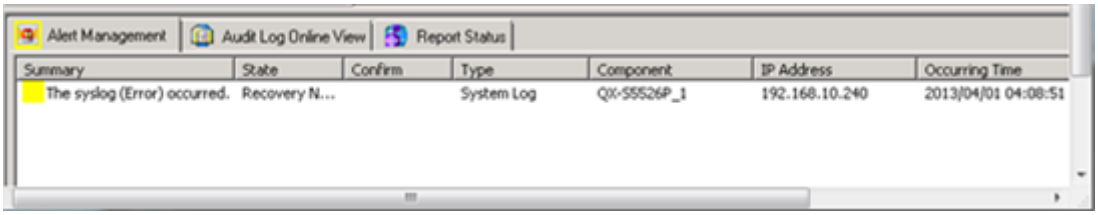
To receive syslogs in Network Manager, confirm the information below.

- The syslog port (514/udp) on the server installed with the manager of Network Manager does not conflict with another product. For details, refer to "11.4.2 Sharing the SYSLOG port with other software (page 778)".

- The source IP address for the syslog, and the **IP Address** in the device icon properties, are the same.

1. Set the "monitoring mode (page 505)" for the target device icon to ON.
2. On the monitored device, set the syslog send destination to the manager IP address of Network Manager.
3. Generate a syslog with WARNING severity or above from the device, and confirm that it is notified in the **Alert Management** tab.

   If any alert is not displayed, refer to "11.3.2 The system logs are not displayed as alerts (page 775)".

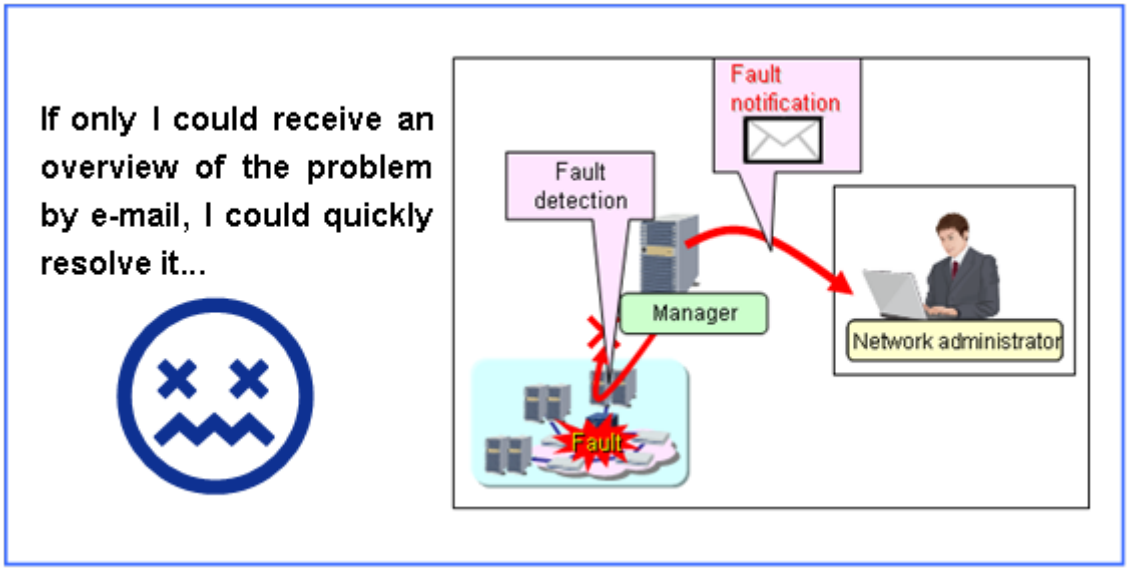


3.3.4 Configuring settings for reporting faults

When a fault occurs on the network, an initial abnormality report can be sent to the network administrator via e-mail, Patlite, or through the execution of another action.

As a result, the network administrator does not need to constantly watch the monitoring window and will be aware of fault events even when in a location other than that of the monitoring system.

3.3.4.1 Sending fault details by e-mail when specific faults occur



Tip

For further information regarding settings, refer to the following:

- "4.14.2 Configuring report settings (page 314)"
- "4.14.3.2 Defining e-mail reports (page 322)"

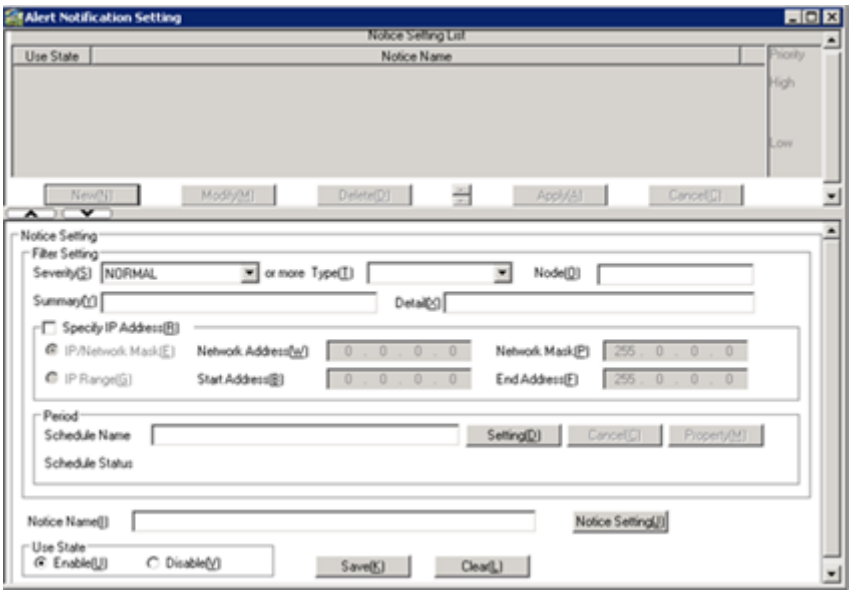
A mail server is needed to send e-mail reports. In addition, the following settings need to be prepared in advance:

- The host name or IP address of the mail server
- The e-mail address of the recipient
- The e-mail address of the sender

You must first change to the "configuration mode (page 27)".

1. Open the **Alert Notification Setting** window.

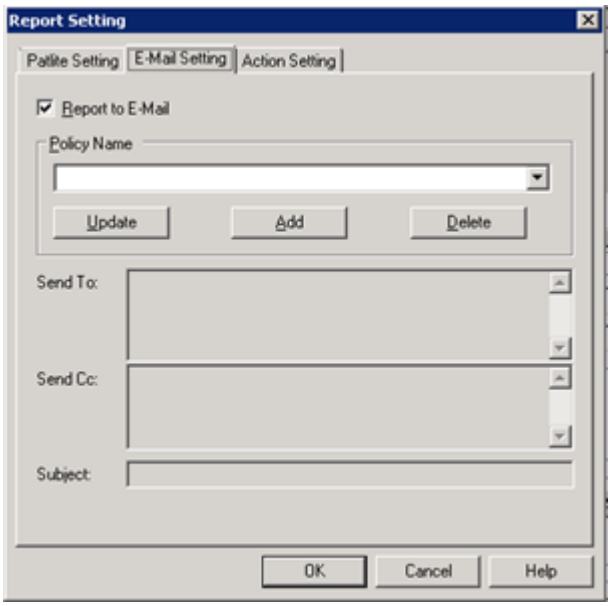
   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Fault Management**>**Alert Notification Setting**.



2. In the Notice Setting List pane, click **New** button.
3. In the Notice Setting pane, enter **Notice Name**.

   According to the monitoring requirements, specify the **Severity** and **Type** and etc.
4. In the Notice Setting pane, click **Notice Setting** button.

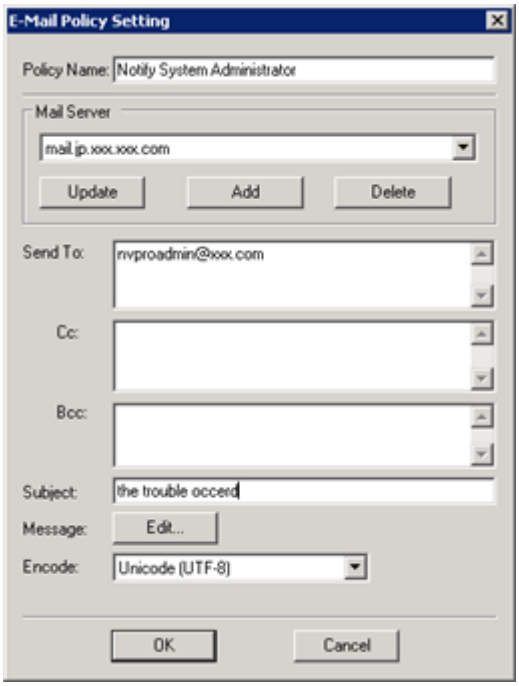
   The Report Setting dialog box is opened.
5. Select the **E-Mail Setting** tab and check **Report to E-Mail**.



6. Click **Add** button.

   The E-Mail Policy Setting dialog box is opened.

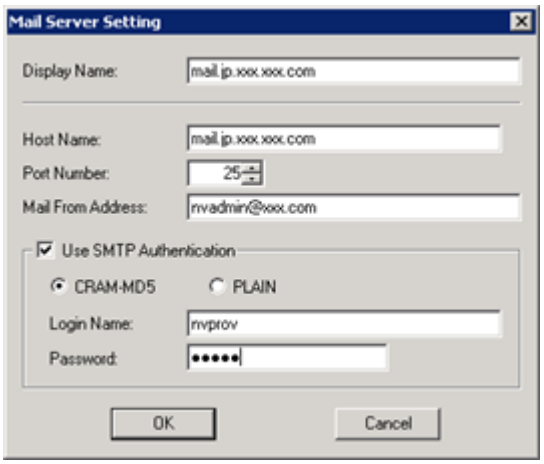
7. In the E-Mail Policy Setting dialog box, specify conditions necessary for sending a mail.



   a. Enter the **Policy Name**.

      This policy name can be selected in the Report Setting dialog box.

   b. Click **Add** button and configure the mail server settings.



The **Display Name** that is set here can be selected in the E-Mail Policy Setting dialog box. For details, refer to "4.14.3.2.2 Defining a mail server (page 325)".

c. Enter an e-mail address into **Send To**.

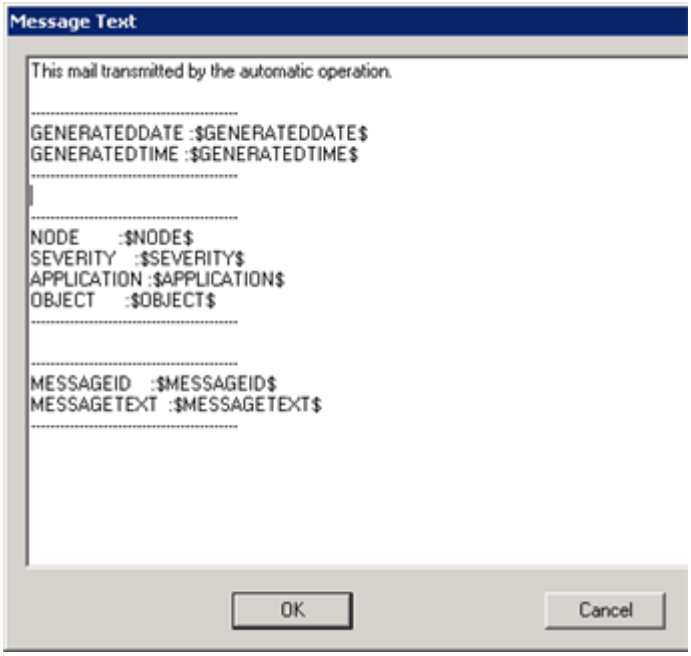
To specify multiple recipients, insert a line break for each recipient. Send destinations can be specified using up to 256 characters per line, and up to 768 characters in total including line break characters.

Tip

If you have multiple delivery addresses, it is recommended to prepare a mailing list and separately specify a mail address in the mailing list as a delivery address.

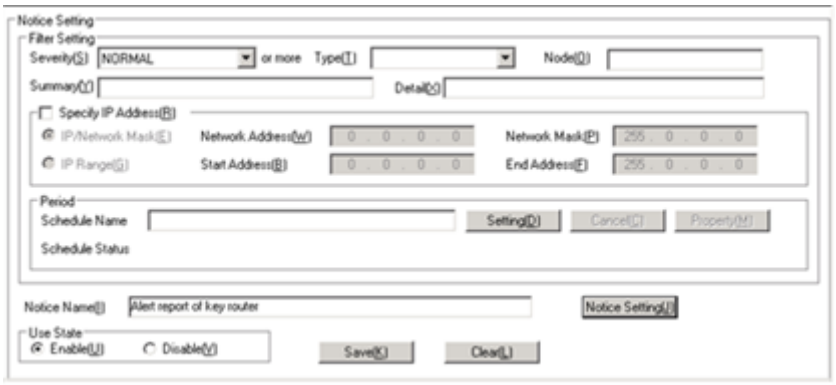
d. Enter the **Subject**.

e. Click **Edit** button, and edit text in the Message Text window.



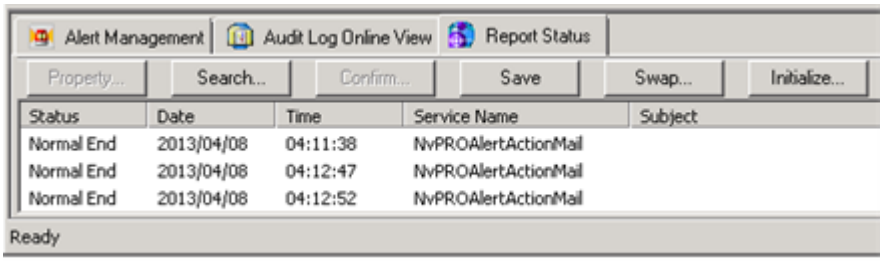
f. Click **OK** button to close the E-Mail Policy Setting dialog box.

8. When you have finished, click **Save** button in the Alert Notification Setting window.



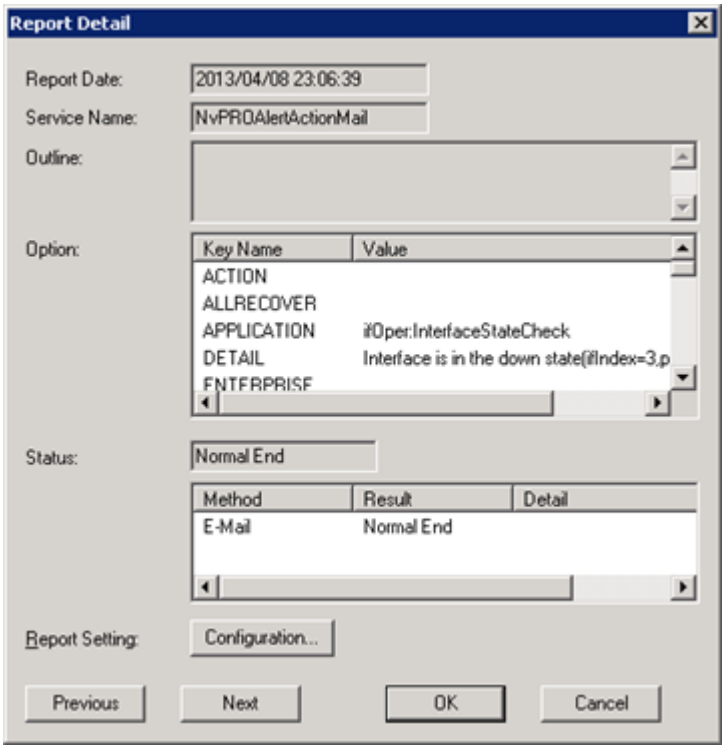
9. Confirm that the fault notification e-mail is sent in accordance with the alert notification conditions when a fault occurs.

   a. Select the **Report Status** tab.

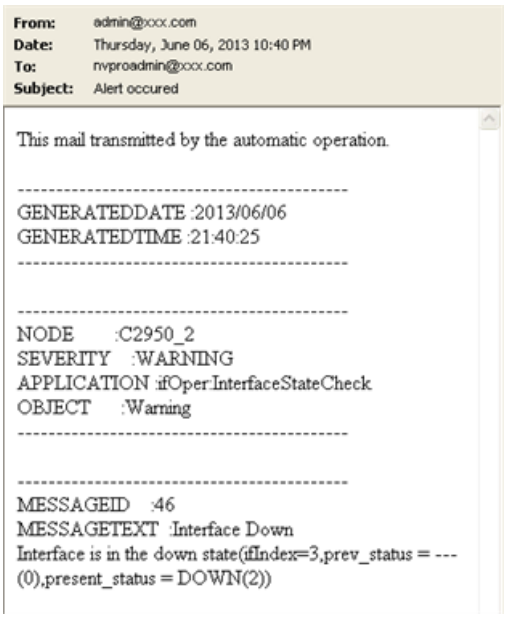


   b. Double-click the selected row.

   c. You can check the failure details and report status in the displayed Report Detail dialog box.



   An example of a fault notification e-mail.


From: admin@xxx.com
Date: Thursday, June 06, 2013 10:40 PM
To: nvproadmin@xxx.com
Subject: Alert occured

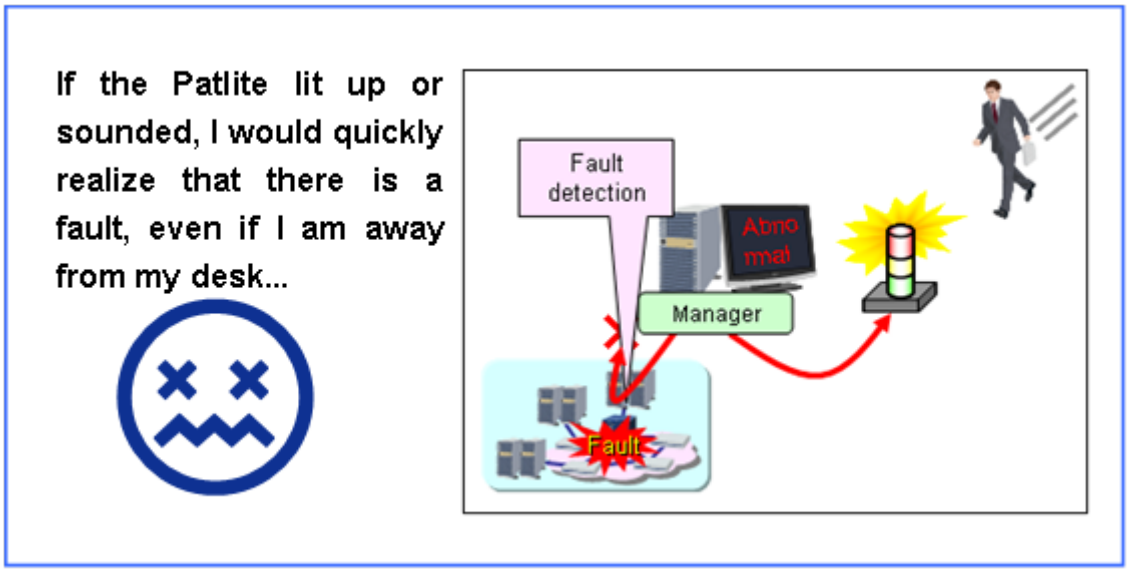
This mail transmitted by the automatic operation.

GENERATEDDATE :2013/06/06
GENERATEDTIME :21:40:25

NODE :C2950_2
SEVERITY :WARNING
APPLICATION :ifOperInterfaceStateCheck
OBJECT :Warning

MESSAGEID :46
MESSAGETEXT :Interface Down
Interface is in the down state(ifIndex=3,prev_status = ---
(0),present_status = DOWN(2))

3.3.4.2 Activating Patlite when specific faults occur



Tip

For further information regarding settings, refer to the following:

"4.14.2 Configuring report settings (page 314)"
"4.14.3.1 Defining Patlite reports (page 318)"

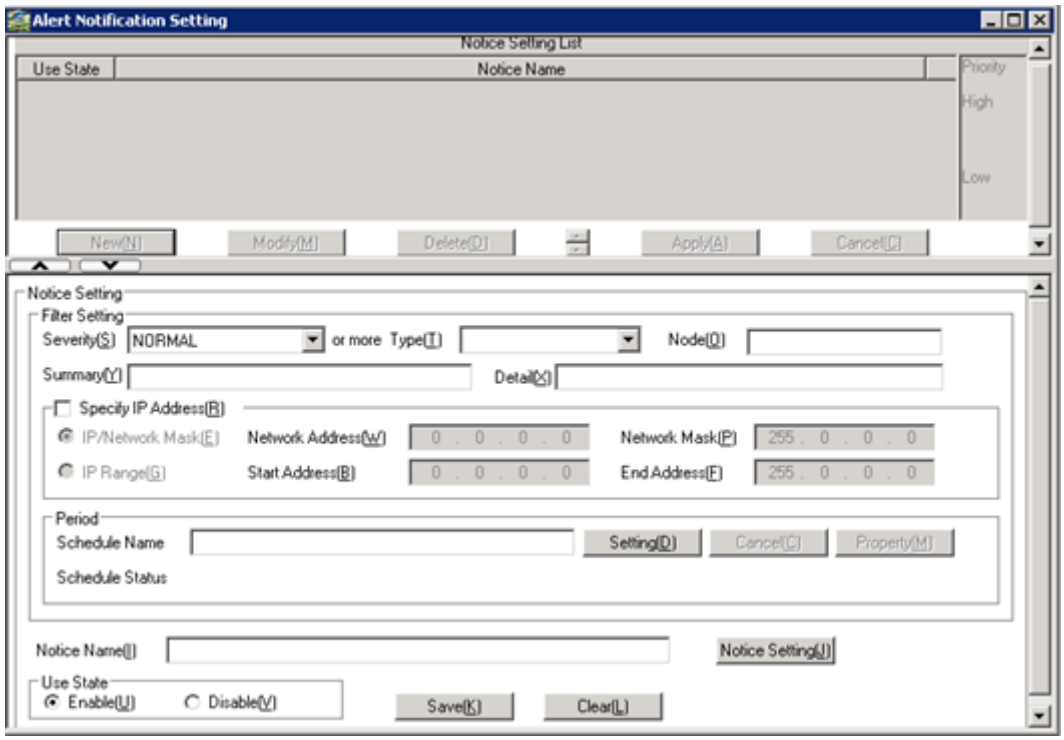
To define a Patlite reporting, the following settings need to be prepared in advance.

- The host name or IP address for Patlite

You must first change to the "configuration mode (page 27)".

1. Open the Alert Notification Setting.

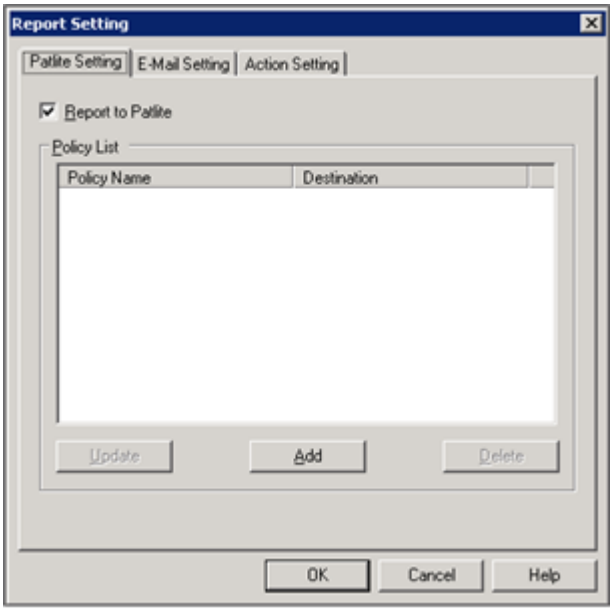
   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Fault Management**>**Alert Notification Setting**.



2. In the Notice Setting List pane, click **New** button.
3. In the Notice Setting pane, enter **Notice Name**.

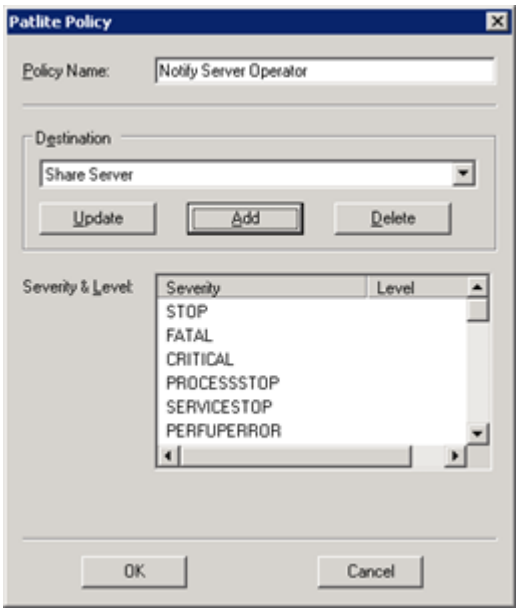
   According to the monitoring requirements, specify the **Severity** and **Type** and etc.
4. In the Notice Setting pane, click **Notice Setting** button.

   The Report Setting dialog box is opened.
5. Select **Patlite Setting** tab and check **Report to Patlite**.



6. Click **Add** button.

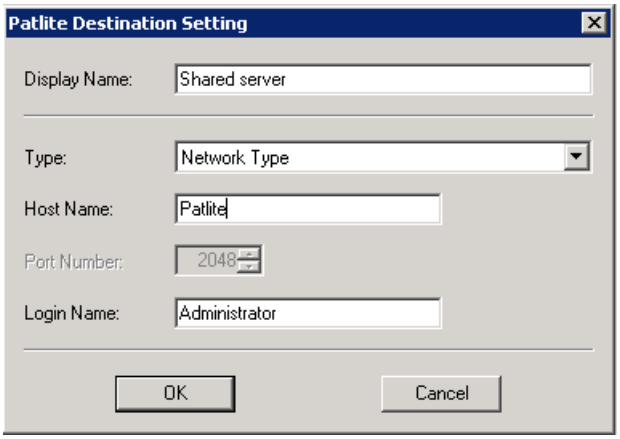
   The Patlite Policy dialog box is opened.
7. In the Patlite Policy dialog box, configure condition settings necessary for a Patlite report.



a. Enter the **Policy Name**.

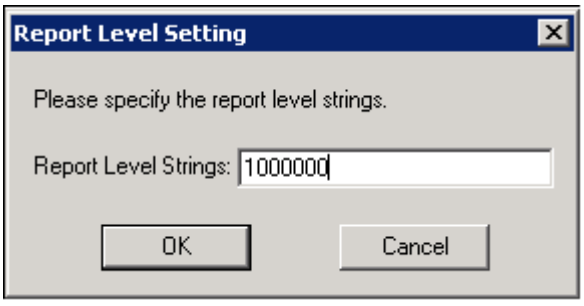
This policy name can be selected in the Report Setting dialog box.

b. Click **Add** button and configure the Patlite destination setting.



The **Display Name** that is set here can be selected in the Patlite Policy dialog box.

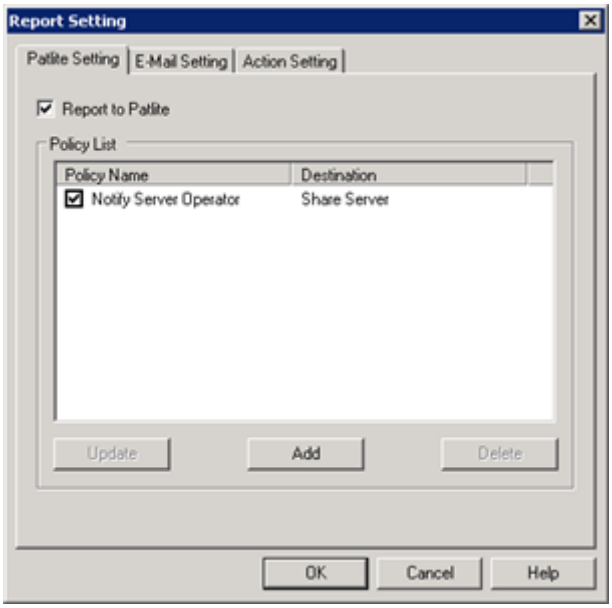
c. Double-click an item in **Severity & Level**, configure the report level settings.



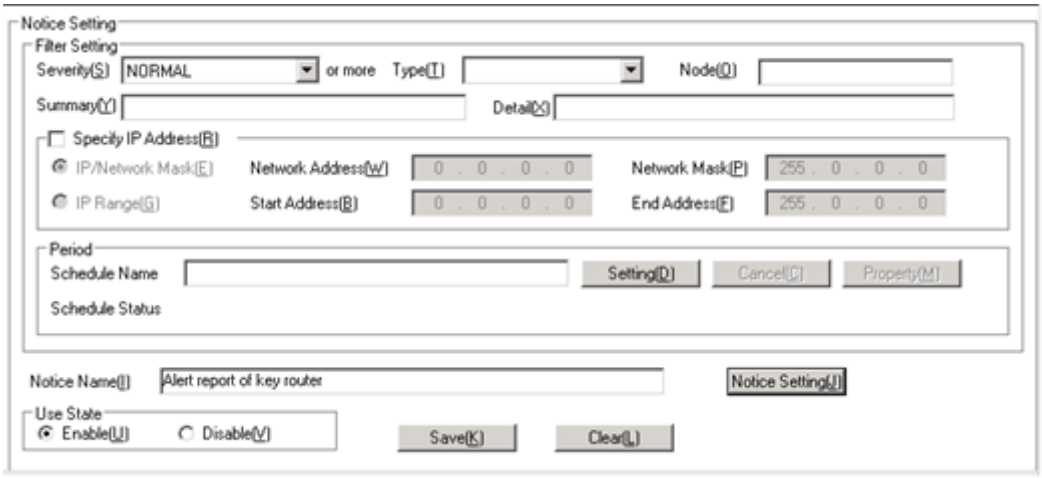
d. Click **OK** button to close the Patlite Policy dialog box.

Tip

To activate Patlites in multiple locations at a time, configure the multiple policies for each Patlite and select them in the **Patlite Setting** tab.

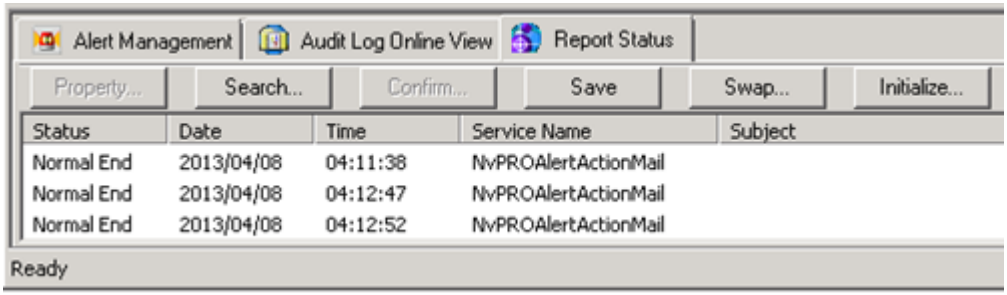


8. When you have finished, click **Save** button in the Alert Notification Setting window.



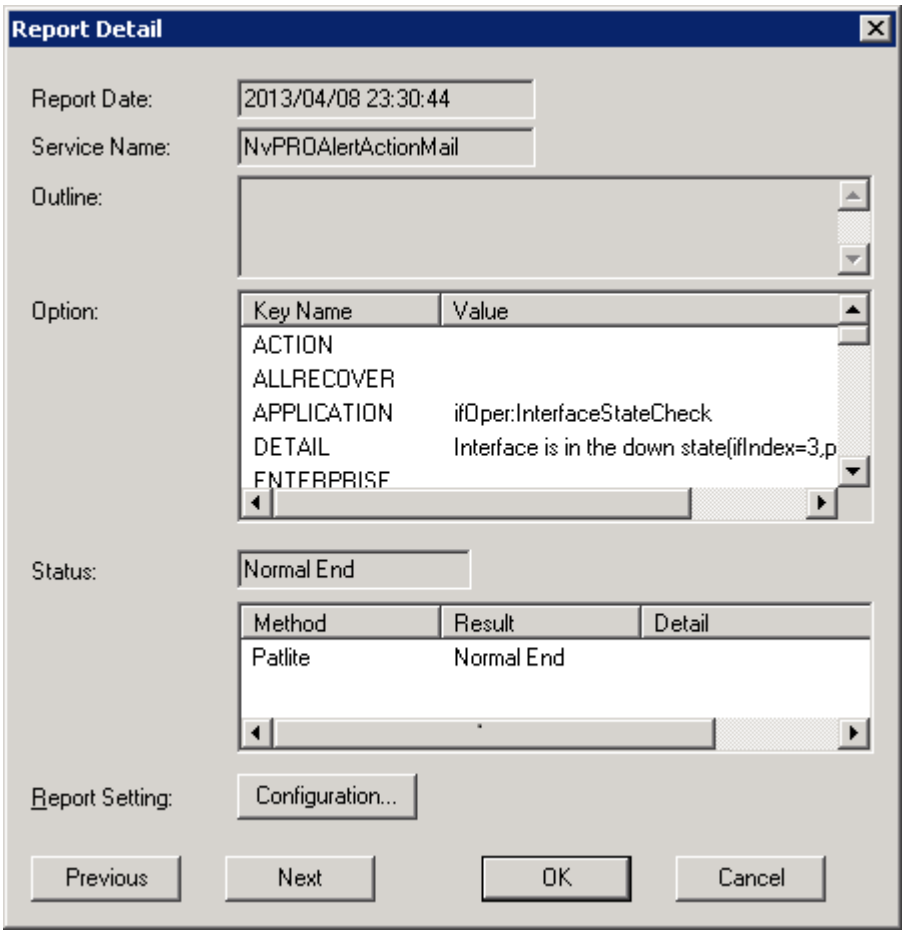
9. Confirm that the Patlite report is sent in accordance with the alert notification conditions when a fault occurs.

   a. Select the **Report Status** tab.

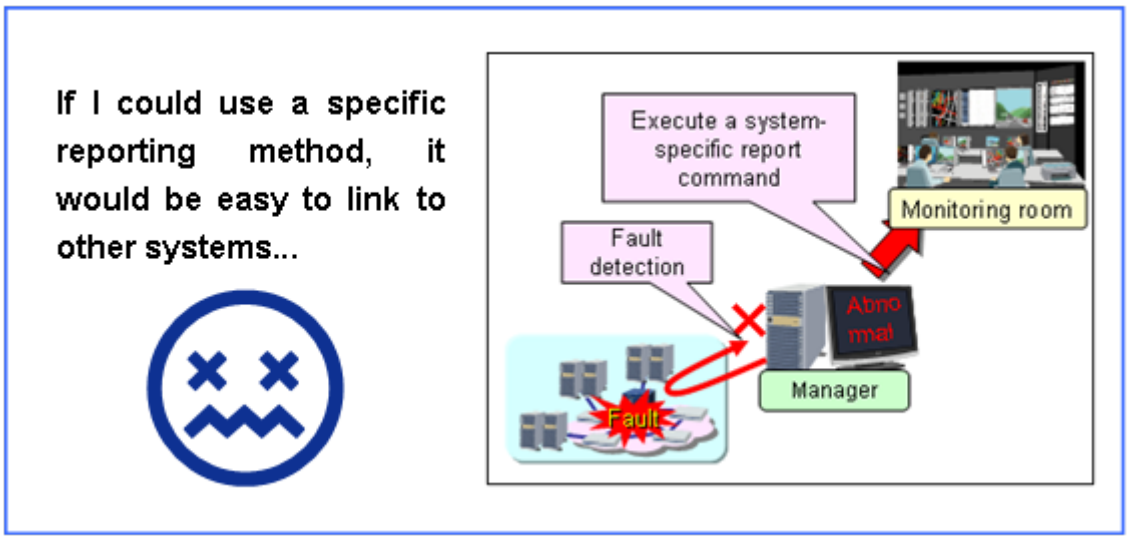


   b. Double-click the selected row.

   c. You can check the failure details and report status in the displayed Report Detail dialog box.



3.3.4.3 Automatically executing commands or programs when specific faults occur



Tip

For further information regarding settings, refer to the following:

"4.14.2 Configuring report settings (page 314)"

"4.14.3.3 Defining action reports (page 326)"

To define an action report, the following settings need to be prepared in advance.

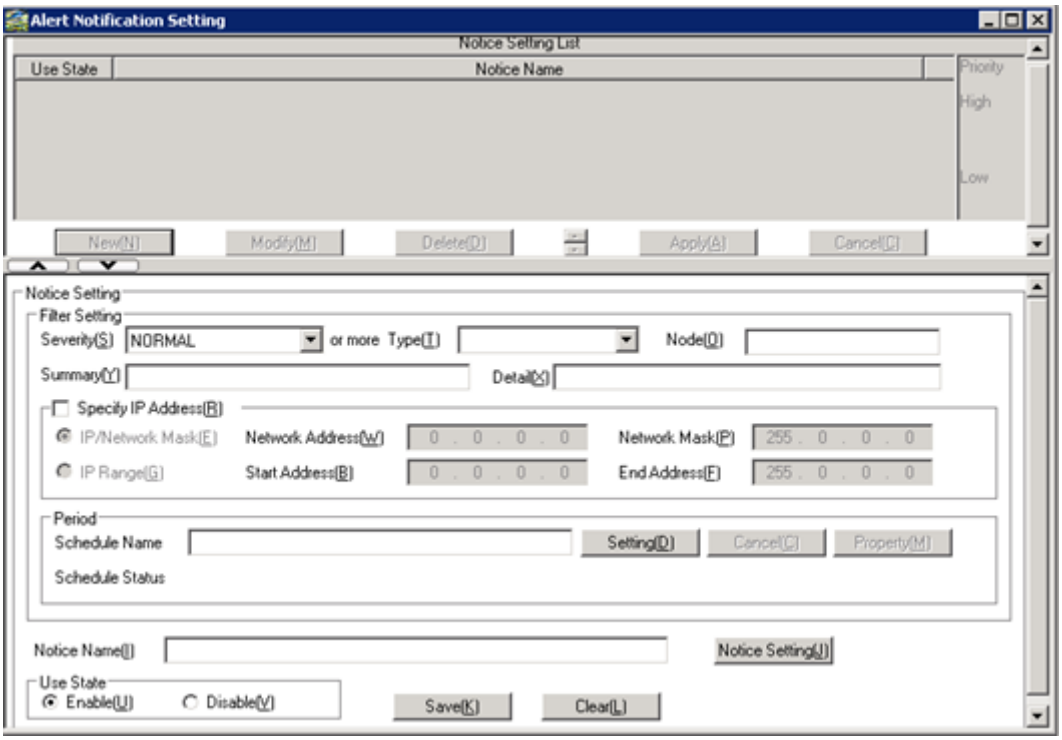
- Path information for the command or program to be executed.

Install the command or program to be executed, into the manger in advance.

You must first change to the "configuration mode (page 27)".

1. Open the Alert Notification Setting.

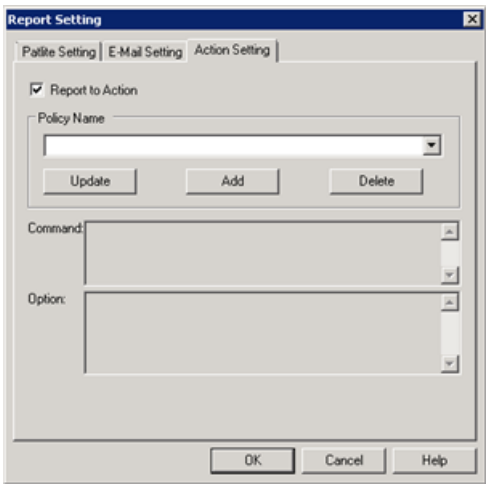
   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Fault Management**>**Alert Notification Setting**.



2. In the Notice Setting List pane, click **New** button.
3. In the Notice Setting pane, enter **Notice Name**.

   According to the monitoring requirements, specify the **Severity** and **Type** and etc.
4. In the Notice Setting pane, click **Notice Setting** button.

   The Report Setting dialog box is opened.
5. Select the **Action Setting** tab and check **Report to Action**.

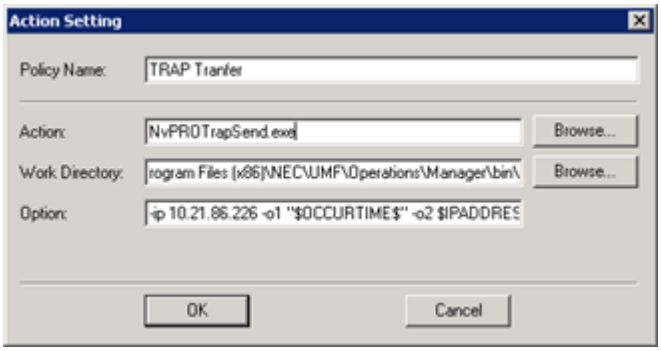


6. Click **Add** button.

   The Action Setting dialog box is opened.

7. In the Action Setting dialog box, specify the necessary conditions for the action report.

   Set up the necessary information for the action report.



   a. Enter the **Policy Name**.

      This policy name can be selected in the Report Setting dialog box.

   b. Enter the command path in the **Action**.

      If multiple commands or programs are executed for one alert, create a batch file or script in order to execute multiple commands or programs, and then register the created script file as the action command.

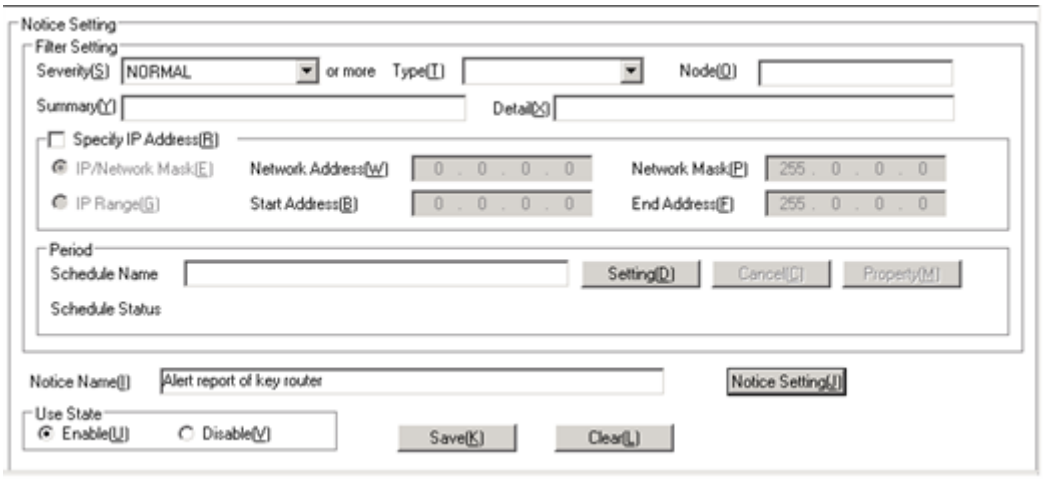
      Tip

      To transfer the detected alert information to another system using SNMP trap, register `NvPROTrapSend` command as a command to be executed. For details, refer to "4.14.4 Linking with other SNMP manager software using SNMP traps (page 330)".

   c. Enter the **Work Directory** and **Option**.

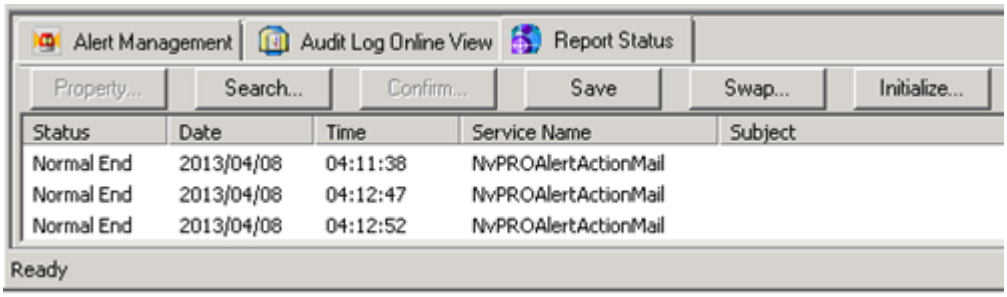
   d. Click **OK** button to close the Action Setting dialog box.

8. When you have finished, click **Save** button in the Alert Notification Setting window.



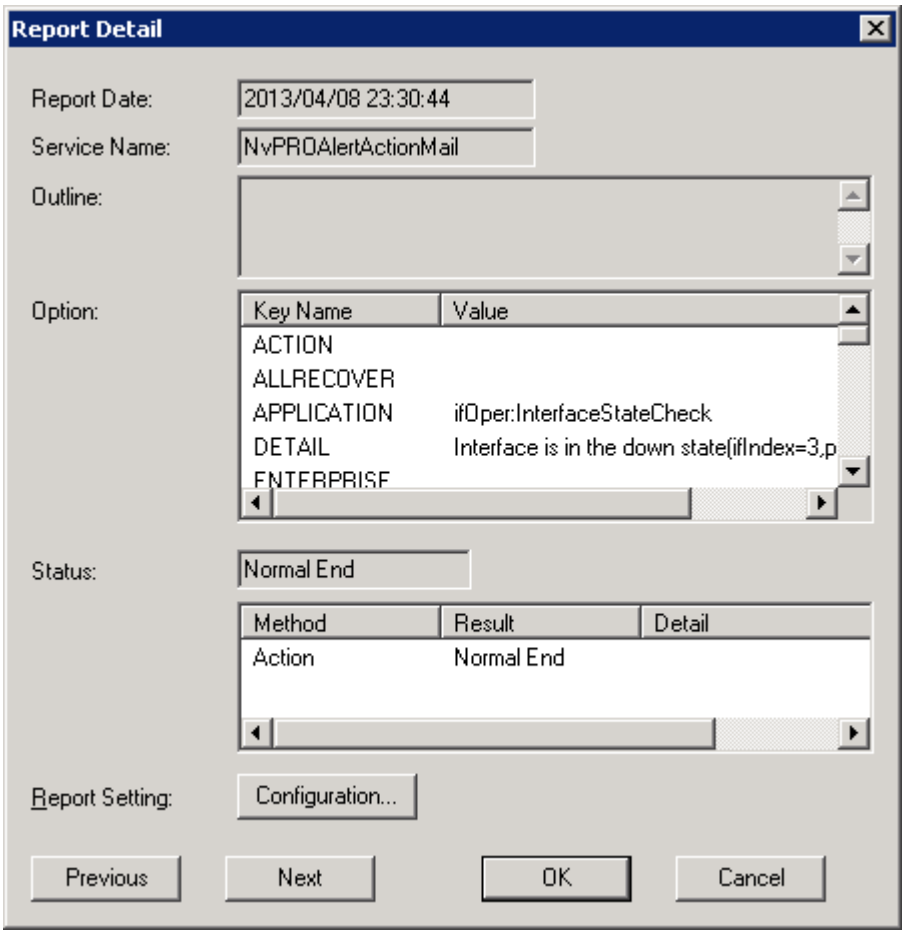
9. Confirm that the action report is executed in accordance with the alert notification conditions when a fault occurs.

   a. Select the **Report Status** tab.



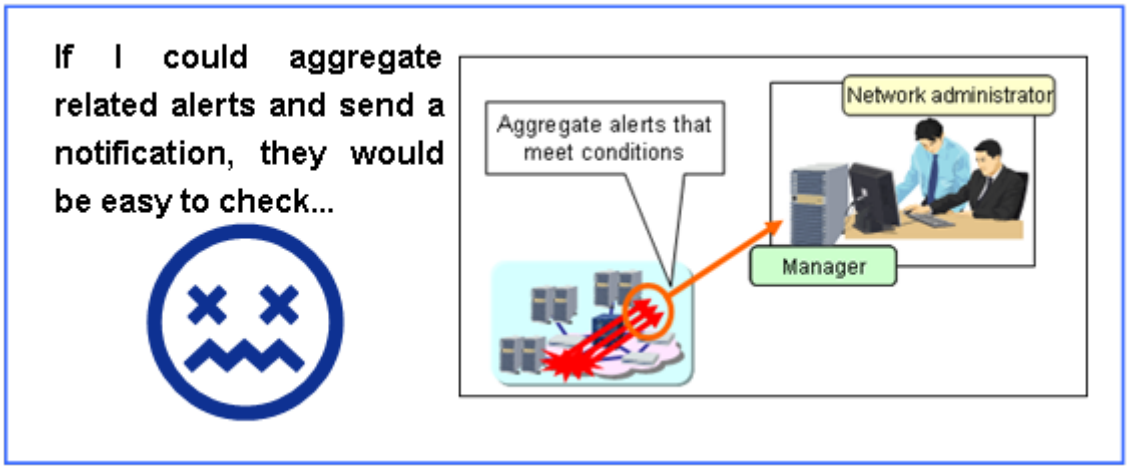
   b. Double-click the selected row.

   c. You can check the failure details and report status in the displayed Report Detail dialog box.



3.3.5 Configuring settings for aggregating alert information

The same events may occur many times in a network fault, or the interface may repeatedly go up and down due to a bad interface connection with the device. In such cases, you can aggregate the alerts that occurred during a specified interval and send only one notification.



To aggregate alert information, the following information needs to be prepared in advance.

- Description of alerts to be aggregated
- Conditions for aggregating alerts

All the settings are configured in the manager.

1. Create a file that defines aggregation conditions.

   Specify the description of alerts that you want to aggregate, into "Summary" and "Detail".

   As an example, we aggregate interface up/down alerts that have occurred for over one minute or ten times for each device name and ifIndex value.

```
[Alert Analyzer]
Component=*
Summary=link(up|Down)
Detail=Interface <ifindex> was link-(up|down).
Priority=10
TimeRange=60
NumberRange=10
Mode=1
ShowFirstAlert=0
CorrelationSummary=
CorrelationDetail=
CorrelationSeverity=3
```

   Tip

   - The directory storing a file of aggregation conditions stores sample files (interfaceUpDown.def, etc.) You can create definitions, referring to these sample files.
   - You can use regular expressions in aggregation conditions and set conditions with flexibility.

   For details, refer to "4.13 Controlling Alerts (Aggregating, Discarding, and Converting Contents) (page 302)".

2. Store the created definition file for aggregation conditions in the location below.

   <On the manager, %sharedfolder%>`\Manager\sg\NvPRO\NVWORK\public\exdll\correlation`

3. To reflect aggregation conditions, execute the `NvPROReloadDllMgr` command.

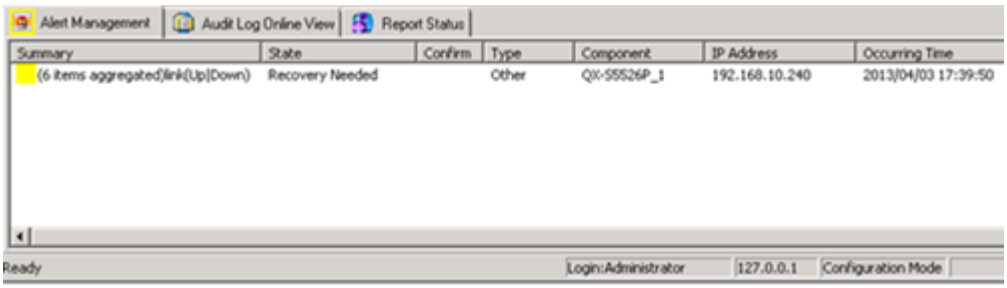
   You can dynamically reflect aggregation conditions without stopping Network Manager processes.

   - For Windows:

```
> cd "C:\Program Files (x86)\NEC\UMF\Operations\Manager\bin"
> NvPROReloadDllMgr
exdll nvalanlz.dll reload succeeded
exdll NvPROAlertConvKnowledgeAPI.dll reload succeeded
exdll NvPROTrapCmdAPI.dll reload succeeded
exdll NvPROAlertAnalyzerAPI.dll reload succeeded
```

4. When alerts that match aggregation conditions are generated, confirm that the alerts are aggregated in accordance with the aggregation conditions.

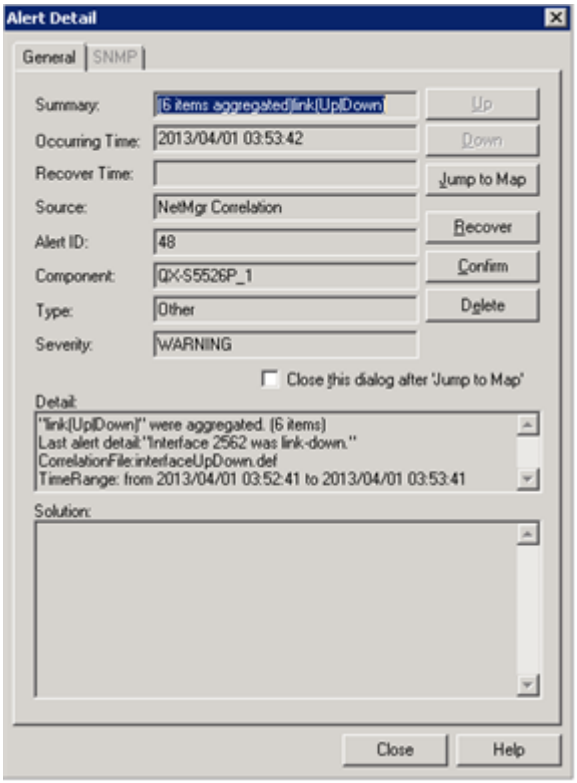
   a. Select the **Alert Management** tab.



Aggregated alerts (one alert for consecutive link ups/downs) is displayed.

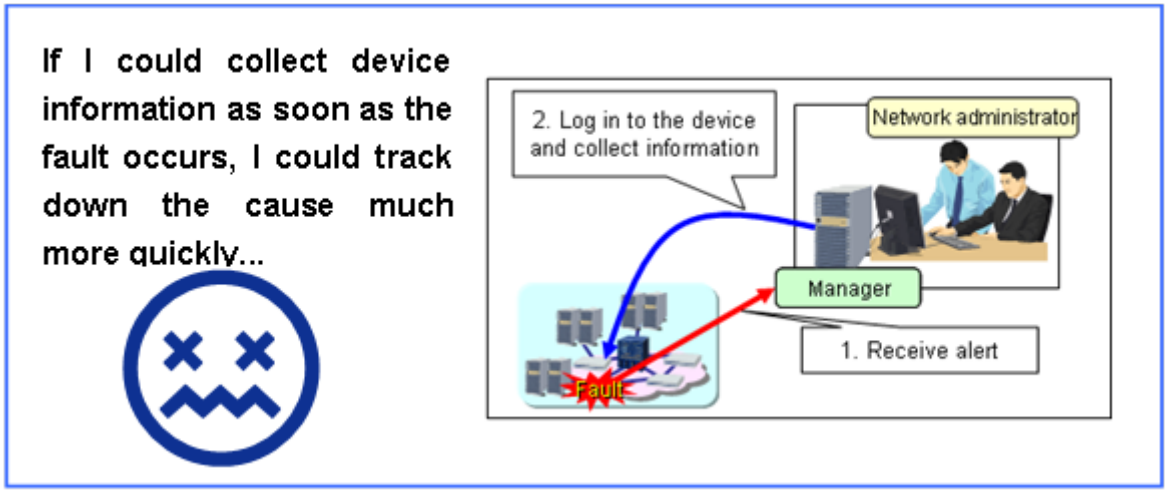
b. Double-click the aggregated alert.

In the ifIndex=2562 interface for the device "QX-S5526P_1", you can see that six up/down alerts occurred and were aggregated.



3.3.6 Automatically collecting device information when an alert is detected

You can set the receipt of an SNMP trap to trigger a telnet or ssh login to the source device and collect device information. This addresses the difficulty in making an assessment on the received alert information alone by automatically collecting information and speeding up assessment of the fault cause.



3.3.6.1 Executing device commands and collecting information when an SNMP trap is received

This section describes how to set the receipt of an SNMP trap as a trigger to perform a telnet or ssh login to a device and collect device information.

To execute device commands and collect information when an SNMP trap is received, you first need to register login information.

1. Create a definition file for executing commands.

```
Enterprise: 1.3.6.1.4.1.119.1.84
GenericCode: 6
SpecificCode: 13
Component: IX-2015
ActionCmd: terminal length 0
ActionCmd: show tech-support
ActionInterruptTm: 3600
```

Set the SNMP trap information and the command to be executed when the SNMP trap is received.

Tip

The sample file (TrapCmd.sample) is stored in the directory containing the definition file. Create the definition using this sample file (TrapCmd.sample) as a reference.

For further information regarding the definition file, refer to "4.15 Settings for Executing Device Commands When Alerts Occur (page 333)".

2. Store the created definition file as "*any_name*.def" in the location below.

   <On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\public\exdll\TRAPCMD\

3. To reflect the contents of the definition file, execute the `NvPROReloadDllMgr` command.

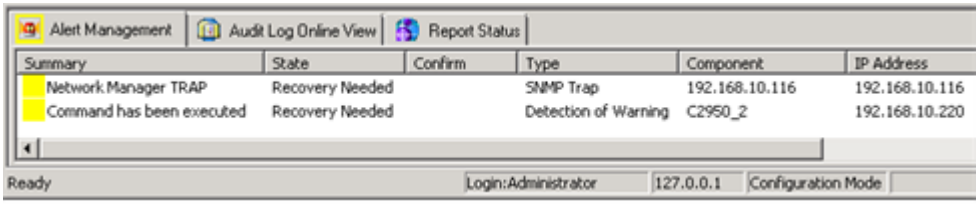
   You can dynamically reflect settings without stopping Network Manager processes.

   - For Windows:

```
> cd "C:\Program Files (x86)\NEC\UMF\Operations\Manager\bin"
> NvPROReloadDllMgr
exdll nvalanlz.dll reload succeeded
exdll NvPROAlertConvKnowledgeAPI.dll reload succeeded
exdll NvPROTrapCmdAPI.dll reload succeeded
exdll NvPROAlertAnalyzerAPI.dll reload succeeded
```

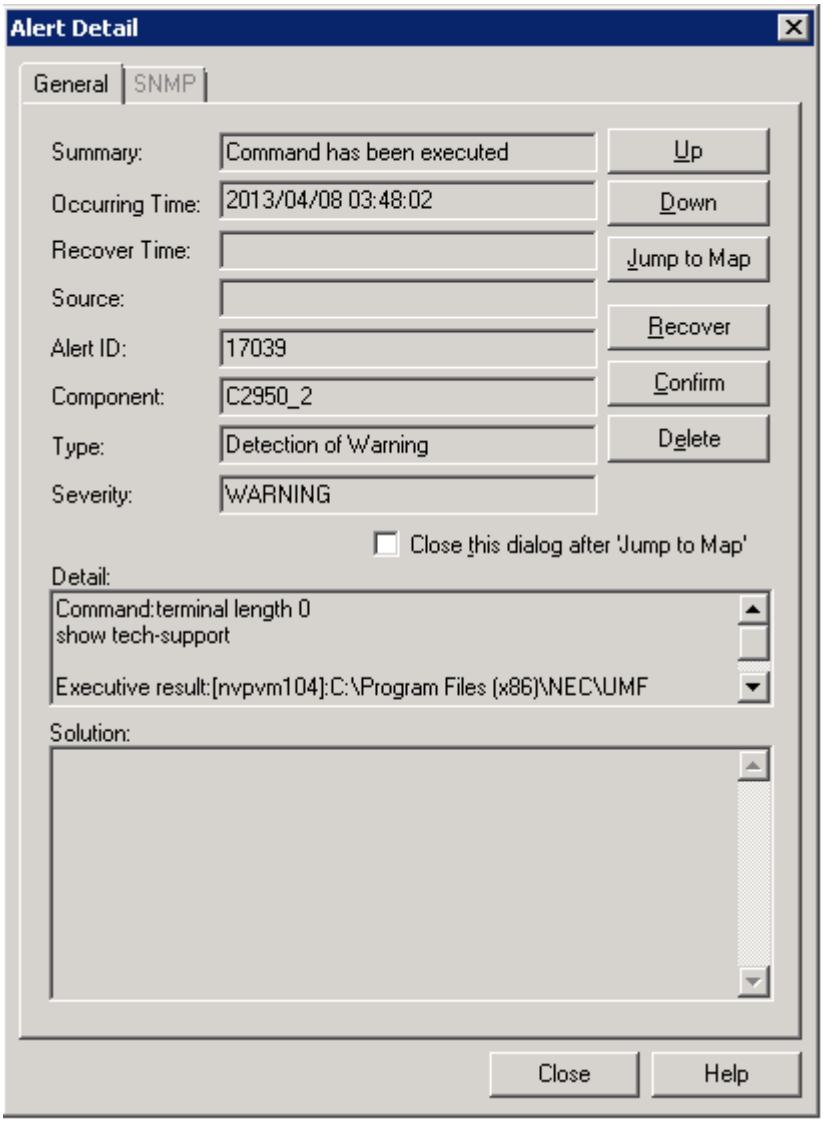
4. Execution of the device command results in a notification of the alert information.

   a. Select the **Alert Management** tab.



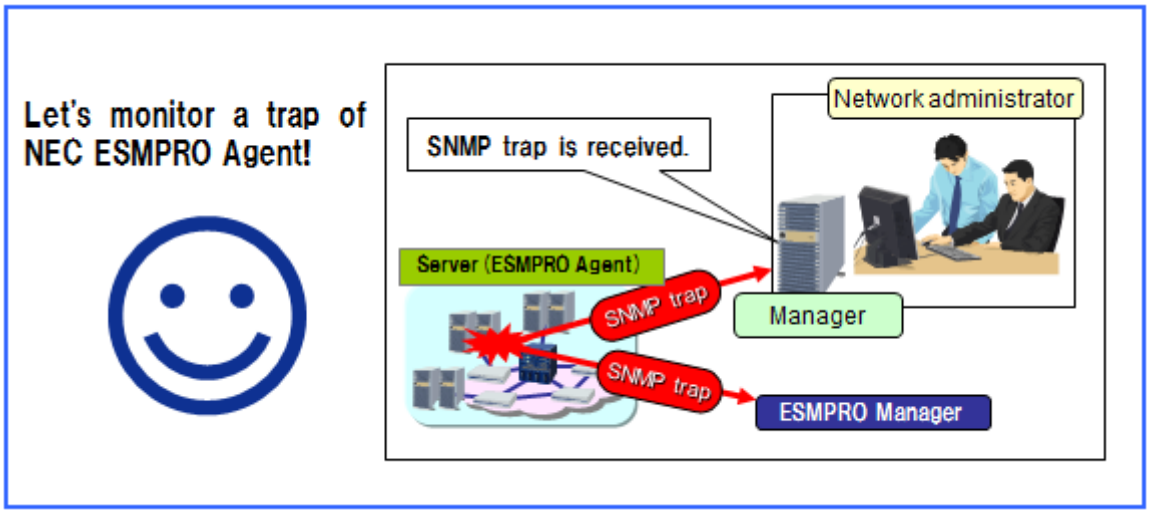
   b. Double-click the alert that is displayed as "`Command has been executed`" in the **Summary** column.

   In the Alert Detail dialog box, check the device command and save destination of the execution result, and confirm that the command was executed as specified.



3.3.7 Configure the setting to manage NEC ESMPRO Agent

This setting enables the manager to receive SNMP traps sent from NEC ESMPRO Agent, and unify monitoring of faults of server and network at one view.



To receive SNMP traps of NEC ESMPRO Agent by Network Manager, confirm the following.

- When both Network Manager and NEC ESMPRO Manager are installed into the same server, SNMP trap reception port (162/udp) conflicts. To avoid this conflict, the settings should be changed so that NEC ESMPRO Manager and Network Manager would use Windows SNMP Trap Service, respectively.

  For details, refer to "11.4.1 Using the Windows SNMP Trap service (page 776)".
- In the list of trap notification destination of NEC ESMPRO Agent, the destination address of SNMP traps should be set to IP address of Network Manager.
- The monitoring mode of the target server icon should be set to ON.

1. Create a file of alert notification management conditions supporting NEC ESMPRO Agent.

   Sample files of definitions to specify management conditions are stored in the following folders.

   <On the manager, %sharedfolder%>`\Manager\sg\NvPRO\NVWORK\public\exdll\correlation\`

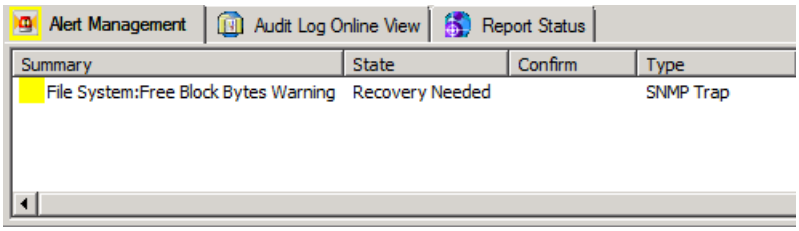
   - `ESM_MAJOR.def.sample`
   - `ESM_MINOR.def.sample`
   - `ESM_NORMAL.def.sample`
   - `ESM_UNKNOWN.def.sample`

   For details, refer to "4.13.4 Control condition sample files (page 308)".
2. Change names of these files to "*any_name*.def", and store them in the above folders.

   Control conditions parameters in the saved definition files do not need to be changed in principle, but only if the value of "Priority" conflicts with other definition, it should be changed.
3. Execute `NvPROReloadDllMgr` command, to reflect description of definition file.
   - For Windows:

```
> cd "C:\Program Files (x86)\NEC\UMF\Operations\Manager\bin"
> NvPROReloadDllMgr
exdll nvalanlz.dll reload succeeded
exdll NvPROAlertConvKnowledgeAPI.dll reload succeeded
exdll NvPROTrapCmdAPI.dll reload succeeded
exdll NvPROAlertAnalyzerAPI.dll reload succeeded
```

4. Generate an SNMP trap such as "File System:Free Block Bytes Warning" etc. from NEC ESMPRO Agent, and confirm that it is notified in **Alert Management** tab.



Tip

If you register the path/URL of NEC ESMPRO Manager management view in the server device icon properties, you can start NEC ESMPRO Manager view from the right-click menu of the server icon. This setting helps you to start NEC ESMPRO Manager quickly when a fault occurs.

For settings to start NEC ESMPRO Manager from a server icon, refer to "4.5 Registering Device-Specific Tools (page 204)".

3.4 Configuration: Collecting Performance Information

In Network Manager, you can check the network performance using two methods, MIB collection and sFlow analysis.

- "MIB collection (page 68)"

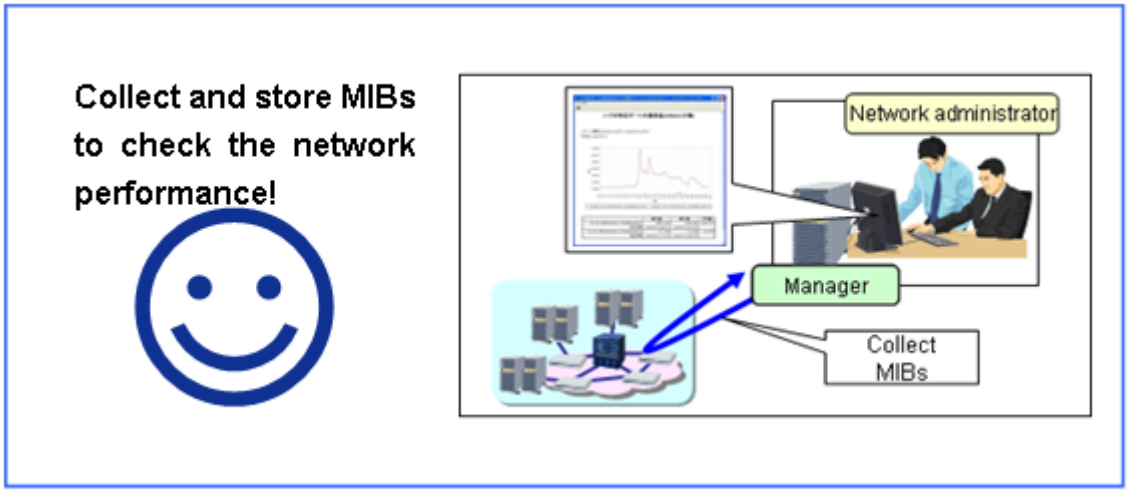
  You can check the performance status of devices from IN/OUT traffic volumes for each interface, and from a range of retained counter information based on specific device types.

- "sFlow analysis (page 72)"

  You can analyze network traffic information for each protocol, IP address, and service port.

3.4.1 Configuring settings to collect and store MIB information

You can collect IN/OUT traffic volumes for each device interface and counter information for specific device types from the MIB, and display the performance status of the network in a graph. Additionally, by setting monitoring threshold, you can be aware of problems because an alert is issued when load exceeds a certain amount.



This section describes how to collect performance information from the MIB by using the "Traffic of the specific hub port (64bit)" rule.

Tip

For details, refer to the following:

- "4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices (page 334)"
- "7.2 Data Collection Rules (page 622)"

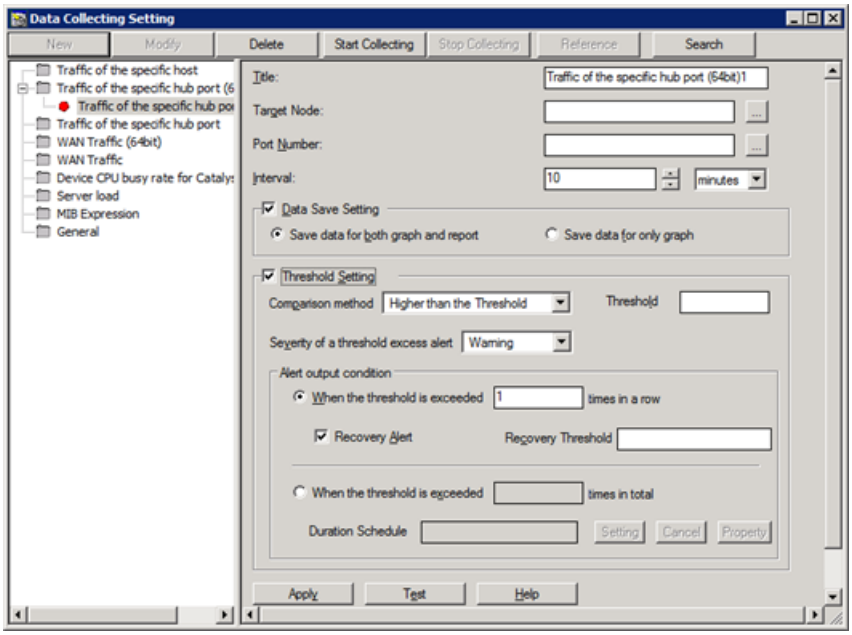
The following information needs to be registered in the icon properties for the device from which information is being collected.

- IPv4 address or IPv6 address
- SNMP community name (get) or SNMPv3 information

You must first change to the "configuration mode (page 27)".

1. Open the "4.16.1 Data Collecting Setting window (page 334)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.



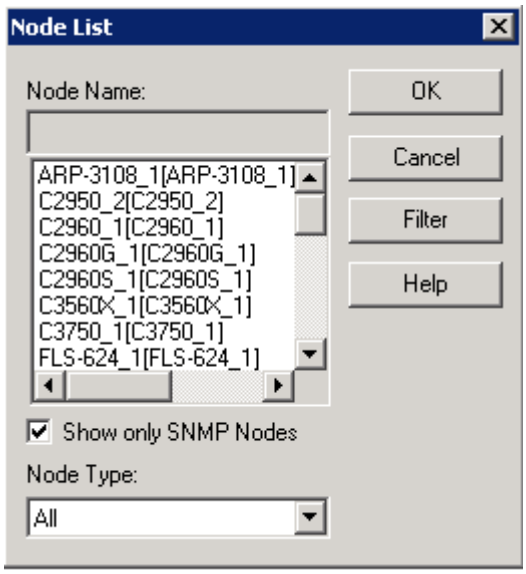
2. Select **Traffic of the specific hub port (64bit)** and click **New** button.
3. Set up each parameter.

- **Title**

  Enter the title name. The text specified in hear is registered below **Traffic of the specific hub port (64bit)** in the tree view.

- **Target Node**

  You can select a node from the list.



Tip

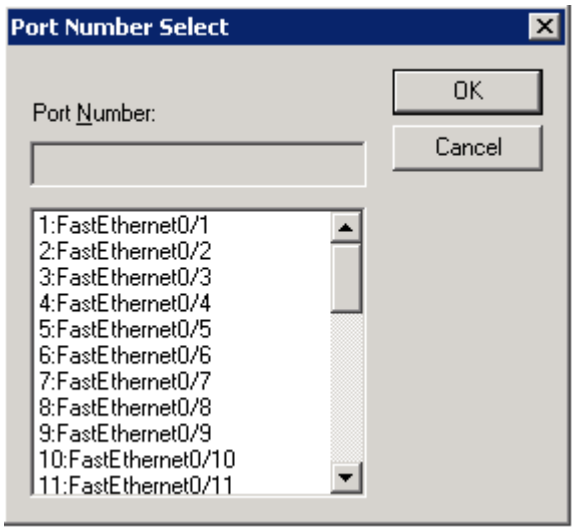
You can specify a group name. If you specify a group as the target of the data collection rules, when new device icon is added, you make the device belong to the target group in order to start the collecting. Change of the monitoring setting is not needed.

To belong the device to a group, specify a group name to the **Group** in the icon properties of the device. For details, refer to the following.

- "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)"
- "6.2.1.7 **Group List** menu (page 568)"
- "6.2.1.8 **Group Member List** menu (page 569)"

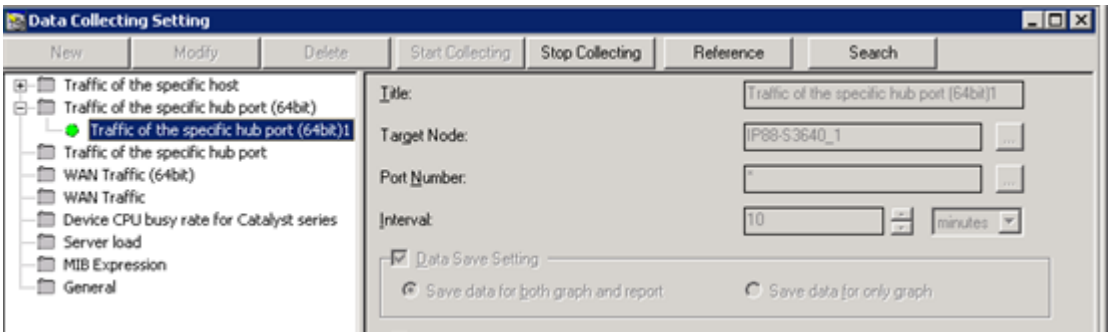
- **Port Number**

  If there is one **Target Node**, you can select the port number targeted for collection in the Port Number Select dialog box.



When setting up rules to collect the traffic volumes for each interface, such as the "Traffic of the specific hub port (64bit)" rule, if you specify a single-byte asterisk (*) in the **Port Number** box, data is collected for the ifIndex specified in Interface Property dialog box or the **Default Target Port** in the icon properties. To configure collection settings for many devices, it is recommended to set up a default port.

4. Click **Test** button and confirm that the MIB can be retrieved.
5. Click **Apply** button to save the settings.
6. Click **Start Collecting** button to start to collect data.



Confirm that data collection has started by checking that the color of the icon for the set entry changes from red to green.

7. After collection starts, check that the collected data is being written to the CSV file.

   The CSV file is stored at the location below.

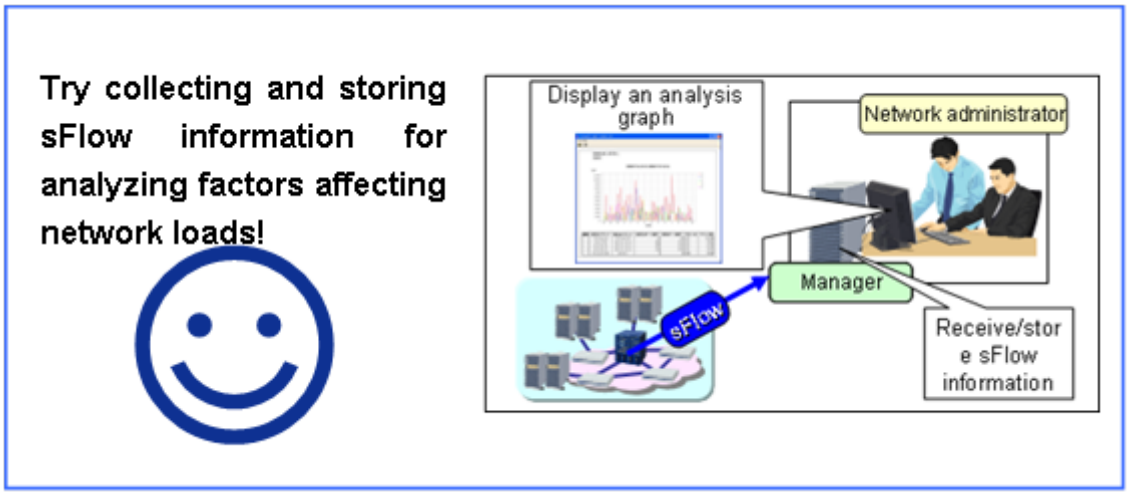
   `<On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\data\report\logdata\collection_entry_name\node_name\YYYY\MM\DD.csv`

   - *YYYY*: Year
   - *MM*: Month
   - *DD*: Day

   If **Save data for only graph** has been selected, you can confirm that collection has been performed by checking the graph display.

3.4.2 Configuring settings to collect traffic flow information

You can analyze network traffic information for each protocol, IP address, and service port by collecting and storing sFlow information.



This section describes the settings required to receive sFlow information.

Tip

For details, refer to the following.

- "4.17.1 Registering sFlow agents (page 373)"
- "4.17.3 Setting duration of flow data retention (page 376)"

Confirm that the following conditions are satisfied on the collection target device.

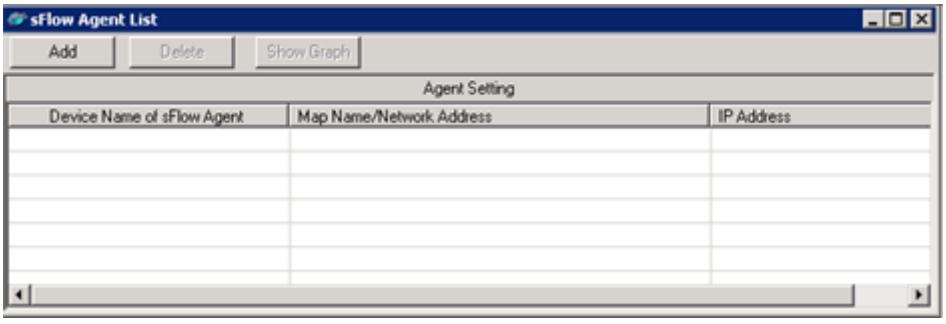
- sFlow version 4 or 5 is supported.
- The IP address for the manager has been set up as the send destination for sFlow packets.

If the manager has been set up so that the external database would be used, you need to configure sFlowDB. For details of configuring of sFlowDB, refer to the setup guide for OS: Using External database - Configuring the Databases - sFlow database settings.

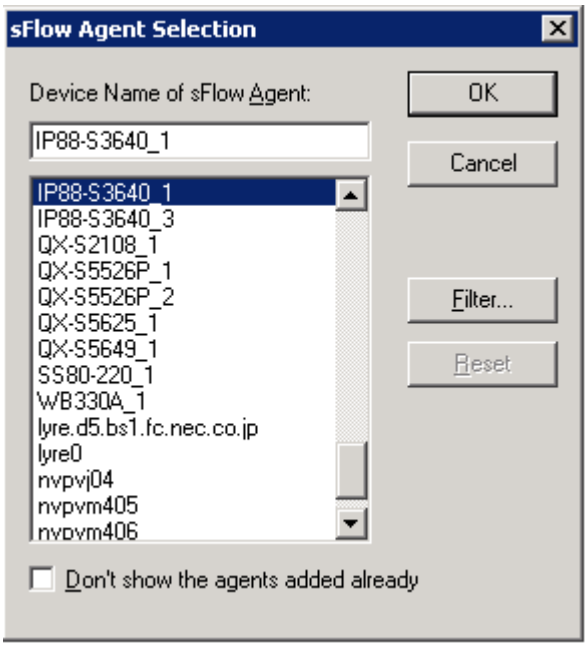
You must first change to the "configuration mode (page 27)".

1. Open the sFlow Agent List window.

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**sFlow Setting**>**sFlow Agent List**.

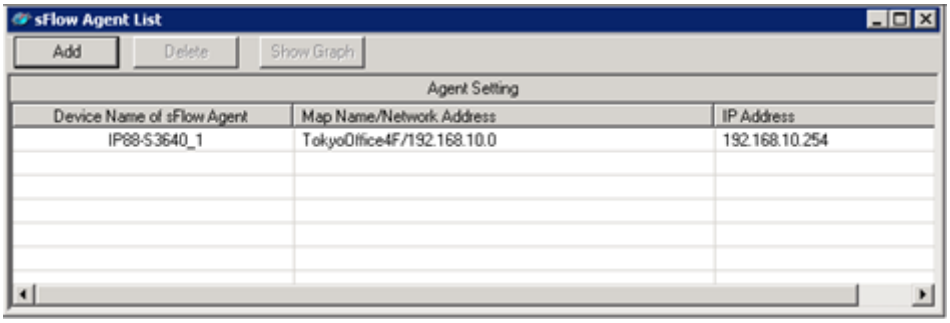


2. Click **Add** button to open the sFlow Agent Selection dialog box.
3. Select the device and click **OK** button.



A maximum of 10 sFlow agents can be registered. For sFlow agents, it is recommend to register devices located in the center of the communication path that the traffic flows through.

4. Confirm that the device names registered as sFlow agents are displayed in the **sFlow Agent List** window.

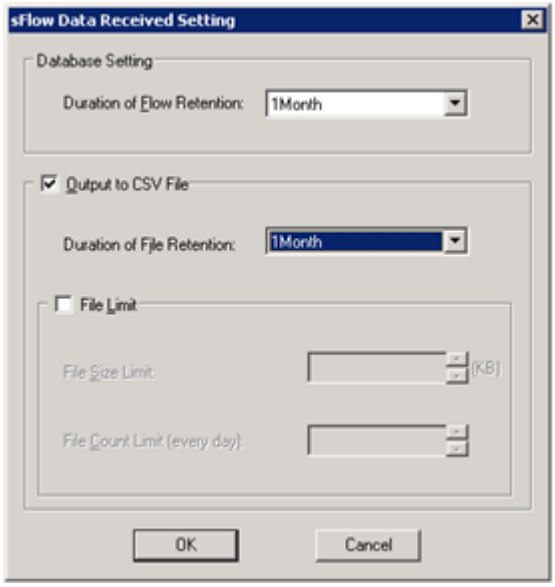


5. Check the CSV file entries to confirm that sFlow packets have been received and stored.

   a. Open the sFlow Data Received Setting dialog box.

      Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**sFlow Setting**>**sFlow Data Setting**.

   b. Check the **Output to CSV File** to output CSV files of sFlow information.



The CSV file is stored at the location below.

<On the manager, %sharedfolder%>\Manager\sg\NvPRO\SFlowCollector\work\dat*sFlow_agent_name**YYYY**MM*\FLA_*DD*.csv

- *YYYY* : Year
- *MM* : Month
- *DD* : Day

In system operation, if you do not need to output to a CSV file, deselect **Output to CSV File** in the sFlow Data Received Setting dialog box.

3.5 Operations: Managing Faults

3.5.1 Checking fault locations and details

When a fault is detected, the color of the corresponding node icon in the tree view and Map View and the color of the map icon at the parent level change to reflect the importance of the fault.

In addition, information regarding the fault is displayed in the list in the Alert Management window.

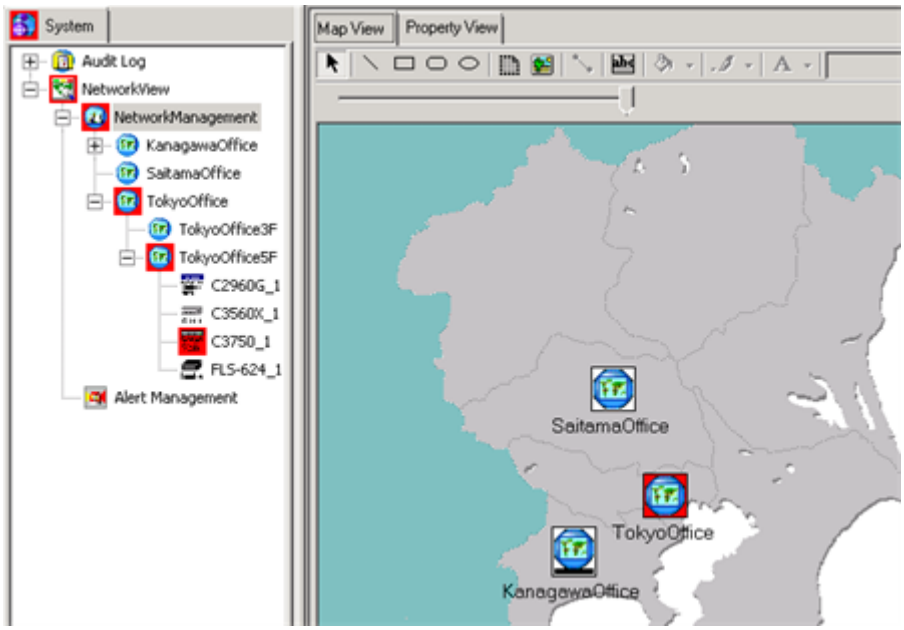
This section describes how to verify the location and details of a fault from the Map View.

Tip

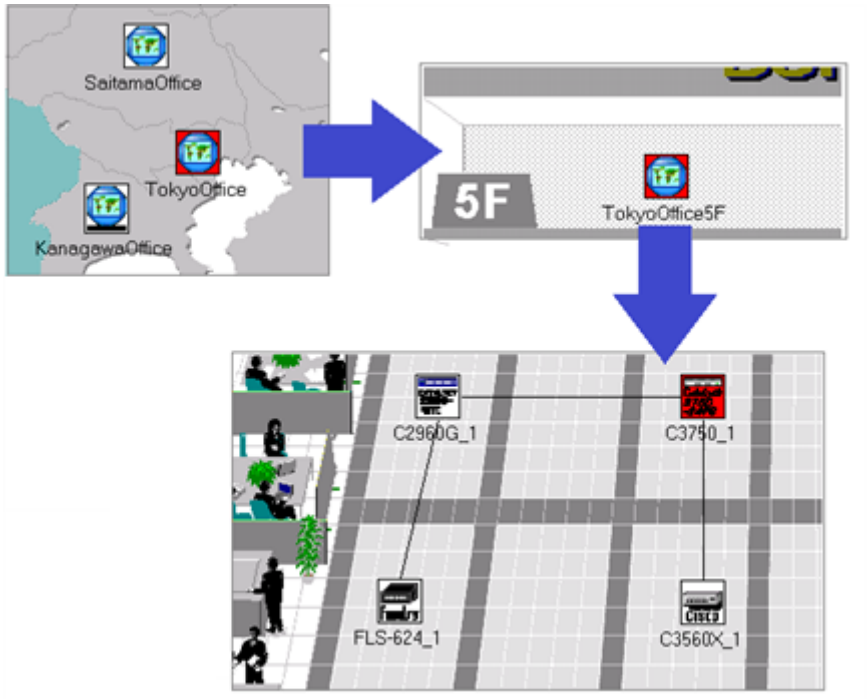
For instructions on checking the alert list, refer to "5.1.4 Managing alerts (page 456)".

Register the monitored device and configure the monitoring settings in advance.

1. When a fault is detected, the color of the map icon that includes the correspoinding device icon changes in the **NetworkManagement** tree and the Map View.

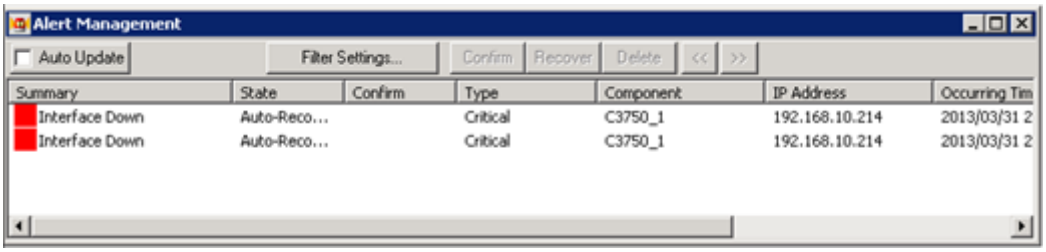


2. Double-click the map icon and drill down to find the specific location of the fault.



3. Right-click the device that has experienced a fault and select **Fault Management>Show Unrecovered Alert**.

   Unrecovered alerts for the selected device are displayed in the Alert Management window.

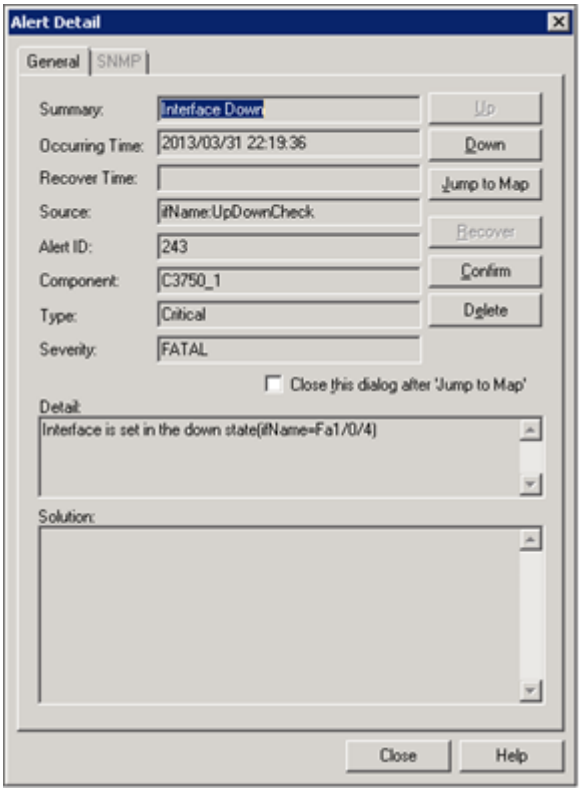


Tip

Use the **Filter Settings** dialog bar to combine conditions and quickly bring up specific alerts.

4. Double-click the alert.

   Alert Detail dialog box is displayed.



Tip

To check the Map View again, click **Jump to Map** button in the Alert Detail dialog box.

The map, to which the device with a fault is registered, is displayed.

3.5.2 Displaying alerts for specific devices only

In the Alert Management window, you can check current alerts that are occurring (unrecovered alerts), and the alerts that have previously occurred for specific devices.

This section describes how to use **Filter Settings** in the Alert Management window.

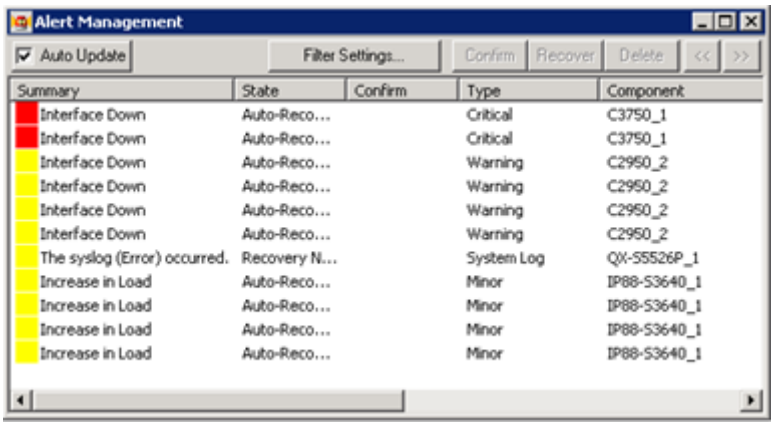
Tip

For setting of a filter, refer to the following:

- "5.1.4.1 Filter Settings dialog bar (page 459)"
- "5.1.4.2 Specifying wildcards (page 460)"

1. Open the Alert Management window.

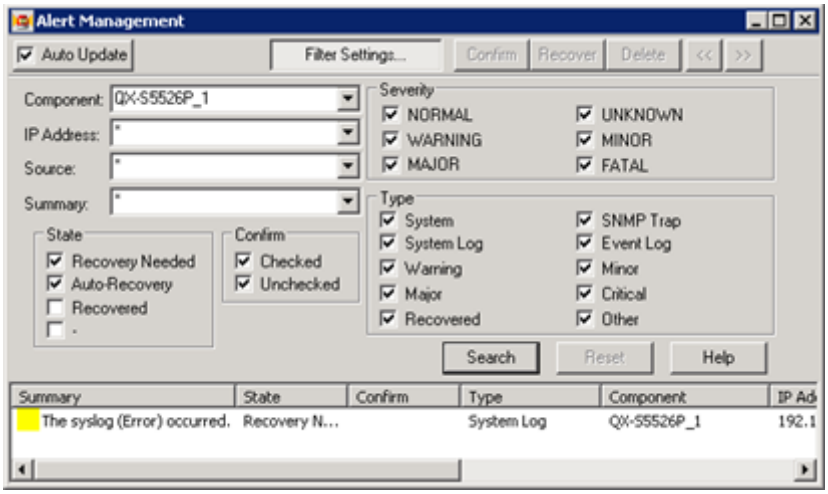
   In the tree view, double-click the **Alert Management** icon.



2. Click **Filter Settings** button.

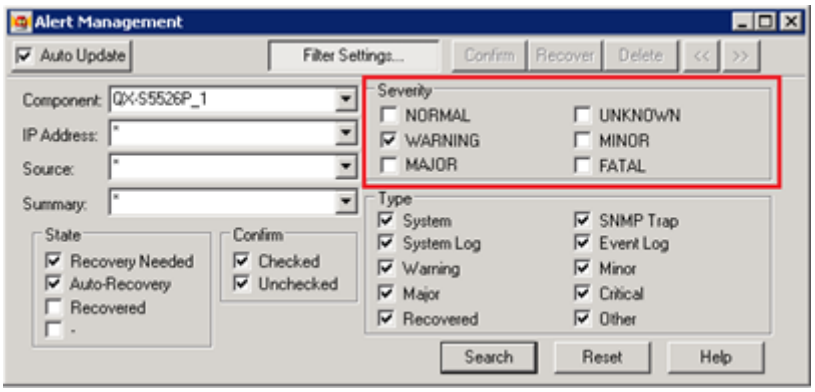
   The dialog bar is displayed.

3. In the Filter Settings dialog bar, enter the **Component** (node name) and click **Search** button.



   Use the Filter Settings dialog bar to combine conditions and quickly bring up specific alerts.

4. If you want to refine the search further and display only alerts with a severity level of fatal, deselect the other severity level options.

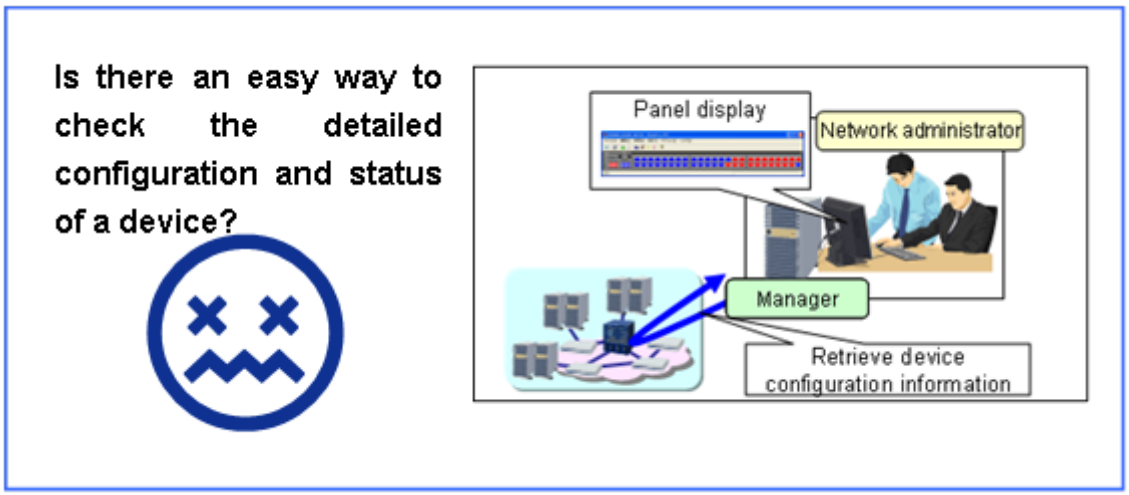


   Only the specified components with a severity level of fatal are displayed.

3.5.3 Checking the detailed status of a device on the front panel display

You can look up detailed configuration information for devices by performing a telnet login to the device and executing a command. However, if logging in to devices is restricted for security purposes, configuration information cannot easily be looked up.

In Network Manager, you can easily check device configuration information through window operations, without logging in to devices.



Tip

For details regarding the panel display, refer to "5.9 Displaying Device Front Panels (page 475)".

Confirm that Network Manager can perform SNMP communication with devices displayed in the front panel.

Node Manager (NM) license must be assigned to the devices.

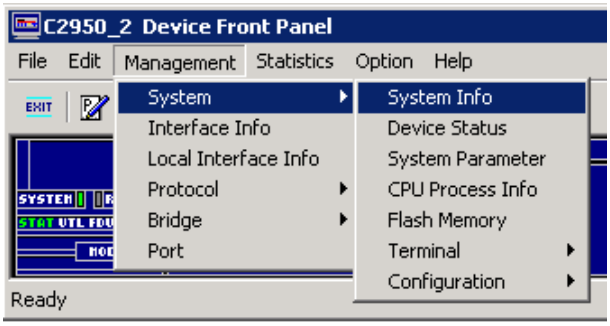
In the icon properties for the device, confirm that the **Device Front Panel** has been set up correctly.

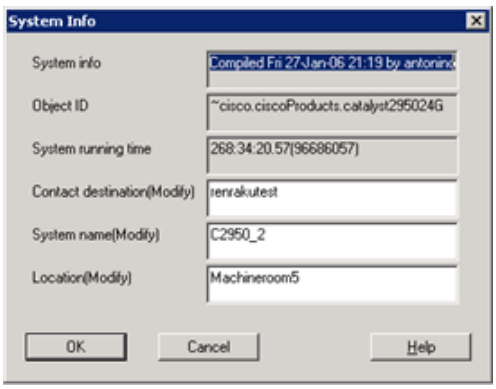
1. Open the Device Front Panel window.

   Right-click the device icon and select **Device Front Panel** menu.

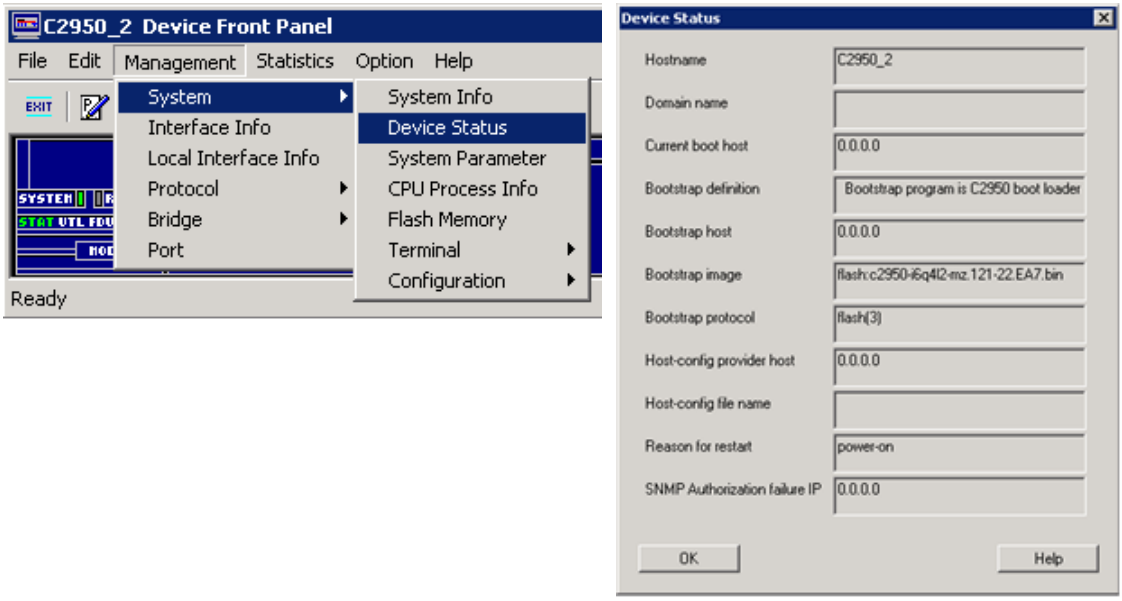
2. Select desired information menu under the the panel window menu **Management**>**System**.

   - Example 1 : **Management**>**System**>**System Info**





   - Example 2 : **Management**>**System**>**Device Status**



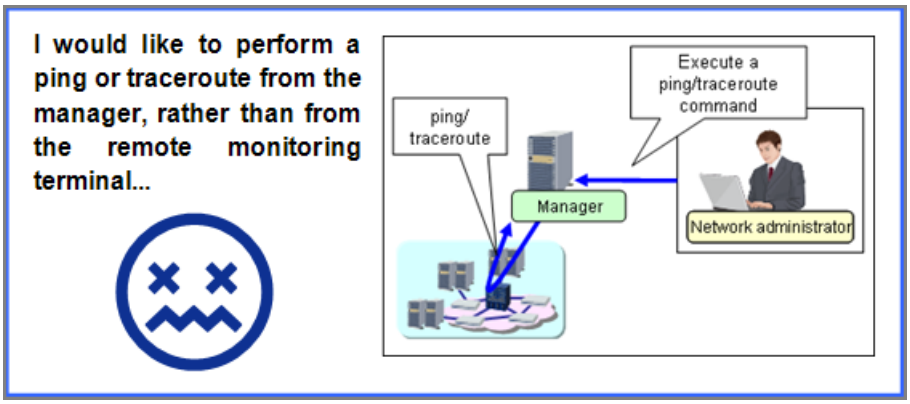
Tip

You can customize the general purpose panel by editing the front panel image and customizing the menu list.

You can also check the statistical information for each interface.

3.5.4 Checking communication and the communication path

You can check communication reachability and the communication path between the manager and monitored devices by executing a ping command or traceroute command from the manager.



3.5.4.1 Executing a ping command

You can check whether TCP/IP communication is currently possible with a specified device by executing a ping command from the manager.

Tip

For details, refer to "5.5.1 Executing a ping command (page 468)".

To perform this operation, the logged in user must belong to a group that has operation authority.

The IPv4 address or IPv6 address must be registered in the icon properties for the target device.

1. Execute in one of the following ways.
   - Check the reachability via IPv4 communication:

Right-click the target device icon and select **Fault Management**>**Ping (IPv4)**.

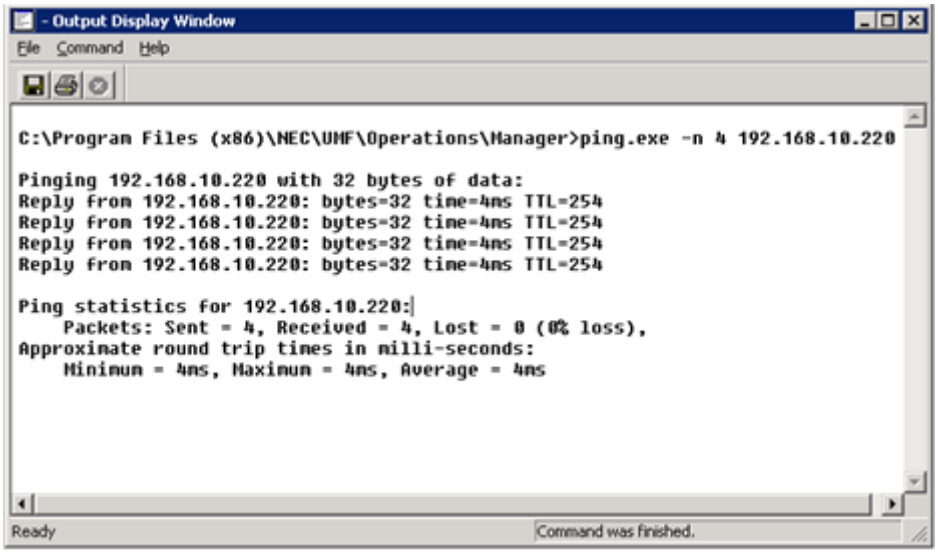
Only select this menu for devices that have an IPv4 address information registered in the device icon properties.

- Check the reachability via IPv6 communication:

  Right-click the target device icon and select **Fault Management**>**Ping (IPv6)**.

  Only select this menu for devices that have an IPv6 address information registered in the device icon properties.

2. The execution result for the ping command is displayed in the Output Display Window window.



3.5.4.2 Executing a traceroute command

You can check the communication path to a specified device by executing a traceroute command from the manager.

Tip

For details, refer to "5.5.2 Executing a traceroute command (page 468)".

To perform this operation, the logged in user must belong to a group that has operation authority.

The IPv4 address or IPv6 address must be registered in the properties for the target device.

1. Execute in one of the following ways.

   - Check path via IPv4 communication:

     Right-click the target device icon and select **Fault Management**>**Trace Route (IPv4)**.

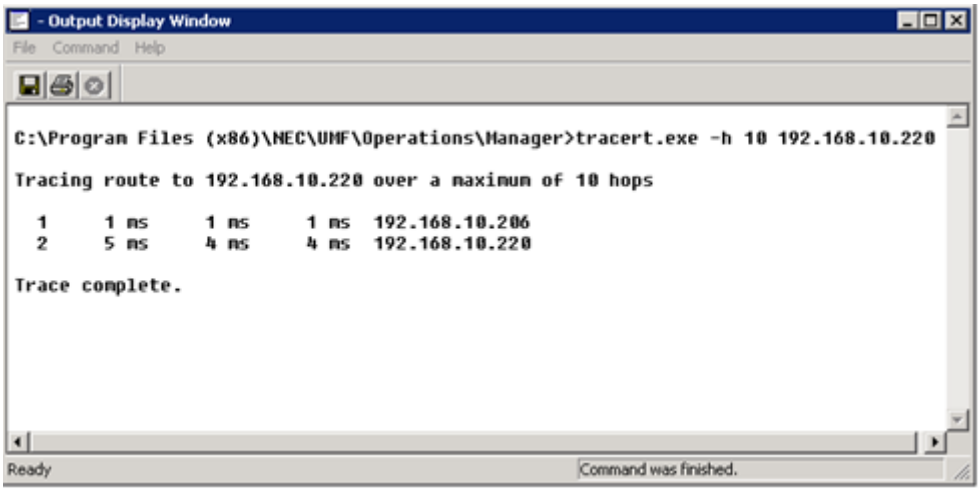
     Only select this menu for devices that have an IPv4 address information registered in the device icon properties.

   - Check path via IPv6 communication:

     Right-click the target device icon and select **Fault Management**>**Trace Route (IPv6)**.

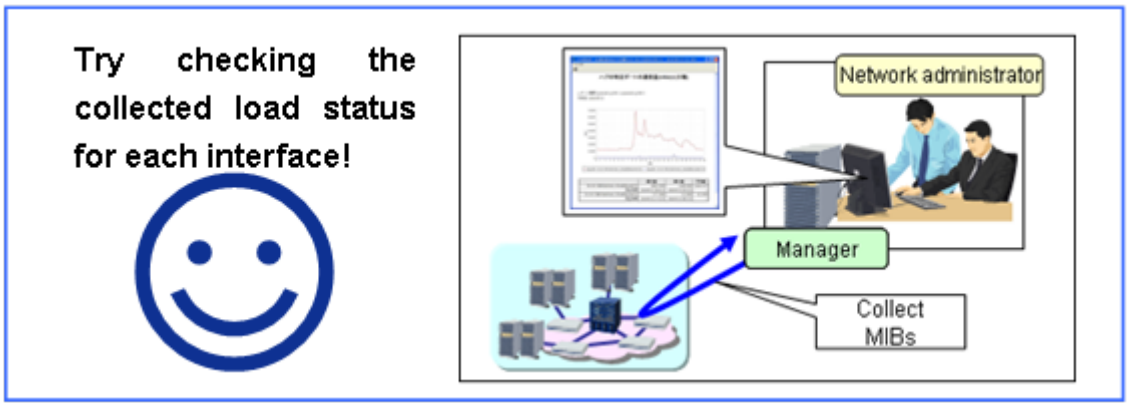
     Only select this menu for devices that have an IPv6 address information registered in the device icon properties.

2. The execution result for the traceroute command is displayed in theOutput Display Window window.



3.6 Operations: Checking Performance Information

3.6.1 Checking the load status for each interface



In advance, configure any of the data collection rules below and start data collection.

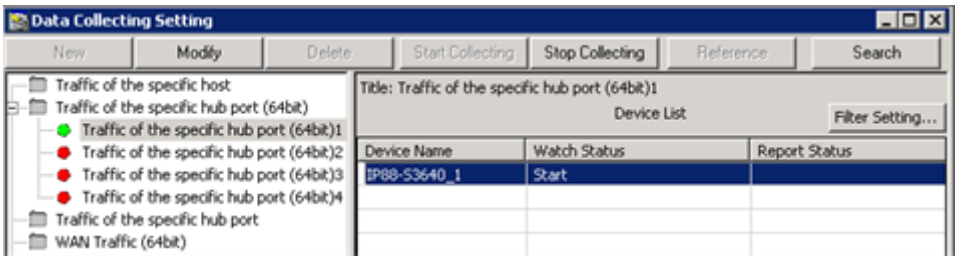
- Traffic of the specific hub port (64-bit)
- Traffic of the specific hub port
- WAN Traffic (64-bit)
- WAN Traffic

For data collecting, refer to "3.4.1 Configuring settings to collect and store MIB information (page 68)".

1. Open the "4.16.1 Data Collecting Setting window (page 334)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.

2. In the tree view, select the entry name.

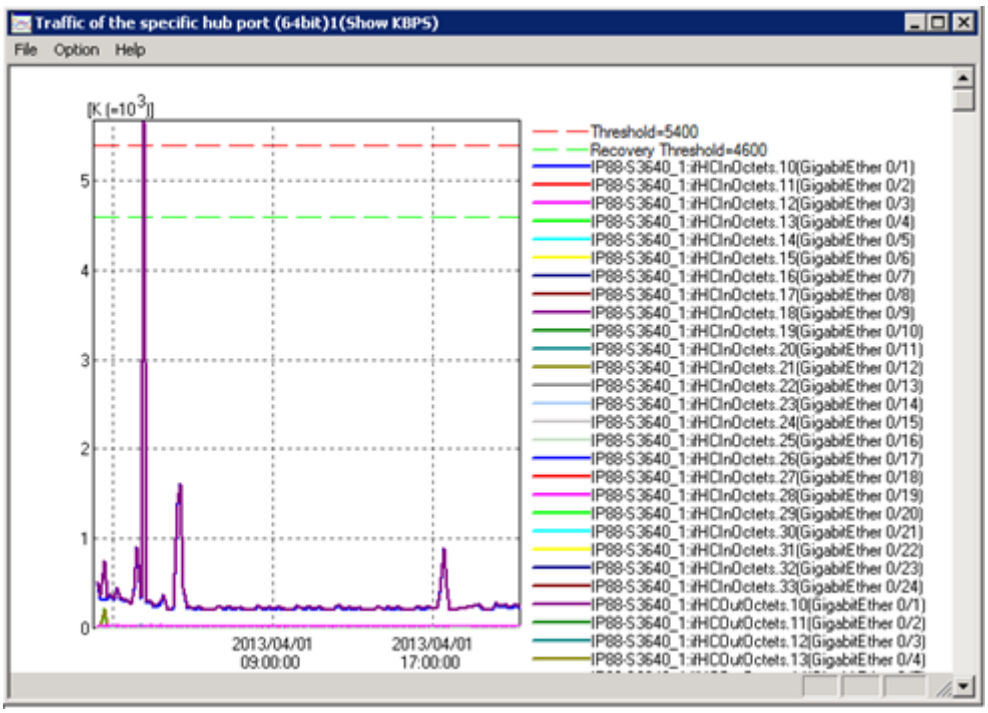


The Device List pane and Report List pane are displayed.

3. Open the graph display.

   In the Device List pane, right-click the row of the target node and select **Graph Display** menu.

   In the graph display, you can check the information that has been collected from 0 o'clock that day until the current moment.

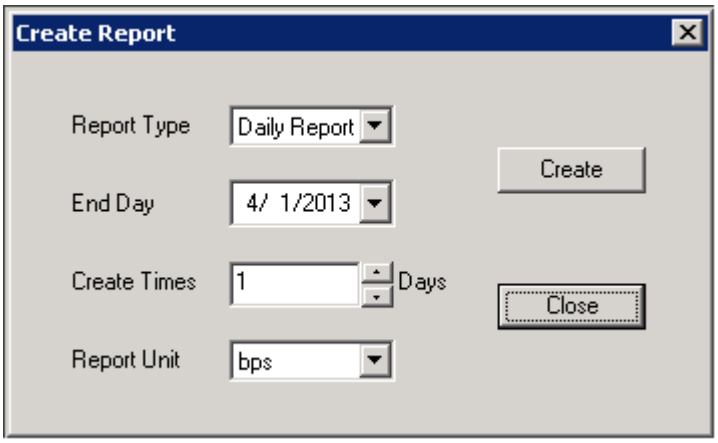


For details, refer to "5.11.1 Displaying a graph (page 486)".

4. Open the report.

   a. In the Device List pane, right-click the row of the target node and select **Report Create** menu.

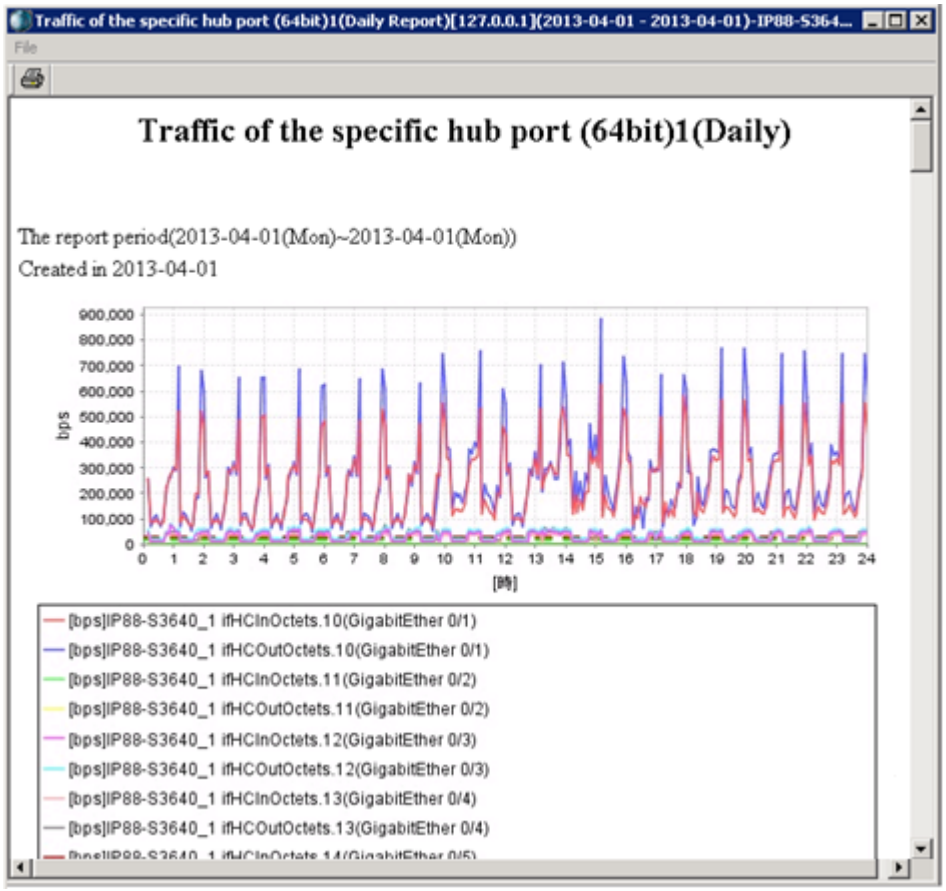
   b. Specify the period of the report in the Create Report dialog box.



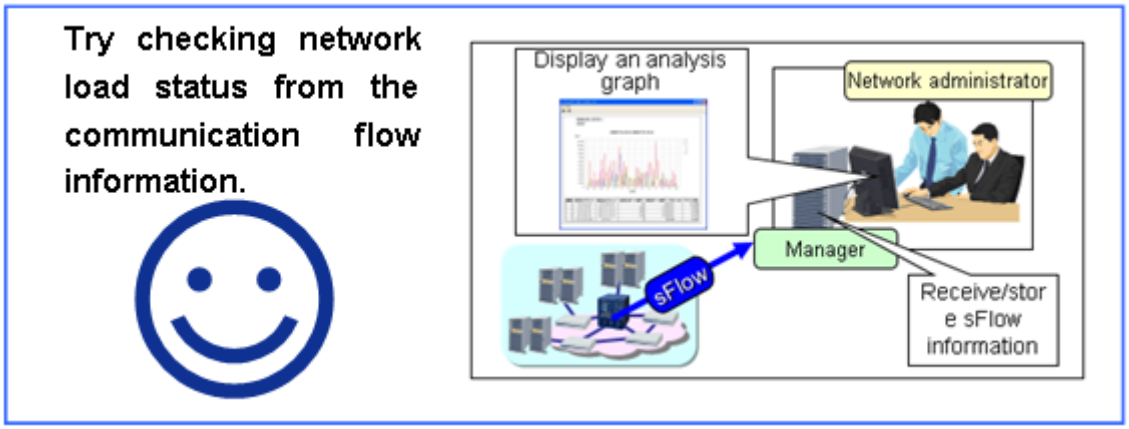
You can specify the past information.

c. Click **Create** button.

d. In the Report List pane, right-click the row of the target report and select **Report Display** menu.



3.6.2 Checking network load status from the traffic flow information



Tip

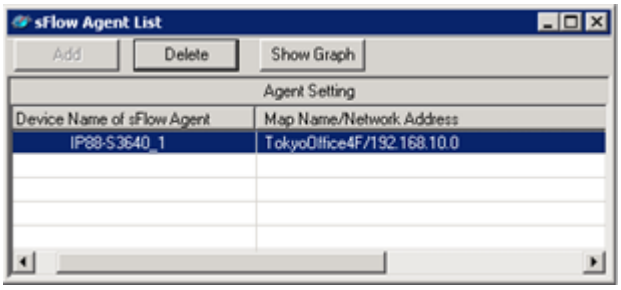
For details, refer to the following:

- "5.12.1 Graph display of traffic-flow information from sFlow (page 500)"
- "5.12.2 sFlow graph structure (page 502)"

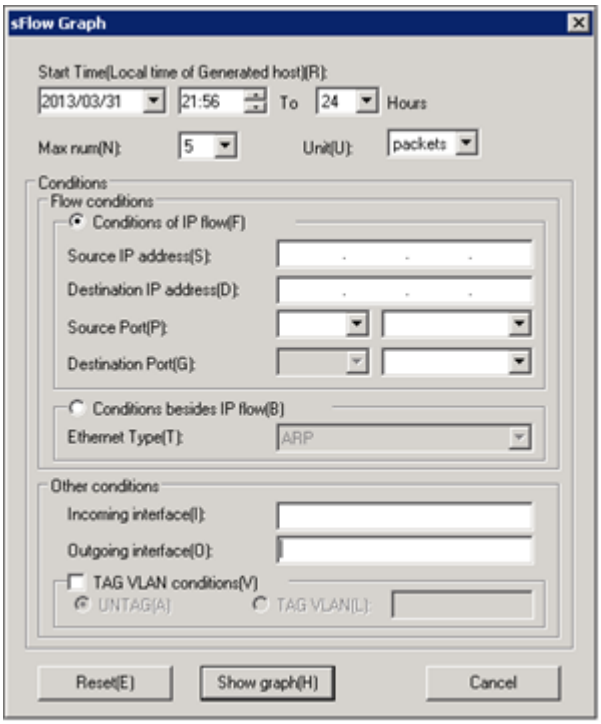
You need to register the sFlow agent for collecting and storing sFlow information in advance.

1. Open the sFlow Agent List window.

   Right-click **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**sFlow Setting**>**sFlow Agent List**.



2. In the list, select the sFlow agent and click **Show Graph** button.
3. In the sFlow Graph dialog box, specify conditions for displaying the traffic flow.



- **Start Time**

  Specify the time that you want to view.

- **Max num**

  Specify the maximum number of traffic flow entries to display.

- **Flow conditions**

  Specify the traffic flow conditions that you want to check.

Tip

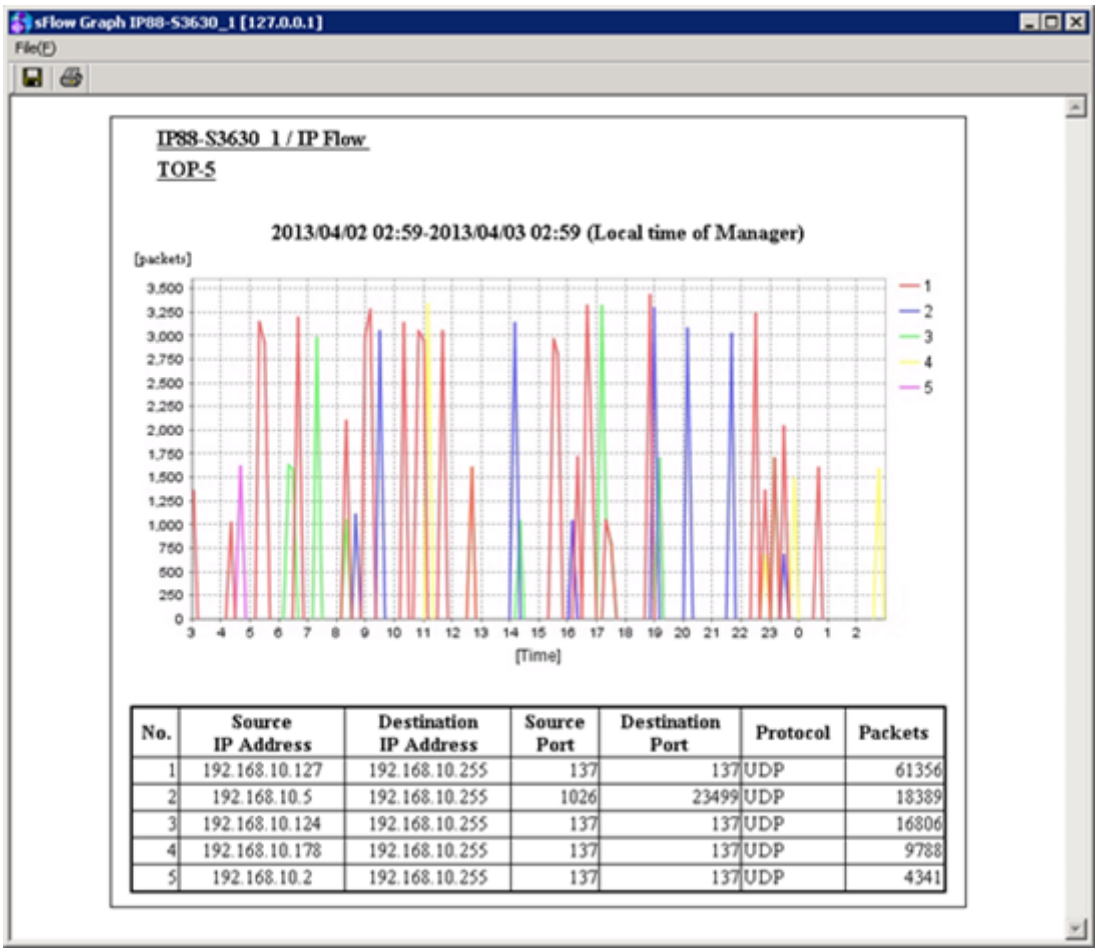
You can edit the definition file below and add port numbers.

<On the manager, %sharedfolder%>\Manager\sg\NvPRO\SFlowAnalyzer\portno.ini

For details, refer to "4.17.2 Customizing search conditions (page 375)".

4. Click **Show graph** button.

   The displayed graph shows data that matches the specified traffic flow conditions.

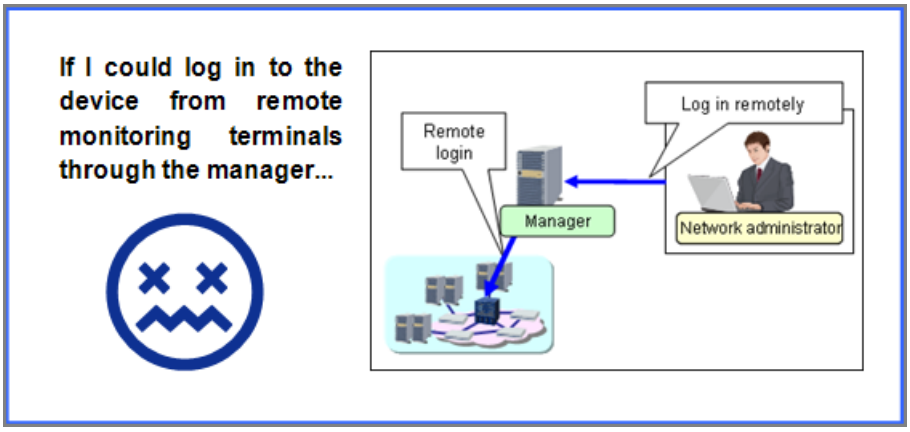


No.	Source IP Address	Destination IP Address	Source Port	Destination Port	Protocol	Packets
1	192.168.10.127	192.168.10.255	137	137	UDP	61356
2	192.168.10.5	192.168.10.255	1026	23499	UDP	18389
3	192.168.10.124	192.168.10.255	137	137	UDP	16806
4	192.168.10.178	192.168.10.255	137	137	UDP	9788
5	192.168.10.2	192.168.10.255	137	137	UDP	4341

3.7 Operations: Accessing Managed Devices

3.7.1 Logging in to managed devices

If managed devices can only be logged in to from a particular server for security purposes, you can still log in to a monitored device from the monitoring window by allowing logins from the manager.



Tip

For further information regarding logging in to the device, refer to "5.5.3 Logging in to devices from the monitoring terminal (page 469)".

For information regarding the registration of login information, refer to "4.3 Registering Login Information (page 189)".

Confirm that the operation environment meets the conditions below.

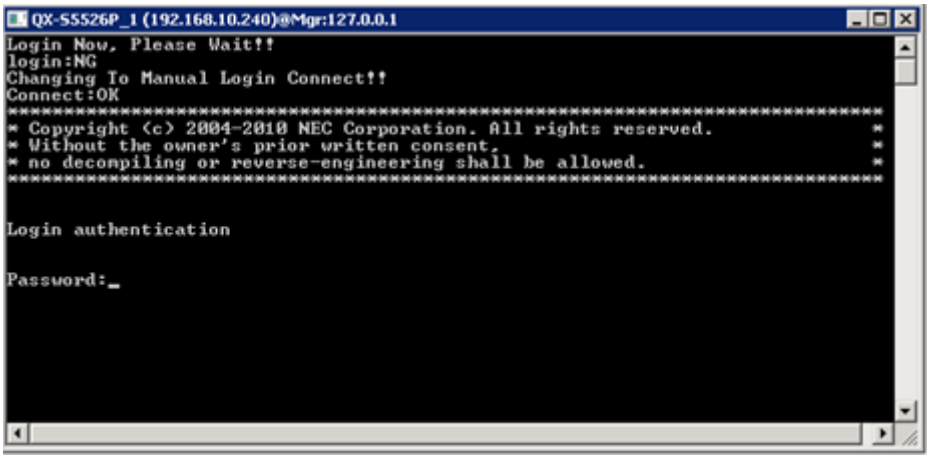
- A telnet client can be used on the monitoring terminal.
- The Telnet or SSH Server function is working on the target device-side.

Confirm that the following information has been registered in the target device properties.

- IP Address
- Telnet Server : ON

To perform this operation, the logged in user must belong to a group that has operation authority.

1. Right-click the device icon and select **Fault Management**>**Remote Login**.



   Connect to the device. The login prompt is displayed.

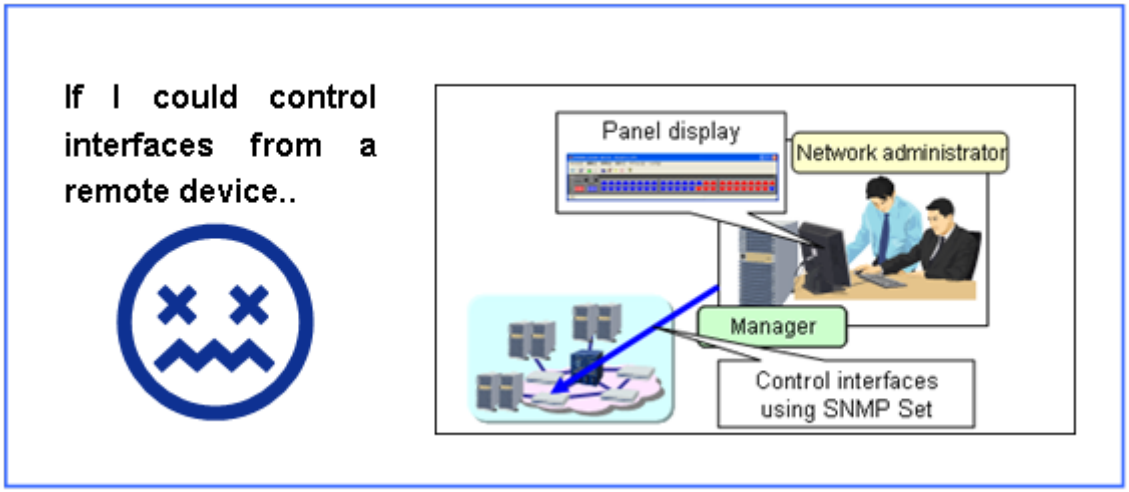
2. Enter the login information to log in to the device.

   - If you register the login information in advance, you can automatically log in to devices by simply selecting the **Fault Management**>**Remote Login**.
   - When registering login information in advance, you can select the Telnet and set up TACACS+/RADIUS authentication to enable connections to devices that require TACACS+/RADIUS authentication.
   - When registering login information in advance, you can select the Telnet and configure a setting of the port server to connect via the port server.
   - When registering login information in advance, you can select the SSH setting to encrypt communication between the manager and the monitored device for security purpose.

Tip

In operation to log in the monitored devices, the operated user information and the operated time are registered in the audio log.

3.7.2 Controlling the opening and closing of interfaces from the front panel display



Tip

For details, refer to "5.9.4 Changing configuration information (page 479)".

Confirm that you can perform SNMP communication with devices displayed in the front panel.

Node Manager (NM) license must be assigned to the target device.

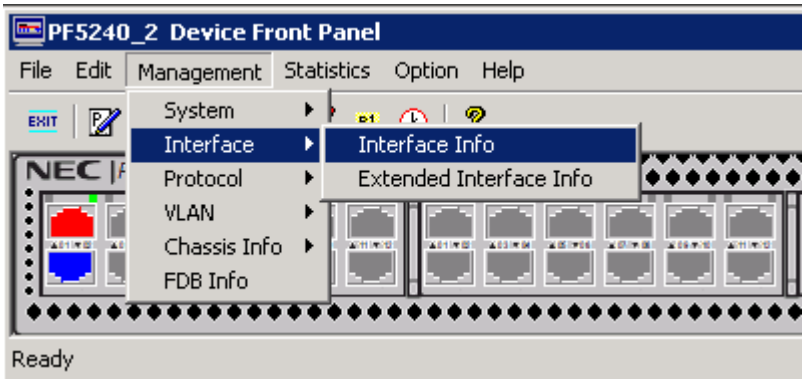
SNMP community name (set) needs to be set up in the device icon properties.

To perform this operation, the logged in user must belong to a group that has operation authority.

1. Open the Device Front Panel window.

   Right-click the device icon and select **Device Front Panel**.

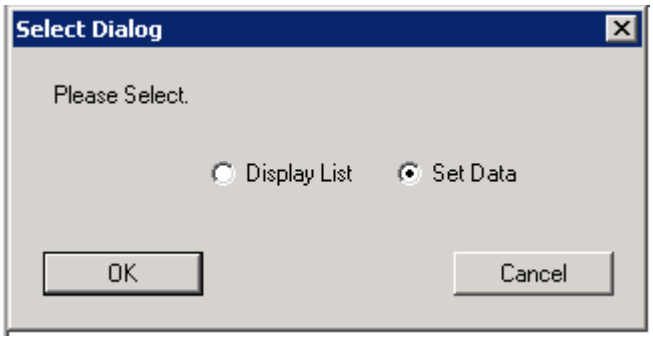
2. In the menu of the panel window, select **Management**>**Interface**>**Interface Info** to open the Select Dialog dialog box.



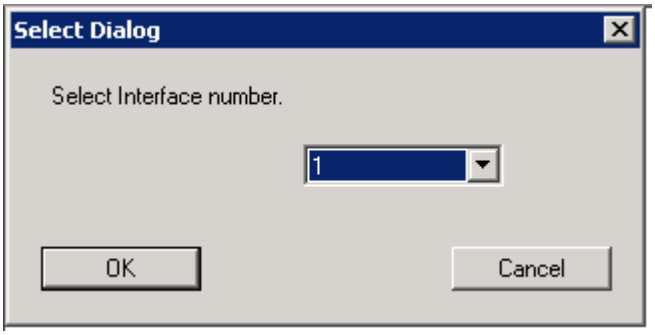
Caution

The content of the **Management** menu varies depending on the device type. As a result, it may not be possible to perform the operations described above.

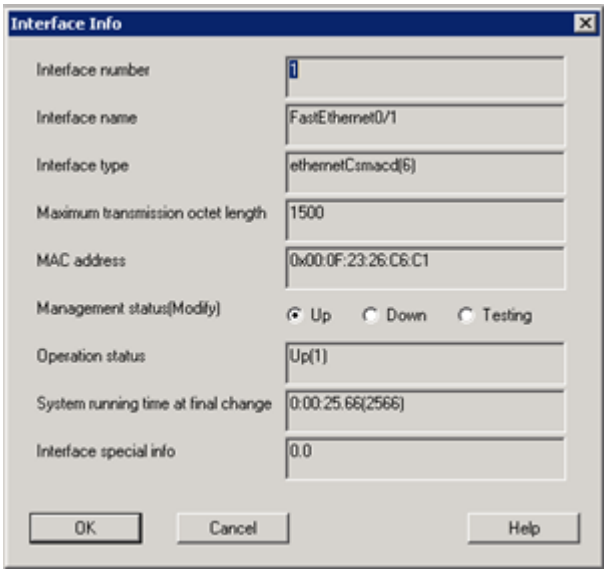
3. Select **Set Data** and click **OK** button.



4. Select the number of the interface that you want to control. Click **OK** button.



5. To open the interface, select **Up**. To close it, select **Down**.



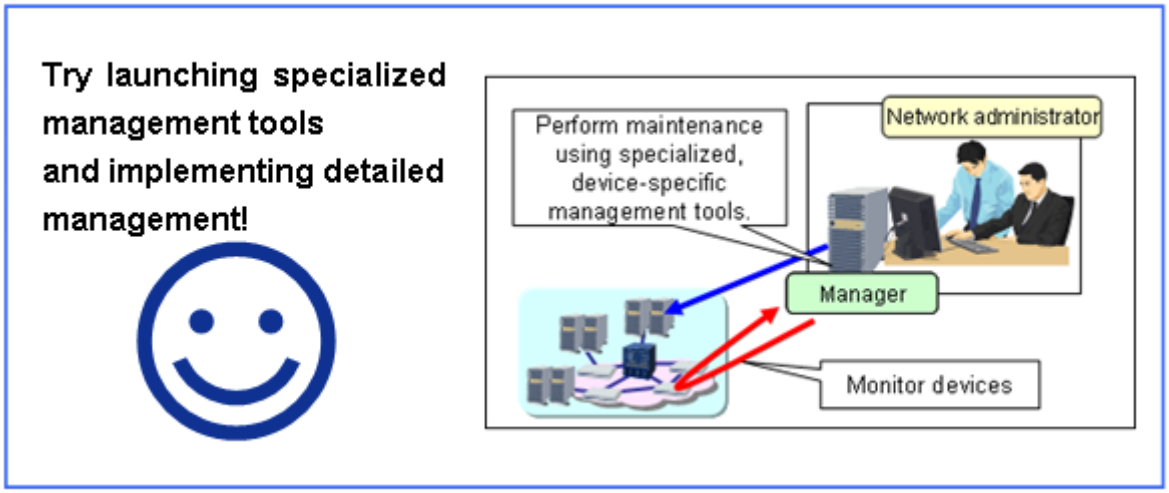
6. Click **OK** button.

   The status of interface is changed.

3.7.3 Using special management tools for specific devices

To launch an application or web page by right-clicking an icon, register the application or URL in the map icon or device icon properties. You can use this as the home window for starting specialized management tools for each monitored device.

To use web interfaces provided by devices, or management tools for individual devices, it is recommended to register the startup information in each device icon. To use management tools for multiple devices or network segments, it is recommended to register the startup information in the map icon.



This section provides an example of configuring settings to launch NEC ESMPRO Manager from the map icon.

Tip

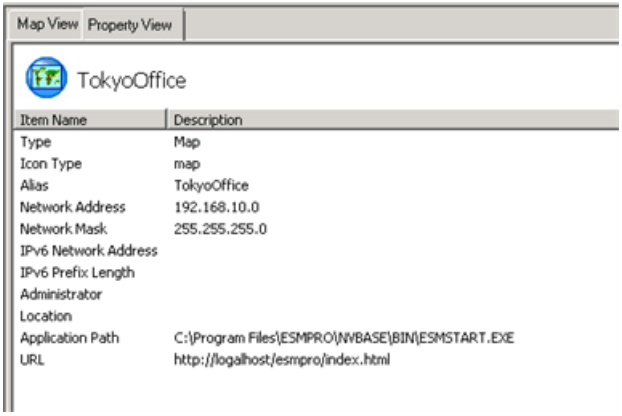
For details, refer to the following.

- "4.5.1 Registering applications launched from icons (page 204)"
- "4.5.2 Registering web URLs launched from icons (page 205)"

The path or URL of the application that will be launched, needs to be registered in the target icon properties.

The application to be launched needs to be installed on the monitoring terminal side.

1. Select the "TokyoOffice" map icon and select the Property View.



2. Confirm the following items.
   - **Application Path**

     Check the application path that will be launched.
   - **URL**

     Check the URLs that will be launched.
3. Start the tool.
   - When starting an application:

Right-click "TokyoOffice" map icon and select **Configuration Management**>**Start Application**.

- When starting a URL:

  Right-click "TokyoOffice" map icon and select **Configuration Management**>**Start Web browser**.

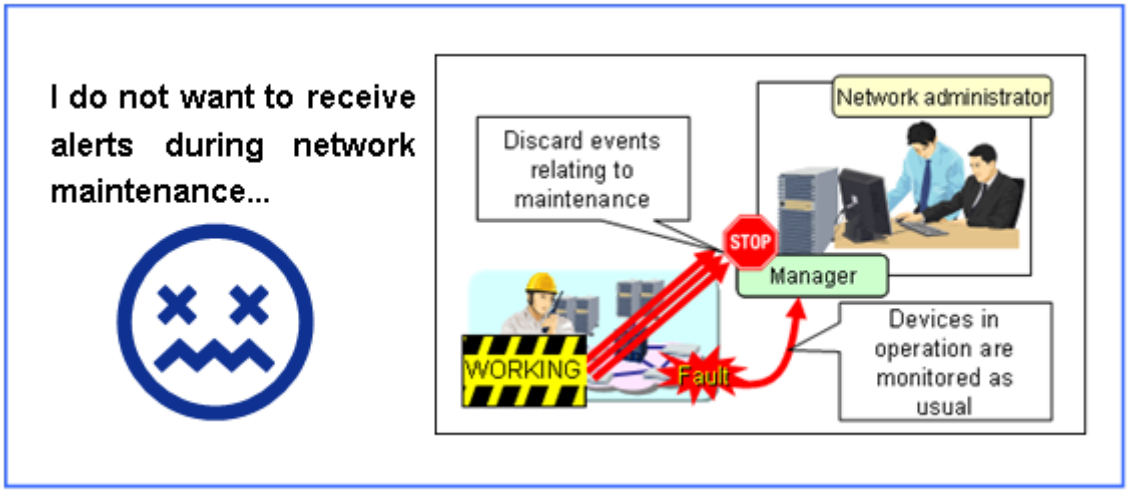
3.8 Operations: Maintaining Managed Devices

3.8.1 Stopping monitoring during network maintenance

During network maintenance, a large quantity of unnecessary alerts may be generated.

In Network Manager, it is possible to turn off monitoring mode for monitored devices affected by the network maintenance and discard alerts generated during the network maintenance period, or stop the monitoring process, without changing the monitoring settings.

This section describes the procedure for switching the monitoring mode OFF and ON according to a schedule.



Tip

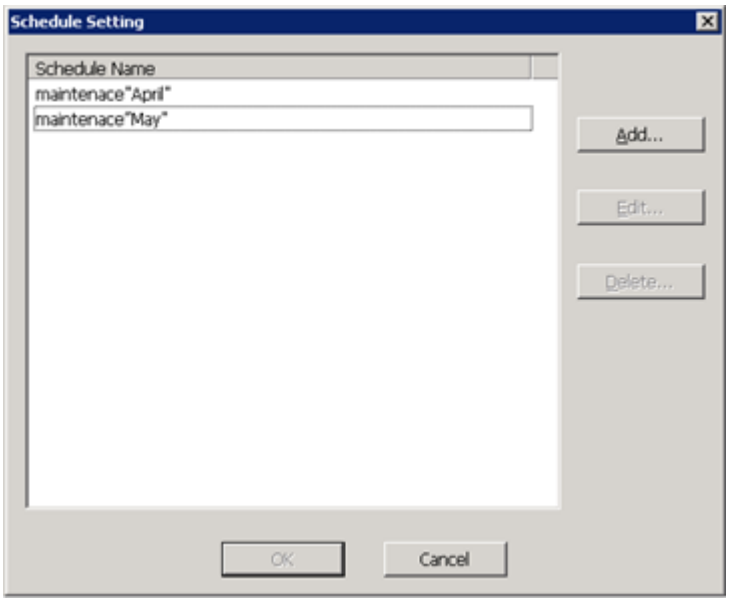
For details, refer to "5.13.2 Setting and changing a monitoring mode schedule (page 506)".

Before starting work, check which managed devices are included in the network maintenance and the duration of the maintenance.

You must first change to the "configuration mode (page 27)".

1. Open the Schedule Setting dialog box for the monitoring mode schedule.

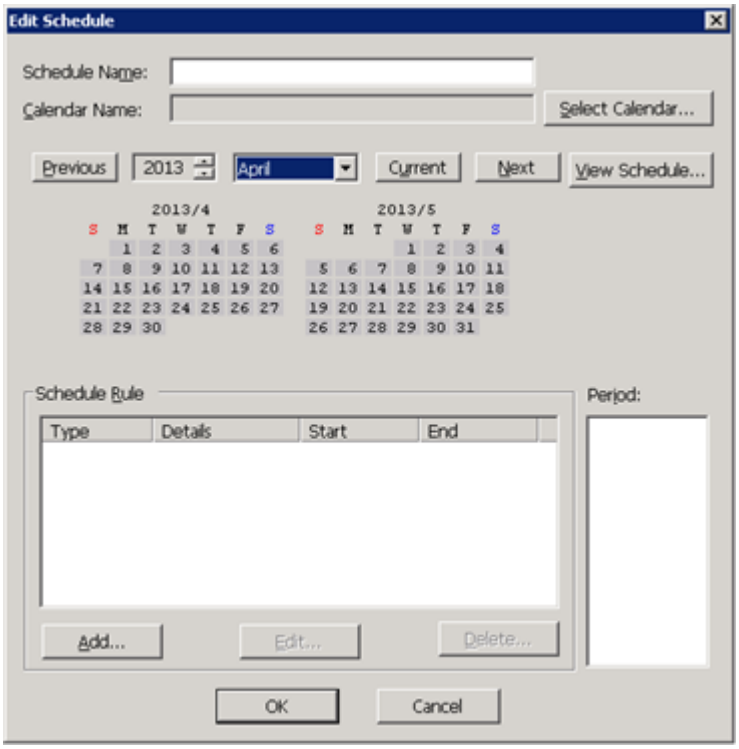
   Right-click the map icon or device icon for which you want to set up a monitoring mode schedule, and select **Configuration Management**>**Monitoring-mode Schedule**>**Setting**.



Tip

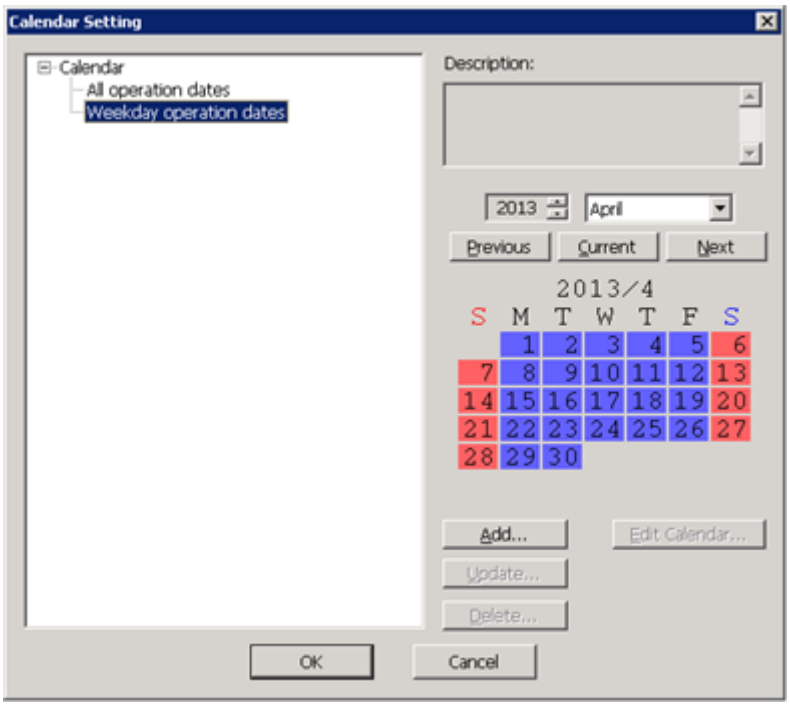
When starting from a map icon, the monitoring mode is set OFF/ON to all device icons under the map icon.

2. In the Edit Schedule dialog box, enter **Schedule Name**.



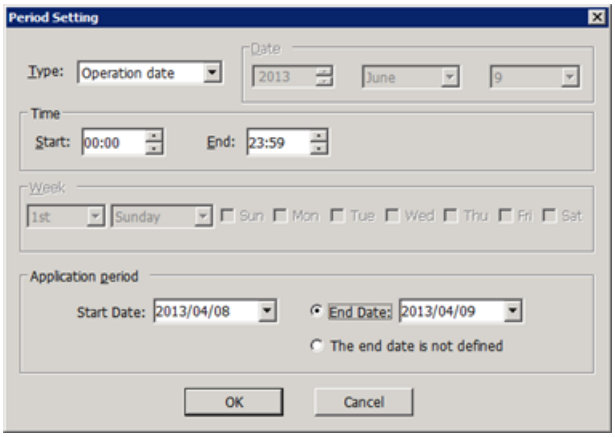
This schedule name can be selected in the Schedule Setting dialog box.

3. In the Edit Schedule dialog box, click **Select Calendar** button, and select a calendar in the "4.22.1.1 Calendar Setting dialog box (page 427)".



The schedule only applies to operation dates (blue). It is not valid on non-operation dates (red).

4. In the Edit Schedule dialog box, click **Add** button, and set the schedule period in the Period Setting dialog box.



   a. Monitoring mode is turned OFF at the **Start** time and ON at the **End** time.

      These values are displayed in the **Schedule Rule** area.

   b. Click **OK** button.

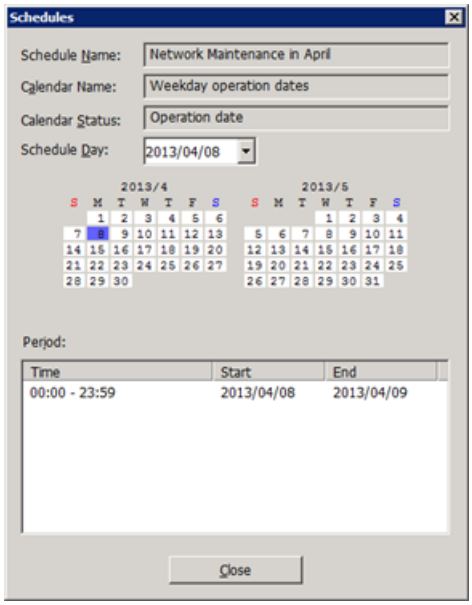
5. In the Edit Schedule dialog box, click **OK** button.

6. In the Schedule Setting dialog box, select a registered schedule information, and click **OK** button.

Tip

To confirm the registered schedule, follow the following steps.

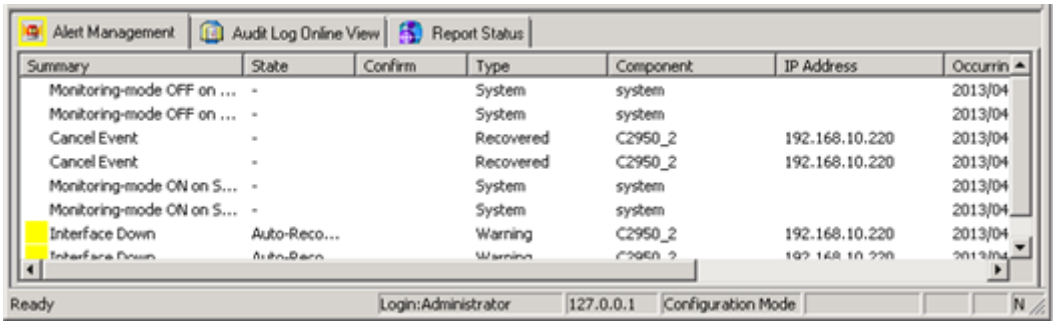
Right-click the icon that has a monitoring mode schedule set up, select **Configuration Management**>**Monitoring-mode Schedule**>**Property**.



Enter the **Schedule Day** to display information for schedules due to be executed on that day in the **Period** area.

7. Confirm the alert.

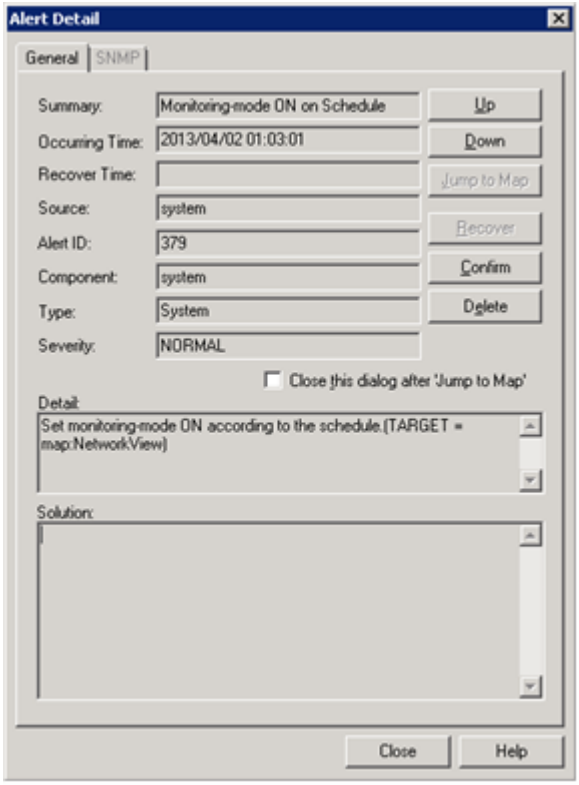
When the monitoring mode is turned ON or OFF according to a schedule, a notification is provided in Network Manager alerts and audit logs.



a. Select the **Alert Management** tab.

b. Double-click the selected row.

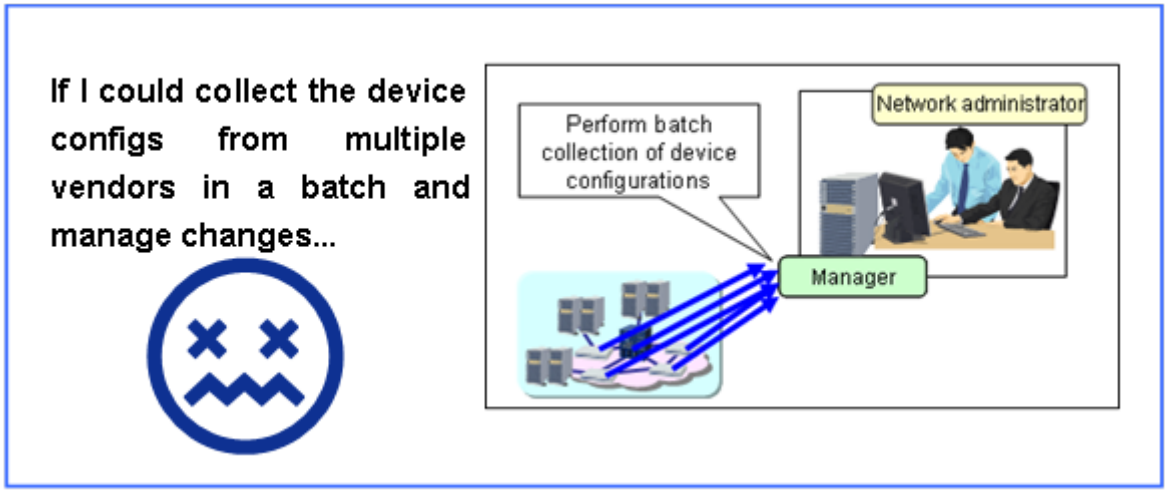
In the displayed Alert Detail dialog box, confirm that the monitoring mode has been changed according to the schedule.



3.8.2 Managing device configurations

Managing the configuration of many devices takes time and human resources. If a network has been configured with devices from multiple vendors, the procedure for collecting configurations varies depending on the device type. This requires even more time.

Network Manager provides the functions to collect the configurations for multiple vendors in a batch and manage change history of configurations efficiently. This section provides an example of a running-config collection operation. (Startup-configs can be managed in the same way.)



Tip

For details, refer to "4.20 Setting for Managing Device Configuration (Resource Manager) (page 399)".

If you want to monitor the running-config, use "Check Configuration Function (page 404)".

To manage configurations, the following target device settings need to be configured in advance:

- Register login information.

  For details, refer to "3.2.3 Registering information for logging in to managed devices (page 39)".

- Assign Resource Manager (RM) function licenses.

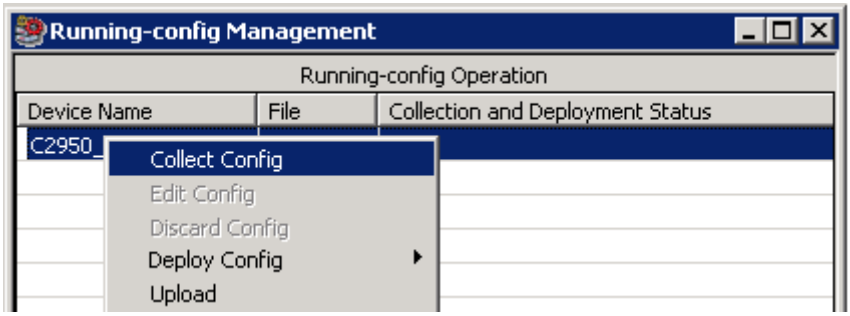
  For details, refer to "3.2.4 Selecting devices that use the panel display and advanced function (page 42)".

You must first change to the "configuration mode (page 27)".

1. Open the "5.14.1.1 Running-config Management window (page 512)".

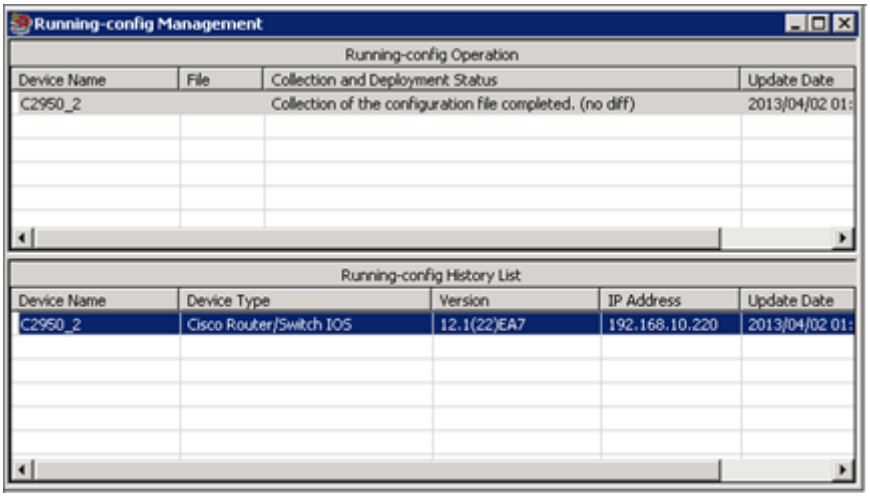
   Right-click the **NetworkView** icon, **NetworkManagement** icon, the map icon, or the divice icon. Select **Device Config Management**>**Running-config Management**.

2. Collect the running-config for the device.



   To collect a device running-config, right-click the target device and select **Collect Config** menu.

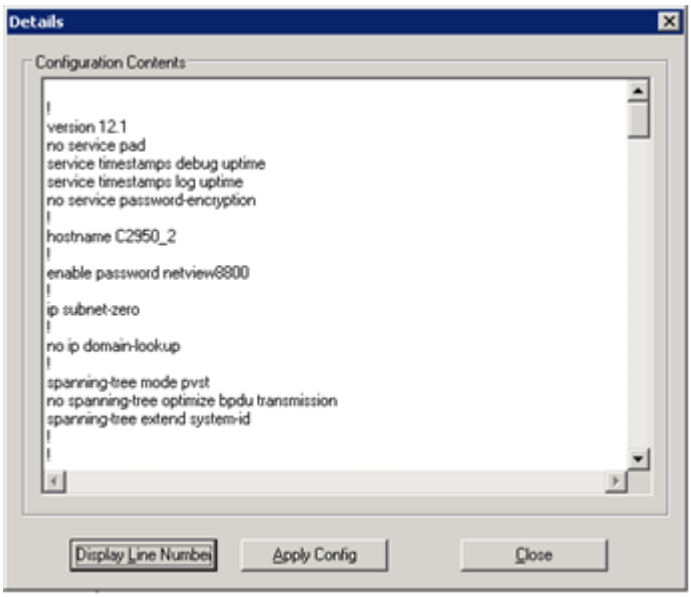
3. Confirm that the running-config collection was completed normally.



   a. Check the **Collection and Deployment Status** column.

   b. Check the collected configuration information in Running-config History List pane.

      In the Running-config History List pane, right-click the configuration that you want to display, and select the **Configuration Contents** menu to open Details dialog box.



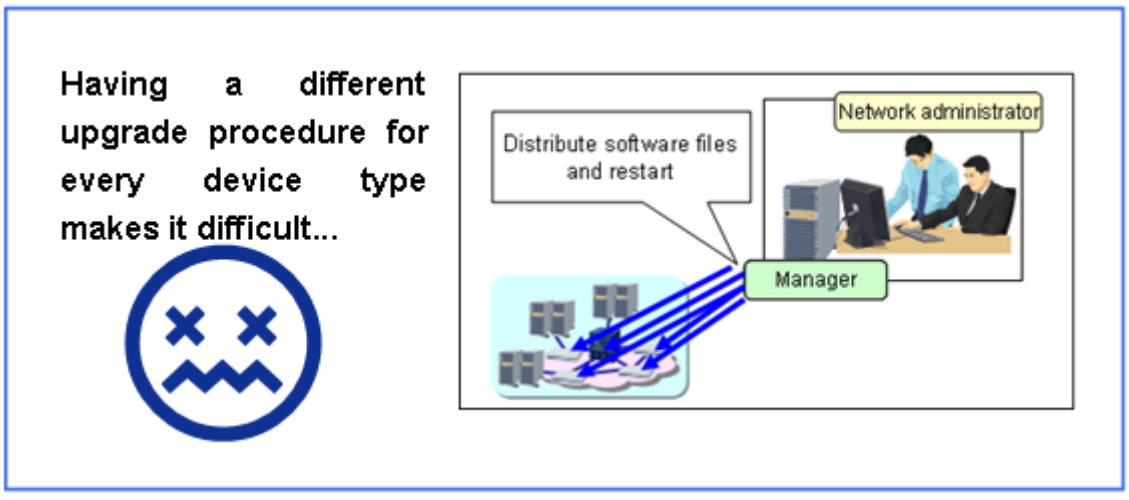
Tip

You can check the differences between two configurations by selecting any two configurations in the history list, right-clicking, and selecting **Show Difference** menu.

3.8.3 Upgrading device software

Device software can be upgraded easily from the monitoring terminal, even if you do not know the various procedures for applying software to each device type.

You can also restart devices to reflect applied software, by specifying a schedule.



Tip

For details, refer to "5.15 Managing Device Software (Resource Manager) (page 531)".

To upgrade software, the following target device settings need to be configured in advance:

- Register login information.

  For details, refer to "3.2.3 Registering information for logging in to managed devices (page 39)".

- Assign Resource Manager (RM) function licenses.

For details, refer to "3.2.4 Selecting devices that use the panel display and advanced function (page 42)".

In addition, prepare the software files for devices in advance.

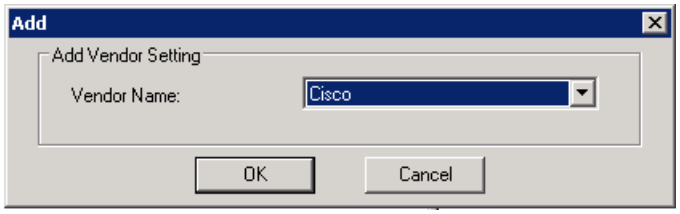
You must first change to the "configuration mode (page 27)".

1. Open the File Management window.

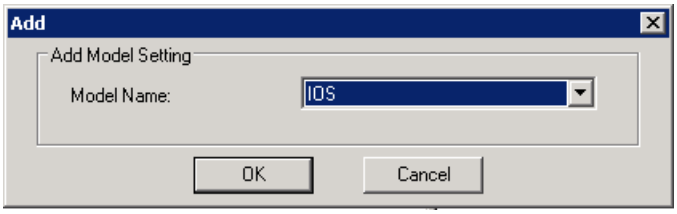
   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Software Management**>**File Management**.

2. Register the software to be distributed in Network Manager.

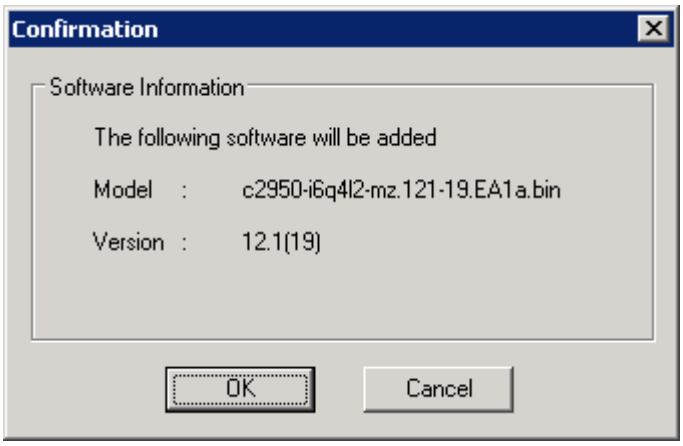
   a. Right-click the **Software** folder and add a vendor.



   b. Right-click the added vendor and add a model.



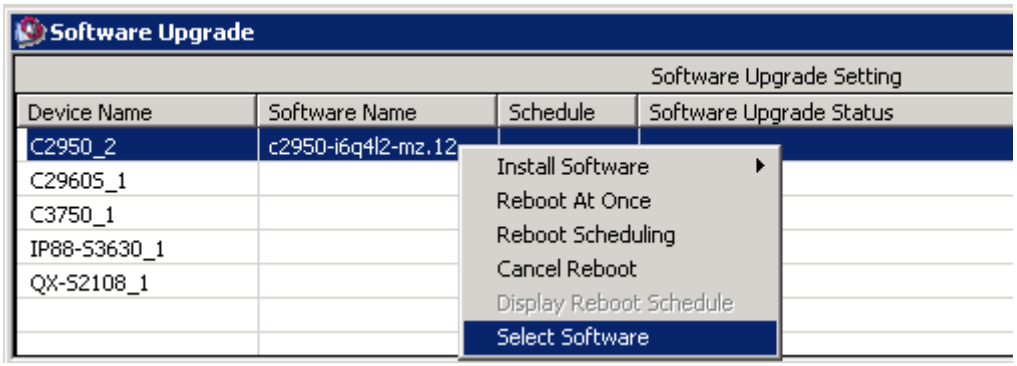
   c. Right-click the added model and register software to be distributed.



3. Open the Software Upgrade window.

   Right-click the **NetworkView** icon, **NetworkManagement** icon, the map icon, or device icon. Select **Software Management**>**Software Upgrade**.

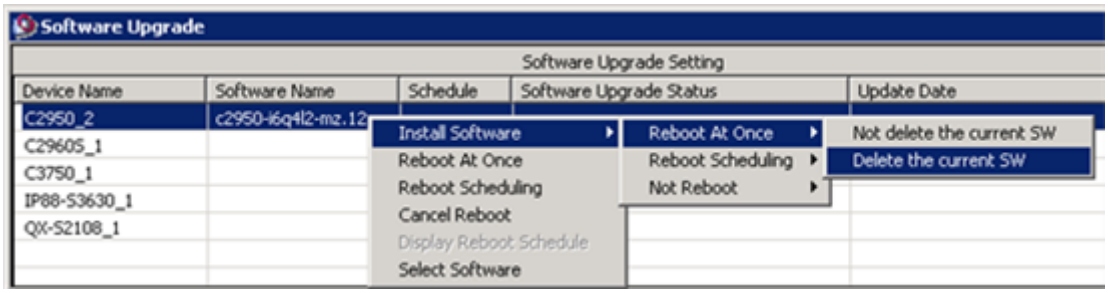
4. Right-click the target device and click **Select Software** menu, and then select software to be distributed.



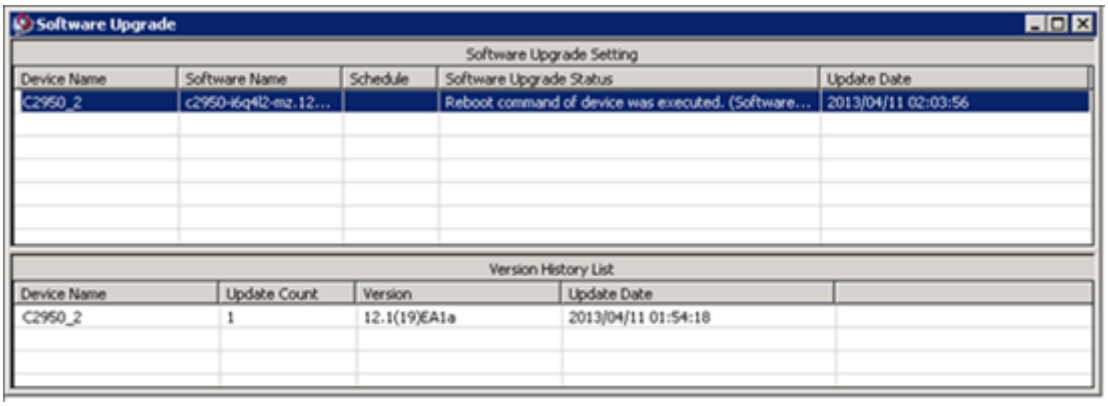
When you finish selecting, the name of software is displayed in the **Software Name** column.

5. Upgrade the software.

Right-click the target device and select **Install Software** menu.



6. Confirm that the software upgrade was succeeded.



a. Check the **Software Upgrade Status** column.

b. After upgrading, confirm that the upgrade has been added to the **Version History List** pane.

When Network Manager receives a warmStart trap or a coldStart trap, it retrieves version information and automatically updates registered information.

Chapter 4. Function Reference (Environment Setup)

Contents

4.1 Managing Users and Groups 101
4.2 Creating Network Configuration Map 127
4.3 Registering Login Information 189
4.4 Managing the Advanced Functions License 201
4.5 Registering Device-Specific Tools 204
4.6 Batch Registering or Deleting Configuration Information 206
4.7 Registering Routing Information for the Map between Two Nodes 231
4.8 Configuring the Operating Environment for the Fault Management 233
4.9 Error Monitoring 236
4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function) 241
4.11 Monitoring SNMP Traps 259
4.12 Monitoring Syslogs 302
4.13 Controlling Alerts (Aggregating, Discarding, and Converting Contents) 302
4.14 Settings for Sending Alert Reports 310
4.15 Settings for Executing Device Commands When Alerts Occur 333
4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices 334
4.17 Collecting Traffic Flow (sFlow) Information 373
4.18 Settings for Displaying Device Front Panel 378
4.19 Setting for Running Device Commands 391
4.20 Setting for Managing Device Configuration (Resource Manager) 399
4.21 Linking with NEC SigmaSystemCenter (Network Provisioning) 415
4.22 Scheduling 426
4.23 Settings for Managing Audit Logs 443

4.1 Managing Users and Groups

Manage information relating to users using the system. By assigning users to groups, users will have authority to perform operations based on the access rights assigned to their group.

- "4.1.1 Managing user information (page 101)"

  Create users who use the system, and manage them.

- "4.1.2 Managing group information (page 108)"

  Create groups to which users belong, and manage them.

- "4.1.3 Changing group authority (page 113)"

  Set authority by group, and limit the function to be used and the managing range.

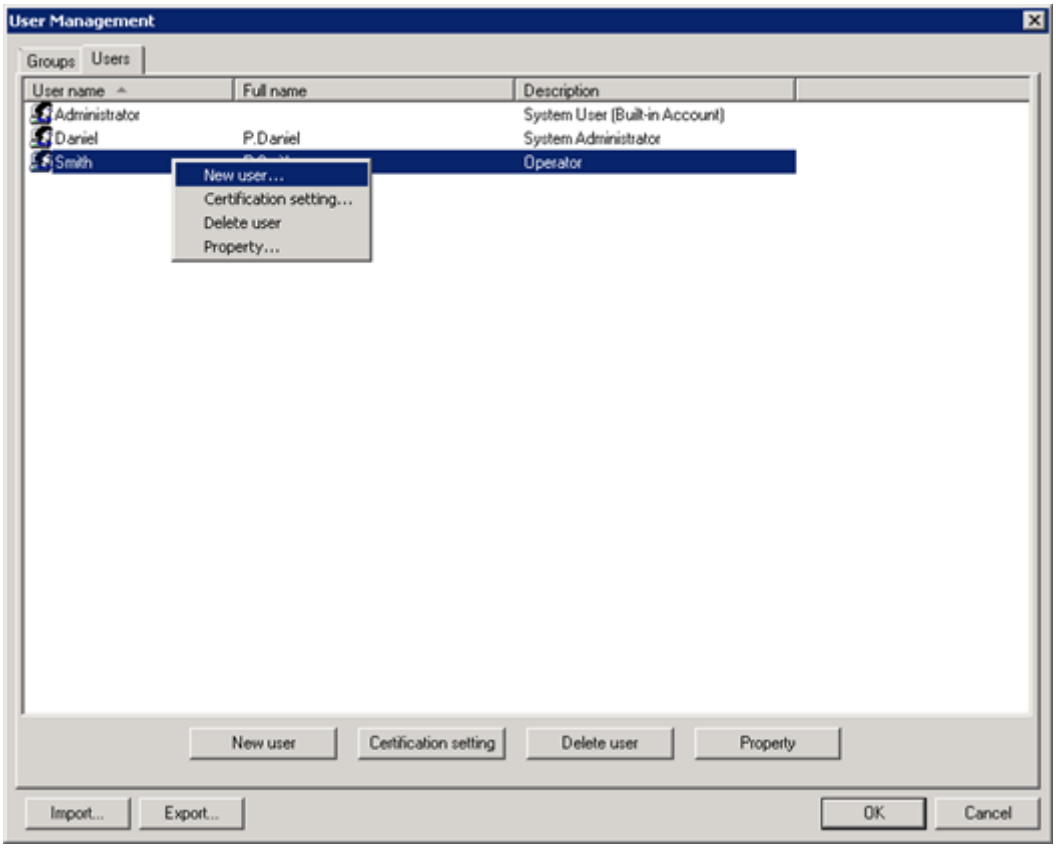
4.1.1 Managing user information

Create users who use the system, and manage them.

4.1.1.1 User Management window (Users tab)

User information is managed in the **User** tab of User Management window.

To display the User Management window, select **Setting**>**User Management** menu, and then click **Users** tab.



- User information display section

Created users are displayed in a list. To create a new user, or change a certification setting (password), delete a user or change properties for a selected user, right-click and select the appropriate menu.

- **User name**

  Displays the login name for the user.

- **Full name**

  Displays the full name of the user.

- **Description**

  Displays a description of the user.

- **New user** button

  Adds a user. For details, refer to "4.1.1.2 Creating a user (page 102)".

- **Certification Setting** button

  Changes the certification setting (password) for the selected user. For details, refer to "4.1.1.5 Changing a user password (page 108)".

- **Delete user** button

  Deletes the selected user. For details, refer to "4.1.1.4 Deleting a user (page 107)".

- **Property** button

  Updates information for the selected user. For details, refer to "4.1.1.3 Changing user information (page 104)".

- **Import** button

  Imports a specified external file, containing user management information, to make change in a batch. For details, refer to "4.1.4.2 Importing user information (page 126)".

- **Export** button

  Exports all user management information to an external file. For details, refer to "4.1.4.1 Exporting user information (page 125)".

Tip

- At the time of installation, as part of the default settings, a default user Administrator for system administration exists.

  Administrator information cannot be modified or deleted.

- You must change the password of Administrator user before starting operation. The initial password is websam.

4.1.1.2 Creating a user

Create a new user.

Log in as the user belonging to a group that has the the following authority.

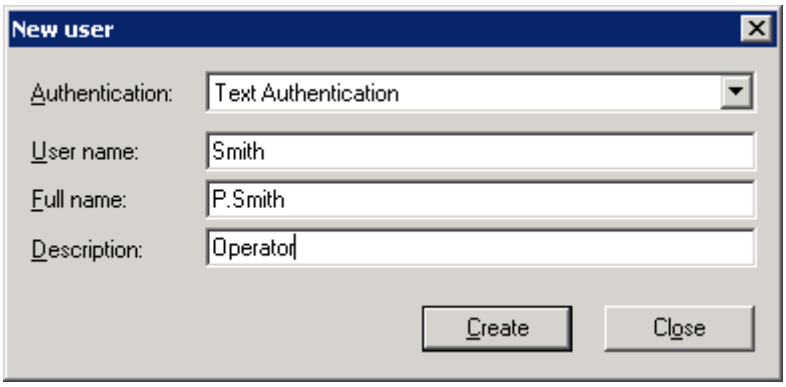
- User management authority
- Add authority in **User Management Service**

You must first change to the "configuration mode (page 27)".

1. Open the "4.1.1.1 User Management window (**Users** tab) (page 101)".

In the main menu, select **Setting**>**User Management**, and click **Users** tab.

2. Click **New User** button.
3. In the New User dialog box, specify the parameters explained below.



- **Authentication**

  Set to **Text Authentication**.

- **User name**

  Enter an user name with 64 or less characters. This user name is used as a login name when starting the monitoring window. There must not be duplicate user names in the system. The following user names cannot be registered.

  - User names that contain following characters: / \ [ ] : ; | = , + * ? < >
  - User names that comprise only of a space or dot marks
  - User names that contain tab or newline characters.
  - User names that start or end with a space.

- **Full name**

  Enter a full name for the user with 256 or less characters. The full name may be omitted. The following full names cannot be registered.

  - Full names that contain tab or newline characters.
  - Full names that start or end with a space.

- **Description**

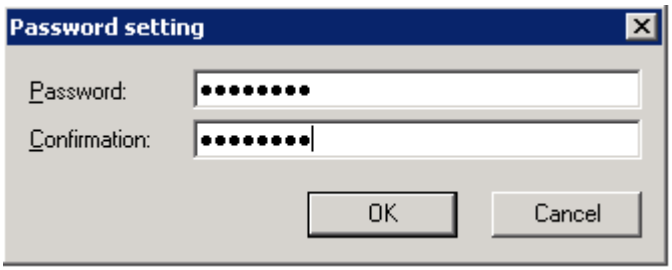
  Enter a description for the user with 256 or less characters. The description may be omitted. The following descriptions cannot be registered.

  - Descriptions that contain tab or newline characters.
  - Descriptions that start or end with a space.

4. Click **Create** button.

   The Password setting dialog box is displayed.

5. Enter a password between 6 and 64 characters.



Passwords that start or end with a space character cannot be registered.

6. Click **OK** button.

Reference authority only is applied to newly created users. To apply other access rights, the user must be added to a group. For reference authority, refer to "4.1.3.1 Group authority settings (page 113)".

4.1.1.3 Changing user information

Change the registered user information and the groups that the user belongs to.

Caution

User names cannot be changed. To change the user name, delete the relevant user and create a new user.

Log in as the user belonging to a group that has the the following authority.

- User management authority
- Update authority in **User Management Service**

You must first change to the "configuration mode (page 27)".

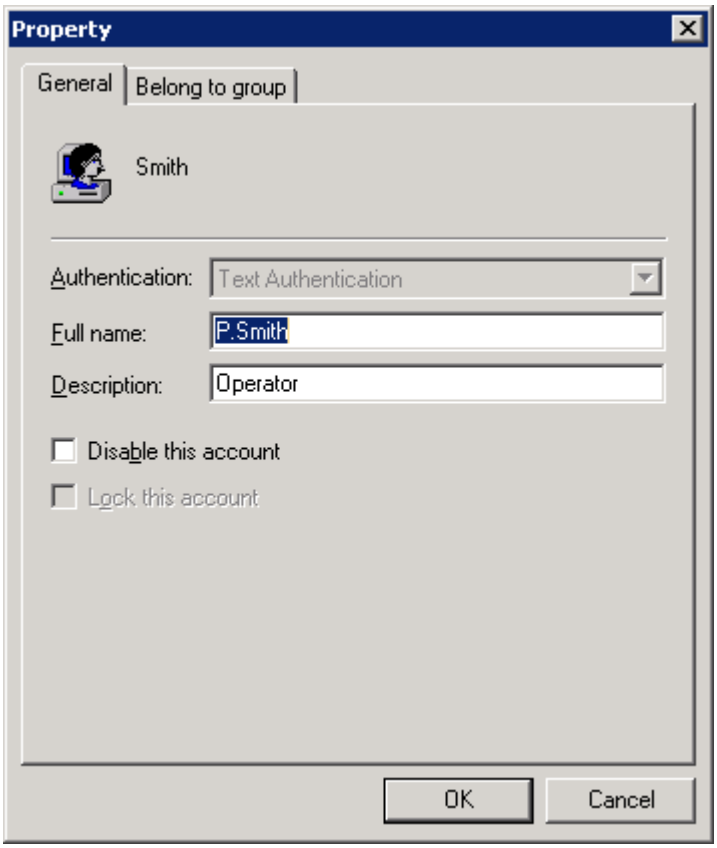
1. Open the "4.1.1.1 User Management window (**Users** tab) (page 101)".

   In the main menu, select **Setting**>**User Management**, and click **Users** tab.

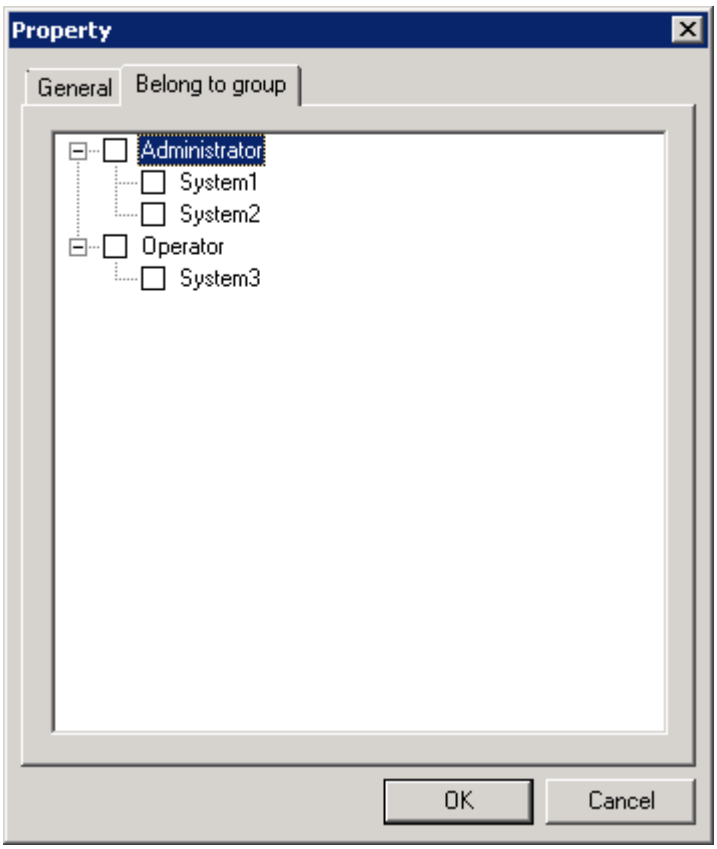
2. Select a user to be updated, and click **Property** button.

   The Property dialog box is opened.

3. In the **General** tab of "4.1.1.3.1 Property dialog box (page 106)", change the user information.



4. In the **Belong to group** tab of "4.1.1.3.1 Property dialog box (page 106)", change the groups that the user belongs to.

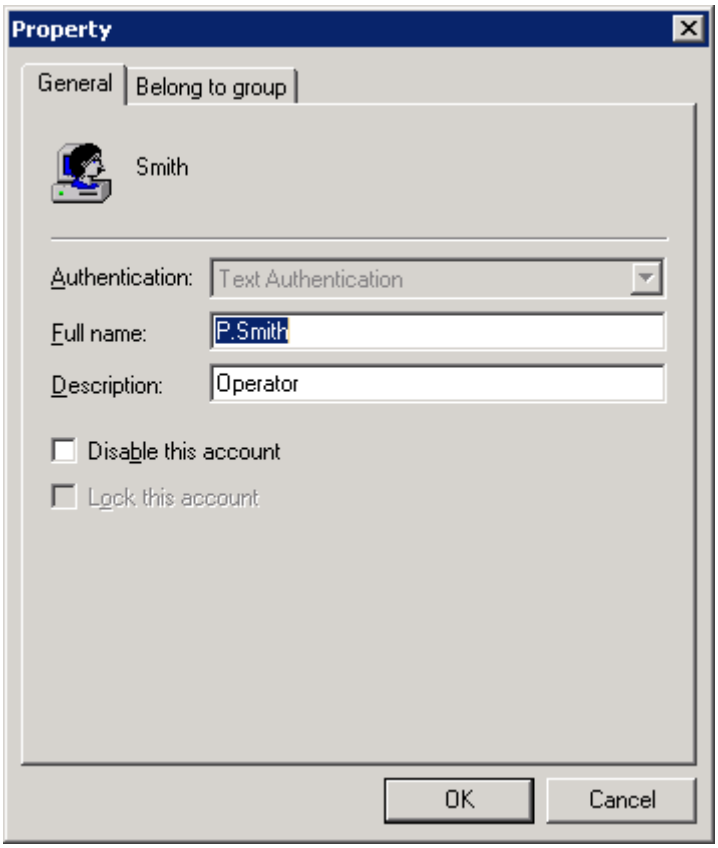


An user is able to belong to multiple groups. If any one of the groups have an access right, the access right is effective on this user.

For details, refer to "4.1.3.1 Group authority settings (page 113)".

5. Click **OK** button to change the user information.

Property dialog box



General tab

- **Authentication**

  Set to **Text Authentication**.

- **Full name**

  Enter a full name for the user with 256 or less characters. The full name may be omitted. The following full names cannot be registered.

  - Full names that are contains tab or newline characters.
  - Full names that starts or ends with a space.

- **Description**

  Enter a description for the user with 256 or less characters. The description may be omitted. The following descriptions cannot be registered.

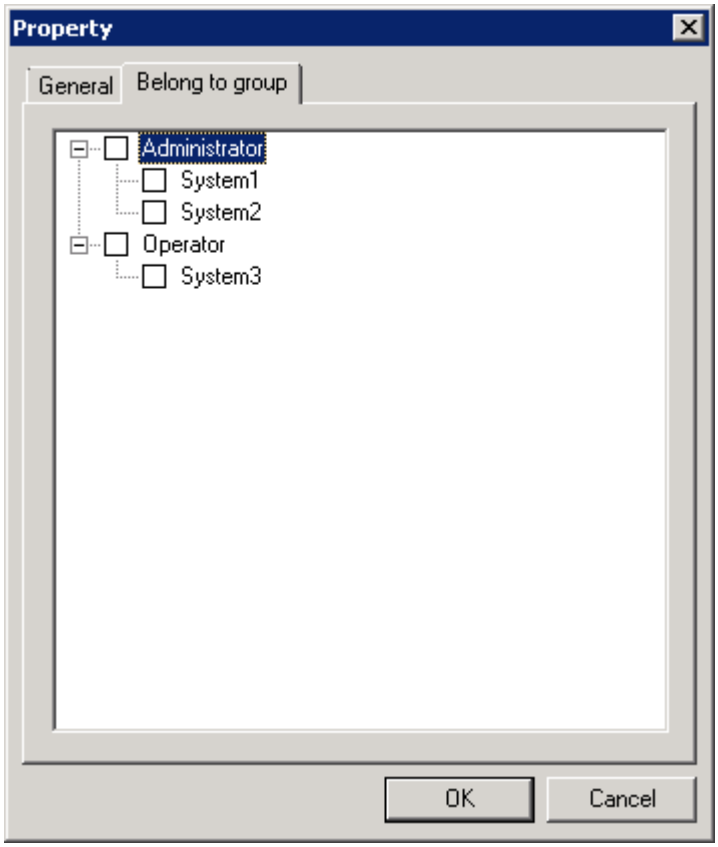
  - Descriptions that are contains tab or newline characters.
  - Descriptions that starts or ends with a space.

- **Disable this account**

If selected, the user will no longer be able to log in. If the user is currently logged in, this will take effect the next time they attempt to log in.

Belong to group tab

- To change the group that the user belongs to, click the **Belong to group** tab.



4.1.1.4 Deleting a user

Delete a registered user.

⚠ Caution

1. A deleted user cannot be restored. To temporarily prevent a user from accessing the system, disable the user's account. For details, refer to "4.1.1.3 Changing user information (page 104)".
2. The Administrator is the default system manager and cannot be deleted.

Log in as the user belonging to a group that has the the following authority.

- User management authority
- Delete authority in **User Management Service**

You must first change to the "configuration mode (page 27)".

1. Open the "4.1.1.1 User Management window (**Users** tab) (page 101)".

   In the main menu, select **Setting**>**User Management**, and click **Users** tab.

2. Select a user to be deleted, and click **Delete user** button.

   However, the logged in user can not be deleted. If the user can not be deleted for any other reason, the reason will be displayed.

4.1.1.5 Changing a user password

Change a password of a registered user. If an user forgets their password, the user password can be reset.

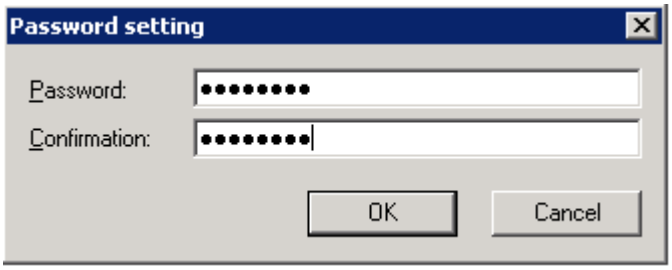
Log in as the user belonging to a group that has the the following authority.

- User management authority
- Update authority in **User Management Service**

You must first change to the "configuration mode (page 27)".

1. Open the "4.1.1.1 User Management window (**Users** tab) (page 101)".

   In the main menu, select **Setting**>**User Management**, and click **Users** tab.
2. Select a user whose passwords are changed, click **Certification Setting** button.
3. In the Password setting dialog box, enter a password between 6 and 64 characters.



   Passwords that start or end with a space character cannot be registered.
4. Click **OK** button.

4.1.2 Managing group information

Create groups that users belong to and manage them.

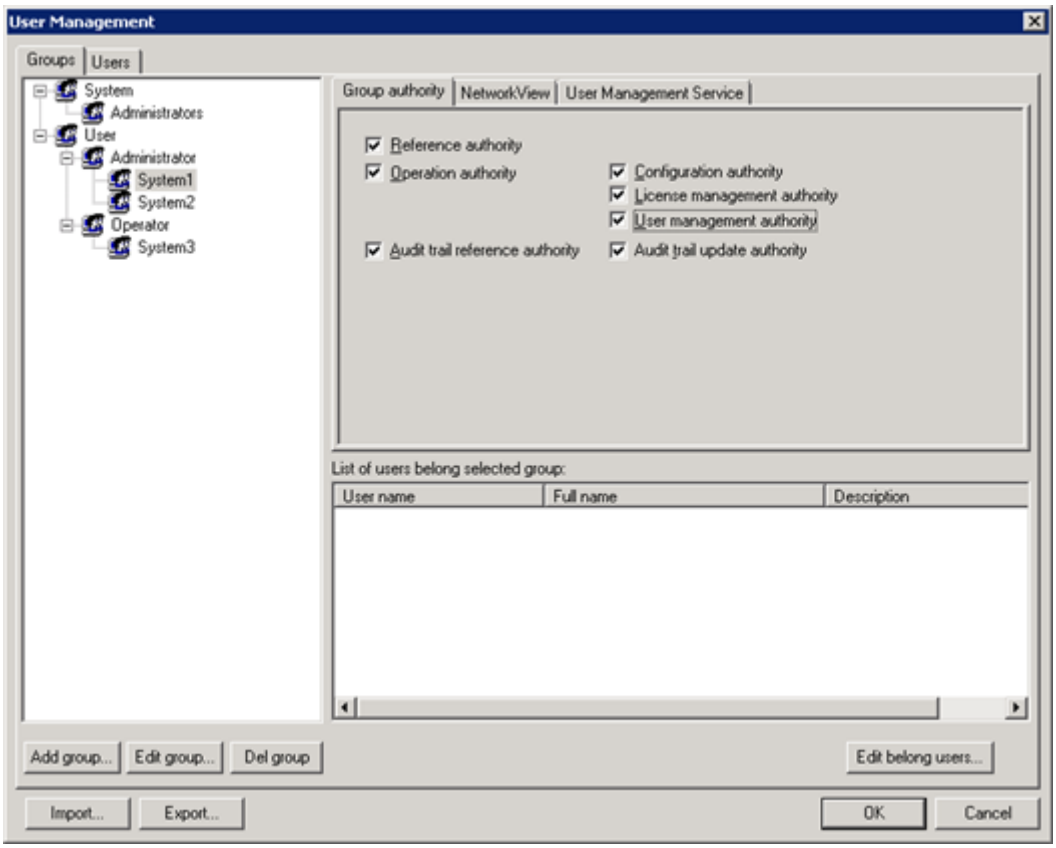
Caution

It is recommended that the number of managing groups should be up to 50.

4.1.2.1 User Management window (Groups tab)

Group information is managed in the **Groups** tab of User Management window.

To open the User Management window, select **Setting**>**User Management** menu, and then click **Groups** tab.



- Group tree in the left pane

  Groups are displayed in a tree. To add a new group, change the name of a selected group, or delete a group, right-click and select the appropriate menu.

  - **System** group

    This is the default group for managing the system. Only "Administrators" group with full authority can belong to this group. It is not possible to make changes to groups under the system group.

  - **User** group

    New groups can be created below the user group.

- **Group authority** tab of the right pane

  Access rights can be assigned to groups. For details, refer to "4.1.3.1 Group authority settings (page 113)".

- **Network View** tab of the right pane

  Authority regarding **Network View** operations can be assigned to group. For details, refer to "4.1.3.3 Detailed authority settings of Network View (page 116)".

- **User Management Service** tab of the right pane

  Authority regarding user and group information can be assigned to groups. For details, refer to "4.1.3.2 Detailed authority settings of the user management function (page 115)".

- **List of users belong selected group**

  Displays information for users belonging to the selected group. For edit of the users belonging to the selected group, refer to "4.1.2.5 Changing member users (page 112)".

- **Add group** button

Adds a group. For details, refer to "4.1.2.2 Adding a group (page 110)".

- **Edit group** button

  Changes the name of the selected group. For details, refer to "4.1.2.3 Changing a group name (page 111)".

- **Del group** button

  Deletes the selected group. For details, refer to "4.1.2.4 Deleting a group (page 111)"

- **Edit belong users** button

  Specify users belonging to the selected group. For details, refer to "4.1.2.5 Changing member users (page 112)".

- **Import** button

  Imports a specified external file, containing user management information, to make change in a batch. For details, refer to "4.1.4.2 Importing user information (page 126)".

- **Export** button

  Exports all user management information to an external file. For details, refer to "4.1.4.1 Exporting user information (page 125)".

⚠ Caution

Access rights are not inherited, even if groups are placed in a hierarchy. Only the access rights assigned to a particular group are effective.

4.1.2.2 Adding a group

Add a new group.

Log in as the user belonging to a group that has the the following authority.

- User management authority
- Add authority in **User Management Service**

⚠ Caution

When a group is added by the user other than Administrator, group authorities for new group are copied from the upper group. For details, refer to "4.1.3.1 Group authority settings (page 113)".

You must first change to the "configuration mode (page 27)".

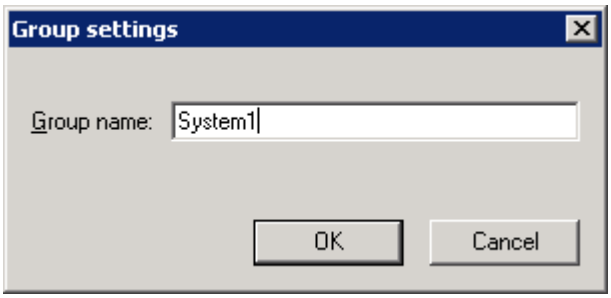
1. Open the "4.1.2.1 User Management window (**Groups** tab) (page 108)".

   In the main menu, select **Setting**>**User Management**, and click **Groups** tab.

2. In the group tree, select an existing group, and click **Add group** button.

   A new group will be added under the selected group.

3. Enter a group name with 64 or less characters.



The following group names cannot be registered.

- Group names that are contains tab or newline characters.
- Group names that starts or ends with a space.
- Group names that are identical to an existing group name in the same hierarchy.

4. Click **OK** button.

4.1.2.3 Changing a group name

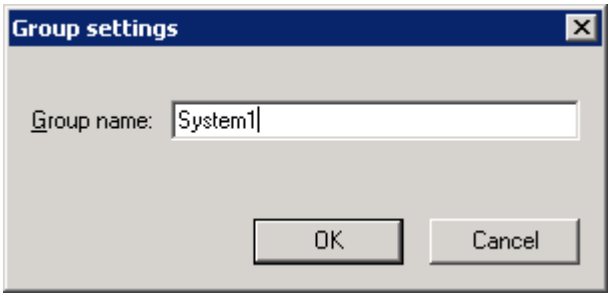
Change a registered group name.

Log in as the user belonging to a group that has the the following authority.

- User management authority
- Update authority in **User Management Service**

You must first change to the "configuration mode (page 27)".

1. Open the "4.1.2.1 User Management window (**Groups** tab) (page 108)".
   In the main menu, select **Setting**>**User Management**, and click **Groups** tab.
2. In the group tree, select a group to be changed, click **Edit group** button.
3. Enter a new group name with 64 or less characters.



The following group names cannot be registered.

- Group names that are contains tab or newline characters.
- Group names that starts or ends with a space.
- Group names that are identical to an existing group name in the same hierarchy

4. Click **OK** button.

4.1.2.4 Deleting a group

Delete a registered group.

Log in as the user belonging to a group that has the the following authority.

- User management authority
- Delete authority in **User Management Service**

You must first change to the "configuration mode (page 27)".

1. Open the "4.1.2.1 User Management window (**Groups** tab) (page 108)".
   In the main menu, select **Setting**>**User Management**, and click **Groups** tab.
2. In the group tree, select a group to be deleted, and click **Del group** button.

Caution

All subordinate groups will also be deleted.

4.1.2.5 Changing member users

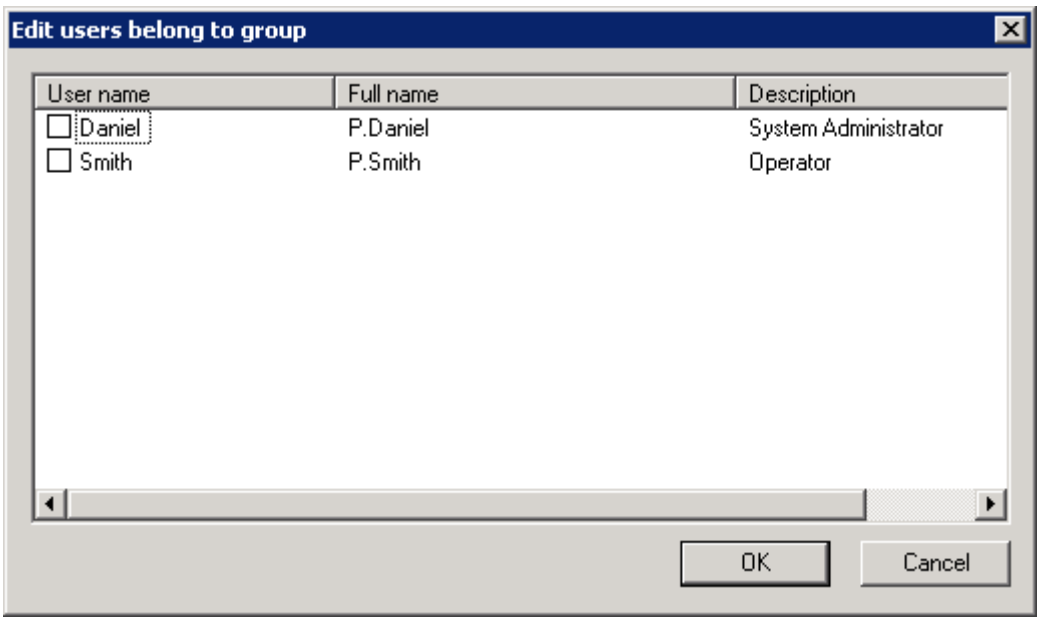
Delete a registered group.

Log in as the user belonging to a group that has the the following authority.

- User management authority
- Add or Delete authority in **User Management Service**

You must first change to the "configuration mode (page 27)".

1. Open the "4.1.2.1 User Management window (**Groups** tab) (page 108)".
   In the main menu, select **Setting**>**User Management**, and select **Groups** tab.
2. In the group tree, click the **Edit belong users** button.
3. In the list of users, select the users that you want to add to the group.



4. Click **OK** button.

4.1.3 Changing group authority

In the user management function, you can set the authority by group and limit the functions to be used and the management range. Users can operate Network Manger within the confines of authority set in the group where the users belong to.

The authority has two main concepts. One is the basic authority setting on the whole functions of the product, and the other is the authority setting to specify the detailed management confines of each function.

The group authority setting is configured in the "4.1.2.1 User Management window (**Groups** tab) (page 108)".

Basic authority setting of groups

The basic authority of groups includes **Reference authority** necessary for reference to the system information, **Configuration authority** necessary for change of various setting by obtaining "configuration mode (page 27)", etc.

Since the authority for groups is structured hierarchically, the group without the master authority is unable to set any subordinate authority.

For details, refer to "4.1.3.1 Group authority settings (page 113)".

Detailed authority setting for each function

In Network Manager, you can set detailed management confines to the following functions.

- "User management (page 115)"

  You can set, in detail, enable/disable of the operation (Reference, Update, Add, and Delete authority) for each user group.

- "Network View (page 116)"

  You can set, in detail, enable/disable of the operation (management authority) for each node of the network.

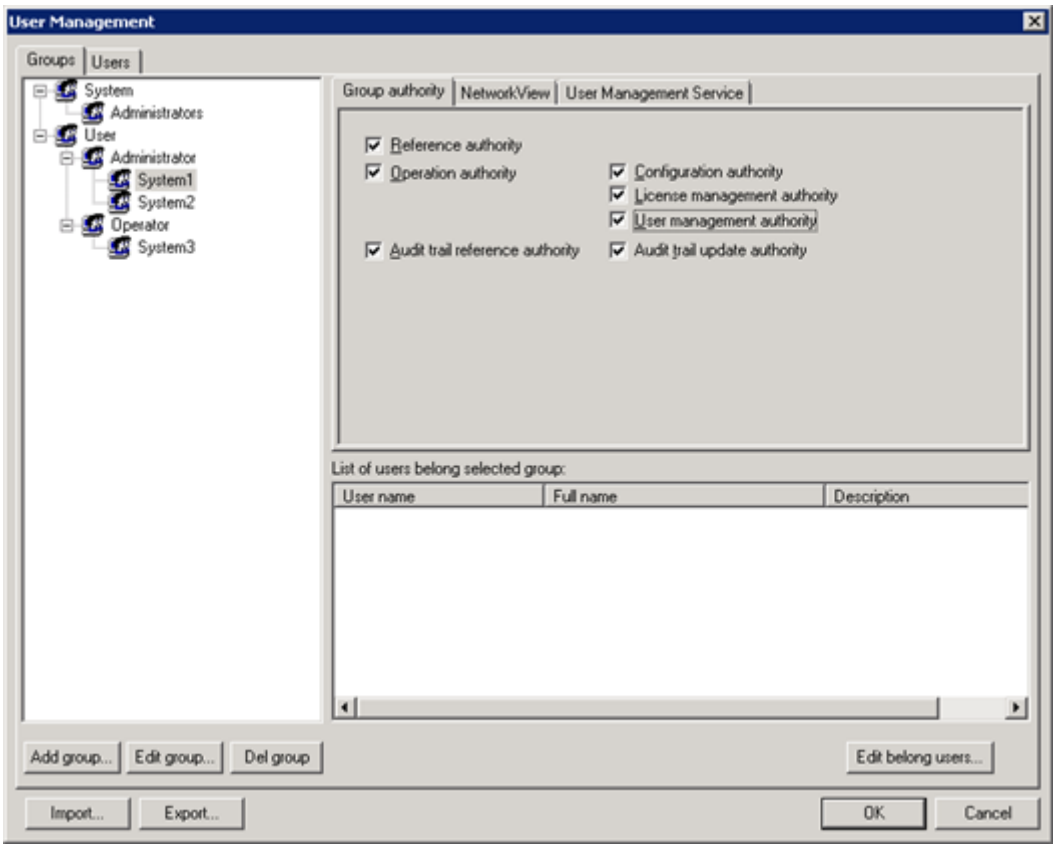
- "Calendar (page 123)"

  You can set, in detail, enable/disable of the operation (Reference, Setup authority) for each calendar.

4.1.3.1 Group authority settings

The basic authority setting of a group is configured in **Group authority** tab of the User Management window (Groups).

Only the default user "Administrator" can make changes to the settings in this tab.



The following types of authority can be assigned to a group.

- Reference authority

  Only view information in the system. Assigned to all groups.

- Operation authority

  In addition to the Reference authority, access monitored devices.

- Configuration authority

  In addition to the Operation authority, a user can change to configuration mode and modify each setting. In the configuration mode, refer to "2.5 Operation Modes (page 27)".

- License management authority

  Registration and management of licenses.

- User management authority

  Create users and groups.

- Audit trail reference authority

  View the audit log.

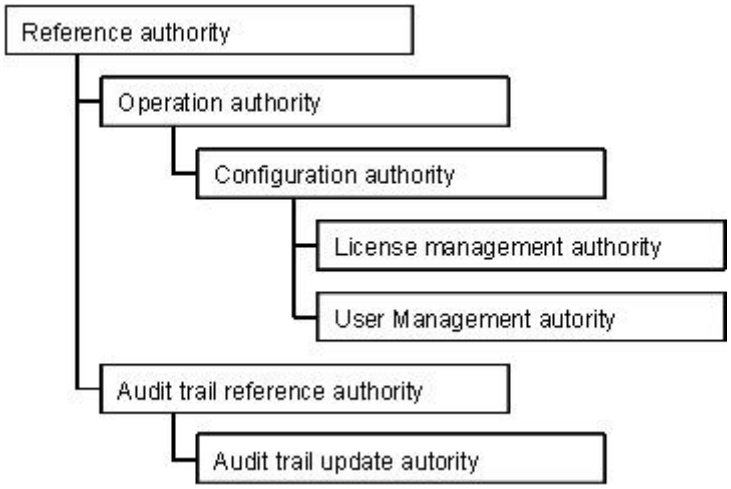
- Audit trail update authority

  Make changes to the audit log.

Caution

1. Reference authority is also granted to users who do not belong to a group.
2. The functions that can be used in Network Manager are restricted by the group authority. Functions that cannot be used are dimmed.

The access rights that can be set will vary depending on which authority is currently enabled. If the master authority in the following diagram is not enabled, subordinate authority cannot be set.



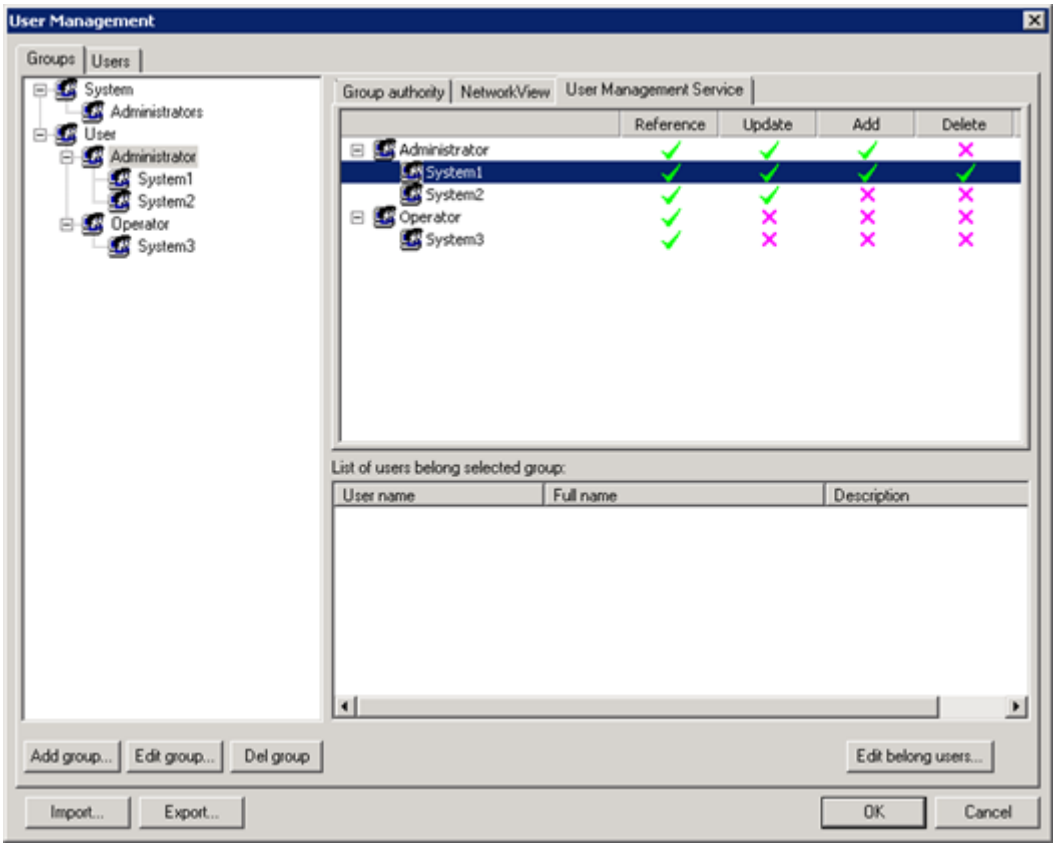
Example:

To set "Configuration authority", "Reference authority" and "Operation authority" must be set.

4.1.3.2 Detailed authority settings of the user management function

The authority setting to specify the detailed management confines to the user management functions is configured in the **User Management Service** tab of User Management window (Groups).

Only the default user "Administrator" can make changes to the settings in this tab.



The Authority for operations of user and group information has the following types.

- Reference authority

  Refer to the user and group information.

- Update authority

  Update the user and group information.

- Add authority

  Add the user and group information.

- Delete authority

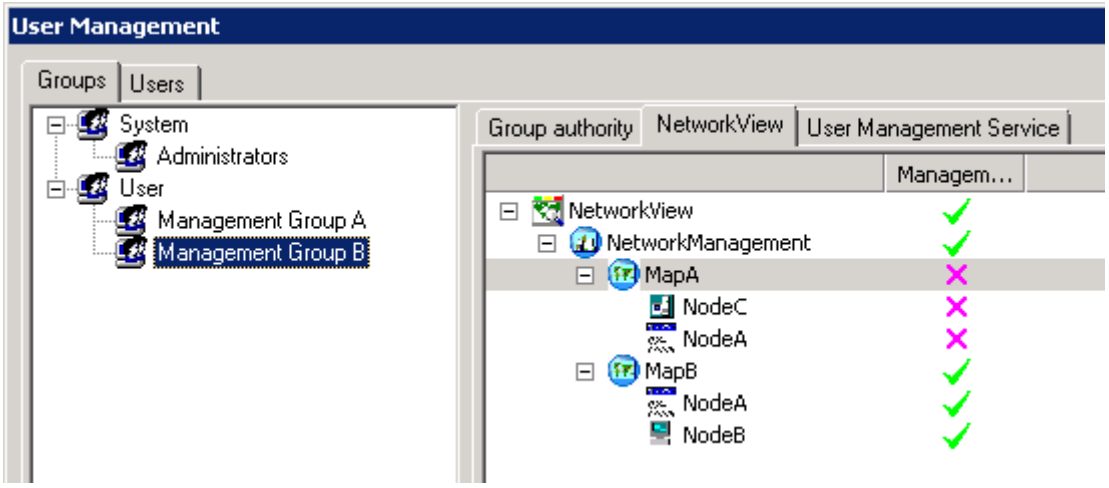
  Delete the user and group information.

⚠ Caution

The authority of "System" group cannot be changed. The background color is displayed in gray.

4.1.3.3 Detailed authority settings of Network View

The authority setting to specify the detailed management confines on the network view is configured in the **NetworkView** tab of User Management window (Group).

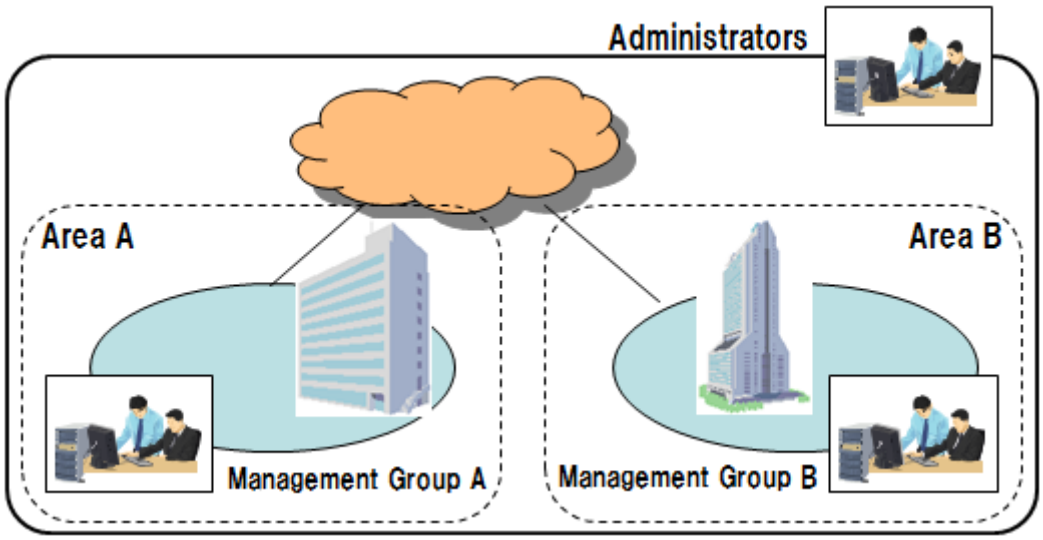


⚠ Caution

The authority of "System" group cannot be changed. The background color is displayed in gray.

By setting of the network view management authority, you can restrict reference to or operation of devices or map managed in Network Manager for each group.

If the setting is configured combing with "4.1.3.1 Group authority settings (page 113)", you can divide a network reference range or operation range by group, and limit the management range in detail.



For instance, in the above figure, "Management Group A" manages "Area A", "Management Group B" manages "Area B", and "Administrators" group manages the whole network. To achieve this situation by using Network Manager, you should set authority as follows:

- For "Management Group A" group, enable management authority of maps and devices in "Area A", and disable authority of maps and devices in "Area B".
- For "Management Group B" group, enable management authority of devices and maps in "Area B", and disable authority of maps and devices in "Area A".

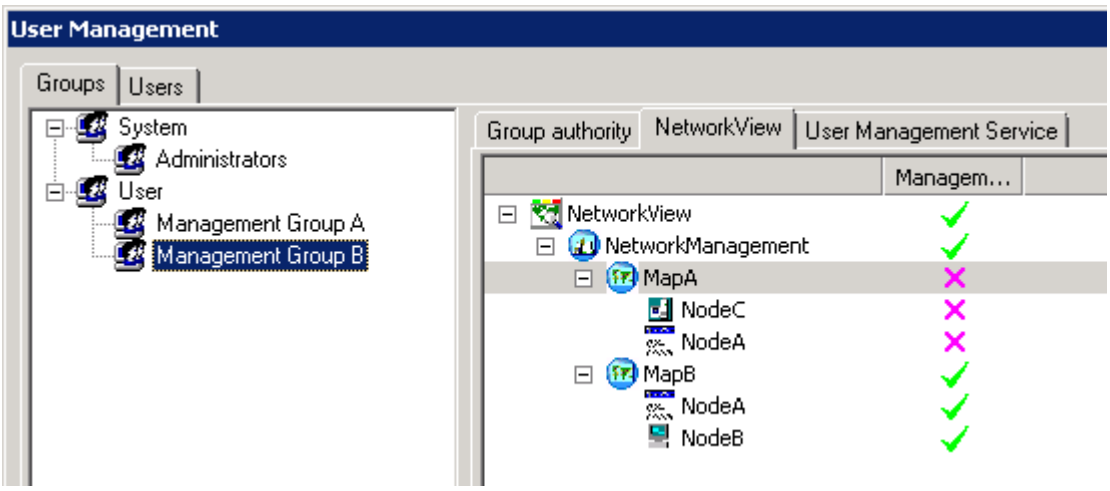
By setting the management authority to maps or devices by group, the display or operation for each group will be restricted as follows:

- Maps, devices, connection lines, and port names without the management authority are not displayed.
- Alerts from the device without management authority is not displayed.
- Users who belong to a group that has one or more maps or devices without management authority (hereafter referred to as an ordinary user) are limited to displaying and editing of part of menus, properties. Users who belong to a group that has all maps and devices with the management authority have no limit.

User with full authority	In **Management** column, all maps and devices that are registered in the Network View are checked as ✓. (No ✗)
Ordinary User	In **Management** column, any one of maps or devices that are registered in the Network View has ✗. For items to be limited for the "ordinary user", refer to "4.1.3.3.1 Items restricted for ordinary users (page 120)".
User with no authority	In **Management** column, Network View is ✗ (all maps and devices are ✗). Users cannot use any of Network Manager functions.

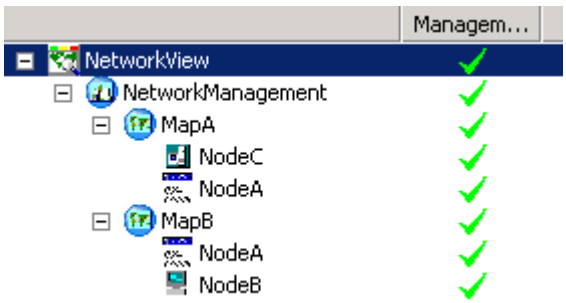
Inheritance of the management authority

- When the manager adds a new map or a new node, the newly added map or node inherits the management authority of of the upper map (one level higher).

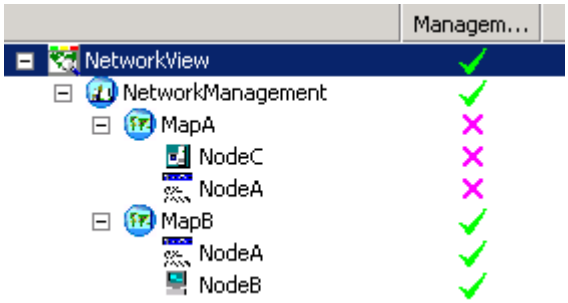


In the above figure, when the administrator adds "NodeC" to "MapA", "NodeC" is registered as , because the upper "MapA" is ✕ . If "NodeC" is registered in "MapB", "NodeC" is registered as ✓ .

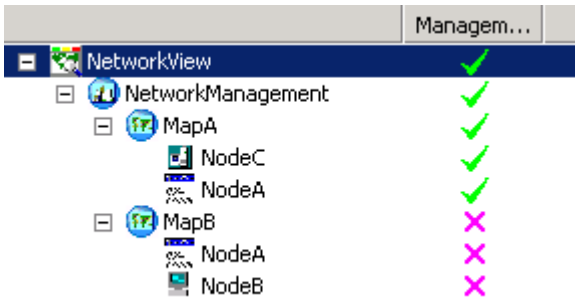
- The authority of the upper map is automatically inherited to the lower map.



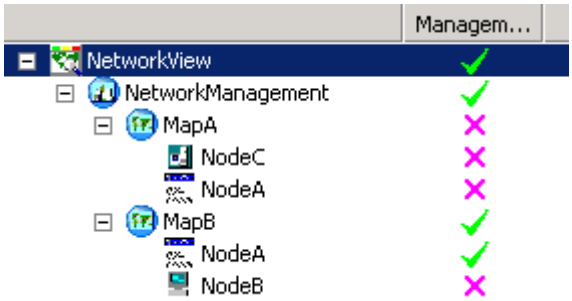
If "MapA" is changed to ✕ , the lower "NodeA" and "NodeC" are also changed to ✕ .



- If the management authority is assigned to the devices included in a map without management authority, the authority is assigned to the map including the device.



If the "NodeA" of "MapB" is changed to ✓, the above "MapB" is also changed to ✓.

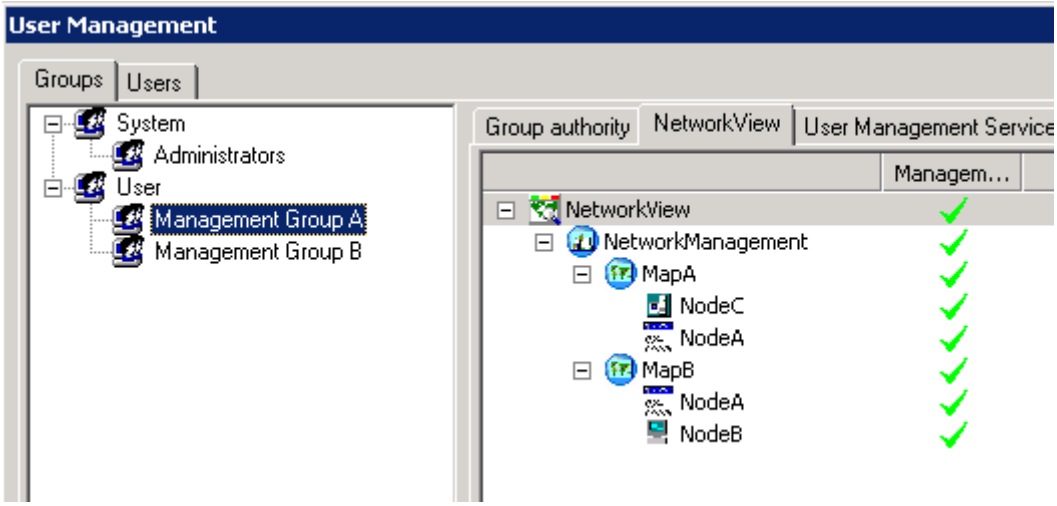


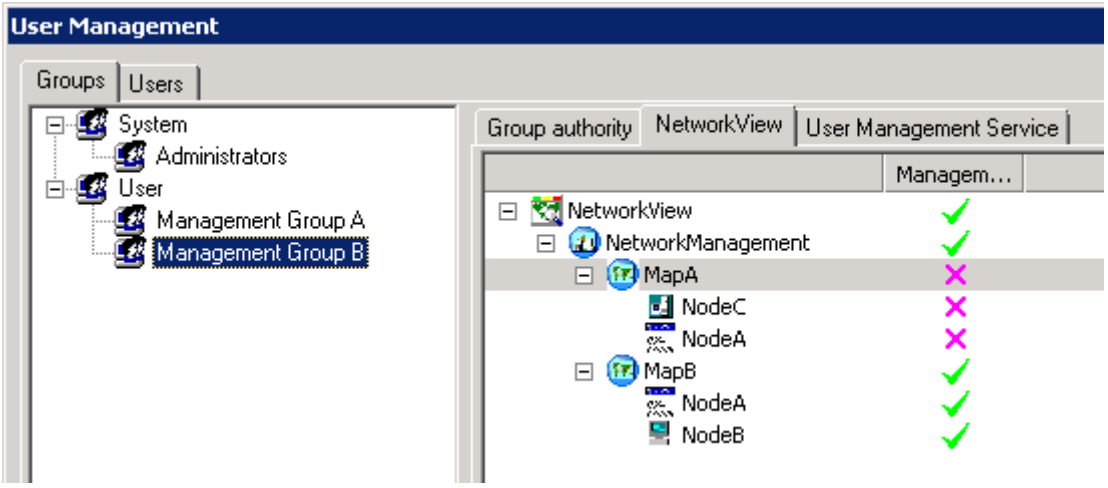
- If multiple icons that indicate the same device are registered in the different maps, the separate management authority can be set to the same device icons.

Effect on the other user groups by the management authority

If there is a group that a different management authority is set to a map or device, the following behaviors occurs. For this reason, it is recommended that the allocation of the authority should be fully discussed among the system users.

For instance, if an administrator configures the setting as follows, the member of the "Management Group A" is only able to manage both "Map A" and "Map B", the member of "Management Group B" is only able to icons under "Map B". In such a status, moving a map or a device. or changing the management authority could effect on respective groups.





- If a device icon is copied or moved to a map that a specified group is unable to manage, users belonging to the specified group become able to manage this map.

  In the above example, if an administrator copies or moves the "NodeB" icon to the "MapB", the members of the "Management Group B" become able to manage "MapA" and "NodeB". However, "NodeA" and "NodeC" under "MapA" are not displayed.

- While viewing the monitoring screen, if the management authority on the currently displayed map or device disappears, icons of maps or devices, and the alert of the devices will not be displayed.

  In the above example, when an administrator deprives the "Management Group A" of the management authority on "NodeA" under "MapA", the members of "Management Group A" become unable to view the "NodeA" icon and alerts from "NodeA", etc. Alerts that have been displayed before the management authority is updated keep being displayed until restarting the monitoring view or searching alerts again.

- When multiple icons indicating the same device are registered in the Network View, users can use the functions that do not originate from a specific icon, such as displaying alerts, data collecting function, Resource Manager function, etc. until the management authority is lost on all icons.

Items restricted for ordinary users

For the "ordinary users" who have one or more unmanaged devices or maps, part of the menus, properties and buttons are not displayed.

The items to be restricted are listed in the following.

Restrictions on the Network View menus

In the right-click menu of **NetworkView** icon, **NetworkManagement** icon, the map icon, or device icon (Network View menu), the following items marked "o" are only enabled. Menus not listed below cannot be used.

For details of all menus, refer to "6.2 Network View Menu (page 564)".

Menu Name			Network View Icon	Map Mangement Icon	Map Icon	Device Icon	Operation enable/ disable (Web monitoring view)
Configuration information management	Autodiscover	Detect physical topology				o	
	Update Device Information	Update required items				o	o
		Update all items.				o	o
	Monitoring Mode	ON				o	
		OFF				o	
	Topology Information Check Tool					o	o
	Monitoring Mode Schedule	Set				o	
		Cancel				o	
		Refer	o	o	o	o	o
	Login Information Setting		o	o	o	o	o
	Ingerface Property					o	o
	Start an Application				o	o	
	Start Web Browser				o	o	o
	Create a Command		o	o			
	Command schedule		o	o	o	o	
Fault Management	Ping (IPv4)					o	o
	Ping (IPv6)					o	o
	Remote Login					o	o
	Route Information (IPv4)					o	o
	Route Information (IPv6)					o	o
	Unrecovered alert display					o	o
	All Alert Display					o	o
Performance Management	Setting of Data collection and Report display		o	o			
	Delete a temporary file for displaying a report on the monitoring terminal		o	o			
	sFlow Setting and Display	sFlow Agent List	o	o			
Config Management	Running-config Management		o	o	o	o	
	Startup-config Management		o	o	o	o	
	Change Management		o	o	o	o	
Software Management	Software Upgrade		o	o	o	o	
Panel Window						o	

Menu Name	Network View Icon	Map Management Icon	Map Icon	Device Icon	Operation enable/disable (Web monitoring view)
Property				o	o
Move				o	o
Copy				o	o
Delete				o	o

Restrictions on the background menus of the map view

Manual Register menu is restricted.

Restrictions on the properties of the device icon

The following properties of the device icon are restricted from editing.

- **Name**
- **IP Address**
- **IPv6 Address**
- **Group**

For details of all properties, refer to "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)".

Restrictions on the properties of the connection-line

The following properties of the connection-line are restricted from editing.

- **Line Name**
- **Name** of source and destination device
- **IP Address** of source and destination device

For details of all properties, refer to "4.2.3.3.2 Connection-line Properties dialog box (page 154)".

Disabled menus and buttons in each function

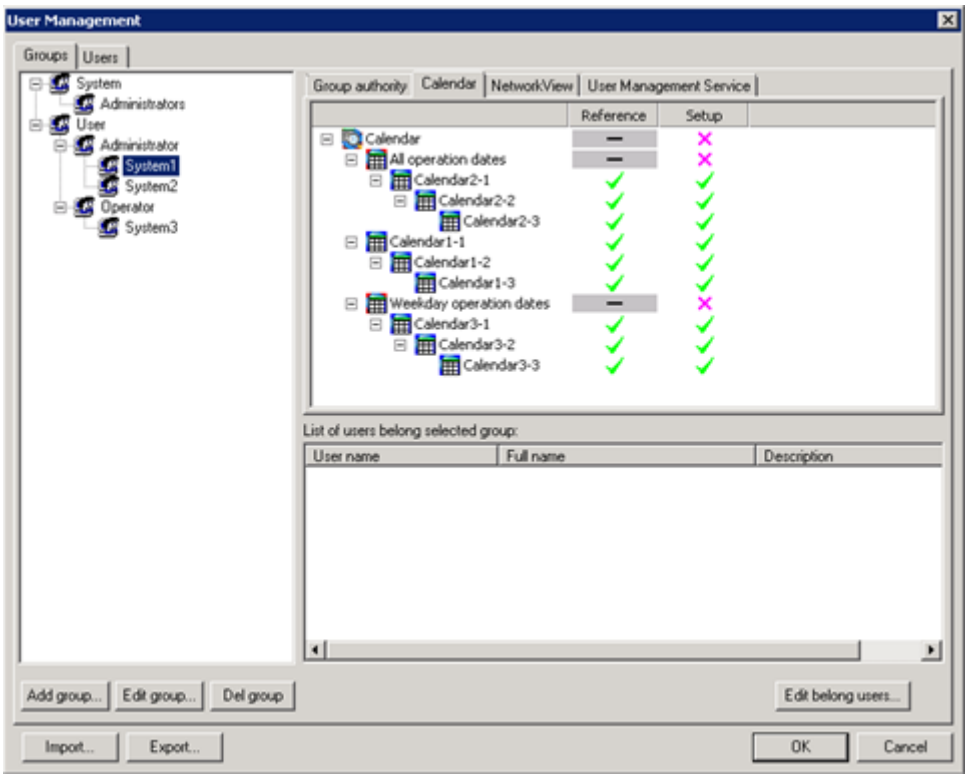
Some menus and buttons are disabled in operating the window of each function.

- Command Creation window ("4.19.1 Defining commands (page 391)")
  - **Command Creation** menu
  - **Edit Command** menu
  - **Delete Command** menu
  - **Upload** menu
- Command Scheduling window ("4.19.2 Scheduling command execution (page 398)")
  - **Execute Scheduling** menu

  - **Start Schedule** menu
- Data Collecting Setting window ("4.16.1 Data Collecting Setting window (page 334)")
  - **New** button
  - **Modify** button
  - **Delete** button
  - **Start Collecting** button
  - **Stop Collecting** button
  - **Reference** button
- sFlow Agent List window ("4.17.1.1 sFlow Agent List window (page 374)")
  - **Add** button
  - **Delete** button
- Check Configuration window ("4.20.2.1 Check Configuration window (page 404)")
  - **Start Checking** menu
  - **Stop Checking** menu
  - **Pause Checking** menu
- Software Upgrade window ("5.15.2.1 Deploying a software file (page 543)")
  - **Reboot Scheduling** menu
  - **Cancel Reboot** menu
- Alert Management tab ("5.1.3 Referencing the new alert list (page 449)")
  - **Search trap definition** menu
  - **Add trap definition** menu
- Alert Management window ("5.1.4 Managing alerts (page 456)")
  - **Search trap definition** menu
  - **Add trap definition** menu
- Alert Detail dialog box ("5.1.3.1 Alert Detail dialog box (page 451)")
  - **Search trap definition** button
  - **Add trap definition** button

4.1.3.4 Detailed authority settings of the calendar

The authority setting to specify the detailed management confines on the calendar is configured on the **Calendar** tab of the User Management window (Group).



The Authority for the root node (calendar node) of the calendar settings and operations of the calendar has the following types.

- Reference authority

  Refer to calendars.

  This authority can be added to every calendar except the root node (Calendar node) and built-in calendars (All operation dates, Weekday operation dates).

  "-" indicates that it cannot be changed.

  The root node (Calendar node) does not need a reference authority because it is not an entity of the calendar. Built-in calendars (All operation dates, Weekday operation dates) can be referenced by all users.

- Setup authority

  Add, update, and delete calendars.

  This authority can be added to every calendar except the root node (Calendar node) and built-in calendars (All operation dates, Weekday operation dates).

Tip

You can differentiate between built-in calendars (All operation dates, Weekday operation dates) and calendars added by users because their icons are different.

Icon	Description
	Icon for the root node (Calendar node).
	Icon for built-in calendars (All operation dates, Weekday operation dates).

Icon	Description
	Icon for added calendars.

Caution

- A newly created calendar inherits the reference and setup authorities from its parent calendar.
- Users who do not belong to any group can refer to built-in calendars (All operation dates, Weekday operation dates) only.

4.1.4 Importing and exporting user information

4.1.4.1 Exporting user information

Export all user management information to an external file.

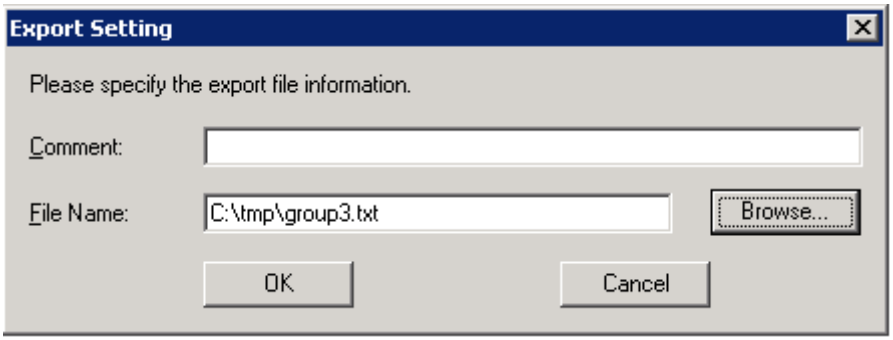
Only the default user "Administrator" can export user information.

You must first change to the "configuration mode (page 27)".

1. Open the "4.1.1.1 User Management window (**Users** tab) (page 101)".

   In the main menu, select **Setting**>**User Management**.

2. Click **Export** button to open the Export Setting dialog box.



- **Comment**

  Specify a comment explaining the exported file. In importing, the comment is displayed in the **Comment** column of the Import Setting dialog box.

- **File Name**

  To specify an export file, click **Browse** button.

Caution

The export may fail if there is a path name for the destination file location that includes "nul" (either uppercase or lowercase). Specify a path name that does not contain "nul" (either uppercase or lowercase).

3. Click **OK** button.

Caution

- When an exported file is imported, a password is not set for the user of the "text authentication". After import, set the password in "4.1.1.1 User Management window (**Users** tab) (page 101)".

- When exported information is imported into another environment, only the group authority can be inherited. Authorities other than the group authority must be reconfigured after import.
- Exported information does not contain Administrator user information.
- When the authority setting target is deleted and then recreated, the settings cannot be inherited after import even if the same name is used.

4.1.4.2 Importing user information

Make changes in a batch to user management information with a specified external file.

Only a default user "Administrator" can import user information.

You must first change to the "configuration mode (page 27)".

1. Create an import file.

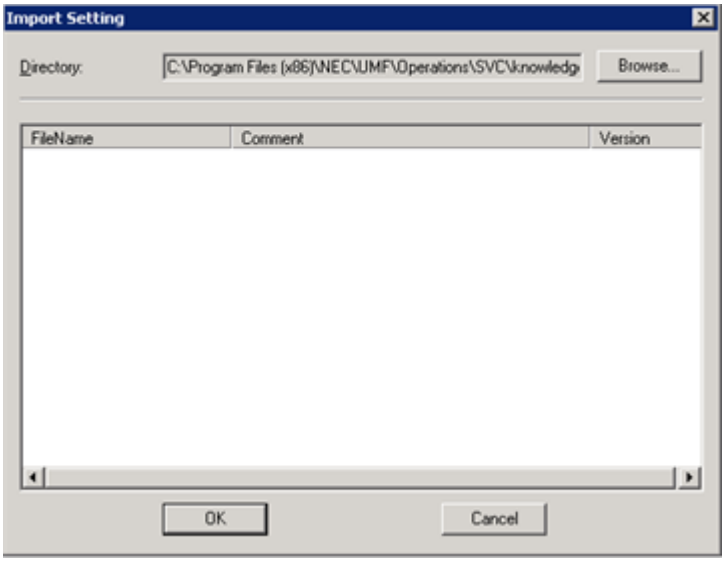
   Caution

   You cannot use other than an exported file in advance. An exported file cannot be edited.

2. Open the "4.1.1.1 User Management window (**Users** tab) (page 101)".

   In the main menu, select **Setting**>**User Management**.

3. Click **Import** button to open Import Setting dialog box.



4. Click **Browse** button, and then specify the directory in which an import file exists.

   A list of files that can be imported is displayed.

5. Select the file that you want to import, and click **OK** button.

   If an error occurs during the import, the import process will be stopped and the user management information will not be updated. Confirm that there are no errors in the import file.

   Caution

   A password is not set to the user information of the "text authentication" that was added by importing operation. After import, set the password in the "4.1.1.1 User Management window (**Users** tab) (page 101)".

4.2 Creating Network Configuration Map

In Network Manager, managed networks and devices must be registered under the Map View of **NetworkManagement** icon below the **NetworkView** icon.

The following three methods can be used to register a device.

- Autodiscover
  - Autodiscover (TCP/IP Hosts)

    Searches under the currently selected map icon for unregistered TCP/IP hosts with IP addresses that fall within the specified range, and if found, registers them as devices. For details, refer to "4.2.1.1 Performing autodiscover (TCP/IP Hosts) (page 127)".
  - Autodiscover (Network or Router)

    Searches for unregistered routers or networks with IP addresses within a fixed hop from a specified device and, if found, registers them as devices. For details, refer to "4.2.1.2 Performing autodiscover (networks and routers) (page 136)".
- Manual Register

  Manually registers devices and sub maps under the currently selected map icon. For details, refer to "4.2.2 Manually registering devices and networks (page 138)".
- Batch Register

  Devices, maps and topology information can be registered in a batch by importing an external file. For details, refer to "4.6 Batch Registering or Deleting Configuration Information (page 206)".

⚠ Caution

1. You can register up to the number of devices stipulated in the basic license. The number of maps and connection lines (physical topology) that can be registered is not limited by the license.
2. It is recommended that a maximum of 250 devices be registered in a map. When you register more than 250 devices by using Autodiscover or in batch, it may take a long time to complete registration.
3. In Autodiscover, during automatic discovering, the manager communicates with devices in the network using SNMP and obtains the name of the devices. If multiple devices in the network have the same device name, or a device in the network has the same device name as the already registered device, they are considered as the same device, and may be overwritten. The device name is obtained from the following MIB value implemented by the device.

   iso.org.dod.internet.mgmt.mib-2.system.sysName
4. You can locate the device icon onto multiple map by setting the same node name. In this case, the device information is managed as an one node and only one license is consumed.

4.2.1 Automatically detecting devices and networks

4.2.1.1 Performing autodiscover (TCP/IP Hosts)

Search under the map icon for unregistered TCP/IP hosts with IP addresses that fall within the specified range, and register them as node icon. Note that autodiscover (TCP/IP host) using IPv6 protocol is not supported.

If there is a device that has multiple addresses and it belongs to the multiple networks specified for discovery, the registration process may vary in the following ways depending on the protocol settings and device types (SNMP devices/ICMP devices):

Protocol Setting	SNMP/ICMP Device	SNMP Device	ICMP Device
SNMP and ICMP	Register the highest priority address in a device 1) as SNMP node, all others as ICMP nodes	Register the highest priority address in a device 1) as SNMP node and register only one	Register all discovered addresses as ICMP nodes
Only SNMP	Register the highest priority address in a device 1) as SNMP node and register only one	Register the highest priority address in a device 1) as SNMP node and register only one	Do not register (not discoverable)
Only ICMP	Register all discovered addresses as ICMP nodes	Do not register (not discoverable)	Register all discovered addresses as ICMP nodes

1) The highest priority address in a device is the address that is set as the sending address when a device responds. It is dependent on the settings on the device side.

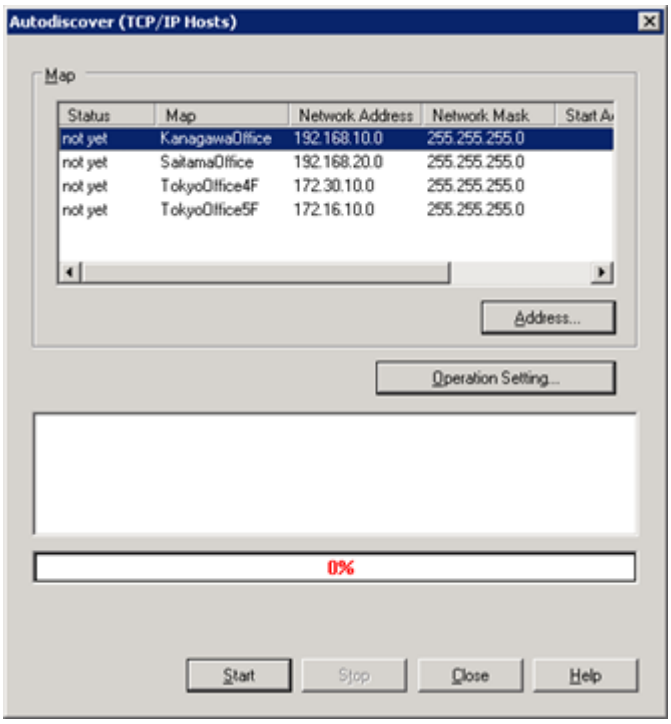
You must first change to the "configuration mode (page 27)".

1. If no map exists, create a map first.

   There are no subordinate maps under the **NetworkManagement** icon when Network Manager is first installed. For this reason, if **Auto discover (TCP/IP Hosts)** is executed, it is necessary to manually register maps prior to performing autodiscover (TCP/IP Hosts). For details of manual register of map, refer to "4.2.2 Manually registering devices and networks (page 138)".

2. Open the "4.2.1.1.1 Autodiscover (TCP/IP Hosts) dialog box (page 131)".

   Right-click the **NetworkManagement** icon or the map icon, and select **Configuration Management**>**Autodiscover**>**TCP/IP Hosts**.

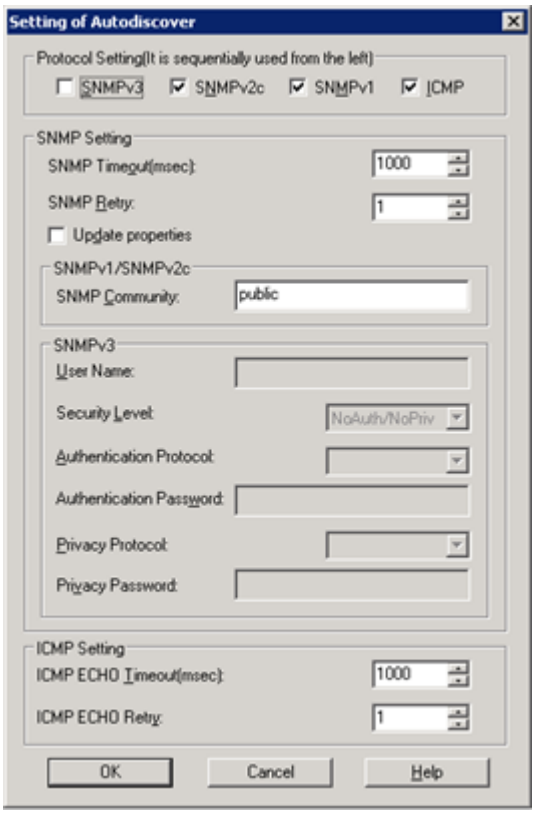


3. In the Autodiscover (TCP/IP Hosts) dialog box, select the map that you want to search with autodiscover.

4. To change the range of the address that will be searched, click **Address** button to start "4.2.1.1.2 Address dialog box (page 131)".

It is usually not necessary to change this.

5. To specify the operation mode of autodiscover such as discovery protocol setting, etc. to be used for autodiscover, click **Operation Setting** button and set the necessary items in the Setting of Autodiscover dialog box.

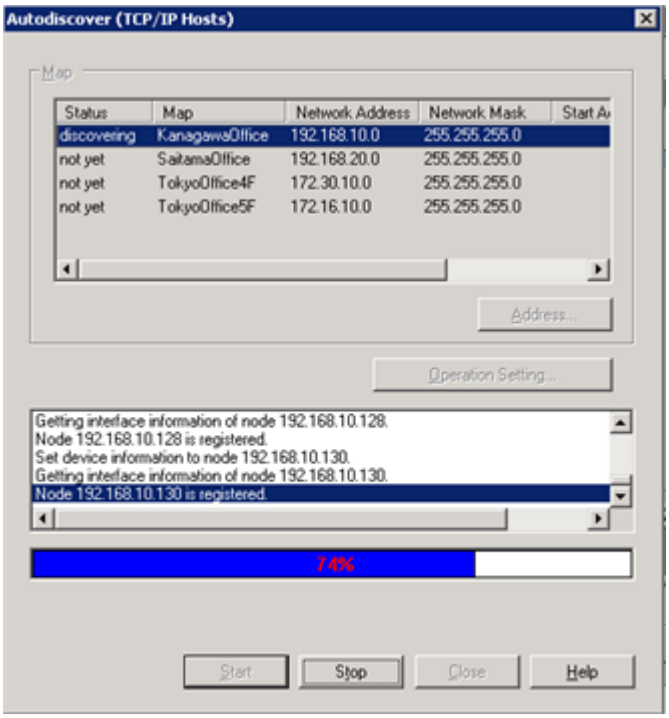


For details, refer to "4.2.1.1.3 Setting of Autodiscover dialog box (page 132)".

⚠ Caution

In accordance with the setting in the Setting of Autodiscover dialog box, perform a discovery in the order of SNMPv3, SNMPv2c, SNMPv1, and ICMP. The highest priority communication method is used to register the device information. For example, if there is no response to SNMPv3 packets, an SNMPv2c packet is sent. Next, if there is a response to SNMPv2c packets, a device is registered as SNMPv2c host. For details, refer to "4.2.1.1.3 Setting of Autodiscover dialog box (page 132)".

6. Click **Start** button.



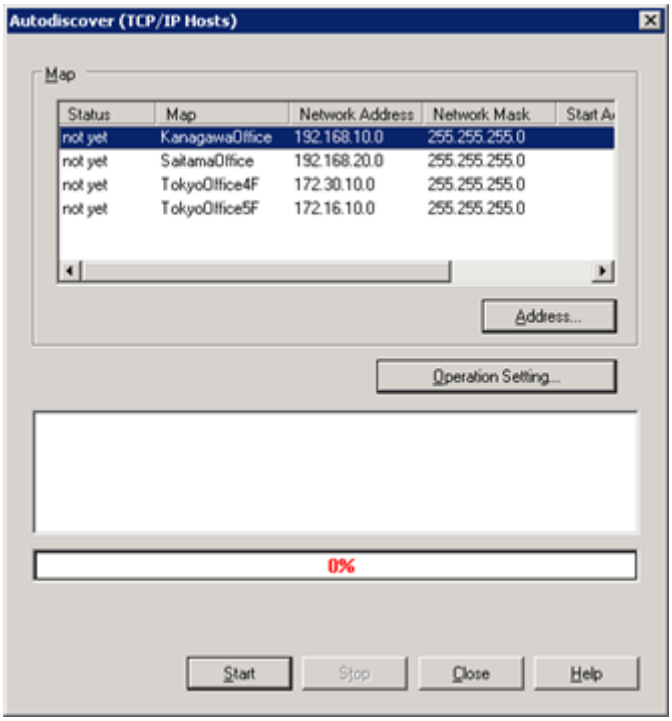
7. Click **Close** button to close the dialog box.

When a device is registered through an autodiscovery process, monitoring mode is set to OFF. If left in this mode, the device will not be included in monitoring. To perform monitoring for the device, change the monitoring mode to ON. For details, refer to, "5.13.1 Manually setting monitoring mode (page 506)".

Caution

- If the attributes (example: IP address) for an automatically discovered device are not correct, check if an icon with the same name or IP address has already been registered. An icon has already been registered with the same name or same IP address, Network Manager assumes that they are the same device (that the device has already been registered) and does not overwrite the attributes. As a result, the newly discovered device icon is given the same attributes as the icon that has already been registered. To avoid this situation, in the "4.2.1.1.3 Setting of Autodiscover dialog box (page 132)", select **Update properties** when performing autodiscover.
- If you are using a version of BIG-IP 3900 that is lower than Version 10.1, the icon displayed during Autodiscover is the general BIG-IP icon, not the BIG-IP 3900 icon. To correctly display the device front panel, you need to either change the icon type to "BIG-IP3900" or the attribute value for **Device Front Panel** to "BIG-IP3900".
- If the node name is set to "nul" (either uppercase or lowercase), some functions may work incorrectly. Change the node name. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".
- In the case of some models such as IP8800 series, P38X series, Catalyst3750 series, an icon different from the actual model may be registered. This is because the manager can not automatically identify the icon type to be registered from the MIB information obtained in the autodiscover. (Implementation of the target devices indicates multiple models with the same ID, etc.) In such a case, change the icon type by manual. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".
- If invalid addresses such as network address, broadcast address, etc. are included in the target range of the autodicover, the autodiscover may be aborted, or an device different from the specified address may be registered. In this case, confirm if the manager network setting, or the setting of the network address/net mask of the discover target map of "Autodiscover (TCP/IP hosts)" is configured properly.
- If any non-ASCII character is included in the property information automatically set in atuodiscover, they may not be displayed correctly.

Autodiscover (TCP/IP Hosts) dialog box



- **Map**

  Allows you to select the map in which you will perform autodiscover. All maps registered in Network Manager are displayed in this area. If a network address or network mask has not been set up for a map, the IPv4 network address that the manager machine is connected to is displayed as the default value.

- **Address** button

  Opens the Address dialog box. For details, refer to "4.2.1.1.2 Address dialog box (page 131)".

- **Operation Setting** button

  Opens the Setting of Autodiscover dialog box. For details, refer to "4.2.1.1.3 Setting of Autodiscover dialog box (page 132)".

- **Start** button

  Starts autodiscover.

- **Stop** button

  Suspends autodiscover.

- **Close** button

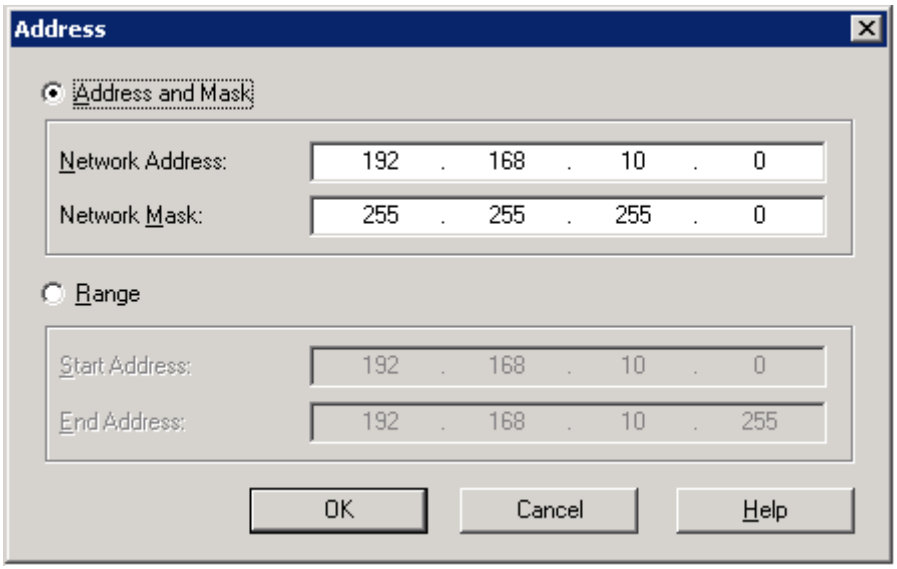
  Closes the dialog box.

- **Help** button

  Displays Help.

Address dialog box

Sets the range for autodiscover.



- **Address and Mask**

  Specify the network address and network mask for autodiscover.

- **Range**

  Specify the starting and ending IP address for autodiscover. The range that can be specified is the address/mask range.

  Caution

  If the specified range has a network address, broadcast address, or invalid address, the autodiscover process may be terminated or unexpected devices may be registered. Check whether the specified address range is correct in advance.

- **OK** button

  Applies the values that have been set.

- **Cancel** button

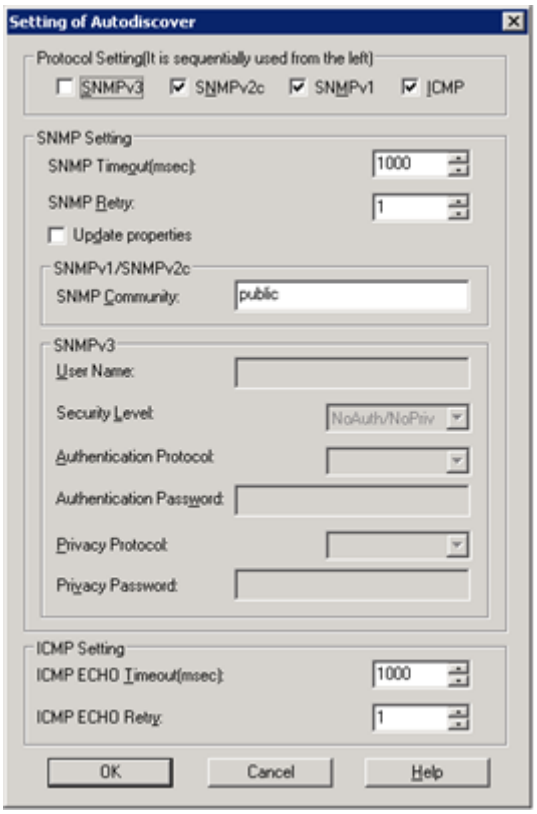
  Cancels the entered information.

- **Help** button

  Displays Help.

Setting of Autodiscover dialog box

Sets detailed parameters for autodiscover.



- **Protocol Setting**

  Select the protocol to be used in the Autodiscover. You can select multiple protocols. In the Autodiscover, they are used in the order of **SNMPv3**, **SNMPv2c**, **SNMPv1**, **ICMP**.

  Hosts that cannot be discovered at the highest-priority protocol are discovered using the next protocol. As an example of how to specify the method, if you want to discover devices that only respond to SNMPv2c, only select **SNMPv2c**. To run an Autodiscover, you need to specify at least one method.

  The table below shows the settings that are valid for each protocol setting. For details of each setting item, refer to each item in this section.

Protocol Setting		Valid Setting
SNMP Setting	Common	SNMP Timeout
		SNMP Retry
		Update properties
	SNMPv3	User Name
		Security Level
		Authentication Protocol
		Authentication Password
		Privacy Protocol
		Privacy Password
	SNMPv2c/SNMPv1	SNMP Community
ICMP Setting	-	ICMP ECHO TImeout (msec)
		ICMP ECHO Retry

- **SNMP Setting**
  - **SNMP Timeout**

    Specify the monitoring time in milliseconds for the SNMP response receipt in response to the SNMP Request message. Specify a value within the range of 1 - 60,000. This item is valid when either **SNMPv1**, **SNMPv2c**, or **SNMPv3** is selected as the **Protocol Setting**.
  - **SNMP Retry**

    Specify the number of times the SNMP Request will be resent in the event that an SNMP timeout occurs. Specify a value within the range of 1 - 10.
  - **Update properties**

    Specify whether or not to overwrite registration information in the event that a registered node is discovered again. The properties that are overwritten are only what are used or retrieved in the Autodiscover. Properties which is not used or retrieved in the Autodiscover are not overwritten.

    To make the required updates to device information, it is recommend to delete the device and then perform another Autodiscover operation for that device.
  - **SNMPv1/SNMPv2c**
    - **SNMP Community**

      Specify SNMP community name to be used for SNMPv1 or SNMPv2c communications. The name can be up to 255 characters in length. Multiple names can be specified using a comma (,) separator.
  - **SNMPv3**
    - **User Name**

      Specify a user name to be used in SNMPv3 communication. The name can be up to 32 characters in length.Valid characters are ASCII characters. Only one user name can be specified. It must be specified if you will be using SNMPv3 communication.
    - **Security Level**

      Specify the security level to be used in SNMPv3 communication. Any of the three levels below can be specified. This setting should be selected in conjunction with the settings on the device to be autodiscovered. It must be specified if you will be using SNMPv3 communications.

Security Level	Description
NoAuth/NoPriv	Authentication such as MD5 and SHA1 is not performed. Packet encryption is also not performed.
Auth/NoPriv	Authentication is performed using the specified authentication protocol. Packet encryption is not performed.
Auth/Priv	Authentication is performed using the specified authentication protocol. Packets are encrypted using the specified privacy protocol.
    - **Authentication Protocol**

      Specify the protocol to be used in the authentication of SNMPv3 communication. You can specify either "MD5" or "SHA1". This setting should be selected in conjunction with the settings on the device to be autodiscovered. It must be specified if you have specified "Auth/NoPriv" or "Auth/Priv" in the **Security Level**.

* **Authentication Password**

  Specify an authentication password to be used in SNMPv3 communication. This setting should be selected in conjunction with the settings on the device to be autodiscovered. The password can be between 8 and 255 characters in length. Valid characters are ASCII characters. It must be specified if you have specified "Auth/NoPriv" or "Auth/Priv" in the **Security Level**. After a password is entered, it will be displayed as eight "********" characters.

* **Privacy Protocol**

  Specify the encryption method to be used in SNMPv3 communication. This setting should be selected in conjunction with the settings on the device to be autodiscovered. "DES" can be specified. An encryption method must be specified if you have specified "Auth/Priv" in the **Security Level**.

* **Privacy Password**

  Specify an encryption password to be used in SNMPv3 communication. This setting should be selected in conjunction with the settings on the device to be autodiscovered. The password can be between 8 and 255 characters in length. Valid characters are ASCII characters. An encryption method must be specified if you have specified "Auth/Priv" in the Security Level. After a password is entered, it will be displayed as eight "********" characters.

Caution

When using SNMPv3 communication, all discovery target devices will be discovered using a security model that contains one set of the information set up here (the **User Name**, **Security Level**, **Authentication Protcol**, **Authentication Password**, **Privacy Protocol**, **Privacy Password**). If you are performing the discovery using only SNMPv3 communication and multiple security models are set to target devices, you need to perform multiple discoveries for each security model.

- **ICMP Setting**
  - **ICMP ECHO Timeout**

    Specify the monitoring time in milliseconds for the receipt of an ICMP Echo Reply message in response to the transmission of the ICMP ECHO Request message. Specify a value within the range of 1 - 60,000.

  - **ICMP ECHO Retry**

    Specify the number of times the ICMP ECHO Request message will be resent in the event that an ICMP ECHO timeout occurs. Specify a value within the range of 1 - 10.

  - **OK** button

    Applies the values that have been set.

  - **Cancel** button

    Cancels the entered information.

  - **Help** button

    Displays Help.

Apart from protocol settings, the items that can be specified are shown in the list below.

o : required, + : optional, - : not used

Item	SNMPv3			SNMPv2c	SNMPv1	ICMP
	Security Level					
	NoAuth/ NoPriv	Auth/ NoPriv	Auth/Priv			
SNMP Timeout	o	o	o	o	o	-
SNMP Retry	o	o	o	o	o	-
Update properties	+	+	+	+	+	-
SNMP Community	-	-	-	o	o	-
User Name	o	o	o	-	-	-
Security Level	o	o	o	-	-	-
Authentication Password	-	o	o	-	-	-
Privacy Password	-	-	o	-	-	-
ICMP ECHO Retry	-	-	-	-	-	o

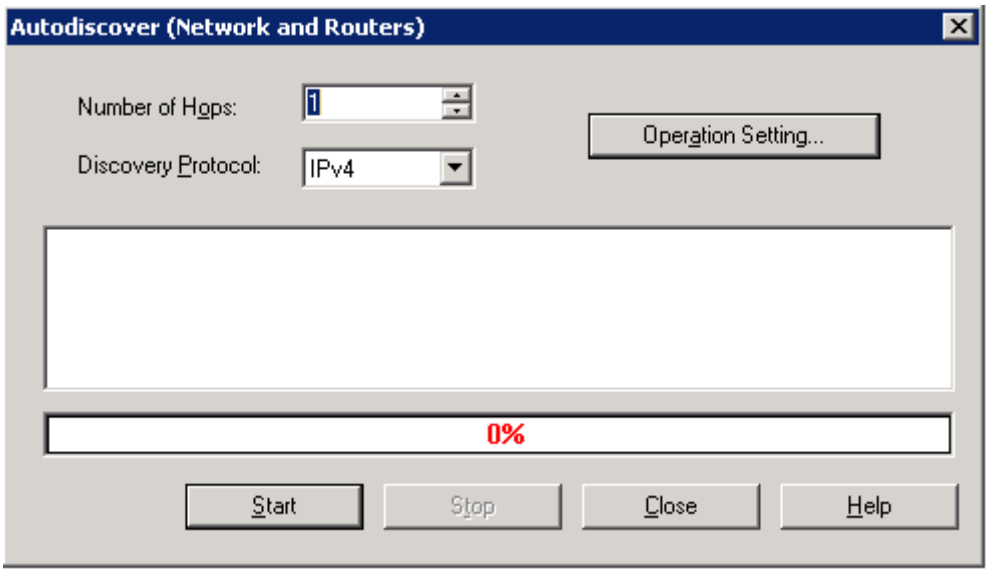
4.2.1.2 Performing autodiscover (networks and routers)

Search for unregistered routers and networks and register discovered routers and networks.

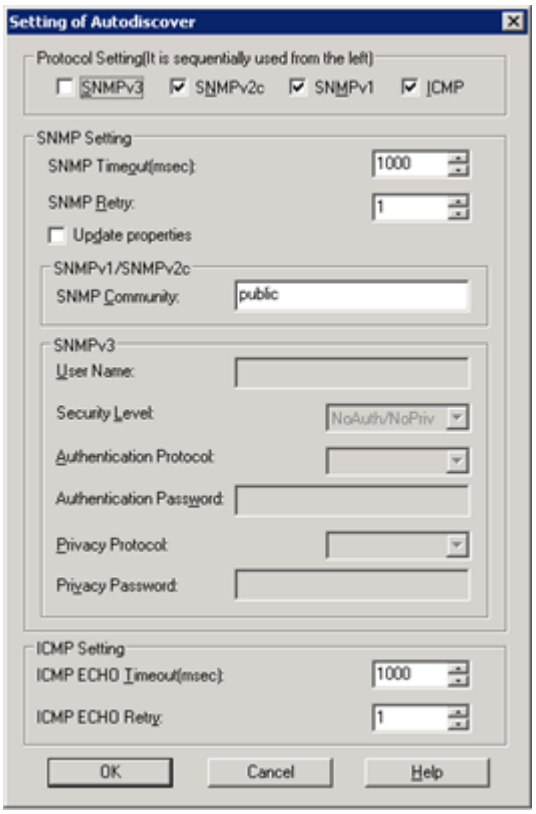
You must first change to the "configuration mode (page 27)".

1. Open the "4.2.1.2.1 Autodiscover (Network and Routers) dialog box (page 137)".

   Right-click the device icon and select **Configuration Management**>**Autodiscover**>**Network and Routers**.



2. In the Autodiscover (Network and Routers) dialog box, specify the **Number of Hops** within which you want to perform autodiscover.
3. To configure the Autodiscovery settings such as the discovery protocol, click the **Operation Setting** button and set the necessary items.



For details, refer to "4.2.1.1.3 Setting of Autodiscover dialog box (page 132)".

4. Click **Start** button.
5. Click **Close** button to close the dialog box.

If you are performing a discovery using the "IPv6" discovery protocol, the map name and the name of the device discovered using ICMP protocol will be converted from the IPv6 address notation of ":" to a "-" notation.

When a device is registered through an autodiscovery process, monitoring mode is set to OFF. If left in this mode, the device will not be included in monitoring. To perform monitoring for the device, change the monitoring mode to ON. For details, refer to, "5.13.1 Manually setting monitoring mode (page 506)".

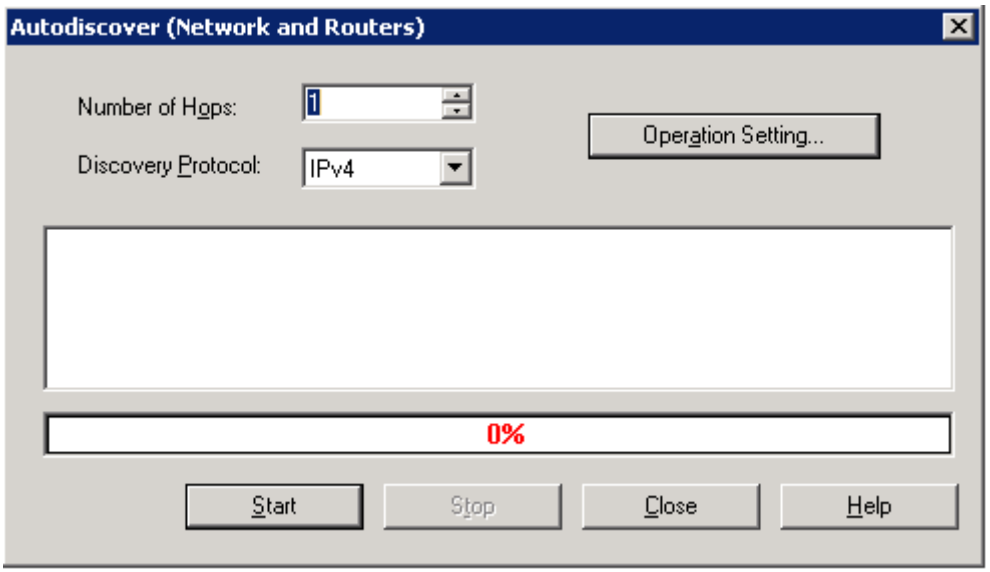
Caution

- If the attributes (example: IP address) for an automatically discovered device are not correct, check if an icon with the same name or IP address has already been registered.

  An icon has already been registered with the same name or same IP address, Network Manager assumes that they are the same device (that the device has already been registered) and does not overwrite the attributes. As a result, the newly discovered device icon is given the same attributes as the icon that has already been registered.

  To avoid this situation, in the "4.2.1.1.3 Setting of Autodiscover dialog box (page 132)", select **Update properties**when performing autodiscover.
- If any non-ASCII character is included in the property information automatically set in atuodiscover, they may not be displayed correctly.

Autodiscover (Network and Routers) dialog box



- **Number of Hops**

  Specify the range (number of hops) that you want to search.

- **Discovery Protocol**

  Specify the protocol to be used when discovering. In the property items for an icon, if a value has been set for the IP address, "IPv4" can be set. If a value has been set for the IPv6 address, "IPv6" can be set.

- **Operation Setting** button

  Opens the Setting of Autodiscover dialog box. For details, refer to "4.2.1.1.3 Setting of Autodiscover dialog box (page 132)".

- **Start** button

  Starts autodiscover.

- **Stop** button

  Suspends autodiscover.

- **Close** button

  Closes the dialog box.

- **Help** button

  Displays Help.

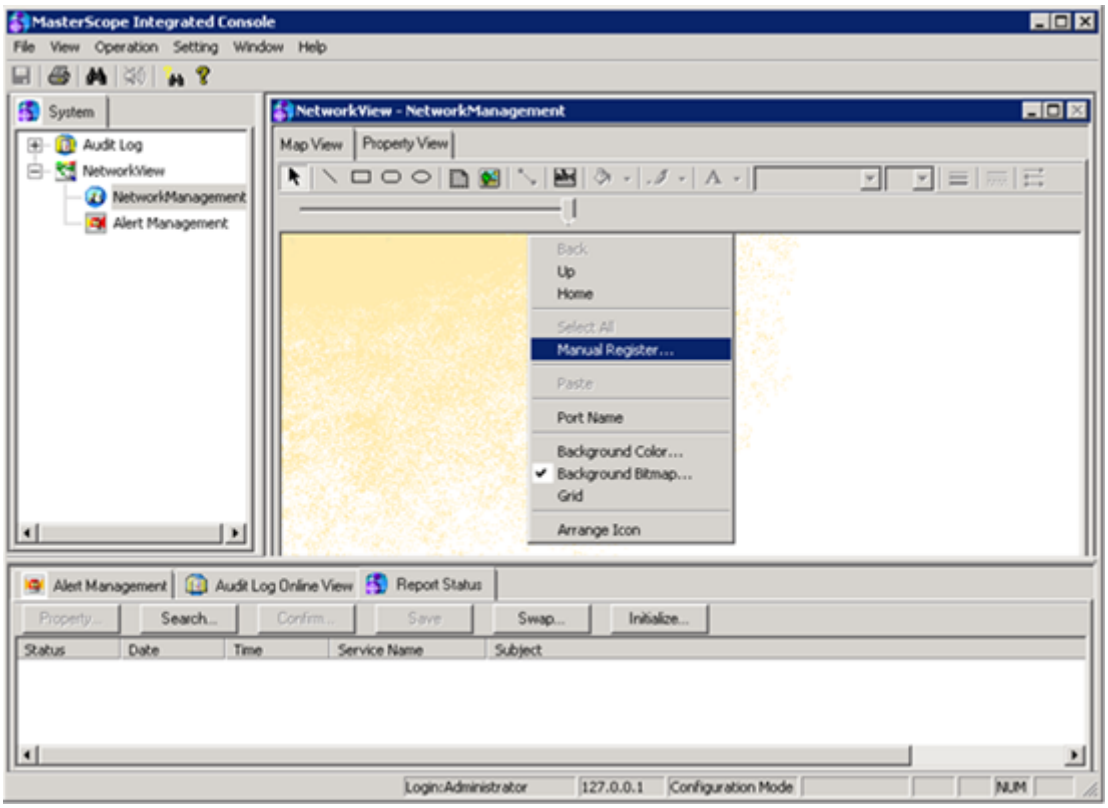
4.2.2 Manually registering devices and networks

Set a name or type, etc. of device or network map by manual, and register them.

You must first change to the "configuration mode (page 27)".

1. Open the Manual Register dialog box.

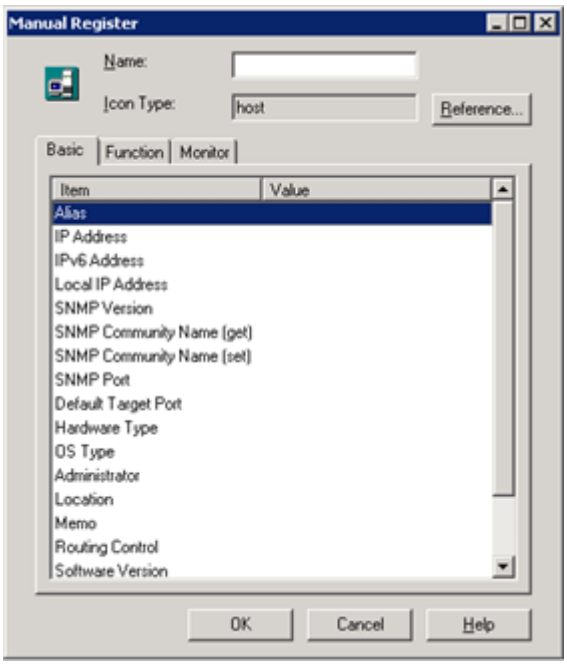
   In the Map View of the **NetworkManagement** icon or the map icon , right-click without selecting the icon and select **Manual Register** menu.



2. Set the following value in the Manual Register dialog box.

Tip

This section describes on the assumption that all properties should be set by manual. However, the setting of parameters can be simplified by using the update of device information function. For details of the update of device information, refer to "4.2.7 Updating device information via a network (page 179)".



- **Name**

- When registering a device, enter a device name.
- When registering a map, enter a map name.

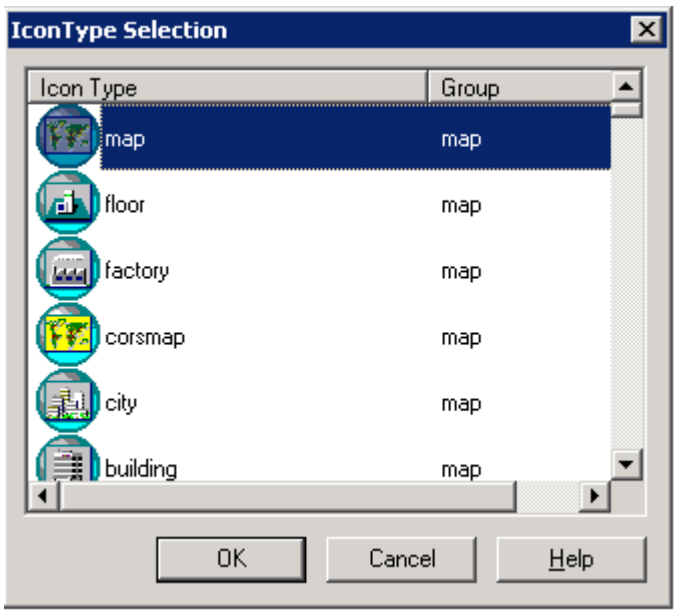
Caution

a. Valid characters for the node and map name include alphanumeric characters, multi-byte characters, hyphen (-), underscore (_), and dot (.). If specifying Unicode surrogate pair characters or "nul" (either uppercase or lowercase), some function may work incorrectly. Do not use Unicode surrogate pair characters and "nul" as the node and map name.

b. If an icon with the same name is already registered, Network Manager overwrites the properties of the existent icon, except the **Icon Type**. If there are no special operational reasons, it is recommended to set the same **Icon Type** for all icons of the same device.

- **Icon Type**

Specify an icon in the "4.2.2.2 Icon Type Selection dialog box (page 146)".



- When a registering device, select an icon type displayed as "node" in the **Group** column.
- When a registering map, select an icon type displayed as "map" in the **Group** column.

If necessary, specify the other properties. For details, refer to "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)".

Caution

If monitoring mode is not selected in the icon properties during Manual Register dialog box, monitoring mode will not be set. If monitoring mode is not set, monitoring mode will be shown as off. If left in this mode, the device will not be included in monitoring. To perform monitoring for the device, change the monitoring mode to ON. For details, refer to "5.13.1 Manually setting monitoring mode (page 506)".

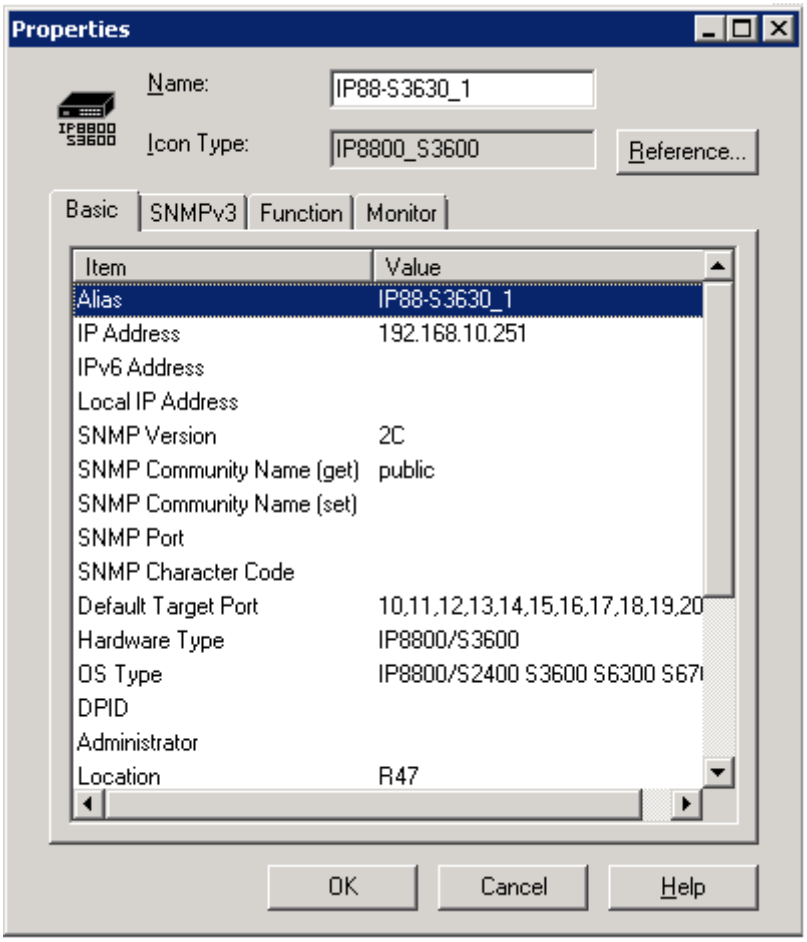
3. Click **OK** button.

4.2.2.1 Manual Register dialog box and Properties dialog box

Displays information for devices being maintained by Network Manager.

To make changes to the information for devices being maintained by Network Manager, double-click each item.

You must change to "configuration mode (page 27)" to make changes to device information.



- **Name**

  Enter a node name up to 63 characters. This is a required parameter. Valid characters include alphanumeric characters, multi-byte characters, hyphens (-), underscores (_), dots (.). If specifying Unicode surrogate pair characters or "nul" (either uppercase or lowercase), some function may work incorrectly. Do not use Unicode surrogate pair characters and "nul".

- **Icon Type**

  Select the icon type. Click **Reference** button to display the Icon Type Selection dialog box. For details, refer to "4.2.2.2 Icon Type Selection dialog box (page 146)".

  Caution

  When you place an icon indicating the same device on multiple maps, you can specify a different value for each icon only in this property. However, it is recommended that the same **Icon Type** be specified for all icons indicating the same device for operational reasons if there is no specific purpose.

- **Basic** tab

  To edit properties, double-click each item.

  - **Alias**

    Specify an alias for the node. The value set here is not displayed in the map. This is optional.

- **IP Address**

  Specify an IP address for the node. If the node is connected via a NAT, specify the IP address that will be seen by Network Manager.

- **IPv6 Address**

  Specify an IPv6 address for the node. If the node is connected via a NAT, specify the IPv6 address that will be seen by Network Manager. The only address that can be specified is a global unicast address.

- **Local IP Address**

  Specify the local IP address for the node. If the node is connected via a NAT, specify the actual IP address for that node.

- **SNMP Version**

  Select an SNMP version for the node. When performing SNMP communication with a device, such as through the Update Property function, SNMP communication is performed using the version specified in this setting. In addition, if "1" or "2C" is selected as the SNMP version, the **SNMP Community Name (get)** / **SNMP Community Name (set)** is used in SNMP communication. If "3" is selected, the values in the **SNMPv3** tab are used.

- **SNMP Community Name (get)**

  Specify a SNMP Get community name. If "1" or "2C" is selected as the **SNMP Version**, it must be set correctly because it is used in SNMP communication.

- **SNMP Community Name (set)**

  Specify a SNMP Set community name. If "1" or "2C" is selected as the **SNMP Version**, it must be set correctly because it is used in SNMP communication. If this item is omitted, the community name specified in **SNMP Community Name (get)**.

- **SNMP Port**

  Specify a port number used for SNMP Get communication. Valid range is between 1 to 65535. If omitted, a default port "161" is used. For SNMP Set communication, a default port "161" is always used.

- **SNMP Character Code**

  Select the character code to interpret non-ASCII characters contained in SNMP Get/Set or SNMP trap/inform data from the following.

  * **Unicode (UTF-8)**

    Non-ASCII characters are interpreted in UTF-8. All characters are supported.

  If this is not specified, non-ASCII characters are not interpreted.

- **Default Target Port**

  Specify a default port to use for collecting data when the port is omitted in the monitoring rules and data collection settings.

  If any one of the following is executed, the default target port is set to the port ID (ifIndex) of the physical port.

  * Autodiscover (TCP/IP hosts)
  * Autodiscover (Network and Routers)
  * Device information update (Update All Property)

* In the Interface Properties dialog box, click **Discovery** button.

When the default target ports are set, reduce the number of packets for collecting data to make the process more efficient.

If **Default Target Port** column is blank, no ports are specified, or invalid ports are specified, all ports in the device are used for monitoring and collecting data.

- **Hardware Type**

  Specify the hardware type for the node. This can be omitted.

- **OS Type**

  Select the type of operating system for the node. For details, refer to "4.6.1.1.1 OS type and software version format (page 223)".

- **DPID**

  Specify Datapath ID if the device supports OpenFlow. The setting range is between 0000-0000-0000-0000 and ffffffff- ffff-fffe. This is optional.

  When the the physical topology autodiscover of ProgrammableFlow is executed, the value is automatically registered. For details, refer to "4.2.4 Registering ProgrammableFlow physical topology information (page 164)".

- **Memo**

  Specify notes relating to the device. This can be omitted.

- **Routing Control**

  Select if the node will have an IP forwarding function.

- **Software Version**

  For the device, specify the versions of software. For details, refer to "4.6.1.1.1 OS type and software version format (page 223)".

- **Serial Number**

  Specify the serial number of the device. This can be omitted.

- **Group**

  Specify groups that the node belongs to. The name of each group consist of 63 or less characters. Valid characters include alphanumeric characters, multi-byte characters, hyphens (-), underscores (_), dots (.). If specifying Unicode surrogate pair characters or "nul" (either uppercase or lowercase), some function may work incorrectly. Do not use Unicode surrogate pair characters and "nul". You can specify multiple groups by separating by a comma. The total length of all group names including commas is up to 1000. The specified group name can be used in the following functions.

  * State monitoring function

    For details, refer to "4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function) (page 241)".

  * Data collection function

    For details, refer to "4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices (page 334)".

  * Alert reporting function

    For details, refer to "4.14 Settings for Sending Alert Reports (page 310)".

In these functions, if a group name is specified in the component (target node) column, all nodes in the same group become the target of the function.

- **Device Front Panel**

  Specify a device front panel type that is compatible with the device. If this was registered during the initial set up,it does not need to be changed. For details, refer to "4.18.1 Setting for displaying device front panel (page 379)".

- **SNMPv3** tab
  - **User Name**

    Specify a valid SNMPv3 user name of the device. If "3" is selected as the **SNMP Version** in the **Basic** tab, it must be set correctly. Enter up to 32 characters. Valid characters are ASCII.

  - **EngineID**

    Specify the engine ID of the device. You can use hexadecimal notation with ":" or whitespace separators. This setting is normally configured and updated through SNMPv3 communication with the device, the "Autodiscover" function or "Update Property" function. For details of "Autodiscover" function, refer to "4.2.1.1 Performing autodiscover (TCP/IP Hosts) (page 127)" and "4.2.1.2 Performing autodiscover (networks and routers) (page 136)". For details of "Update Property" function, refer to "4.2.7 Updating device information via a network (page 179)".

  - **Security Level**

    Specify the security level to be used in SNMPv3 communication with the device. You need to set the security level that corresponds with the user specified in **User Name**. If "3" is selected as the **SNMP Version** in the **Basic** tab, it must be set correctly.

Security Level	Description
NoAuth/NoPriv	Authentication such as MD5 and SHA1 is not performed. Packet encryption is also not performed.
Auth/NoPriv	Authentication is performed using the specified authentication protocol. Packet encryption is not performed.
Auth/Priv	Authentication is performed using the specified authentication protocol. Packets are encrypted using the specified privacy protocol.

  - **Authentication Protocol**

    Specify the authentication protocol to be used in SNMPv3 communication with the device. Select the authentication protocol that corresponds to the user specified in **User Name**. You can select either "MD5" or "SHA1".

  - **Authentication Password**

    Specify the authentication password that corresponds with the user specified in **User Name**. The password can be between 8 and 255 characters in length. Valid characters are ASCII characters.

  - **Privacy Protocol**

    Specify the encryption protocol to be used in SNMPv3 communication with the device. SNMPv3 communication with the device. Select the authentication protocol that corresponds to the user specified in **User Name**. You can specify "DES".

  - **Privacy Password**

Specify the encryption password that corresponds with the user specified in **User Name**. The password can be between 8 and 255 characters in length. Valid characters are ASCII characters.

- **Severity of Invalid EngineID**

  Specify the severity of alerts that are generated when the **EngineID** property and the engine ID of the SNMPv3 trap received from the device do not match.

  The values that can be specified are the following four types. If it is omitted, an alert regarding the invalid engine ID will not be generated.

  * "Warning"
  * "Minor Fault"
  * "Major Fault"
  * "Critical State"

  For the alert severity corresponding to the specified type, refer to "4.9.2.1 About severity extension (page 237)".

- **Function** tab

  - **Application Path**

    Specify a path to the application that will be executed in **Start Application** menu. For details, refer to "4.5.1 Registering applications launched from icons (page 204)".

  - **URL**

    Specify the URL that will be displayed in **Start Web browser** menu. For details, refer to "4.5.2 Registering web URLs launched from icons (page 205)".

  - **Discovery Protocol**

    Specify the discovery protocol to determine how to process the physical topology autodiscover and topology check tool. This is automatically set depending on the icon type, but if you want to set it manually, refer to "4.2.3.1 Discovery Protocol (page 148)" and set the appropriate value.

  - **Telnet Server**

    Select if the device will be a telnet server. Check if using the remote login function.

  - **Agent Type**

    Specify the device agent type. It is usually not necessary to change this setting.

  - **Floating IP Address**

    If a ProgrammableFlow controller is a redundant configuration, specify an IP address for Web API.

    It is used in the physical topology autodiscover of ProgrammableFlow. For details, refer to "4.2.4 Registering ProgrammableFlow physical topology information (page 164)".

  - **Web Access Port Number**

    Specify a port number for Web API access of ProgrammableFlow controller. This item is displayed only if the icon type seems a ProgrammableFlow controller.

    It is used in the physical topology autodiscover of ProgrammableFlow. For details, refer to "4.2.4 Registering ProgrammableFlow physical topology information (page 164)".

  - **Administration Node Name**

Specify a node name that manage this node. For example, if this node indicates a virtual device, specify a node name of a host device that manages this node. Enter up to 63 characters.

- **sysName**

  Specify an administratively-assigned name for this node. This item must equal to the value of ".iso.org.dod.internet.mgmt.system.sysName.0". Enter up to 255 characters.

- **Monitor** tab
  - **Monitoring-mode**

    For details of Select the monitoring mode for the device. Monitoring-mode, refer to "5.13 Starting or Stopping Monitoring by the Monitoring Mode (page 505)".

- **OK** button

  Reflects the settings in Network Manager.

- **Cancel** button

  Closes the dialog box without reflecting the settings.

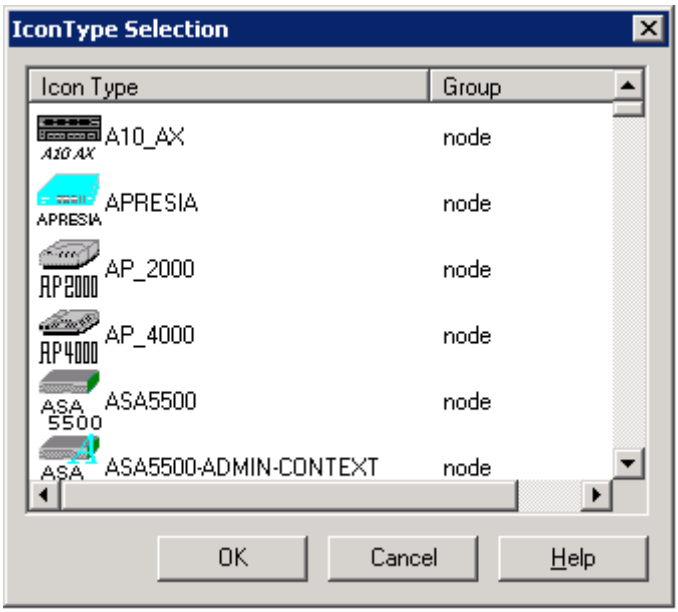
- **Help** button

  Displays Help.

4.2.2.2 Icon Type Selection dialog box

Specify an icon type for the icon that will be registered. The node group shows the device and the map group shows the map that the icon is registered under.

It is possible to select an icon from either group during a new registration. If an icon has already been registered, you cannot change to an icon type from a different group.



- **Icon Type**

  This displays the icon types that can be registered. When opened, the list is sorted alphabetically (upper case A-Z and lower case a-z). Click the label to switch the sort to ascending or descending order.

- **Group**

This shows the group to which the icon type belongs. Click the label to switch the sort to ascending or descending order.

- **OK** button

  Reflects the specified icon type in the Properties dialog box.

- **Cancel** button

  Closes the dialog box.

- **Help** button

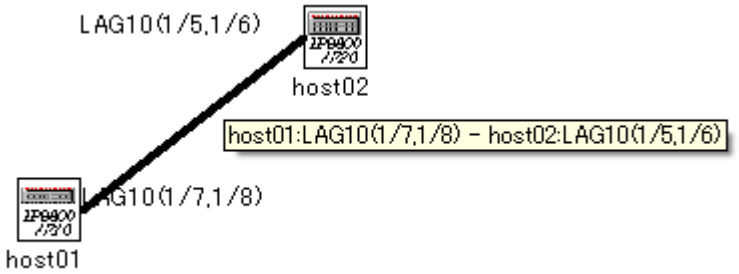
  Displays Help.

4.2.3 Registering topology information

In Network Manager, the connection relationship and connection status between a network device and a neighboring network device, including information regarding which devices are connected to which ports, are displayed graphically in the Map View. In addition It is possible to display connections through link aggregation.

Tip

In Network Manager, the connection relationship and connection status between a network device and a neighboring network device, including information regarding which devices are connected to which ports, are displayed graphically in the Map View. In addition, it is possible to display connections through link aggregation.



The following three methods can be used to register topology information

- Autodiscover

  Collect topology information regarding a device icon under a selected map icon or regarding a selected device icon by the setting value of **Discovery Protocol** in the icon properties to display the connection relationship in the Map View . For details, refer to "4.2.3.2 Automatically detecting topology information (page 149)".

- Manual register

  By using the connection tool in the Map View with selecting the device icons of the two devices for which you want to plot the connection line, you can manually register the connection line. For details, refer to "4.2.3.3 Manually registering topology information (page 151)".

- Batch register

  If you enter the connection relationship information between device icons in the configuration information file to import the information, the connection relationship among multiple device icons can be registered in batch. For details, refer to "4.6 Batch Registering or Deleting Configuration Information (page 206)".

As a method to check whether information registered manually or in batch is consistent with actual network environment or any changes that occur during the course of network operation, Network Manager provides **Check Topology** menu. **Check Topology** menu collects topology information through the setting value of **Discovery Protocol** to compare with the registration information. For details, refer to "4.2.3.4 Checking topology information (page 162)".

4.2.3.1 Discovery Protocol

To use **Configuration Management**>**Autodiscover**>**Physical Topology** menu or **Configuration Management**>**Check Topology** menu, the **Discovery Protocol** setting must be specified in the icon properties. Normally it is automatically set depending on an icon type. However, you can specify a corresponding value below when you use LLDP on your environment or when you manually register topology information.

Discovery Protocol 1) 2)	**Model**	**Neighboring protocol operating on device side**
1	IP8800/700series, ES8800/1700series	OADP
2	Cisco router series, Catalystseries	CDP
3	CX-uH24	OADP
4	IP8800/S300, S400series	OADP
5	IP8800/R400series	OADP
6	ProCurve2800	CDP
7	Brocade Communications Systems (former Foundry Networks) device	FDP
8	IP8800/S2400, S3600, S6300, S6700series	OADP
9	LLDP support devices 3)	LLDP
100	Other switch devices 4)	-
101	Other routers 4)	-
200	Other server models 5)	-
201	Other terminals 5)	-

1) If you leave the setting value of **Discovery Protocol** blank, Network Manager runs as if 100 was specified. Even though specifying values other than shown in the above table does not affect the operation of Network Manager, it is recommended not to specify values other than those shown in the above table.

2) 2. Regarding the setting value of **Discovery Protocol** for a device in which multiple discovery protocols are operating, determine according to the discovery protocol of a peripheral device with which a connection relationship exists. For example, when CDP and LLDP are operating on a Catalyst series device, if all the peripheral devices connected to this device are Catalyst devices (CDP support device), **Discovery Protocol** value should be "2", and if all the peripheral devices are LLDP support devices, should be "9".

If there are multiple types of peripheral devices, it is recommended not to change values that are automatically specified according to the types of icons.

3) LLDP support device supports the following MIB of the LLDP-MIB that conforms to IEEE802.1ab-2005.

- lldpLocSysName (1.0.8802.1.1.2.1.3.3.0)
- lldpLocPortIdSubtype (1.0.8802.1.1.2.1.3.7.1.2) (The value must be 5 (interfaceName).)
- lldpLocPortId (1.0.8802.1.1.2.1.3.7.1.3)
- lldpRemSysName (1.0.8802.1.1.2.1.4.1.1.9)
- lldpRemPortIdSubtype (1.0.8802.1.1.2.1.4.1.1.6) (The value must be 5 (interfaceName).)

- lldpRemPortId (1.0.8802.1.1.2.1.4.1.1.7)

Before using **Physical Topology** menu or **Check Topology** menu, confirm that the above MIB can be acquired using `NvPROAmibGetSvc` / `NvPROAmibGetMgr` command. For details about the `NvPROAmibGetSvc` and `NvPROAmibGetMgr` commands, refer to "9.7.1 NvPROAmibGetSvc/ NvPROAmibGetMgr (page 712)".

4) **Physical Topology** menu is not supported. **Check Topology** menu only supports checking sysName, port names/port IDs and connection bandwidth. For details, refer to "4.2.3.4 Checking topology information (page 162)".

5) **Physical Topology** menu is not supported. **Check Topology** menu only supports checking the connection bandwidth. For details, refer to "4.2.3.4 Checking topology information (page 162)".

4.2.3.2 Automatically detecting topology information

The **Physical Topology** menu detects physical connection to plot the connection line in a specified map based on the neighboring information stored in MIB of a device that supports OADP/CDP/FDP/ LLDP. For details about devices that support **Physical Topology** menu , refer to the MasterScope Network Manager product website information indicated below.

URL:http://www.nec.com/en/global/prod/masterscope/networkmanager/index.html

⚠ Caution

When the **Physical Topology** menu is executed, the following operations may be prohibited by exclusive control to ensure the integrity of the configuration information until the process is completed.

- Opening the menu for the target icon (map or node)
- Operations from WebAPI (configuration management API) for the target icon (map or node)

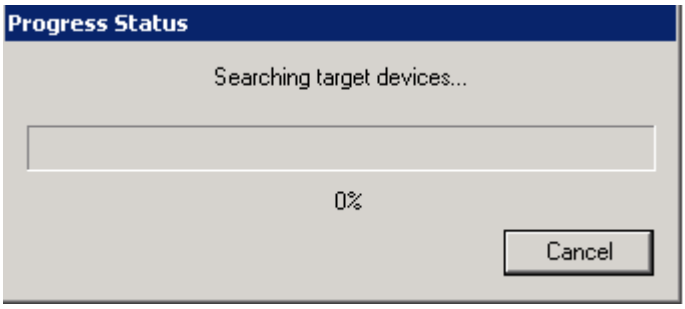
When you select a map and execute the menu, the operations for all the maps and nodes under the map are affected. If you select multiple nodes and execute the menu, operations for the selected nodes and the maps to which the nodes are registered are affected.

Before performing this operation, check the following.

- The **Physical Topology** menu targets devices that specify the value of "1 to 9" in **Discovery Protocol** of the icon properties. For details, refer to "4.2.3.1 Discovery Protocol (page 148)".
- Each device is required to run the neighboring protocol (CDP, OADP, FDP, or LLDP). For the configuration of each device, refer to the manual of the device.
- If a device specifies **1** (IP8800/700 series or ES8800/1700 series) in **Discovery Protocol**, configure the device-type of OADP to sysName. For details, refer to the manual of the device.
- For the icon properties of a targeted device, register **SNMP Community Name(get)** or **SNMPv3** tab information and create an environment that can carry out SNMP communication. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)"
- Make the values of the sysName(1.3.6.1.2.1.1.5) of a device and the **sysName** in the icon properties consistent.
- Confirm if **Discovery Protocol** in the icon properties is properly specified. For details, refer to "4.2.3.1 Discovery Protocol (page 148)".

You must first change to the "configuration mode (page 27)".

1. Select the **NetworkManagement** icon, map icon or multiple device icons and right-click, and select **Configuration Management**>**Autodiscover**>**Physical Topology** menu.

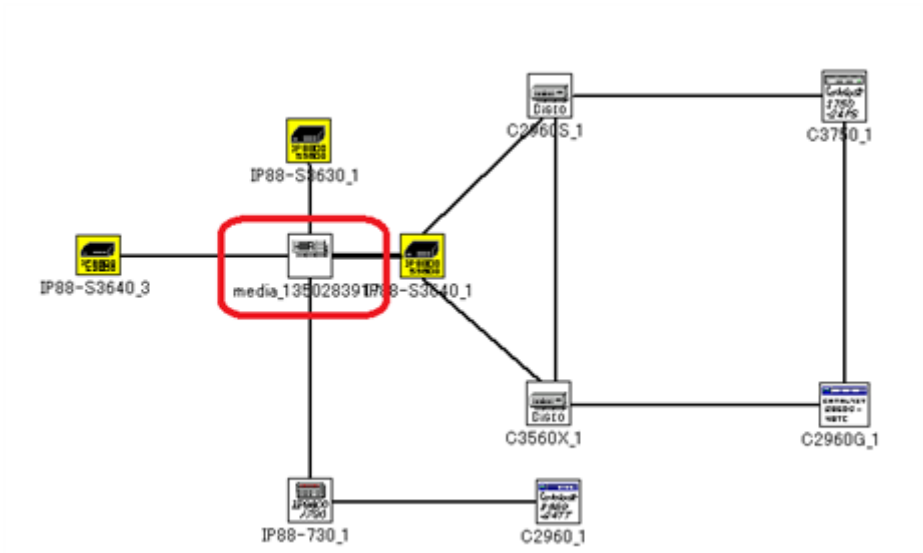


Tip

- If you want to select multiple device icons to execute a menu, select all the device icons you would like to target, right-click while holding the Ctrl key, and execute the menu.

  In this case, Network Manager detects the connection information among the selected icons to plot a line.
- If you register a large number of connection lines in a map, it may take a long time to complete registration. It is recommended that a maximum of 200 connection lines be registered in a map.
- If network workloads are high, such as when a network delay has occurred, registration may take longer than usual to complete. It is recommended that the menu be executed when network workloads are not high.

1. If there is a dumb hub between devices or a device that does not understand the neighbor protocol (OADP, CDP, FDP, or LLDP), multiple sets of neighbor connection data will appear for one port. In this case, the media icon will automatically be registered in the physical topology discovery.



   Media icons are automatically registered, but they are not automatically deleted. They must be deleted manually.

2. If there are multiple icons registered in one map that show the same device, a line will only be shown for only one of the icons.

3. 3.Connections with LACP, PAgP, LoadSharing, Trunk, or other aggregation are plotted using a bold "if" line. In addition, they are plotted using a port name that indicates that they are aggregation lines. However, among devices that specify the value of **Discovery Protocol** of the icon properties as "9 (LLDP support device)", the aggregation connection is not drawn but the "if" lines are drawn one by one that constitute the aggregation.

4. The port name of a port with link aggregation is displayed as a configuration port only if it is a physical port and the link is up. (Example: "LAG(1/2,1/15)")

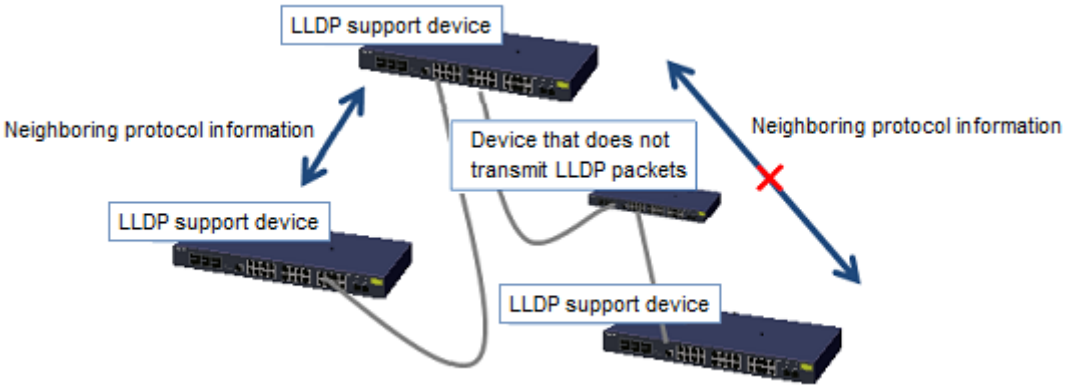
   Even if a device is configured to be aggregated, a physical port that is currently down is not included as a configuration port.

5. Even if an identical connection is on multiple maps, only the physical connection in the map for which physical topology discovery was executed will be updated.

   If a physical connection between identical devices is drawn in multiple maps, update all maps by right-clicking the **NetworkManagement** icon or map icon and select **Configuration Management**>**Autodiscover**>**Physical Topology** menu.

6. Neighboring information may sometimes not be notified to neighboring nodes.

   LLDP transmits multicast packets to a sending destination "01-80-C2-00-00-0E". In IEEE802.1D, IEEE802.1Q, this address is reserved as an address "not to be forwarded to". As an environment where an L2 switch and bridge that are conformed to this standard cannot collect neighboring information, a connection line is not drawn.



4.2.3.3 Manually registering topology information

Between any two device icons on the **Map View**, you can manually register a connection line that indicates a physical connection.

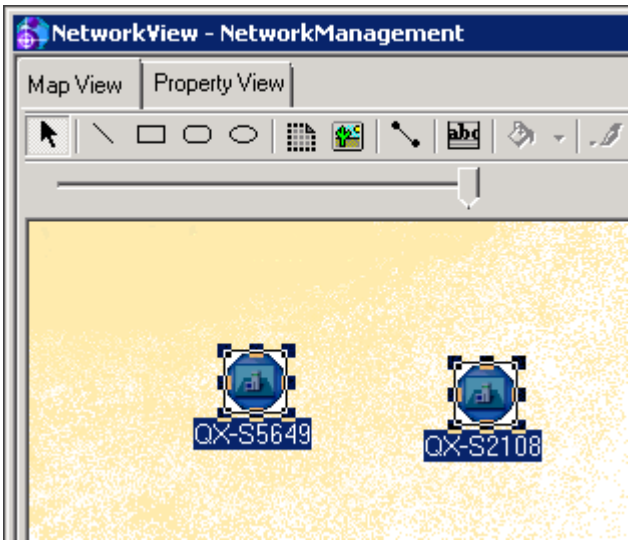
You must first change to the "configuration mode (page 27)".

1. Click the source device icon.
2. Hold down CTRL key and click the destination device icon.

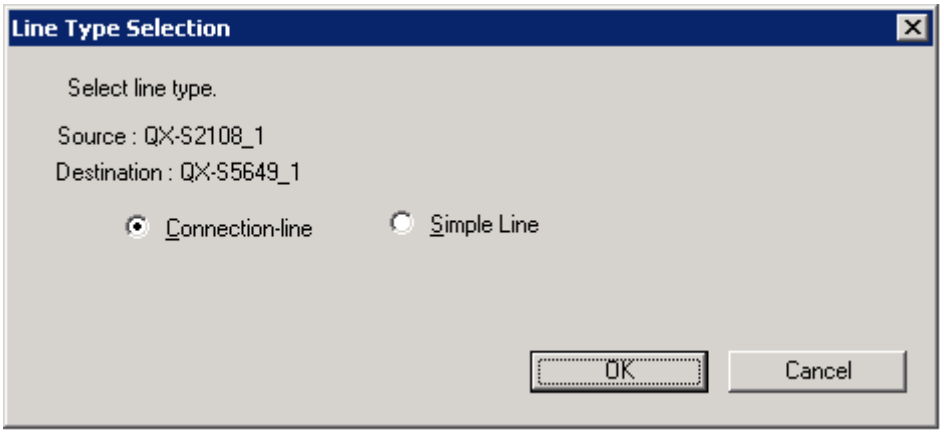
   Caution

   In Network Manager, the source/destination devices of the connection-line are not distinguished. The source/destination devices of the connection-line may be displayed in reverse.

3. Click the  in the toolbox.



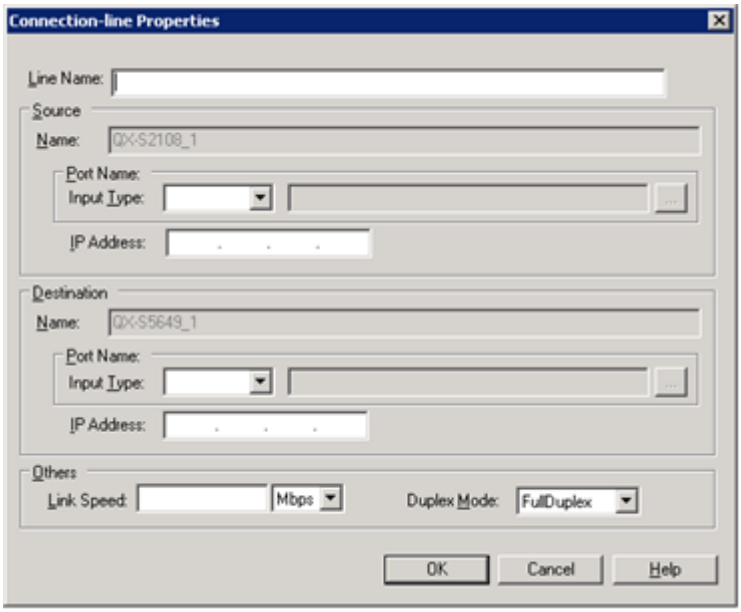
4. In the Line Type Selection dialog box, select **Connection-line** and set the line attributes.



For details, refer to "4.2.3.3.1 Line Type Selection dialog box (page 154)".

Click **OK** button, the Connection-line Properties dialog box is displayed.

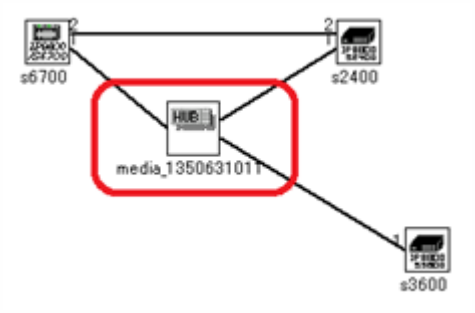
5. In the Connection-line Properties dialog box, specify the line attributes.



For details, refer to "4.2.3.3.2 Connection-line Properties dialog box (page 154)".

6. Click **OK** button.

1. If there are multiple destination nodes and topology information is registered, a media icon is automatically displayed.



On condition that a connection line has already been registered between s6700 port 1 and s2400 port1, a media icon is automatically displayed when a connection line is registered between s3600 port 1 and s2400 port 1.

Media icons are automatically registered, but they are not automatically deleted.

2. In the following cases, existing information is overwritten with no warning.
   - (Regardless of connection line being new or preexisting) A line already exists for a port that matches the specified port ID, but the registered port name is different.
   - (Regardless of connection line being new or preexisting) A line already exists for a port that matches the specified port name, but the registered port ID is different.

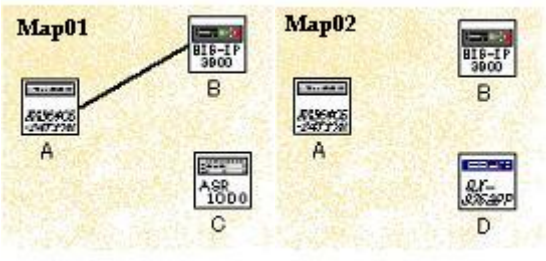
   A check for inconsistencies in port names and IDs can be performed by checking the consistency of device-side information using the Topology Check Tool.
3. The source and destination nodes for an existing connection cannot be changed.
4. If there are multiple icons in a map that display the same device, a line can only be drawn from one of these icons. If a line has already been drawn from an icon and you select another icon displaying the same device and attempt to add a line, the following warning will be displayed and the operation will not be completed.

   ```
   "A connection line has already been drawn for the specified device.
   Select the icon to register a new connection line."
   ```
5. Even if one is a media type, the device with the same name cannot be specified as the connection source and destination. If you select this type of icon and attempt to add a line, the following warning message appears and the operation is not completed.

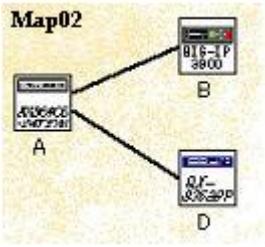
   ```
   "The Source and Destination Name must be different."
   ```
6. When a connection line is registered manually, this connection line is displayed only in the registered map. If the source node and destination node of the connection line exist in another map, registered connection line is not displayed. But connection line information is shared among all maps. When another connection line is registered, undisplayed connection lines become to be displayed.

   Example:

   The connection line between node A and B is registered in Map01, This connection line is not displayed in Map02 even if node A and B are also registered in Map02.

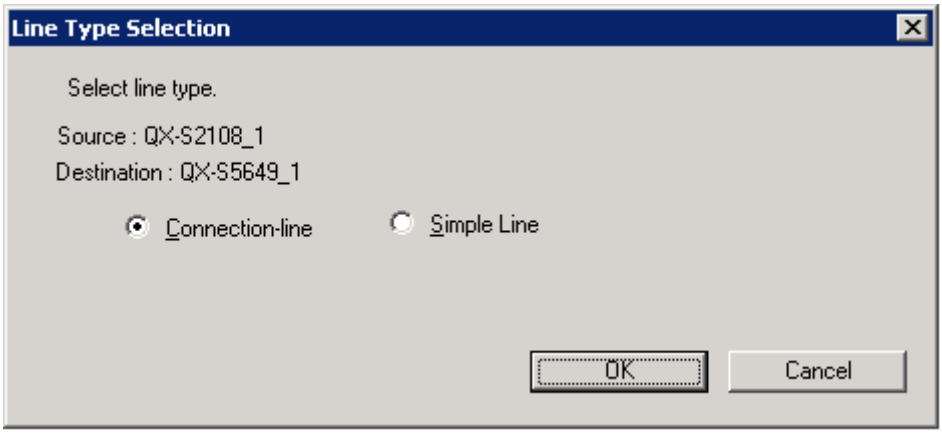


If the connection line between node A and D is registered in Map02, the connection line between node A and B will also be displayed.



Line Type Selection dialog box

Selects the line type to be registered.



- **Connection-line**

  Registers a connection line. The connection line is a special node that shows the physical connection between devices. Depending on its status, the line changes color.

- **Simple Line**

  The simple line option registers a simple figure in order to connect icons.

- **OK** button

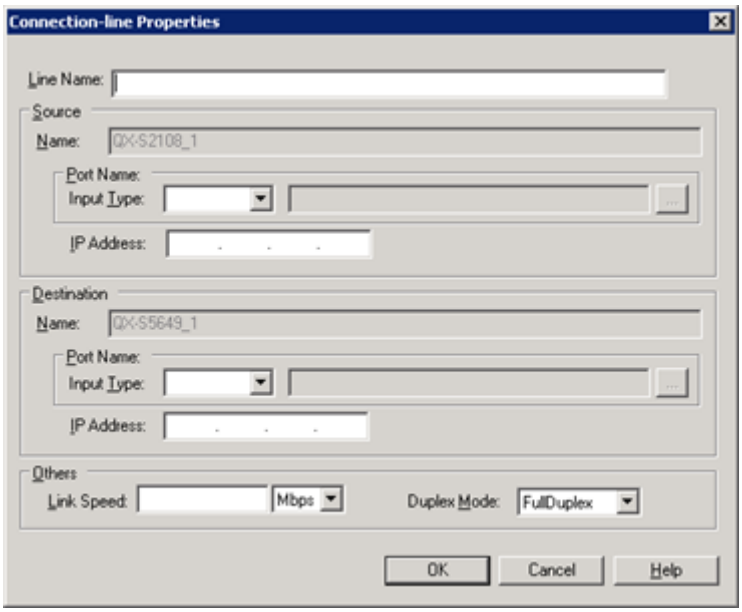
  Applies the values that have been set.

- **Cancel** button

  Cancels the settings.

Connection-line Properties dialog box

Sets the attributes of the line. The items other than **Line Name** may be omitted.



- **Line Name**

  Specify the line name (maximum of 63 characters). Required parameter.

  There must not be any duplication in the names of devices, maps, and lines registered in Network Manager.

- **Source**

  - **Name**

    Displays the device name for the source node.

  - **Port Name**

    First, select "Port Name" or "Port ID" as the **Input Type**. For format of port name, refer to "4.2.3.3.5 About port names in the topology information (page 158)".

    The port ID must be within the range of 1 - 2147483647. If there is a port ID that matches the entered **Port Name** or a port name that matches an entered **Port ID** in the port list information for that device, those details will be set automatically.

    Click  to display the Port Name Setting dialog box. In the Port Name Setting dialog box, type the **Port Name** and click **OK** button.

    If "Port Name" was selected in **Input Type** field, the entered port name is displayed. If "Port ID" was selected, the port ID that corresponds with the port name is displayed. For details, refer to "4.2.3.3.5 About port names in the topology information (page 158)".

    Caution

    * If no data is obtained from the port table, or if there is no port ID that corresponds with the entered port name, a port ID is not set and nothing is displayed in the port ID box.

      The selected port name is set. You can confirm by switching the **Input Type** to "Port Name".

    * To properly report alerts to registered connection-lines during monitoring according to the following state monitoring rules, you must register the correct port ID information. Change the port input type to **Port ID** and confirm that the correct value has been registered.

      + nvtp-topchk:InterfaceDownCheck
      + nvtp-stpstat:STP_PortStateCheck

+ nvtp-bandchk:BandTraffic

- **IP Address**

  Specify the IP address if an IP address has been set for the physical port that is the source node.

- **Destination**
  - **Name**

    Displays the device name for the destination node.
  - **Port Name**

    Type the name or port ID of the source node physical port.
  - **IP Address**

    Specify the IP address if an IP address has been set for the physical port that is the destination node.
- **Others**
  - **Link Speed**

    Specify a link speed for the connection. If unknown, this can be omitted.
  - **Duplex Mode**

    Specify a mode (full-duplex or half-duplex) for the connection. If unknown, this can be omitted.
- **OK** button

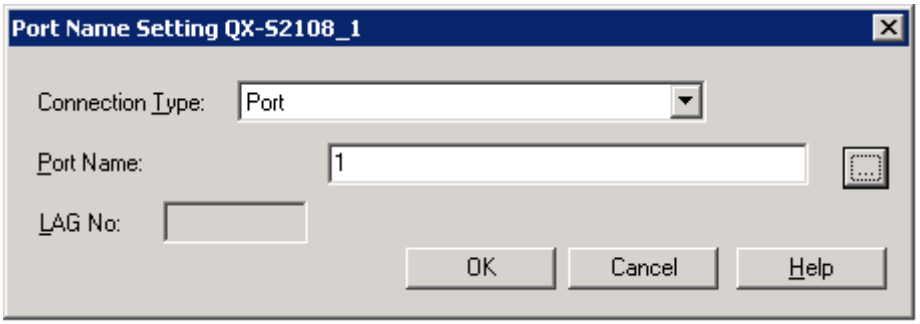
  Applies the values that have been set.
- **Cancel** button

  Cancels the settings.
- **Help** button

  Displays Help.

Port Name Setting dialog box

Select a physical port or LinkAggregation for the device.



- **Connection Type**

  Select either "Port" or "LinkAggregation (LAG)". "LAG" can be selected for the following connection types, based on device type as listed below. For details of the discovery protocol settings, refer to "4.2.3.1 Discovery Protocol (page 148)".

Discovery Protocol	Device Type (Protocol)	Connection Type
1	IP8800/700 series, ES8800/1700 series (OADP)	LinkAggregation (LAG)
2	Cisco router series, Catalyst series (CDP)	PortChannel (Po)
3	CX-uH24 (OADP)	LoadSharing (Sharing)
4	IP8800/S300, S400 series (OADP)	LinkAggregation (LAG)
5	IP8800/R400 series (OADP)	LinkAggregation (LAG)
6	ProCurve2800 (CDP)	Trunk (Trk) Dynamic (Dyn)
7	Brocade Communications Systems (former Foundry Networks) device (FDP)	Trunk (Trk)
8	IP8800/S2400, S3600, S6300, S6700 series (OADP)	PortChannel (CH)
9	LLDP support device (LLDP)	Link Aggregation (LAG)
100	Other switch	Link Aggregation (LAG)
101	Other rooter	Link Aggregation (LAG)
200	Other server	Link Aggregation (LAG)
201	Other device	Link Aggregation (LAG)

- **Port Name**

  Type the name or ID of the physical port or click  and make a selection in the Port Name Selection dialog box. For details, refer to "4.2.3.3.4 Port Name Selection dialog box (page 157)".

- **LAG No.**

  Type the LAG number. Enter a value within the range of 1 - 2147483647. A value cannot be entered here if it is a device that does not require a LAG number. For details, refer to "4.2.3.3.5 About port names in the topology information (page 158)".

- **OK** button

  Applies the values that have been set.

- **Cancel** button

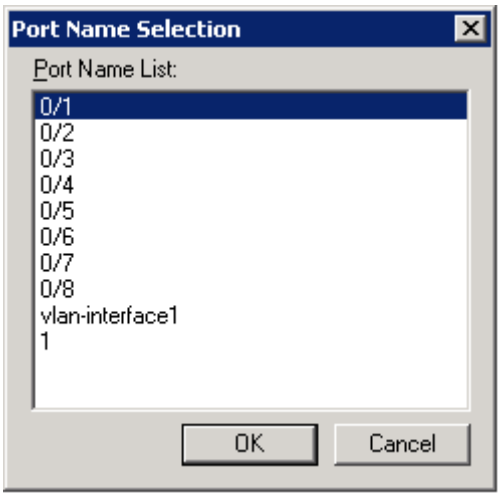
  Cancels the settings.

- **Help** button

  Displays Help.

Port Name Selection dialog box

Select the port for a device.



Caution

This dialog box will not be displayed if the port list data set for the device cannot be obtained because communication with the device cannot be established.

- **Port Name List**

  Displays a list of ports for the device.

  One port name can be selected if "Port" was selected in the Port Name Setting dialog box, multiple port names can be selected if "LinkAggregation (LAG)" was selected.

- **OK** button

  Applies the values that have been set.

- **Cancel** button

  Cancels the settings.

About port names in the topology information

Check Topology menu acquires neighboring information stored in MIB to compare with topology information registered in Network Manager. Therefore if a port name is registered in Network Manager in a format that does not comply with the following naming rules, **Check Topology** menul will never fail to detect the inconsistency, and will not proceed with proper checking. In order to properly check topology information registered by **Check Topology** menu, register port names by complying with the following naming rules.

Port name naming rules vary depending on **Discovery Protocol**l registered in the icon properties. For details about the discovery protocol, refer to "4.2.3.1 Discovery Protocol (page 148)".

Connection Type "Port": Normal connection (a connection with no aggregation)

Discovery Protocol	Device Type (Protocol)	Rule
1	IP8800/700 Series, ES8800/1700 Series (OADP)	Slot no. / Port no.
2	Cisco Router Series, Catalyst Series (CDP)	Two alphanumeric characters + [module no/]slot no./port no.

Discovery Protocol	Device Type (Protocol)	Rule
3	CX-uH24 (OADP)	Port no.
4	IP8800/S300, S400 Series (OADP)	NIF no. / Port no.
5	IP8800/R400 Series (OADP)	NIF no. / Port no.
6	ProCurve2800 (CDP)	Port no.
7	Brocade Communications Systems (former Foundry Networks) (FDP)	Port no. or Slot no./ Port no.
8	IP8800/S2400, S3600, S6300, S6700 Series (OADP)	Slot no. / Port no.
9	LLDP support device (LLDP)	Same value names of ifName(1.3.6.1.2.1.31.1.1.1.1). For devices that cannot acquire ifName, select the same value names of ifDescr(1.3.6.1.2.1.2.2.1.2).
100	Other switches	
101	Other routers	
200	Other servers	
201	Other terminals	

Connection Type "Link Aggregation (LAG)": a connection where multiple physical ports are aggregated

Based on the entered port name, an assessment will be made as to whether or not the connection for the entered connection registration information is a LAG (Link Aggregation), and this information will be registered. If registered as a LAG connection, in addition to the source and destination nodes, the port name must be entered in accordance with the device type-specific rules listed below. Connections that are assessed as being a LAG connection are displayed with a bold-line icon in the map.

Discovery Protocol	Device type (Protocol)	Rule [1)]
1	IP8800/700Series, ES8800/1700 Series (OADP)	LAG*N*(*physical port name1*,*physical port name2*,...) *N*: LAG no.
2	Cisco Router Series, Catalyst Series (CDP)	Po*N*(*physical port name1*,*physical port name2*,...) *N*: PortChannel no.
3	CX-uH24 (OADP)	Sharing(*physical port name1*,*physical port name2*,...)
4	IP8800/S300, S400 Series (OADP)	LAG*N*(*physical port name1*,*physical port name2*,...) *N*: LAG no.
5	IP8800/R400 Series (OADP)	LAG*N*(*physical port name1*,*physical port name2*,...) *N*: LAG no.
6	ProCurve2800 (CDP)	Dyn*N*(*physical port name1*,*physical port name2*,...) *N*: Dynamic LAG no.

Discovery Protocol	Device type (Protocol)	Rule [1)]
7	Brocade Communications Systems (former Foundry Networks) device (FDP)	Trk*N*(*physical port name1*,*physical port name2*,...) [1)] *N*: Trunk no.
8	IP8800/S2400, S3600, S6300, S6700 Series (OADP)	Trk(*physical port name1*,*physical port name2*,...)
9	LLDP support device (LLDP)	LAG*N*(*physical port name1*,*physical port name2*,...) *N*: LAG no.
100	Other switches	
101	Other routers	
200	Other servers	
201	Other terminals	

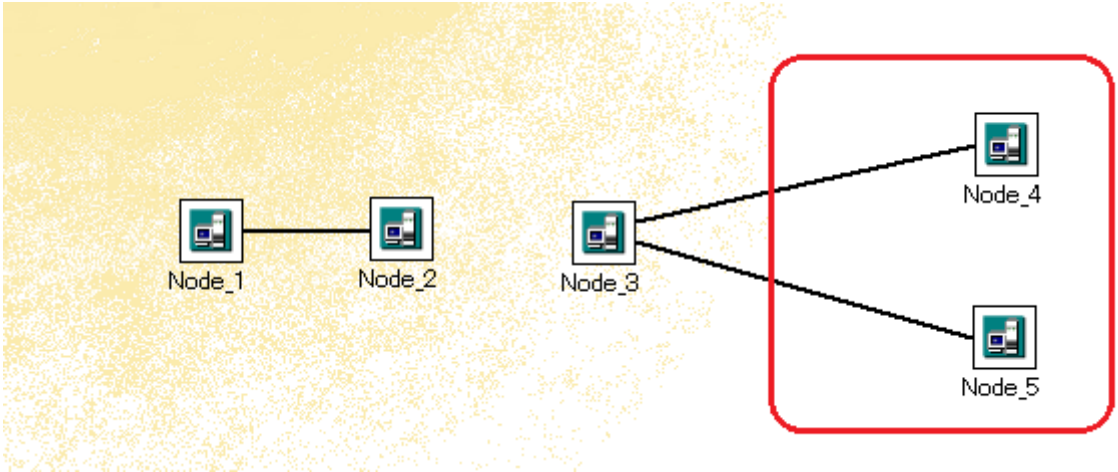
1) Physical port names must be compliant with the rules in "Connection Type "Port": Normal connection (a connection with no aggregation) (page 158)".

Caution

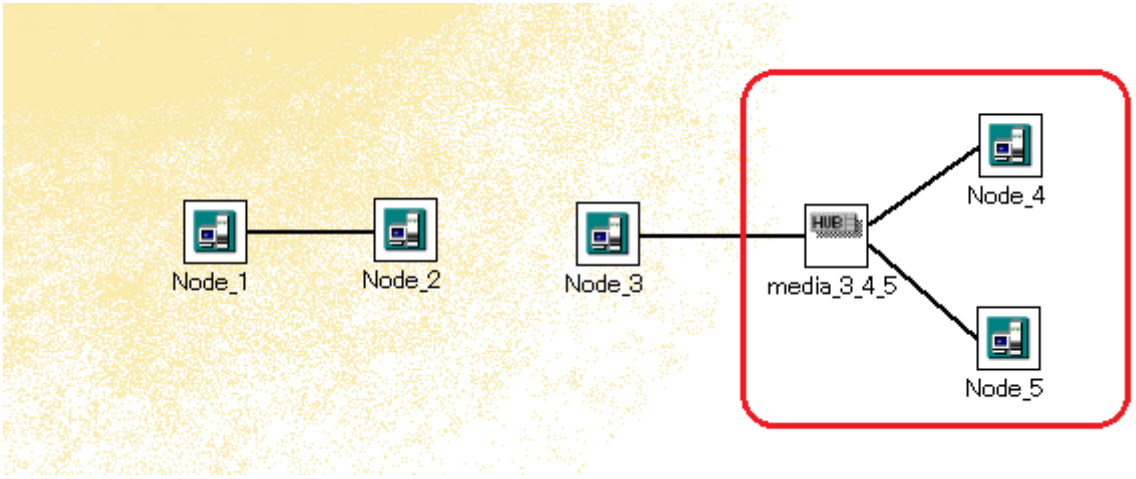
1. In the LAG port configuration elements, select all physical port names that were included in the device configuration link aggregation group. If the device configuration and port names are different, the Topology Check Tool will detect inconsistencies in the link aggregation information.
2. When registering ports with aggregation in the Connection-line Properties dialog box dialog box, specify the configuration physical ports in ascending order and then register. If the ports are not specified in ascending order, an inconsistency `"Does not match the device LAG information".` will be detected by the Topology Check Tool. For a CX-uH24 load-sharing connection, first specify the master port and then register.
3. In the LAG port configuration elements, if a device physical port name includes ")" or "," character, Topology Check Tool cannot check correctly.

About map displays for the shared port

If a connection line is registered between one device and the other device, a connection line is drawn directly between devices as illustrated below. Also, if a line is connected from one device to multiple devices via different ports, the connection lines are displayed as shown in the red frame.



However, when there are multiple connection lines that have different destinations (device/port) and the source ports of these connection lines are considered as the same (for example, the same port on the same device), the connection lines are displayed via a media icon as shown in the red frame.



The rules listed below are for evaluating whether two ports are some or not.

Normal connection port: Normal connection (a connection with no aggregation)

The connection port identification is performed using either the port name or the port ID.

1. If "Port Name 0/1 Port ID1" already exists in the system:

   If "Port Name 0/2 Port ID1" is registered, they are recognized as the same port because they match the port ID1. The connection line information for this port is overwritten.

2. If "Port Name 0/1 Port ID1" already exists in the system:

   If "Port Name 0/1 Port ID2" is registered, they are recognized as the same port because they match the port name 0/1. The connection line information for this port is overwritten.

3. If "Port Name 0/1 Port ID1" and "Port Name 1/1 Port ID2" already exists in the system:

   If "Port Name 0/1 Port ID2" is registered, since port ID has a higher priority than port name, the connection information of "Port 1/1 Port ID2" is overwritten by the newly added information.

LAG (Link Aggregation) connection port: a connection with aggregated multiple physical ports

If a port ID is specified, the identification process is performed based on the following.

1. Load-Sharing connection port for CX uH24 devices

   Only the LAG prefix is used to identify whether or not it is the same LAG connection. The physical configuration port details are not affected.

2. Foundry Trunk link port

   Whether or not it is the same LAG connection is recognized based on if the physical configuration port is shared. Even if there is only one physical configuration port that is the same, it is assumed to be the same trunk port.

   Example:

- If "Trk(1/1,1/2)" already exists, and "Trk(1/1)" is registered, "Trk(1/1,1/2)" is replaced with "Trk(1/1)".
- If "Trk(1/1,1/2)" already exists, and "Trk(1/3)" is registered, "Trk(1/3)" is registered as new.

Further, if there are two items with the same configuration physical port, it is assumed that it is the same connection as the connection that was initially obtained using the existing connection line information.

Example:

- If "Trk(1/1)" and "Trk(1/2)" already exist, and "Trk(1/1,1/2)" is registered, "Trk(1/1)" is replaced with "Trk(1/1,1/2)". The port for "Trk(1/2)" is maintained.

3. Other LAG (Link Aggregation) ports

   The LAG prefix + LAG no. are used to identify whether or not it is the same LAG connection. The physical configuration port details are not affected.

   Example:

   - "LAG1(1/1,1/2)" and "LAG1(1/3,1/4)" are the same LAG port.

4.2.3.4 Checking topology information

Check Topology menu acquires the latest information using SNMP from MIB in a device connected to the network to check the consistency of the topology information that Network Manager maintains. This is used to check whether the topology information registered in "4.2.3.3 Manually registering topology information (page 151)" or "4.6 Batch Registering or Deleting Configuration Information (page 206)" is correct or if the topology information registered in "4.2.3.2 Automatically detecting topology information (page 149)" has been changed during the operation.

⚠ Caution

When the topology information for a node is checked, node operations performed from WebAPI (configuration management API) may be prohibited by exclusive control to ensure the consistency of the configuration information until the process is completed.

Devices to be checked are those that register topology information (if line) and that are possible to conduct SNMP communication. In addition, devices once specified as a source or destination device are to be checked even after deleting the connection lines.

Checked items by Topology Check Tool

- Is it possible to conduct SNMP communication with the device?

  By acquiring sysUpTime(1.3.6.1.2.1.1.3) from the device, Network Manager checks if SNMP communication is possible with the device.

  If communication is conducted through SNMPv1/v2c, the tool can check if the setting of the SNMP community name is correct, and if communication is conducted through SNMPv3 the tool can check the setting of the user names and security levels.

- Is the value of sysName correct?

  The tool checks if the value of sysName(1.3.6.1.2.1.1.5) acquired from the device is the same as that of **sysName** that is registered in the icon properties of Network Manager.

- Is it possible to acquire neighboring information?

The tool checks if you can acquire neighboring information from MIB of the device by a method in accordance with the value of **Discovery Protocol** registered in the icon properties of Network Manager.

- Are port names/port IDs correct?

  The tool checks if port names/port IDs registered in Network Manager are the same as those that actually exist. The actual port names are acquired from ifName(1.3.6.1.2.1.31.1.1.1.1). If the port names cannot be acquired from ifName, they are acquired from ifDescr(1.3.6.1.2.1.2.2.1.2)). The actual port IDs are acquired from ifIndex(1.3.6.1.2.1.2.2.1.1). The tool also checks if the port names correspond to the port IDs.

- Is the bandwidth of connection correct?

  The tool checks if the actual line speed is the same as that in the topology information registered in Network Manager. The actual line speed is acquired from ifHighSpeed(1.3.6.1.2.1.31.1.1.1.15). If actual line speed cannot be acquired from ifHighSpeed, it is acquired from ifSpeed(1.3.6.1.2.1.2.2.1.5). The tool does not check aggregated ports or a connection whose bandwidth is not specified when registered manually.

- Are the LAG configuration ports correct?

  When ports are aggregated, the tool checks if the configuration physical ports of the aggregation ports specified when registered manually are same as the ports configured in the actual device.

  The tool does not check devices that specify a value "other than 1 to 9" in **Discovery Protocol** in the icon properties.

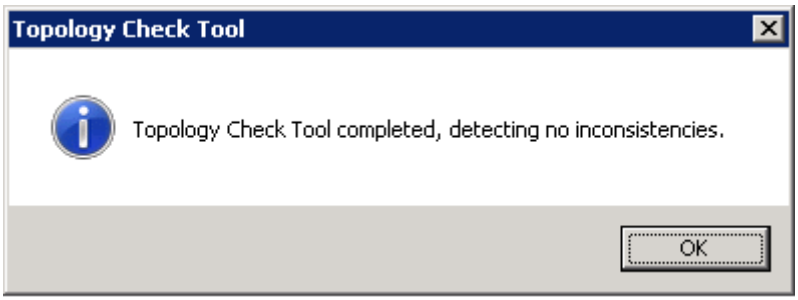
- Is the connection information correct?

  The tool checks whether neighboring information acquired from MIB in the device and the topology information (connection information) registered in Network Manager of other devices are consistent.

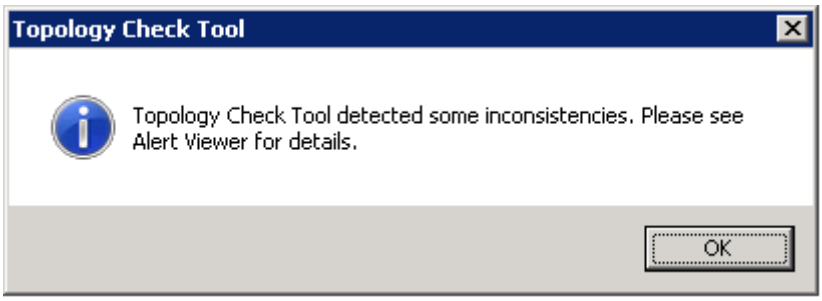
  The tool does not check devices that specify a value "other than 1 to 9" in **Discovery Protocol** in the icon properties.

- In the case of a device that specifies a value of "1 to 9" in **Discovery Protocol** in the icon properties, the neighboring protocol (CDP, OADP, FDP, or LLDP) must be operating. For the configuration of each device, refer to the manual of the device.
- For a device for which "1" is specified in **Discovery Protocol** of the icon properties (in the IP8800/700 series and ES8800/1700 series), the OADP device-type must be set to the sysName. For details, refer to the manufacturer's documentation.
- Set the "monitoring mode (page 505)" of the node to ON.
- You must first change to the "configuration mode (page 27)".
- As for OADP/CDP/FDP/LLDP devices that support an SNMP agent, the sysName should be consistent with the **sysName** that is registered in Network Manager of the icon properties. If they are not consistent, Network Manager may not properly check the connection information. In addition, regarding the setting on the OADP device side, specify the device-type as the sysName.

1. To check topology information, execute in either of the following procedures.
   - Right-click the device icon and select **Configuration Management**>**Check Topology**.
   - Right click the Connection-line and select **Check Topology** menu.
2. If no inconsistencies are detected, the following dialog box is displayed.



If inconsistencies are detected, the following dialog box is displayed and a warning alert is generated. The color of devices and lines with inconsistencies changes.



For reference to the alert, refer to "5.1 Checking Alert Information (page 448)".

4.2.4 Registering ProgrammableFlow physical topology information

Network Manager can discover automatically the physical connection between the ProgrammableFlow switches based on the information managed by the ProgrammableFlow controller, and draw it on the map. For the target devices in the physical topology autodiscover of ProgrammableFlow, refer to the MasterScope Network Manager product information.

Tip

The physical connecting-line can be registered by manual. For details, refer to "4.2.3.3 Manually registering topology information (page 151)".

4.2.4.1 Preparing for autodiscover of ProgrammableFlow physical topology

Physical topology information of ProgrammableFlow switches (hereafter referred to as PFS) is obtained using Web API of ProgrammableFlow controller (hereafter referred to as PFC). For this reason, before autodiscover, you must configure the setting to access to Web API of PFC.

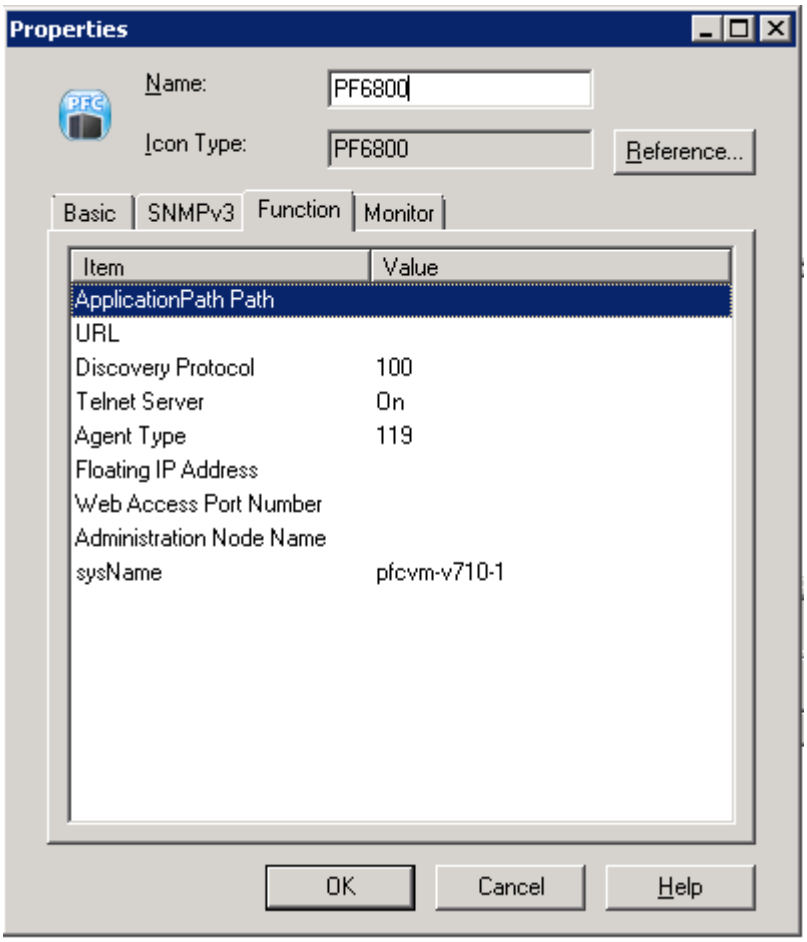
- Web API of PFC needs to be set up in advance. For user authentication method of Web API, select the authentication method: "Username/Password defined in system password file". For details, refer to the manual provided by PFC.
- Device icons of PFC and PFS must be registered in the same map. The connecting-line regarding PFS that is not registered is not drawn.
- The detailed information of the device interfaces should be registered in the PFS device icon. For details of the registration method, refer to "4.2.8.1 Discovering interface information (page 180)".
- ProgrammableFlow physical topology is drawn in only the map executed the autodiscover.

You must first change to the "configuration mode (page 27)".

1. Open Properties dialog box of PFC icon.

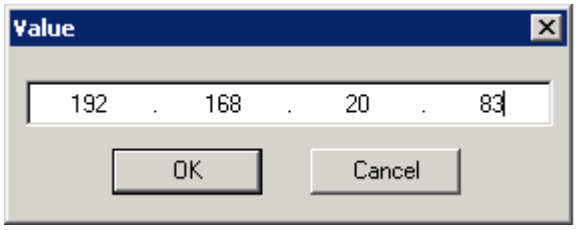
   Right click of PFC icon, and select **Property** menu.

2. In the **Function** tab of the Properties dialog box, enter the necessary information to Web API access.



- **Floating IP address** (If PFC is a redundant configuration)

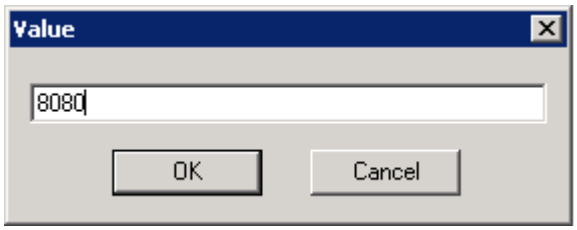
  If PFC is a redundant configuration, set the virtual IP address to access to Web API.



  If nothing is specified, use the value of **IP Address** of the **Basic** tab for accessing.

- **Web access port number**

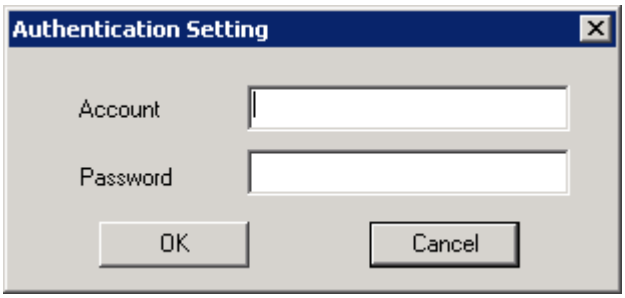
  Specify TCP port number of Web API on the ProgrammableFlow controller.



Valid range is 0 - 65535.

If nothing is specified, the default value, 8080 port is used.

3. Right-click PFC icon, and select **Configuration Management**>**Autodiscover**>**ProgrammableFlow Authentication Setting**.
4. Enter an account name and password of PFC Web API in the Authentication Setting dialog box.



The account name and password are up to 32 characters.

5. Click **OK** button.

   Authentication setting is saved.

4.2.4.2 Automatically detecting ProgrammableFlow physical topology

Accesses Web API of ProgrammableFlow controller (hereafter referred to as PFC), and automatically discover the physical topology information of the ProgrammableFlow switches (hereafter referred to as PFS).

⚠ Caution

When ProgrammableFlow physical topology autodiscover is executed, the following operations may be prohibited by exclusive control to ensure the consistency of the configuration information until the process is completed.

- Opening the menu for the target map and nodes under the map
- Operations from WebAPI (configuration management API) for the target map and nodes under the map

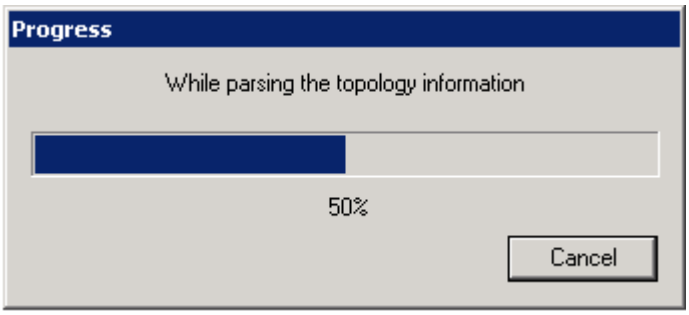
Before performing this operation, first execute the steps in "4.2.4.1 Preparing for autodiscover of ProgrammableFlow physical topology (page 164)" in advance.

You must first change to the "configuration mode (page 27)".

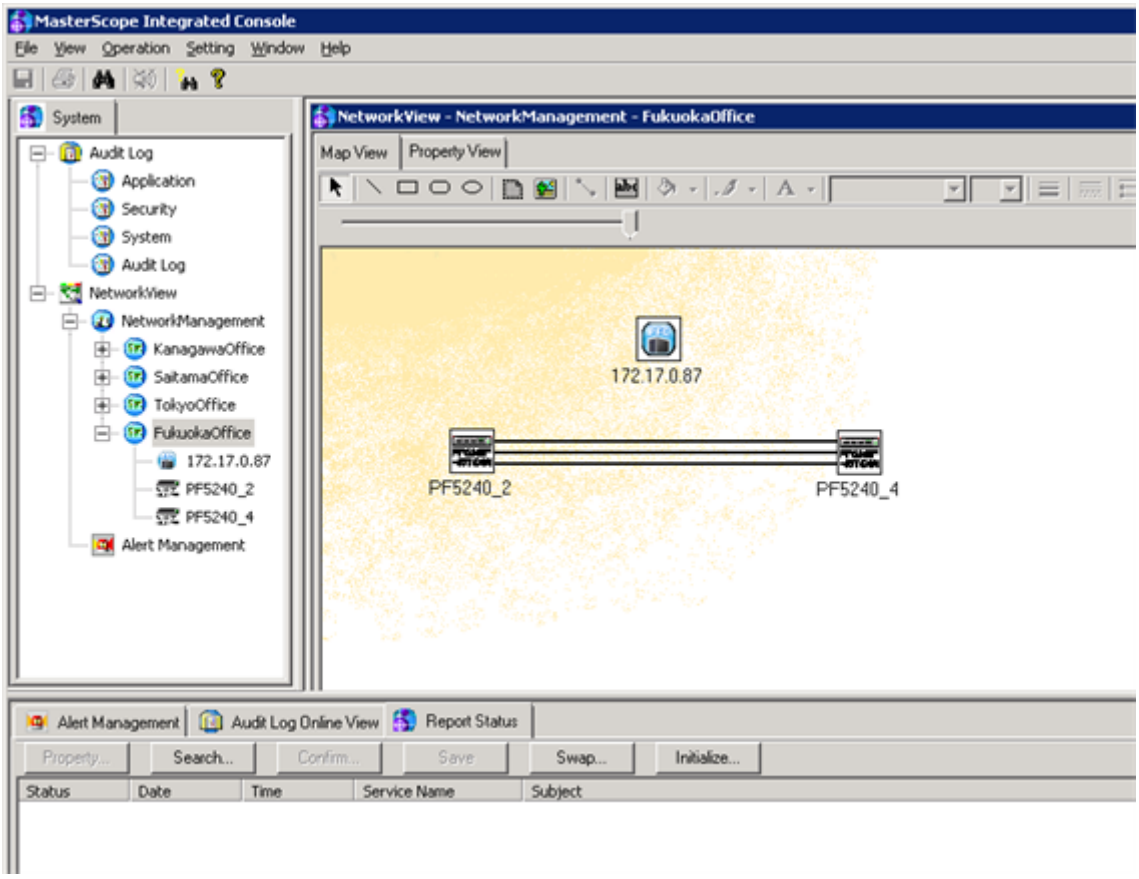
1. Right-click PFC icon, and select **Configuration Management**>**Autodiscover**>**ProgrammableFlow Topology**.

   Collecting the physical topology information of PFS managed by the specified PFC is started.

If it takes ten seconds or more to collect, the Progress dialog box appears.



When execution of discovery is finished, connecting-lines are drawn on the specified map.



Tip

If the physical connection configuration of PFS is changed, the autodiscover should be performed again. Existing connection-lines will be cleared and new lines will be registered.

4.2.4.3 Registering the virtual/physical interface name conversion definition file

The ProgrammableFlow physical topology detecting function automatically draws a ProgrammableFlow physical topology by comparing interface names acquired both from MIB (physical) in PFS and WebAPI (virtual) in PFC with an internal corresponding definition. More specifically, based on the internal corresponding definition, this function enables the automatic drawing of ProgrammableFlow physical topology by converting (loading) virtual interface names acquired from WebAPI in PFC to physical interface names acquired from MIB in PFS.

This function enables you to freely add the corresponding definition of both physical and virtual interface names acquired from MIB in PFS and WebAPI in PFC against devices whose corresponding definition is not registered in the product of Network Manager as standard. This enables the automatic drawing of all ProgrammableFlow physical topologies that are supported by PFC.

Preparation for registering conversion definition files

Confirm specific contents in advance because a conversion definition file requires the following parameters.

Item name	Description
sysObjectId	sysObjectId of the relevant device
Virtual interface name	Virtual interface name of the relevant device
Physical interface name	Physical interface name of the relevant device

Creation of conversion definition file

Create a conversion definition file under the following file names and formats. You need to create a new file because the file does not exist immediately after the installation of Network Manager. In addition, if the following files exist while autodiscover is being executed, this function re-reads the file every time. Therefore, the settings are applied in the following autodiscover processes by placing the file.

<On the manager, %installfolder%>\Manager\sg\NvPRO\PFLOW\config\NvPROPFlow_usr.ini

Manager OS	Character code	BOM
Windows	Unicode(UTF-16LE)	With BOM
Linux	UTF-8	Without BOM

Create a conversion definition file under the following formats.

```
# Comment
sysObjectId: x.x.x.x.x.x.x.x.x.x.x.x{
"virtual-interface-name_1"="physical-interface-name_1",
"virtual-interface-name_2"="physical-interface-name_2",
  :
"virtual-interface-name_N"="physical-interface-name_N"
}
```

- Available characters are ASCII characters.
- Lines beginning with "#" are treated as a comment.
- Creates a definition file for each sysObjectId in PFS that is newly added. For sysObjectId, you can register multiple sysObjectId with one setting by specifying an asterisk ("*"). However, it is possible only for certain subsequent elements such as "1.3.6.1.4.1.119.1.203.2.2.*" but not for an element in the middle of a string such as "1.3.6.1.4.1.119.1.*.2.2.2".
- Specify conversion contents for each device within {} in "sysObjectId: x.x.x.x.x.x.x.x.x.x.x.x{}" in a format "virtual-interface-name_N"="physical-interface-name_N". If multiple definitions are necessary, specify them in a row separated by commas.

Virtual interface name

Confirm "Name:PortName" displayed by running show topology detail of the pfcshell command provided by PFC.

Example: Port: Name:GBE0/1 ID1

Display example of show topology detail:

```
  PFC# show topology detail
Date: 2013-11-17 20:35:04 JST
OFS DPID:0000-0000-0000-0002  Name:PF5240_2
  IP Address :192.168.10.204
  Status     :connected
  AvoidStatus:
    PolicyIndex 0:off
  Port:  Name:GBE0/1  ID:1
    AdminStatus:up
    PortStatus :down
    AvoidStatus:
      PolicyIndex 0:off
    MAC Address:0025.5ce6.4bc2
    Duplex     :unknown
    Speed      :unknown
    Neighbor:  OFS DPID:  Port:  LinkStatus:  BCMC_Spt_Use:  Weight:
  :
```

Physical interface name

Confirm the following MIB contents in PFS that are newly added.

iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName (1.3.6.1.2.1.31.1.1.1.1)

Example: GigabitEther 0/1

You can also confirm the contents of ifName MIB by using the `NvPROAmibGetSvc` / `NvPROAmibGetMgr` command. For details, refer to "9.7.1 NvPROAmibGetSvc/ NvPROAmibGetMgr (page 712)".

Conversion definition method

Specify a virtual interface name (PortName) to the left of the definition line as a character string before conversion. Specify a physical interface name to the right of the definition line as a character string after conversion. Through forward match, the specified character string before conversion will be replaced by the specified character string after conversion up to the specified number of characters.

If multiple conversion definitions exist, they are processed from the beginning, and the function adopts a corresponding definition when it is detected.

Therefore, if a certain definition is included in another definition, be sure to describe a definition whose number of characters is larger as shown below prior to other definitions.

```
# Invalid definition
sysObjectId: x.x.x.x.*{
"GBE"="GigabitEther ",
"GBEAAA"="GigabitEtherAAA " # Because the previous definition is always val
id, this definition is always invalid.
```

```
}

# Valid definition
sysObjectId: x.x.x.x.*{
"GBEAAA"="GigabitEtherAAA ",
"GBE"="GigabitEther "
}
```

Example of conversion definition file

A specific definition example of conversion definition file is shown below.

```
# PFS-MODEL-001
sysObjectId: 1.3.6.1.4.1.99999.1.203.2.2.*{
"GBE"="GigabitEther ",
"10GBE"="TenGigabitEther "
}
```

Built-in conversion definition

Network Manager provides the following file that includes the built-in conversion definition.

<On the manager, %installfolder%>\Manager\sg\NvPRO\PFLOW\config\NvPROPFlow_sys.ini

```
# PF5200
sysObjectId: 1.3.6.1.4.1.119.1.203.2.2.*{
"GBE"="GigabitEther ",
"10GBE"="TenGigabitEther ",
"LAG"="channel-group "
}

# PF5459-48XP-4Q/PF5459-48GT-4X2Q
sysObjectId: 1.3.6.1.4.1.119.1.126.2.*{
"GE"="GigabitEthernet",
"XGE"="Ten-GigabitEthernet",
"FGE"="FortyGigE",
"BAGG"="Bridge-Aggregation"
}

# PF5820
sysObjectId: 1.3.6.1.4.1.26543.1.7.6{
""="Ethernet"
}
```

Each definition reads in the order of `NvPROPFlow_sys.ini` and `NvPROPFlow_usr.ini`, and if the same definitions are specified, the content specified later is prioritized. In other words, the above built-in definition can be changed in `NvPROPFlow_usr.ini`. Therefore, note that a virtual interface name may be converted to an unexpected physical interface name depending on the definition.

Treatment when the conversion definition file is not properly read

If the conversion definition file cannot be read as there is a problem in the description, an error code and the contents of the problematic definition line are output to the following file.

<On the manager, %installfolder%>\Manager\sg\NvPRO\PFLOW\config\NvPROPFlow_ini_ErrInfo.txt

Correct the problematic definition line according to the error codes described below.

Error codes

Error Code	Description	Problem Cases
01	There are many ":", "{}".	`sysObjectId: : 1.3.6.1.4.1.99999.1.7.6{` `""="Ethernet"` `}` Problem: There are many "{}". `sysObjectId: 1.3.6.1.4.1.99999.1.7.6{{` `""="Ethernet"` `}` Problem: There are many ":".
02	Positions of ":", "{}" are invalid.	`sysObjectId : { 1.3.6.1.4.1.99999.1.7.6` `""="Ethernet"` `}` Problem: The position of ":" is invalid. `sysObjectId  1.3.6.1.4.1.99999.1.7.6 :{` `""="Ethernet"` `}` Problem: The position of "{}" is invalid.
03	In specifying sysObjectId, an asterisk ("*") is specified only for an element in the middle of a string such as "1.3.6.1.4.1.119.1.*.2.2.2".	`sysObjectId : 1.3.6.1.4.1.99999.*.7.6{` `""="Ethernet"` `}`
04	The format of sysObjectId is invalid.	`sysObjectId : 1{` `""="Ethernet"` `}`
05	In specifying sysObjectId, there are some characters other than numbers or dot (.).	`sysObjectId : 1.3.6.1.4.1.99999.a.7.6{` `""="Ethernet"` `}`
06	The format of the definition of "virtual-interface-name_N"="physical-interface-name_N" is invalid.	`sysObjectId: 1.3.6.1.4.1.99999.1.203.2.2.*{` `"GBE"="GigabitEther ",` `"10GE"="TenGigabitEther ",` `LAG=channel-group` `}` `sysObjectId: 1.3.6.1.4.1.99999.1.203.2.2.*{` `"GBE"="GigabitEther "gbe,` `"10GE"="TenGigabitEther ",` `xxx"LAG"="channel-group "` `}`
07	There is no definition for "sysObjectId".	`{` `"GBE"="GigabitEther ", "10GE"="TenGigabitEther ", "LAG"="channel-group "` `}`

Error Code	Description	Problem Cases
08	In the "sysObjectId" definition, "." is redundant.	`sysObjectId: 1.3.6.1.4.1.99999.1.203.2.2.. ...*{ "GBE"="GigabitEther ", "10GE"="TenGigabitE ther ", "LAG"="channel-group " }`
09	An opening ("{?E or closing brace ("}?E is missing.	`sysObjectId: 1.3.6.1.4.1.99999.1.203.2.2. *{ "GBE"="GigabitEther ", "10GBE"="TenGigabit Ether ", "LAG"="channel-group "`
10	Multiple definitions of "virtual-interface-name_N"="physical-interface-name_N" are defined but they are not separated by commas.	`sysObjectId: 1.3.6.1.4.1.99999.1.203.2.2. *{ "GBE"="GigabitEther ", "10GE"="TenGigabitE ther " "LAG"="channel-group " }`

Caution

If the sysObjectId format is valid but does not correspond to the target node, the definitions are not referred to. In other words, note that all the definitions are not checked when referring to definition files.

4.2.5 Registering Nexus 2000 configuration

In Network Manager, the connection between the Nexus 5000 series (parent devices) and the Nexus 2000 series is displayed graphically in the Map View.

The Nexus 2000 series is integrated with Nexus 5000. For this reason, only the Nexus 5000 series is registered in the TCP/IP based Autodiscover function and the Nexus 2000 series is not registered.

Use the procedure below to register the Nexus 2000 series device connected to a Nexus 5000 series device.

- Autodiscover (Nexus)

  Searches for Nexus 2000 series devices that are connected to the currently selected Nexus 5000 and displays them in the Map View. For details, refer to "4.2.5.1 Automatically detecting Nexus 2000 information (page 172)".

- Manual register

  Manually registers Nexus 2000 series devices that are connected to the Nexus 5000, draws a connection line for the connection with Nexus 5000. For details, refer to "4.2.5.2 Manually registering Nexus 2000 information (page 175)".

Caution

1. When managing multiple Nexus 5000 series devices, if there is a different device with the same ID in the FEX ID of the Nexus 2000 at the next level down, you will not be able to manage them properly.
2. The topology check tool is not supported on the Nexus 2000 icon.

   It is possible to start Topology Check Tool from the right-click menu of the connecting-line between Nexus 2000 and Nexus 5000 or between Nexus 2000 and host, however, inconsistency of connection information can not be detected.
3. There is no support for batch registration of Nexus 2000 information from a file. Register by Autodiscover or manual.

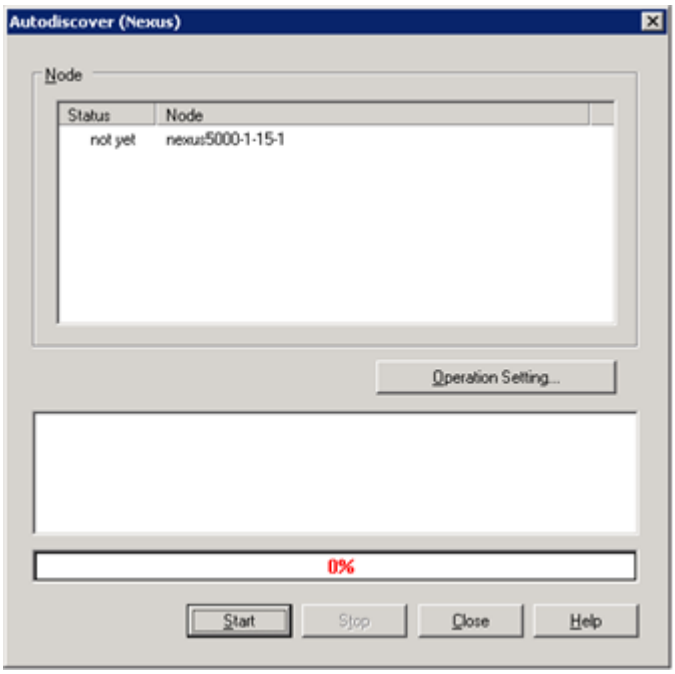
4.2.5.1 Automatically detecting Nexus 2000 information

Searches Nexus 2000 series connecting to the currently selected Nexus 5000, and displays them in the Map View.

You must first change to the "configuration mode (page 27)".

1. Open the "4.2.5.1.1 Autodiscover (Nexus) dialog box (page 173)".

   Right-click the Nexus 5000 icon and select **Configuration Management**>**Autodiscover**>**Nexus**.

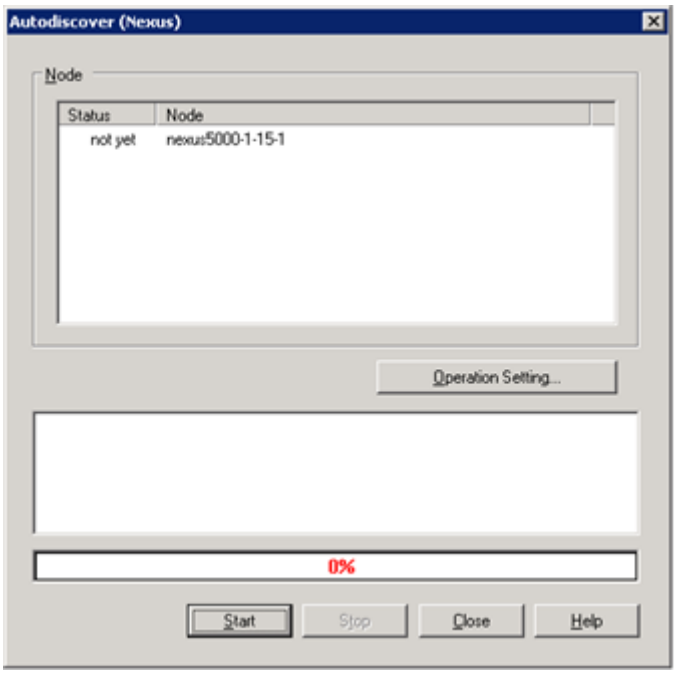


2. Select the Nexus 5000 node to which Nexus 2000 is connecting.
3. To configure the Autodiscovery setting such as a generation rule of Nexus 2000 node names, click **Operation Setting** button and then set the necessary items.

   For details, refer to "4.2.5.1.2 Setting of Autodiscover (Nexus) dialog box (page 174)".
4. Click **Start** button.
5. When the autodiscover process has finished, Click **Close** button to close the dialog box.

For autodiscover of Nexus, register the Nexus 2000 series with the Nexus 2000 icon. To use the Nexus 2200 icon for it, execute **Configuration Management**>**Autodiscover**>**Nexus** and then manually change the **Icon Type** in the icon properties.

Autodiscover (Nexus) dialog box



- **Operation Setting** button

  Open the Autodiscover (Nexus) dialog box. For details, refer to "4.2.5.1.2 Setting of Autodiscover (Nexus) dialog box (page 174)".

- **Start** button

  Starts the Nexus 2000 Autodiscover process.

- **Stop** button

  Suspends the Nexus 2000 Autodiscover process.

- **Close** button

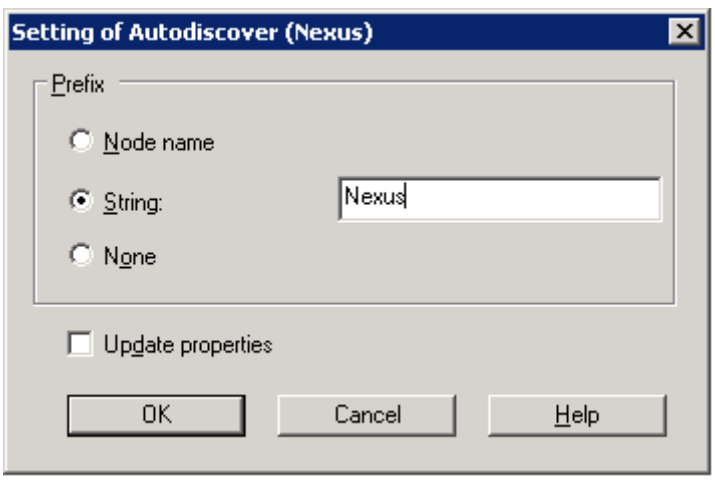
  Closes the dialog box.

- **Help** button

  Displays Help.

Setting of Autodiscover (Nexus) dialog box

Specifies the method for generating Nexus 2000 node names. The default value is node name.



- **Prefix**
  - **Node name**

    The node name is generated using the "*Nexus 5000 node name*"+"_"+"*Nexus 2000 FEX ID*".
  - **String**

    The node name is generated using the "*any character string*"+"*Nexus 2000 FEX ID*".
  - **None**

    The node name is generated using only the "*Nexus 2000 FEX ID*".
- **Update properties**

  Specify whether to update attributes when rediscovering Nexus 2000 devices that are already registered.

Caution

If a Nexus 2000 device is detected using Autodiscover for Nexus, the connection-line between Nexus 5000 and Nexus 2000 will be registered as simple straight lines.

4.2.5.2 Manually registering Nexus 2000 information

The Nexus 2000 manual registration is performed using the same procedure as a normal manual registration.

For information on registering device information, refer to "4.2.2 Manually registering devices and networks (page 138)". For details of connection lines, refer to "4.2.3.3 Manually registering topology information (page 151)".

Caution

- When registering the connection lines between Nexus 2000 and Nexus 5000 devices, the name of the Nexus 2000 management port is not displayed in the Port Name Setting dialog box. To set a port name, use a number between 1 and 4.
- When establishing an aggregated connection between Nexus 2000 and Nexus 5000 devices, set the connection type to "Port connection".

4.2.6 Changing the background and drawing diagrams

4.2.6.1 Changing the background of Map View

In the Map View, you can insert a bitmap image as the background of the map.

- Changing the background color
  1. Right-click an area in the Map View where there are no graphics and select **Background Color** menu.
  2. The Color dialog box is displayed. Select a color and click **OK** button.
- Displaying a file in the background
  1. Right-click an area in the Map View where there are no graphics and select **Background Bitmap** menu.
  2. The Open dialog box is displayed. Select a bitmap file.

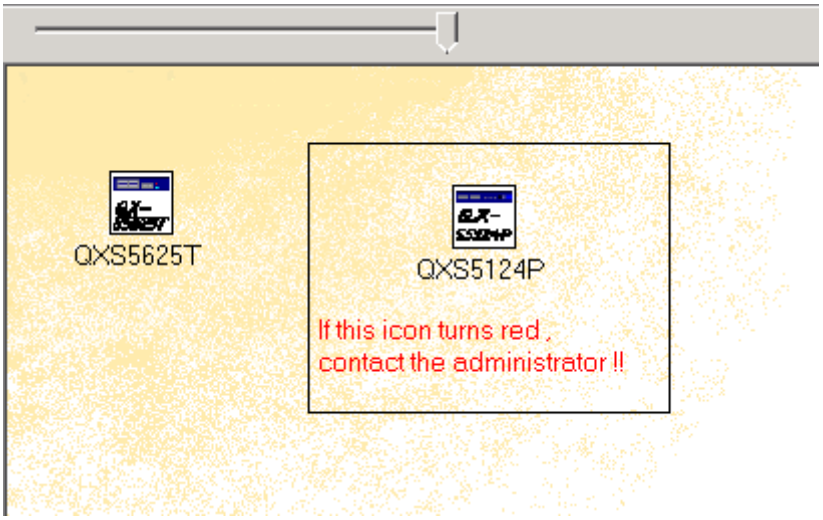
Caution

To display the same images in the multiple monitoring terminals, it is necessary to put same bitmap files on the same path (absolute path) in all monitoring terminals.

- Displaying a grid in the background
  1. Right-click an area in the Map View where there are no graphics and select **Grid** menu.
- Displaying port names for connection line destination nodes and source nodes
  1. Right-click an area in the Map View where there are no graphics and select **Port Name** menu.

4.2.6.2 Drawing diagrams in the Map View

In the Map View, you can draw diagrams and attach a description of a window.



You must first change to the "configuration mode (page 27)".

- Drawing a straight line
  1. Click the icon in the toolbox.
  2. Hold the left mouse button and drag the pointer to draw a line.
- Drawing a rectangle
  1. Click the icon in the toolbox to draw a rectangle with square corners. Click the icon to draw a rectangle with rounded corners.
  2. Drag the pointer in a diagonal direction while holding down the left mouse button.
- Drawing a circle
  1. Click the icon in the toolbox.
  2. Drag the pointer in a diagonal direction while holding down the left mouse button.
- Inserting an icon
  1. Click the icon in the toolbox.
  2. Click the location where you want to insert the icon.

3. Select the icon that you want to insert.

   The files that can be inserted as icons include icon files ("ico" extension) or executable files with icon resources ("exe" extension). If the specified file is incorrect, the default icon will be used.

   Caution

   To display the same icons in the multiple monitoring terminals, it is necessary to put same icon files on the same path (absolute path) in all monitoring terminals.

- Inserting an image

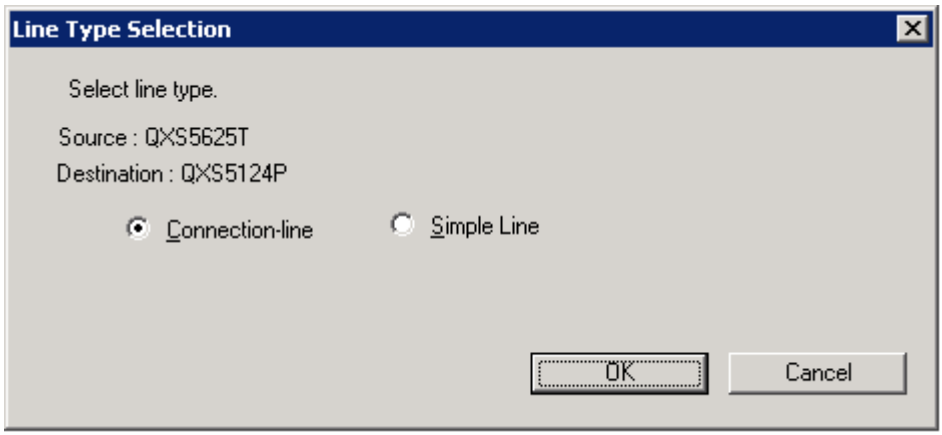
1. Click the  icon in the toolbox.
2. Click the location where you want to insert the image.
3. Select the image that you want to insert. Only bitmap files ("bmp" extension) can be inserted.

   Caution

   To display the same images in the multiple monitoring terminals, it is necessary to put same bitmap files on the same path (absolute path) in all monitoring terminals.

- Consolidating graphics

1. Click the graphics that you want to consolidate.
2. Click the graphics that you want to consolidate to while holding the CTRL key.
3. Click the  icon in the toolbox.
4. In the Line Type Selection dialog box, select **Simple Line**.



   Caution

   Simple Line is a simple graphic for creating a connection between icons. The **Connection-line** is a particular type of node that displays the physical connection line between devices and, like device icons, changes color depending on its status. For drawing of connection-lines, refer to "4.2.3.3 Manually registering topology information (page 151)".

- Drawing a text box

1. Click the  icon in the toolbox.
2. To create a text entry frame, drag the pointer in a diagonal direction while holding down the left mouse button until you reach the desired size.

3. Double-click inside the text box and type text.

- Changing the background color of graphics
  1. Select the image for which you want to change the background.
  2. Click the  icon in the toolbox.
- Changing the color of a line
  1. Select the image for which you want to change the line color.
  2. Click the  icon in the toolbox.
- Change the color of text
  1. Select the image for which you want to change the text color.
  2. Click the  icon in the toolbox.
- Changing the font
  1. Select the image for which you want to change the font.
  2. Click the 

box in the toolbox and select a font.
- Changing the font size
  1. Select the image for which you want to change the font.
  2. Click the 

box in the toolbox and select a font size.
- Changing the weight of a line
  1. Select the image for which you want to change the line weight.
  2. Click the  icon in the toolbox and select a line weight.
- Changing the line type
  1. Select the image for which you want to change the line type.
  2. Click the  icon in the toolbox and select a line type.
- Changing a line into an arrow
  1. Select the line that you want to change into an arrow.
  2. Click the  icon in the toolbox and select an arrow type.
- Deleting an image
  1. Select the graphic that you want to delete.
  2. Right-click and select **Delete** menu.
- Changing the display order of graphics
  1. Select the image for which you want to change the display order.
  2. Right-click, point to **Change Order** and select a display order.
- Changing the icon text display position
  1. Select the icon for which you want to change the icon text display position.
  2. Right-click, point to **Icon Text** and select a display position.

4.2.7 Updating device information via a network

Obtain the most current information from a device, and update the device and interface information maintained by Network Manager. The device information update function is designed to be used for supplementing manually or batch registered device information with information obtained from devices connected to the network.

You can choose "Update Required Property" or "Update All Property" according to the property items you want to update.

In the **Update Required Property** menu, the following information is updated.

- **Device properties**
  - Agent type
  - Software version
  - Routing control
  - SNMP engine ID
  - sysName
- **Interface properties**
  - Interface information (ifTable information, IPv4 information, IPv6 information)
  - Fex ID (only if OS type is NX-OS)

In the **Update All Property** menu, updates the following information in addition to the required properties listed above.

- **Device properties**
  - OS type
  - Administrator
  - Location
- **Interface properties**
  - Default target port

⚠ Caution

There are several restrictions when updating device information for the Nexus series. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".

To update the device information, it is necessary to enable SNMP communication between Network Manager and the device. On the Network Manager side, it is necessary to configure the appropriate settings device icon information (property information) items below.

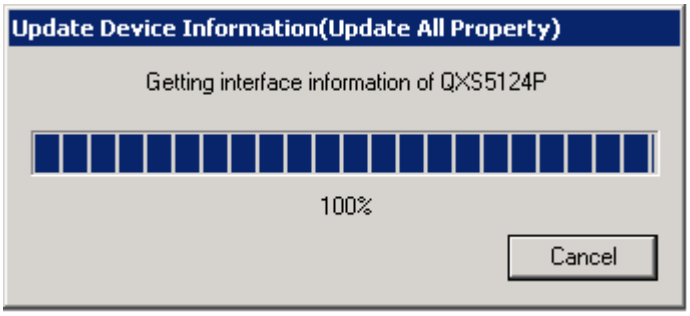
- If the target device supports SNMPv1 or v2c:
  - IPv4 address or IPv6 address
  - SNMP community name (get)
- If the target device supports SNMPv3:
  - IPv4 address or IPv6 address
  - The following items in the **SNMPv3** tab.
    - User name

* Security level
* Authentication protocol and password (if "Auth/NoPriv" or "Auth/Priv" is selected in the security level)
* Privacy protocol and password (if "Auth/Priv" is selected in the security level)

For details of property, refer to "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)".

You must first change to the "configuration mode (page 27)".

1. To update the device information, execute one of the following ways.
   - Right-click **NetworkManagement** icon, the map icon, or device icon. Select **Configuration Management**>**Update Property**>**Update Required Property**.
   - Right-click **NetworkManagement** icon, the map icon, or device icon. Select **Configuration Management**>**Update Property**>**Update All Property**.
2. The device information is updated.



Caution

If any non-ASCII character is included in the property information to be updated, they may not be displayed correctly. In that case, configure the **SNMP Character Code** property and retry the operation.

4.2.8 Registering interface information

4.2.8.1 Discovering interface information

In Network Manager, store and manage all interface information for monitored devices that support SNMP. After registering interface information in Network Manager, there is support for the following tasks:

- Check the relation between ifIndex values and interface names in a list.

  Example, look up interface names from ifIndex values contained in the alert notification.
- Check all information for IPv4 and IPv6 addresses assigned to monitored nodes.

  In an environment that uses Network Address Translation (NAT), even if the "IP Address" value used for monitoring and registered in the node property information is different from the IP address assigned to the monitored device, it is still possible to accurately check IP address information on the device side.
- If an SNMP trap is received that has a different send source IP address from the "IP address" value registered in the property information for the node, it is still possible to receive that

SNMP trap appropriately and perform notifications after checking the send source IP against all of the IP addresses in the interface information.

Interface information for monitored devices is found from the monitored device MIB, and is then registered. Use any of the following three methods to find and register interface information:

- Use Autodiscover to register node information

  For Autodiscover, refer to "4.2.1 Automatically detecting devices and networks (page 127)".

- Update device information

  When using the monitoring terminal windows, refer to "4.2.7 Updating device information via a network (page 179)". When using commands, refer to "9.10.2 Configuration information update command (nvpnodeup) (page 725)".

- Open the Interface Properties dialog box.

  If there are nodes where interface information has not been registered, communication is automatically established with those devices when the Interface Properties dialog box is opened and the interface information is retrieved and registered. If an extension card for the device is inserted or removed and the interface configuration is changed, update the interface information by opening the Interface Properties dialog box dialog box and then click **Discovery** button. For details, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

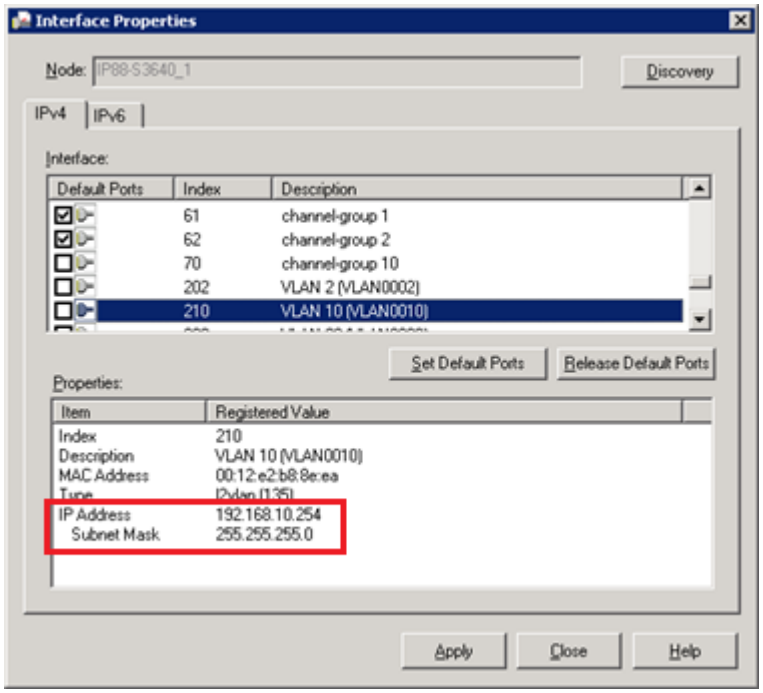
Interface Properties dialog box

Displays interface information for devices being maintained by Network Manager. You must change to "configuration mode (page 27)" in order to change information.

- **Node**

  Displays the device name.

- **IPv4** tab



  - **Interface**

Device interface information is displayed in a list. The list can be sorted by clicking the column labels.

- **Default Ports**

  Select the port that you want to set as the default port. You can set multiple ports to be defaults. If **Default Target Port** is not specified in the Properties dialog box of the node, nothing is checked in the **Default Ports** column of the Interface Properties dialog box. Also, if **Default Target Port** registered in the Properties dialog box of the node is incorrect, it shows that only the physical ports are checked. If you want to change the default ports, correct the check marks and click **Apply** button.

- **Set Default Ports** button

  Select the interface and then select the **Default Ports** check box. Select multiple ports by holding down the CTRL key while clicking. After making changes, always click the **Apply** button. No information is saved after clicking **Close** button.

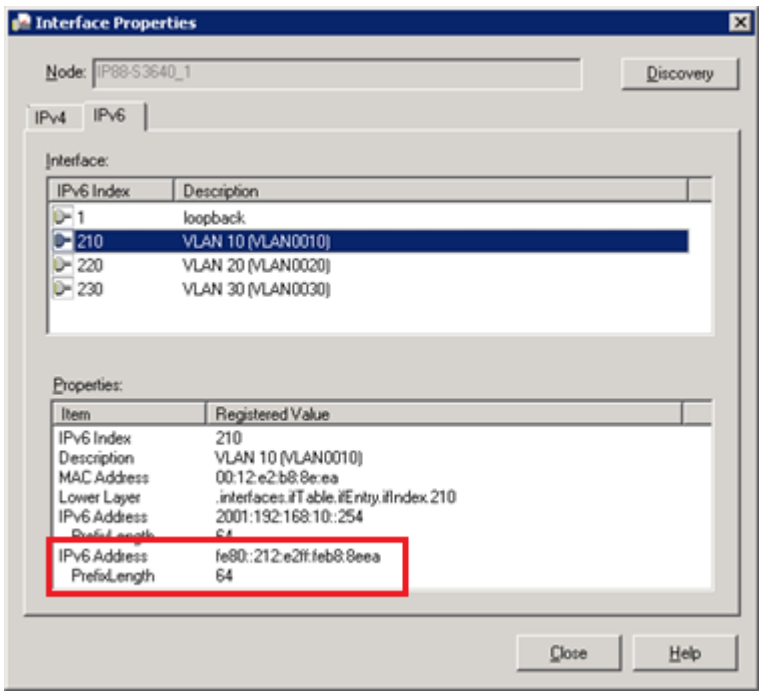
- **Release Default Ports** button

  Select the interface and then clear the checkbox for the **Default Ports**. Select multiple ports by holding down the CTRL key while clicking. Always click the **Apply** button after making changes. No information is saved after clicking **Close** button.

- **Properties**

  Shows detailed information for selected ports in a list. The IP address and the subnet mask are displayed on two separate lines as shown in the figure above (inside the red frame).

- **IPv6** tab



The **IPv6** tab is displayed if one or more device interfaces have IPv6 addresses and Network Manager manages information of these interfaces. (Even if IPv6 protocol is not used for communication with the target device, if the device interfaces have IPv6 address information of the interface, this tab is displayed.) **Default Ports** cannot be specified in this tab.

- **Interface**

The information of interfaces that have IPv6 address is displayed in a list. The list can be sorted by clicking the column labels.

- **Properties**

  Shows detailed information for selected ports in a list. The IPv6 address and the prefix length are displayed on two separate lines as shown in the figure above (inside the red frame).

- **Discovery** button

  Obtains interface information from the device specified under node. Details in the **IPv4** tab and the **IPv6** tab are updated together. In addition, the default port information is also updated. The default port is reset to the physical port.

  Caution

  If the interface information is changed as a result of the switch or router board being disconnected and reconnected, or changes to config, click the **Discovery** button in Interface Properties dialog box to update the Network Manager registration information.

- **Apply** button

  Reflects the default port settings in Network Manager. This button is displayed when **IPv4** tab is selected.

- **Reload** button

  Reloads the latest interface information that is registered in Network Manager.

- **Close** button

  Closes the dialog box.

- **Help** button

  Displays Help.

4.2.8.2 Setting default target ports

The default target port is the port that Network Manager uses for collecting information when a user does not specify a port (port number or interface number) when setting up state monitoring rules and data collection settings. (This does not affect SNMP trap/syslog monitoring.)

By setting the default target port, data can be obtained efficiently. This is because the number of packets necessary to obtain data can be decreased. If **Default Target Port** property is blank or the port number described in the **Default Target Port** property is incorrect, all ports will be the monitoring and collecting targets.

For information about "state monitoring rules", refer to "4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function) (page 241)". For information regarding "data collection settings", refer to "4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices (page 334)".

Use any of the following three methods to set default ports:

- Register ports from the Interface Properties dialog box.

  For details, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

- Register ports from the Properties dialog box for each node

  For details, refer to "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)".

- Register using batch configuration registration

  If setting up a large number of ports is required, use batch configuration registration. For details, refer to "4.6 Batch Registering or Deleting Configuration Information (page 206)".

4.2.9 Changing icon properties and locations

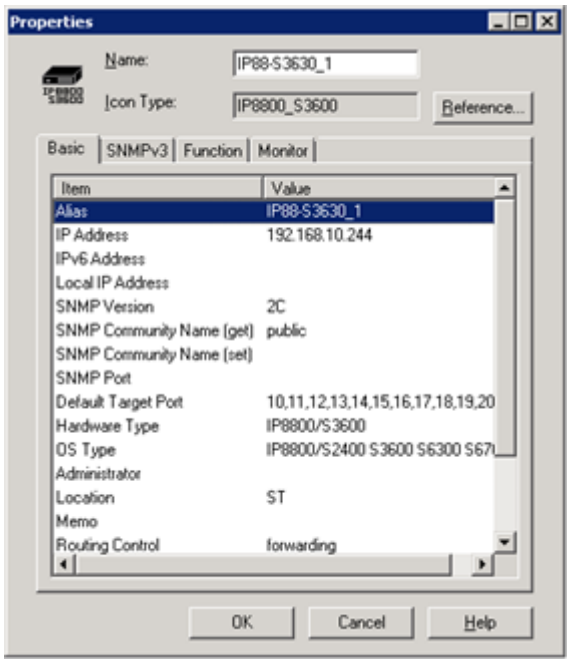
4.2.9.1 Changing icon properties manually

You must first change to the "configuration mode (page 27)".

- Verify and change device and map information

  1. Open the Properties dialog box.

     Right-click the device icon and select **Property** menu.



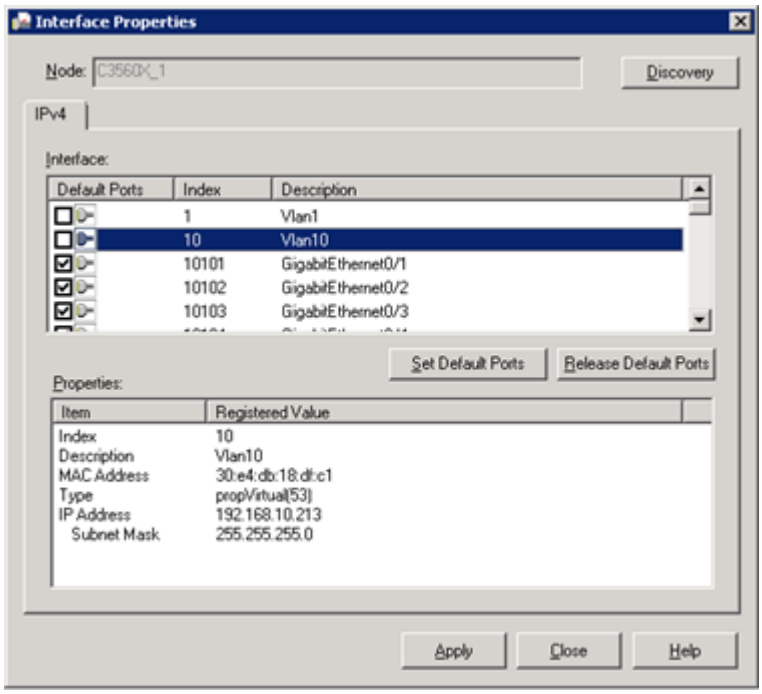
     For details, refer to "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)".

  2. Double-click the item and change the value.
  3. Click **OK** button.

- To update device interface information

  1. Open the Interface Properties dialog box.

     Right-click the device icon and select **Configuration Management**>**Interface Property**.



For details, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

2. Click **Discovery** button to update interface information, or check/uncheck **Default Ports** to change the default target ports.
3. Click **Apply** button.

4.2.9.2 Changing topology information manually

You must first change to the "configuration mode (page 27)".

1. Open the "4.2.9.2.1 Connection-line Properties dialog box (page 185)".

   Right-click the connection-line in the Map View and select **Property** menu.
2. Change the setting information.

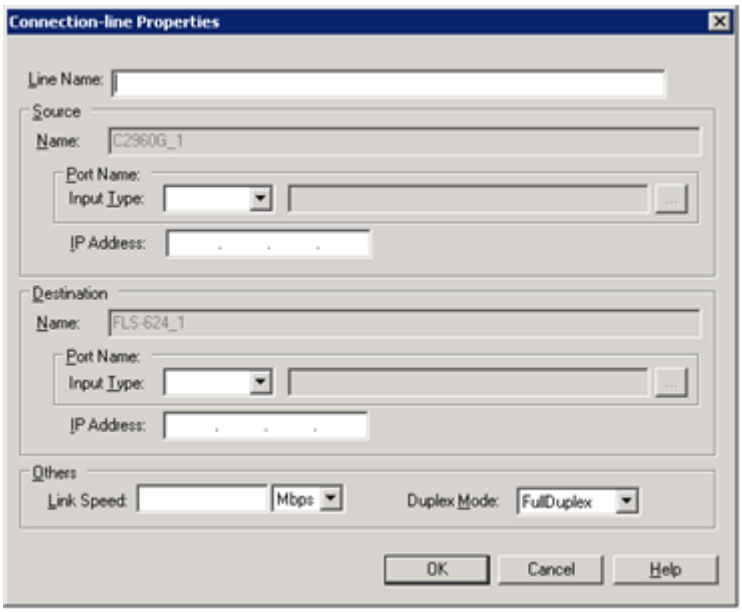
   For details of input items, refer to "4.2.3.3.2 Connection-line Properties dialog box (page 154)".
3. Click **OK** button.

Connection-line Properties dialog box

The properties of a selected line can be displayed and edited in the Connection-line Properties dialog box.

If an operation is being performed in configuration mode, the mode will change to edit mode and the line information can be updated.

For contents of each items and input method, refer to "4.2.3.3 Manually registering topology information (page 151)".



Caution

1. Information cannot be updated while operating in the normal mode (non-configuration mode).
2. Even if a link speed was entered in Gbps units, it will be displayed in Mbps units in the properties display.
3. In Network Manager, the source/destination devices of the connection-line are not distinguished. The source/destination devices of the connection-line may be displayed in reverse.

4.2.9.3 Moving an icon to another map

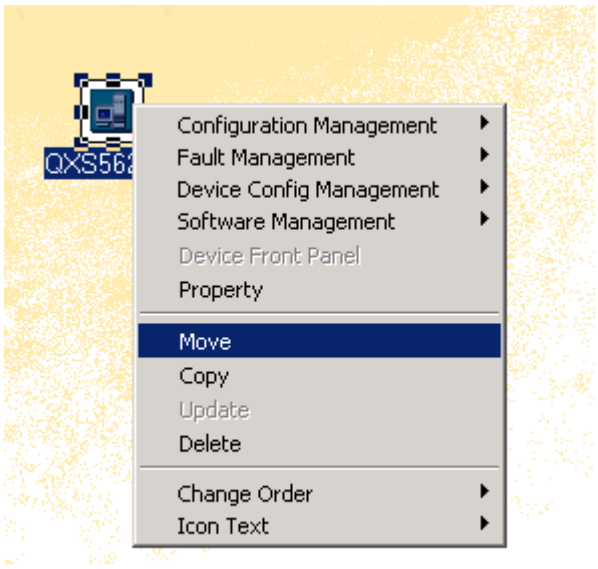
You must first change to the "configuration mode (page 27)".

1. Use one of the following steps to move an icon that displays in the tree or Map View.
   - In the tree view, right-click the icon to move, and then click **Move** menu.

     Caution

     If you try to right-click an icon that cannot be moved, the **Move** menu is not be available.

   - In the Map View, right-click the icon to move, and then click **Move** menu.



Caution

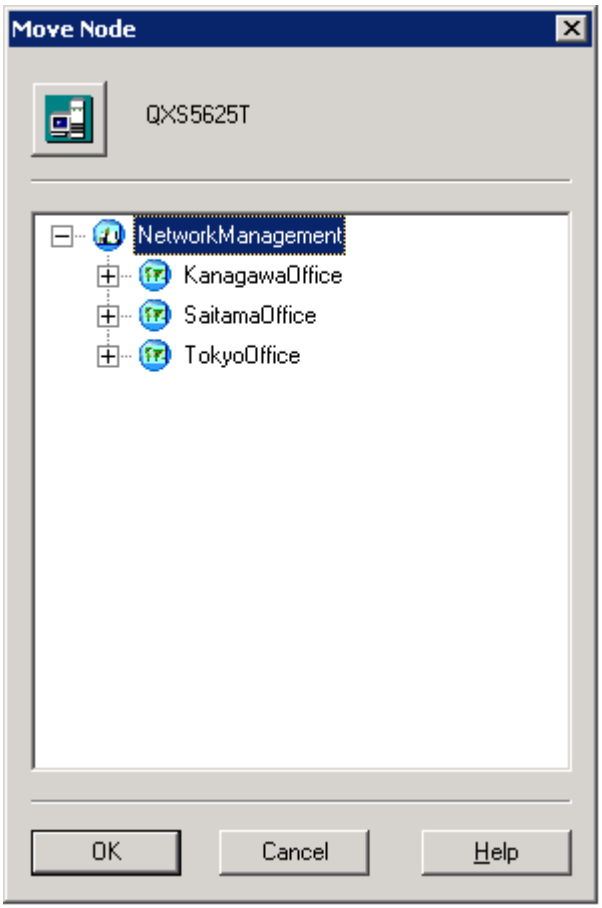
If you try to right-click an icon that cannot be moved, the **Move** menu is not be available.

- In the tree view, use drag-and-drop.

Caution

- Cannot use for icons that cannot be moved.
- Cannot use for icons in the Map View.

2. When **Move** menu is selected, select a destination map in the Move Node dialog box, and click **OK** button.



- Icons that cannot be moved do not display.
- When moving a map icon, all icons below the map also move.

4.2.9.4 Copying an icon

You must first change to the "configuration mode (page 27)".

1. On the Map View or tree view, select a copy target node.
2. Right-click the target icon and select **Copy** menu.

⚠ Caution

Cannot copy multiple icons at the same time. To copy multiple icons or connection lines, use the batch register function and register the same node information in multiple maps.

3. In the Map View, right-click a blank area where you want to paste the icon, and select **Paste** menu.

4.2.9.5 Deleting topology information

You must first change to the "configuration mode (page 27)".

1. To delete topology information, right-click the connection-line and select **Delete** menu.
2. In the confirmation dialog box, click **OK** button.

4.2.9.6 Deleting an icon

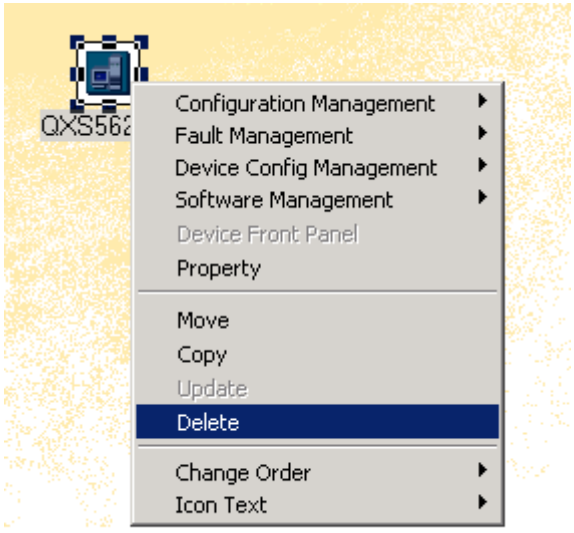
When deleting a map icon, all subordinate nodes is also deleted.

When device information is deleted, the license for that device is cancelled. A cancelled license can be used to register another device.

If the device icon that you want to delete is registered under multiple maps, delete all of its registered device icons. To confirm that all of its registered device icons have been deleted, use the search feature. For the search function, refer to "5.17 Searching for a Node (page 556)".

You must first change to the "configuration mode (page 27)".

1. To delete an icon displayed in the tree view, Map View, execute one of the following steps.
   - To delete an icon that displays in the tree view, right-click the icon to delete, and click **Delete** menu.
   - To delete an icon that displays in the Map View, right-click the icon to delete, and click **Delete** menu.



Caution

- If right-click an icon that does not delete, the **Delete** menu is not available.
- To delete multiple icons in a single operation, in the Map View, select the icons to delete. Hold down the CTRL key, right-click, and select **Delete**. To select multiple icons in the Map View, hold down the CTRL key and click the icons to select. Or if no icons are selected, drag the mouse over the items to select.

2. In the confirmation dialog box, click **OK** button.

Caution

If deleting several hundred or more icons (especially when nodes with faults are deleted), it may take time to complete. If you execute some operation on the view during the deletion, the window status may change to "Not Responding". To avoid this, wait without operation on the view.

4.3 Registering Login Information

For some of the Network Manager product functions, a telnet or ssh login is required for target devices to perform each management function. For this reason, it is necessary to set up password information for the login on each device.

Login information is used for managed devices for the following Network Manager functions:

- Resource Manager function
  - "4.20 Setting for Managing Device Configuration (Resource Manager) (page 399)"
  - "5.14 Managing Device Configuration (Resource Manager) (page 512)"
  - "5.15 Managing Device Software (Resource Manager) (page 531)"
- Remote login function
  - "5.5.3 Logging in to devices from the monitoring terminal (page 469)"
- Device command execute function
  - "4.19 Setting for Running Device Commands (page 391)"
- Execute command when an alert occurs function
  - "4.15 Settings for Executing Device Commands When Alerts Occur (page 333)"

⚠ Caution

There are some network devices that do not support simultaneous multi-user logins or, even if multi-user logins are supported, there is a limit to the number of logins at one time. For these devices, the user is logged in via a different path, the login from Network Manager fails and the various functions cannot be used.

The following two methods can be used to register login information.

- Manual register

  Register login information in the Login Setting window. For details, refer to "4.3.2 Registering device login information (page 191)".

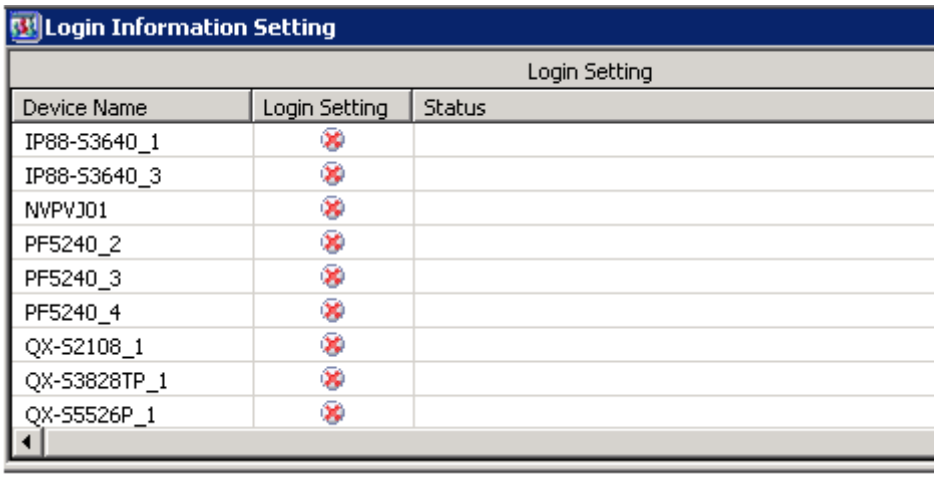
- Batch register

  Imports login settings from a configuration information file. For details, refer to "4.6 Batch Registering or Deleting Configuration Information (page 206)".

4.3.1 Login Information Setting window

Login information is registered, tested and verified in the Login Information Setting window.

To open the Login Setting window, right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Configuration Management**>**Login Information Setting**.



- **Device Name**

  Displays the names of devices registered in Network Manager that have login settings support.

- **Login Setting**

  Login settings have not been conducted for devices with a  symbol. Devices with a  symbol do have login settings.

- **Status**

  Displays the status of the login test.

- **Date**

  Displays the date and time that the login test was performed.

Caution

If the following operations are performed while this window is opened. The device list in this window is not updated immediately. To reflect changes, open this window again.

- Add and delete a device icon.
- Change a device name.
- Move an icon to another map.

4.3.2 Registering device login information

Login information is registered in the Login Information Setting window. Login information can be registered only to nodes that have IPv4 address property.

Caution

1. There are some network devices that do not support simultaneous multi-user logins or, even if multi-user logins are supported, there is a limit to the number of logins at one time. For these devices, the user is logged in via a different path, the login from Network Manager fails and the various functions cannot be used.
2. Resource Manager function might fail for a network device that cannot suppress console logs in each connection. In this case, configure a device to suppress console logs beforehand.
3. When the target device in the login setting is PF6800, The value that can be specified to the user name is the user who has administrator authority such as pfcadmin, etc. However, root cannot be specified.
4. When the target device model is supported by Resource Manager function and the version of the its software is not supported, login information may not be registered.

   In such a case, change **OS type** to any model that is not supported by Resource Manager function such as "OtherSwitch"

   For the list of models supported by Resource Manager function, refer to "8.1.2 Supported Devices in Resource Manager function (page 671)". For details of **OS Type**, refer to "4.6.1.1.1 OS type and software version format (page 223)".

To register login information to a node, a node must have the following propetry settings.

1. IPv4 address
2. Telnet Server: ON

To confirm device icon properties, refer to "4.2.9.1 Changing icon properties manually (page 184)".

Caution

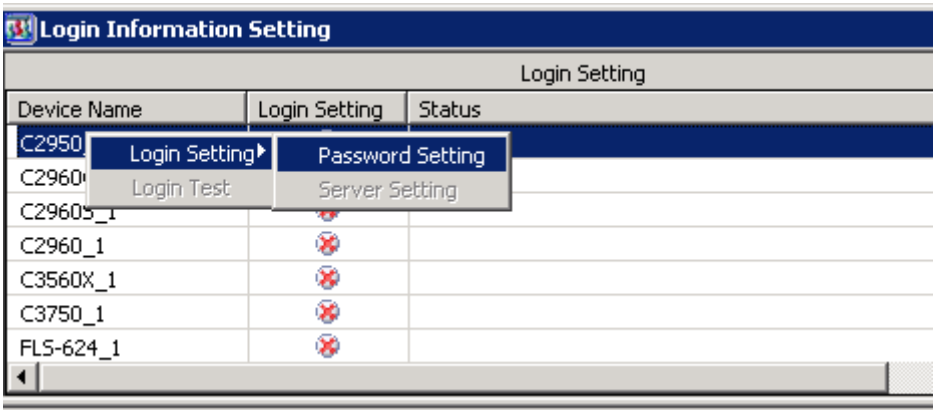
Login information cannot be registered to a node that has only IPv6 address property.

You must first change to the "configuration mode (page 27)".

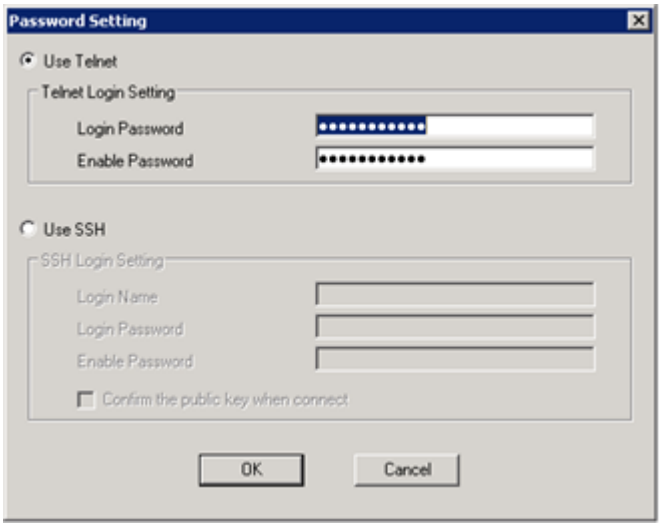
1. Open the "4.3.1 Login Information Setting window (page 190)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Configuration Management**>**Login Information Setting**.

2. Right-click the device for which you want to set up login information and select **Login Setting**>**Password Setting**.



3. The Password Setting dialog box is displayed.



   Select **Use Telnet** or **Use SSH**, and enter in the necessary items.

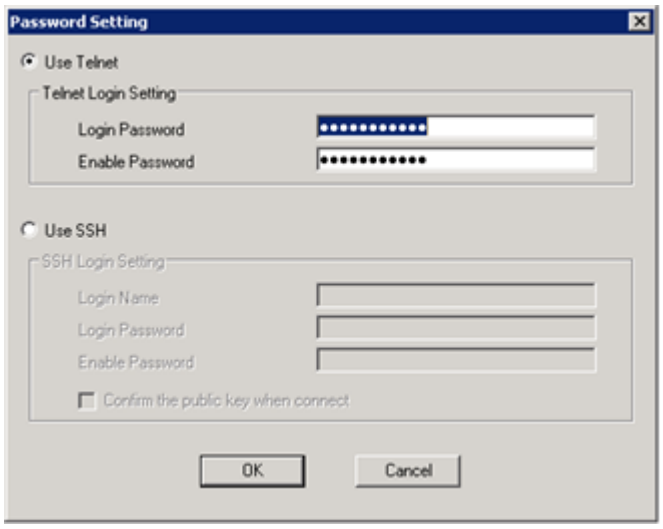
   For details, refer to "4.3.3 Password Setting dialog box (page 192)".

4. Click **OK** button.

4.3.3 Password Setting dialog box

Select a protocol to be used for login from Telnet or SSH, and configure the setting of login information such as user name or password, etc.

- **Use Telnet**



To use the Telnet for connecting to the device

- **Telnet Login Setting**

  Type the user name and password that you use to log in to telnet. Each item must be no longer than 63 characters. The information entered in this dialog box changes depending on the type of device.

  * For a model supported by Resource Manager function:

    Items necessary for login to the device or transition to the privilege mode (enable mode) are displayed. For the list of models that Resource Manager function supports, refer to "8.1.2 Supported Devices in Resource Manager function (page 671)".

  * For a model not supported by Resource Manager function:

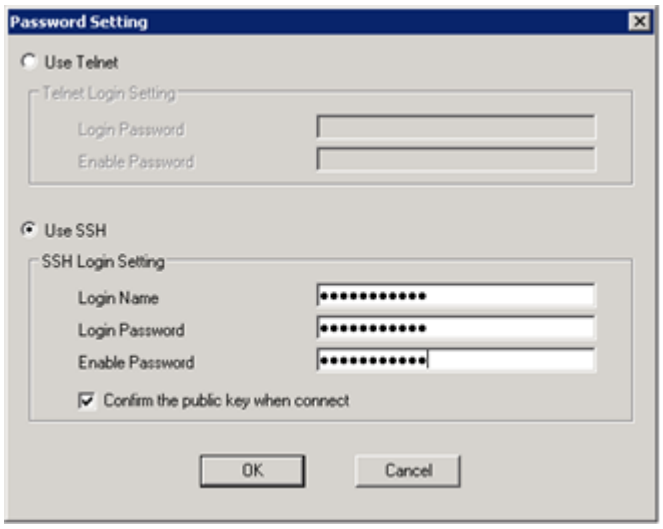
    Up to five items are displayed. The contents entered in each item are sent to the device in order. Enter items necessary for login and transition to the privilege mode such as user name, password, a command for transition to the privilege mode, or its password, etc.

    Example:

    If an user name and password are required to log in, "enable" command and its enable password are required for transition to the privilege mode, enter the user name, password, "enable", and enable password in this order. The character strings are sent to the device in this order, and then the login processing and transition to the privilege mode are performed.

  If an item remains blank, only the linefeed code is sent. If you would like to send a control code, specify `"%<hexadecimal>"`. For example, to send Ctrl+Y (Press CTRL key and Y key at a time), specify `"%19"`.

- **Use SSH**



To use the SSH for connecting to the device.

- **SSH Login Setting**

  Type the user name and password that you use to log in to ssh. Each item must be no longer than 63 characters.

  * **Login Name**

    Specify a login user name. Do not leave this item in blank.

  * **Login Password**

    Specify the password of the login user. Do not leave this item in blank.

  * Additional Items

    Some additional items are displayed, depending on models.

    + For a model supported by Resource Manager function:

      Items necessary for transition to the privilege mode (enable mode) is displayed. For the list of models that Resource Manager function supports, refer to "8.1.2 Supported Devices in Resource Manager function (page 671)"

    + For a model not supported by Resource Manager function:

      Up to three additional items are displayed. The contents entered in each item are sent to the device in order, after connecting and logging in to the device using SSH. Enter items necessary for transition to the privilege mode such as a command to transition to the privilege mode or its password, etc.

      Example:

      If "enable" command and its enable password are required for transition to the privilege mode, enter "enable" and enable password in this order. The character strings are sent to the device in this order, and the transition to the privilege mode is performed.

      If an item remains blank, only the linefeed code is sent. If you would like to send a control code, specify "%<hexadecimal>". For example, to send Ctrl+Y (Press CTRL key and Y key at a time), specify "%19".

  * **Confirm the public key when connect**

    When connecting to the device using SSH for the first time, the public host key of the device is registered in Network Manager. If check is enabled, in login processing, the

public host key and the host key registered in Network Manager are compared. If keys do not match, login process is terminated.

⚠ Caution

1. Even if check is enabled, when it has never connected to the device using SSH, and the public host key is not registered in Network Manager, the public host key on the device are not confirmed.
2. When login method is changed from SSH to Telnet, all public host keys registered in Network Manager are deleted.
3. When multiple devices have same IP address (redundant configuration), use one of the following procedures to login normally.
   + Unify the public host key among the devices that have same IP address.
   + Uncheck **Confirm the public key when connect** and perform the login test for all devices, in order to register all public host keys of the devices in Network Manager. Then, check **Confirm the public key when connect**.

4.3.4 Testing login information

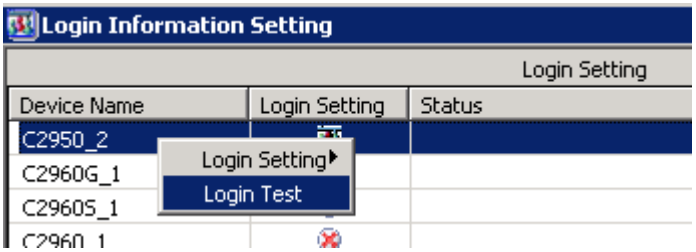
This operation is only available to users belonging to a group that has operation authority.

You can confirm that the set user name and password are correct.

1. Open the "4.3.1 Login Information Setting window (page 190)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Configuration Management**>**Login Information Setting**.

2. Right-click the line of the device for which you want to perform a login test and select **Login Test** menu.



The test results are displayed in the **Status** column.

⚠ Caution

When you perform a login test to a device that is not supported by Resource Manager function, `"Succeeded in login."` message might be displayed, even if the login was failed.

When the target device is not supported by Resource Manager function, to confirm that the login information to the device is correct, in addition to the **Login Test** menu, right-click the device icon and select **Fault Management**>**Remote Login**, and then confirm that the device can be logged in to properly.

For the list of models that Resource Manager function supports, refer to "8.1.2 Supported Devices in Resource Manager function (page 671)".

4.3.5 Setting external server information

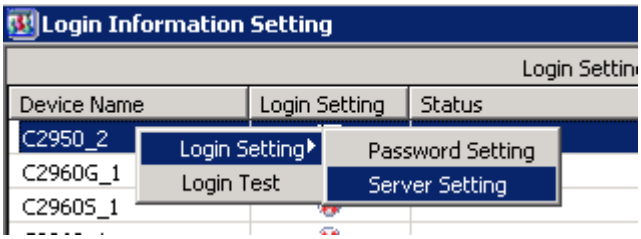
Specify file-transfer servers external to this product, or set a login used for TACACS+/RADIUS authentication servers.

You must first change to the "configuration mode (page 27)".

1. Open the "4.3.1 Login Information Setting window (page 190)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Configuration Management**>**Login Information Setting**.

2. Right-click the device to which you want to set the external server information, and select **Login Setting**>**Server Setting**.



3. Enter the required items in the Server Setting dialog box.

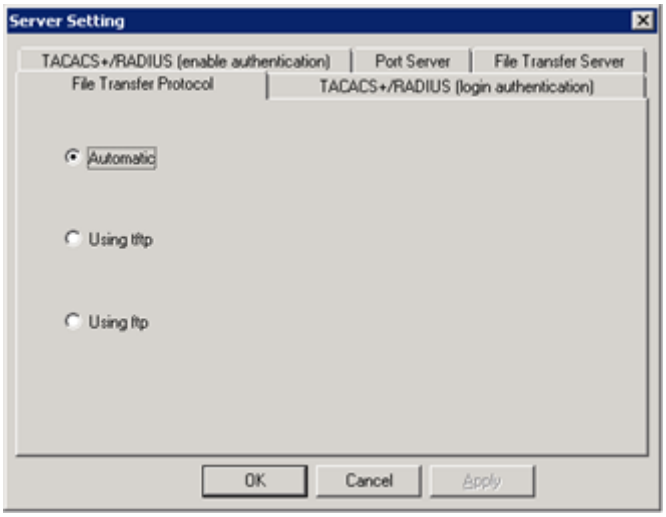
   For the setting contents in the Server Setting dialog box, refer to the following.

   - "4.3.5.1 **File Transfer Protocol** tab (page 196)"
   - "4.3.5.2 **TACACS+/RADIUS (login authentication)** tab (page 197)"
   - "4.3.5.3 **TACACS+/RADIUS (enable authentication)** tab (page 197)"
   - "4.3.5.4 **Port Server** tab (page 198)"
   - "4.3.5.5 **File Transfer Server** tab (page 200)"

4. Click **OK** button.

4.3.5.1 File Transfer Protocol tab

Select setting of file transfer protocol used in Resource Manager function.



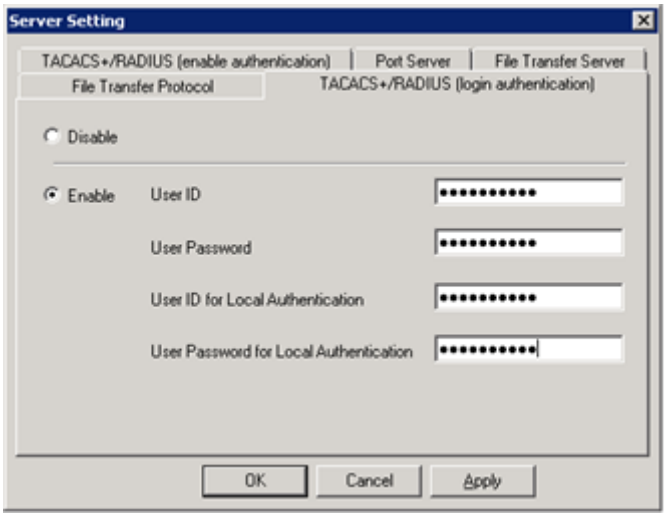
- **File Transfer Protocol**

  Specify the file transfer protocol to be used for configuration file and software collection and delivery. If the device supports both FTP and TFTP, select one of these two file transfer protocols. The default automatic option gives priority to TFTP.

The protocol that can be used for transferring a file varies depending on device models. For the list of protocol that can be used, refer to "8.1.2 Supported Devices in Resource Manager function (page 671)".

4.3.5.2 TACACS+/RADIUS (login authentication) tab

If the device is set to use TACACS+ or RADIUS client authentication when logging in, select **Enable** and set the user information used for authentication. The settings in this tab are enabled only if **Use Telnet** is selected in Password Setting dialog box.



- **User ID**

  Enter the user name used in TACACS+ or RADIUS authentication. The user name must be no longer than 63 single-byte characters.

- **User Password**

  Enter the user password used in TACACS+ or RADIUS authentication. The user name must be no longer than 63 single-byte characters.

- **User ID for Local Authentication**

  Type the user name used for local authentication by the device in the case that the TACACS+ or RADIUS server is down. The user name must be no longer than 63 single-byte characters.

- **User Password for Local Authentication**

  Type the user password used for local authentication by the device in the case that the TACACS + or RADIUS server is down. The user name must be no longer than 63 single-byte characters.

Tip

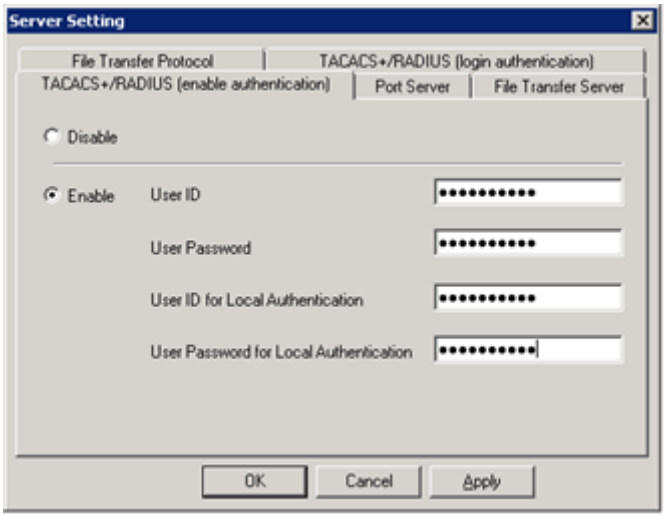
1. If registration is completed without specifying anything in the password box, the setting is for no password. In addition, eight asterisks will be displayed in the password box for the device that was configured. This is a preventative measure to avoid calculation of the number of password characters.
2. If the Password Setting (Use Telnet), TACACS+/RADIUS settings, and Port Server settings were set, they are prioritized in the following order.

   Port Server settings > TACACS+RADIUS settings > Password Setting (Use Telnet)

4.3.5.3 TACACS+/RADIUS (enable authentication) tab

If the device is set to use TACACS+ or RADIUS client authentication when entering into the enable mode, select **Enable** and set the user information to be used for the authentication.

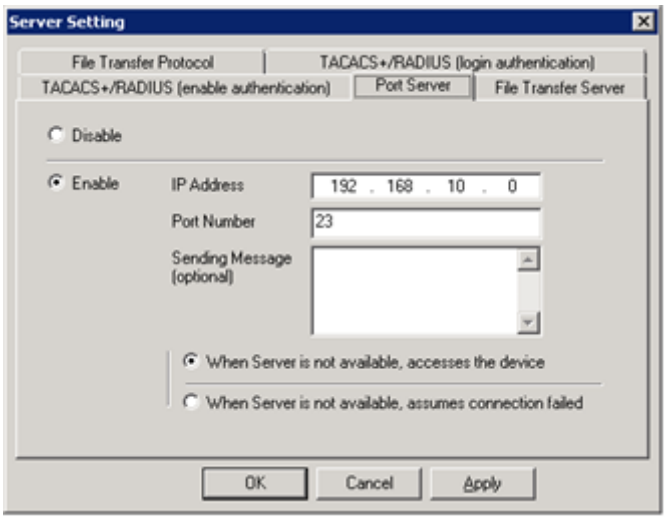
The settings in this tab are enabled only if **Use Telnet** is selected in Password Setting dialog box.



The meanings of the input items in this tab are same as in "4.3.5.2 **TACACS+/RADIUS (login authentication)** tab (page 197)".

4.3.5.4 Port Server tab

Configure the setting of the port server. This setting is configured when performing a Telnet login to a device console via a port server, instead of direct login to the device.



- **IP Address**

  Enter the IP address of the port server. Enter the address in decimal format (xxx.xxx.xxx.xxx). The range is: 1.0.0.0 - 223.255.255.255. This item cannot be omitted.

- **Port Number**

  Enter the Telnet TCP port number for the port server as a decimal number. The range is 1 - 65535. This item cannot be omitted.

- **Sending Message**

Type the sending message for logging in to a device via a console after the telnet login to the port server.

The sending message is sent in single-line conversation format in response to inquiries from the port server or device console. The sending message must be no longer than 511 single-byte or double-byte characters.

Example:

If the screen image after performing a login via a port server is as follows. The characters without the under line are the received message. The characters with the under line are the entered message.

```
> connect 1
login: root
Password: password1

> enable
Password: password2
#
```

The message sent after the telnet login to the port server is as follows:

```
connect 1
root
password1
enable
password2
```

To send control code, express it as "%<*hexadecimal*>". For example, if you need to send a BS (backspace), it is represented as "%08".

- **When Server is not available, accesses the device**

  Select this option if you want to perform a telnet login using the device IP address whenever the port server cannot be accessed.

  The password that was entered in the **Password Setting** dialog box is used in this case.

- **When Server is not available, assumes connection failed**

  Select this option if you want the system to assume that the telnet login failed when the port server cannot be accessed.

Tip

1. **Password Setting (Using Telnet)**, **TACACS+/RADIUS** settings, and **Port Server** settings were set, they are prioritized in the following order.

   Port Server settings > **TACACS+/RADIUS** settings > **Password Setting**

2. In performing a Telnet login to a device via a port server, when the port server prompt (for example, the "***#" in "#" or ">") and the device prompt are the same, "`Succeeded in login.`" may be displayed, even if **Login Test** fails. To confirm that the device can be logged in to properly with the port server settings, perform any of the following verification methods in addition to the **Login Test** before starting the system operations.
   - In the Command Scheduling window, select **Execute At Once** and review the results file.
   - In the Running-config Management window for each device, select **Collect Config** and review the results.
   - Check the access log on the device.
3. If the port server setting is configured, despite selection of the connection method in the Password Setting dialog box, the connection to the device is performed by Telnet.

4. To use Resource Manager function (configuration management, software management) on the device that the port server setting is configured, the setting relating to the file transfer server may be required depending models.
   - If the device transfers a file as ftp/tftp client, one of the following settings should be configured in the **File Transfer Server** tab or the FTP/TFTP Server Setting dialog box.
     - Set the file transfer server to the **Inside Server**, and set IP address of Network Manager that can access from the managed devices, in the **IP for Device**.
     - Set the file transfer server in the **Outside Server**.
   - If the device transfers a file as ftp/tftp server, the setting of file transfer server is not required.

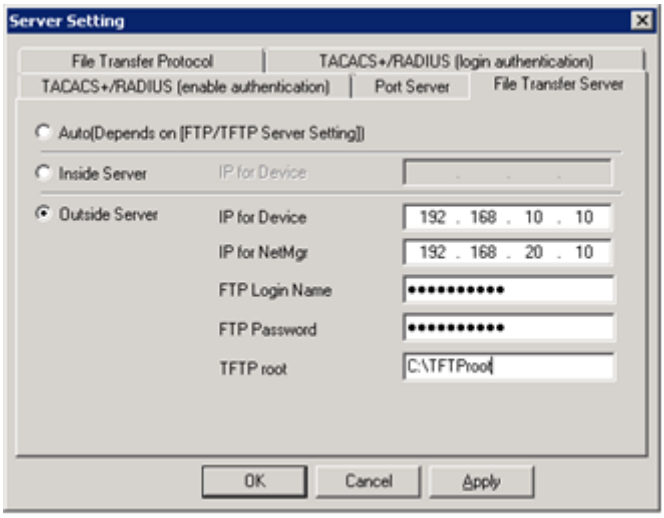
   For behaviors in transfering a file of device, refer to "8.1.2 Supported Devices in Resource Manager function (page 671)". For details of **File Transfer Server** tab, refer to "4.3.5.5 **File Transfer Server** tab (page 200)". For details of setting in the FTP/TFTP Server Setting dialog box, refer to "4.20.1 Registering an FTP or TFTP server (page 400)".

4.3.5.5 File Transfer Server tab

Specify the file transfer server to be used for configuration file and software collection and delivery.

Tip

1. The following precautions are necessary when using a TFTP server with built-in Windows RIS:
   - TFTP servers with built-in Windows RIS on external PCs cannot be used.
   - Specify the TFTP root, rather than an IP address, when specifying the login settings.
   - Make the TFTP server settings overwritable.
2. For the model using FTP/TFTP server of the device in transfering a file, the **File Transfer Server** tab is not disapleyd. For the list of models using FTP/TFTP server of the device in transfering a file, refer to "8.1.2 Supported Devices in Resource Manager function (page 671)".



- **Auto (Depends on [FTP/TFTP Server Setting])**

  The file transfer server is determined based on the information set in the "4.20.1 Registering an FTP or TFTP server (page 400)". This is the default action.

- **Inside Server**

  The file transfer server prepared by Network Manager will always be used. If, during processing, the machine that Network Manager operates is already being operated by another file transfer server, an error will arise in the process.

- **IP for Device**

  If the IP address of the outside file transfer server when sent from Network Manager is different from the IP address when sent from a managed device (for example, if the outside file transfer server belongs to multiple subnets), the file transfer server IP address sent from the managed-device side is set. The range is: 1.0.0.0 - 223.255.255.255.

- **Outside Server**

  An outside file transfer server will always be used.

  Including when using another file transfer server prepared on the same server as Network Manager.

  - **IP for Device**

    If the IP address of the outside file transfer server when sent from Network Manager is different from the IP address when sent from a managed device (for example, if the outside file transfer server belongs to multiple subnets), the file transfer server IP address sent from the managed-device side is set. The range is: 1.0.0.0 - 223.255.255.255.

  - **IP for NetMgr**

    Sets the IP address of the outside file transfer server sent from Network Manager. This setting must be made if using an outside FTP server. The range is:1.0.0.0 - 223.255.255.255.

    If you are using an outside TFTP server and it resides on the same server as Network Manager, set the **TFTP root**.

  - **FTP Login Name**

    Sets the login name for the outside FTP server.This setting must be made if using an outside FTP server. The user name must be no longer than 63 single-byte characters.

  - **FTP Password**

    Sets the login password for the outside FTP server. The user name must be no longer than 63 single-byte characters.

  - **TFTP root**

    Specify the TFTP root path when using a TFTP server that is on the same server as Network Manager. The path must be no longer than 255 characters. If this option is set, the **IP for NetMgr** is ignored.

Tip

1. If registration is completed without specifying anything in the **FTP Login Name** or **FTP Password**, the setting is for no password. In addition, eight asterisks will be displayed in the password box for the device that was configured. This is a preventative measure to avoid calculation of the number of password characters.

4.4 Managing the Advanced Functions License

To use the functions included in the advanced functions license, you must first assign an advanced functions license to a device. For the advanced functions licenses, refer to "1.2 Network Manager Licenses (page 12)".

The following two methods can be used to assign an advanced functions license to devices.

- Manual register

Assign advanced functions license information in the NetMgr License Manager dialog box. For details, refer to "4.4.1 Manually registering advanced functions licenses (page 202)".

- Batch register

  Automatically assign advanced functions licenses using a configuration information file. For details, refer to "4.6 Batch Registering or Deleting Configuration Information (page 206)".

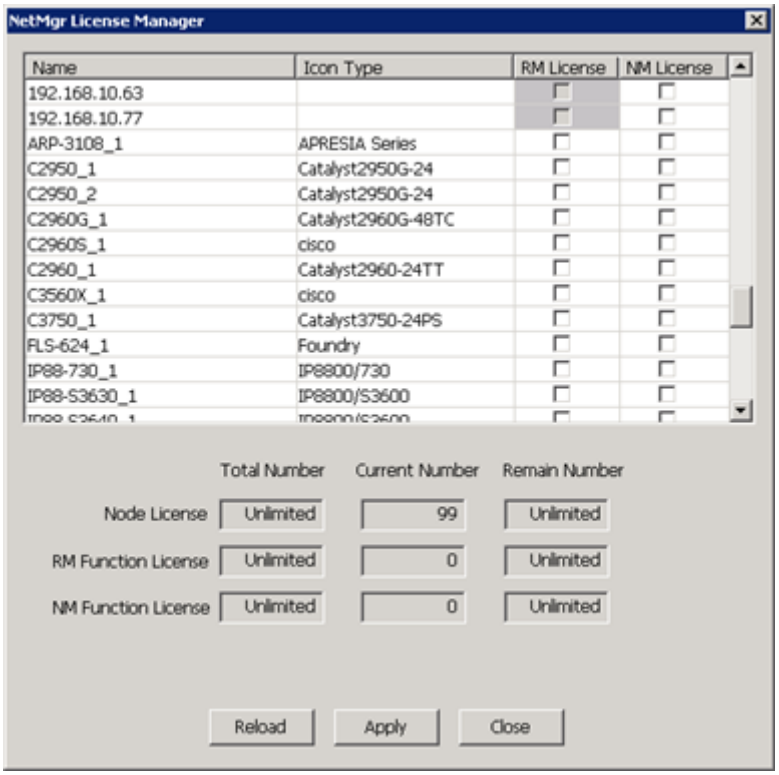
4.4.1 Manually registering advanced functions licenses

You must first change to the "configuration mode (page 27)".

This operation is available to users belonging to a group that has configuration authority. The license management authority is not needed.

1. Open the "4.4.1.1 NetMgr License Manager dialog box (page 202)".

   Right-click the **NetworkView** icon or the **NetworkManagement** icon, or the map icon. Select **NetMgr License Management** menu.



2. To select or deselect a device to which you want to assign a license, double-click the check box field for the device.

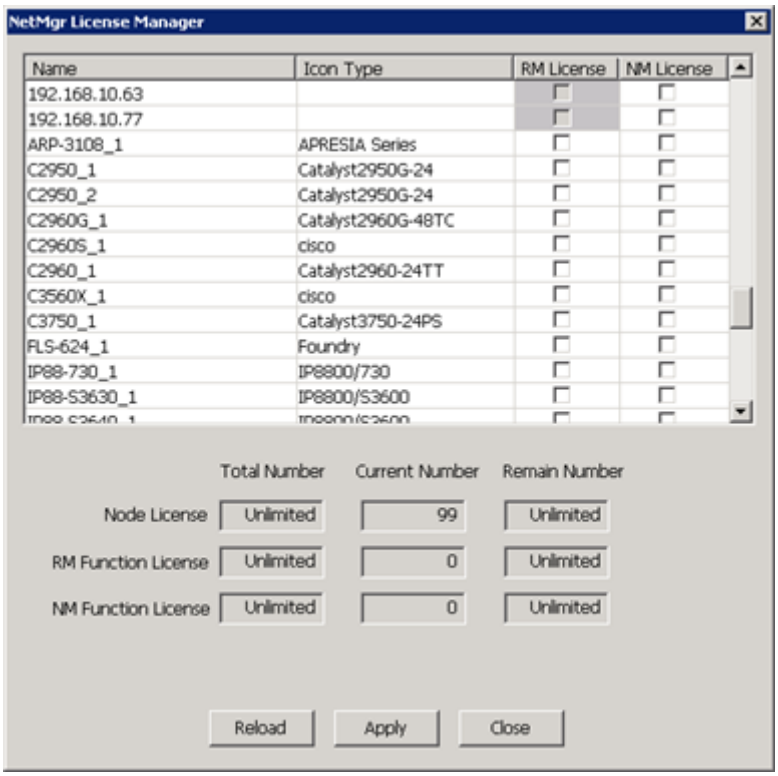
   The device can also be selected or deselected through the right-click menu.

3. Click **Apply** button.

4.4.1.1 NetMgr License Manager dialog box

Assigns or cancels an advanced functions license for devices.

For the outline of the advanced functions license, refer to "1.2 Network Manager Licenses (page 12)".



- **Name**

  Displays the names of devices registered in Network Manager.

- **Icon Type**

  Displays the device type.

- **RM License**

  Assigns or cancels an RM license (Resource Manager advanced functions license). An RM license can be assigned if one has been purchased.

  Selected: A license has been assigned.

  Not selected: A license has not been assigned.

  Not available: An unsupported device (a license cannot be assigned).

- **NM License**

  Assigns or cancels an NM license (the license for displaying panels). Five of these licenses can be assigned if you only have a basic license.

- **Total Number**

  Displays the number of licenses that have been purchased. The number of licenses assigned cannot exceed this number.

- **Current Number**

  Displays the number of licenses currently assigned to devices.

- **Remain Number**

  Displays the number of purchased licenses that have not yet been used.

  There is a relation: Remain Number = Total Number - Current Number.

- **Reload** button

Loads the latest license status from the manager machine. The **Reload** button is used to load the latest number of licenses to the monitoring terminal after registering or canceling a license key, without having to reboot the manager machine.

The **Reload** button is also used after changing the OS type to reflect the new OS type in the NetMgr License Manager dialog box.

- **Apply** button

  Applies the settings in Network Manager.

- **Close** button

  Closes the dialog box.

4.5 Registering Device-Specific Tools

4.5.1 Registering applications launched from icons

You can launch an application directly from the icon menu by setting up the application path in the icon properties.

Caution

1. There is one application path per the manager. For this reason, if you are accessing a single manager from multiple monitoring terminals, you will not be able to register different application paths for each monitoring terminal.
2. If the user operting Network Manager (the logged in user of OS) has no execution privilege for the specified application, the application can not be executed.
3. This function dose not support behaviors or errors of the application after launching the application.

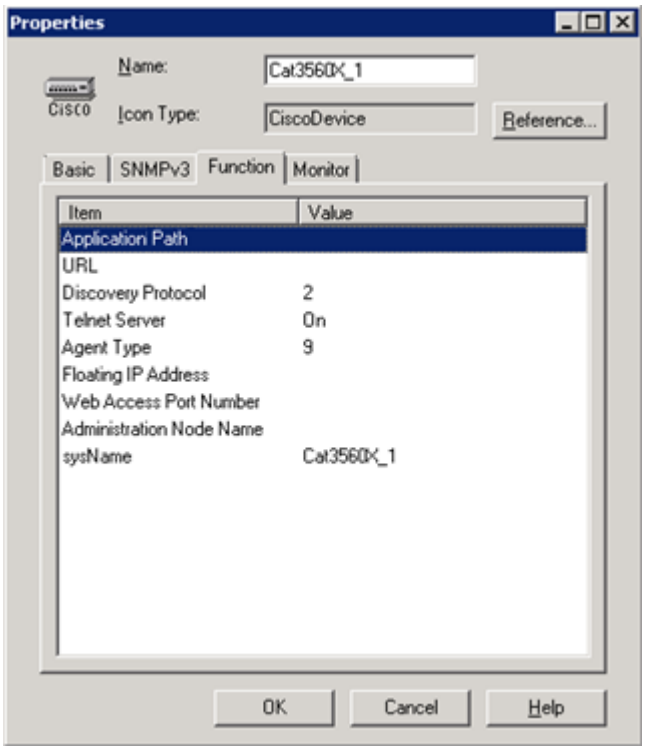
To launch an application, the application must be installed at the place specified by the application path on the monitoring terminal where this operation is performed.

You must first change to the "configuration mode (page 27)".

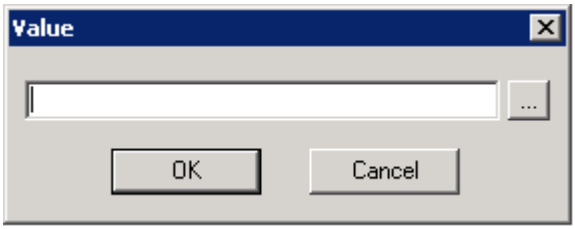
1. Open the Properties dialog box.

   Right-click the icon and select **Property** menu.

2. Click the **Function** tab.



3. Double-click the **Application Path** row to open the Value dialog box.



Perform one of the following methods to specify an application.

- Click  button to display the Open dialog box. You can select the program that you want to launch.

  Tip

  The Open dialog box displays *<On the monitoring terminal, %installfolder%>*`\Svc\bin`.

- Specify the full application path. You can enter up to 4,096 characters.

4. Click **OK** button.

4.5.2 Registering web URLs launched from icons

You can launch a web browser directly from the icon menu by setting up the URL in the icon properties. Network devices can be managed more easily by setting up URLs in device icons in advance. For example, you can set up the URL for the device management window, which can be browsed from a web browser.

⚠ Caution

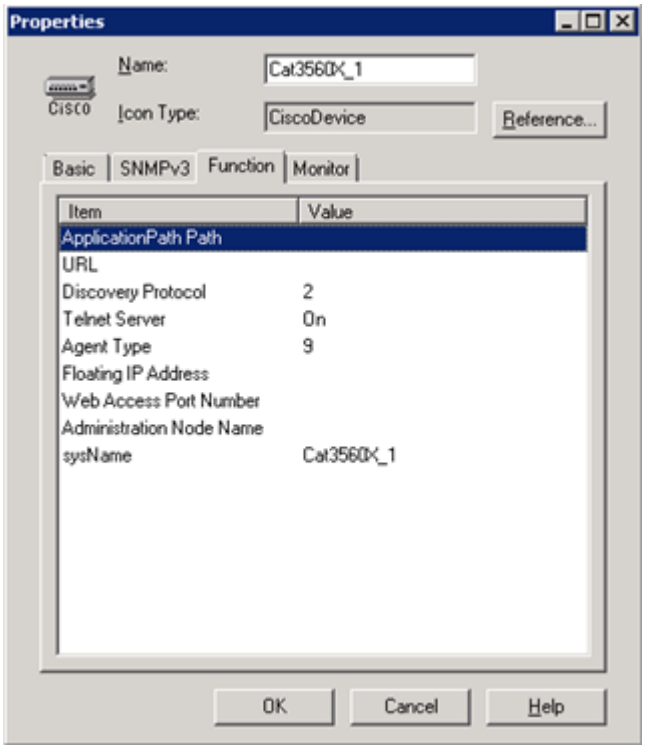
There is one URL per manager. For this reason, if you are accessing a single manager from multiple monitoring terminals, you will not be able to register different URLs for each monitoring terminal.

You must first change to the "configuration mode (page 27)".

1. Open the Properties dialog box.

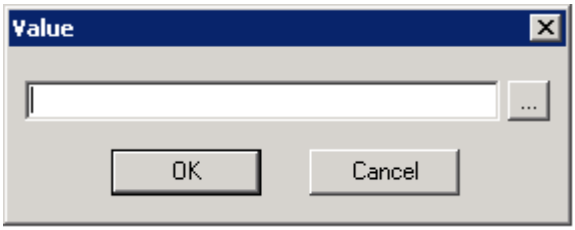
   Right-click the icon and select **Property** menu.

2. Click the **Function** tab.



3. Double-click the **URL** row to open the Value dialog box.

   Specify the URL such as http://, ftp://, and c:\. You can enter up to 2083 characters.



4. Click **OK** button.

4.6 Batch Registering or Deleting Configuration Information

Batch register device and map information by importing the information from an external file. Batch delete devices already registered in Network Manager, or batch update registration information by listing in an external file and importing the file.

This function is designed for use in cases where there are many devices to register or delete, or in preliminary test environments where managed devices are not connected to a network. This function can also reduce the number of GUI operations required to create network configuration maps.

Currently registered device and map information can also be exported to external files. This function operates from the monitoring terminal GUI or by running commands in Manager.

⚠ Caution

If the icon type of the node is Nexus 2000, it cannot be imported or exported.

4.6.1 Preparing the configuration information file

It is necessary to prepare files that already contain descriptions of device and map information (configuration information files) when batch registering device information. For details regarding the configuration information file format, "4.6.1.1 Configuration information file format (page 207)".

- When running an import operation from the monitoring terminal

  Store the configuration information files in a directory on the monitoring terminal. For details, refer to "4.6.2.1 Importing from the monitoring terminal (page 228)".

- When running an import operation from a command

  Store the created configuration information files in a directory on Manager. For details, refer to "4.6.2.2 Importing using the manager command (page 228)".

- When deleting devices

  It is recommended that you prevent accidental deletion of a device by exporting device information in advance and creating a configuration information file from the outputted file. The procedure for creating an import file for deleting devices is explained below.

  1. Export device information. For details, refer to "4.6.3 Exporting configuration information (page 229)".
  2. Open the file that was created in the device information export and edit the rows containing the devices that you want to delete.
     - Specify "1" in the [Delete Node] column.
     - If "1" is output in the [Regist Node], [Login Setting], [License Setting], and [Monitoring-mode Setting] columns, remove the values.

     Image before edit:

Regist Node	Delete Node	Login Setting	Regist Topology	License Setting	Monitoring-mode Setting
~1		~1		~1	~1

     Image after edit:

Regist Node	Delete Node	Login Setting	Regist Topology	License Setting	Monitoring-mode Setting
	~1				

4.6.1.1 Configuration information file format

Description Rules

The description rules of the information file is as follows:

- There is support for the following file formats:

  When importing or exporting from the monitoring terminal:

Monitoring Terminal OS	Encoding	BOM	Separator Characters	File Name Extension
Windows	OS multi-byte character encoding		Comma	.csv
	Unicode (UTF-16LE)	Yes	TAB	.txt

  When importing or exporting using the Manager command

Manager OS	Encoding	BOM	Separator Characters	File Name Extension
Windows	OS multi-byte character encoding		Comma	.csv
	Unicode (UTF-16LE)	Yes	TAB	.txt
Linux	UTF-8	No	TAB	.txt

- Lines beginning with the "#" symbol are treated as comment lines.

  Example:

```
#,,,1,,1,1,1,,,OSID43
```

- Write the item name in the first line (excluding comment lines).
- Unicode surrogate pair characters cannot be specified in data.
- One line represents one device, one map or one connection line.
- If the information of the same map, device, and connection line are described in multiple rows, the latter row is valid.
- When registering both map and device information in one file, device setting for a map must be specified after the map registration.
- When registering both device and topology information in one file, topology settings for a device must be specified after the device registration.
- If you are registering and deleting using the same file, the deletion process will be performed first, regardless of the order in the file.
- Solution for auto correction of data by the editor

  Some tools used to verify an export file or create an import file have an automatic correction function and some output values (input values) display (input) as a different value. In this fix, a tilde (~) is added to the beginning of each item in a file to prevent auto correction of the data. The following shows examples.

  Example:

  1. The [Source Port Name] item "1/1" is sometimes "January 1". When a tilde (~) is added to make it "~1/1", it is not corrected.
  2. The [SW Version] item "02.0" is sometimes "2". When a tilde (~) is added to make it "~02.0" it is not correct.

The behavior for adding a tilde (~) is as follows:

When adding "#Format: [~OriginalItem]" to the first line

- Ignore the tilde (~) at the beginning of the item, and remaining characters are recognized as data.
- If the beginning of the item is not tilde (~), entire item is recognized as data.

When "#Format: [~OriginalItem]" is not added to the first line

- The entire item is recognized as data.

Tip

How to create a file in Windows for importing to Linux Manager

When a command on Linux Manager to import a file created in Windows, convert the encoding because the file encoding and line breaks vary depending on the OS.

Convert the encoding using the file conversion command (nvpfileconv); included in the Monitoring Terminal function. For information about code conversion command, refer to "9.13 File Code Conversion Command (nvpfileconv) (page 739)".

Details of each row

The following shows that the detailed meaning in each row and whether omission is disabled/enabled.

When "omit" is "o", the row itself can be omitted. If the row itself is omitted, the operations will differ between new node registration and update. For new registration, values appropriate to the specified [Icon Type] column are automatically set for some items. For details, refer to "Description setting" of each item. In the case of update, the current settings are not changed.

No.	Item name	Description setting	Omit
1	Regist Map	Specifies whether to register map during the import process. Enter *"1"* to register map information. Leave blank or enter *"0"* to not register the map. Entering *"1"* enables following columns:[Icon Type], [Map Name], and from [Map Path] to [Map URL]. Cannot specify simultaneously [Regist Map] and [Regist Node] columns in the same row.	o
2	Regist Node	Specifies whether to register node during the import process. Enter *"1"* to register node information. Leave blank or enter *"0"* to not register the node. Entering *"1"* enables the columns from [IP Address] to [URL]. Cannot specify simultaneously [Regist Map] and [Regist Node] columns in the same row.	
3	Delete Node	Specifies whether to delete node information during the import process. Enter *"1"* to delete node. Leave blank or enter *"0"* to not delete node. Entering *"1"* enables [Device Name] and [Map Name] columns. Cannot specify simultaneously another import columns such as [Regist Map], [Regist Node], [Login Setting], [Regist Topology], [License Setting], and [Monitoring-mode Setting], in the same row.	o
4	Login Setting	Specifies whether to register telnet login information for a device during the import process. Enter *"1"* to register login information. Leave blank or enter *"0"* to not register. Entering *"1"* enables [Device Name] and from [Password 1] to [File Transfer Server (TFTP root)] columns.	

No.	Item name	Description setting	Omit
5	Regist Topology	Specifies whether to register device topology (connection line) information during the import process. Enter *"1"* to register topology information. Leave blank or enter *"0"* to not register. Entering *"1"* enables [Map Name] and from [Connection-Line] to [Duplex Mode] columns.	
6	License Setting	Specifies whether to register license information. Enter *"1"* to register license information. Leave blank or enter *"0"* to not register. Entering *"1"* enables [RM License], [NM License] and [Device Name] columns.	
7	Monitoring-mode Setting	Specifies whether to conduct monitoring mode registration. Enter *"1"* to register monitoring mode. Leave blank or enter *"0"* to not register. Entering *"1"* enables [Monitoring-mode] and [Device Name] columns.	
8	RM License	The following settings are used to specify the status of the Resource Manager advanced functions license. ***1*** **:** enables license ***0*** **:** disables license ***Blank*** **:** not change license When newly registering device, blank has the same effect as *"0"*. Enabled only when [License Setting] column is *"1"*.	
9	NM License	The following settings are used to specify the status of the Node Manager advanced functions license. ***1*** **:** enables license ***0*** **:** disables license ***Blank*** **:** not change license When newly registering device, blank has the same effect as *"0"*. Enabled only when [License Setting] column is *"1"*.	
10	Monitoring-mode	The following settings are used to set monitoring for devices. ***1*** **:** conducts device monitoring ***0*** **:** stops device monitoring ***Blank*** **:** not change monitoring status When newly registering device, blank has the same effect as *"0"*. Enabled only when [Monitoring-mode Setting] column is *"1"*.	
11	IP Address	Specifies the IP address (in the x.x.x.x format, where x represents integers comprising the IP address) used for monitoring a device. Enabled only when [Regist Node] column is *"1"*.	
12	Device Name	Specifies a device name using up to 63 characters. Valid characters include alphanumeric characters, multi-byte characters, hyphen (-),	

No.	Item name	Description setting	Omit
		underscore (_), and dot (.). If specifying Unicode surrogate pair characters or "nul" (either uppercase or lowercase), some functions may work incorrectly. Do not use Unicode surrogate pair characters and "nul". If there is any identical device-name information subordinate to the map name specified in [Map Name] column, it will be overwritten. If identical device-name information exists outside the map specified in [Map Name] column, the icon for the preexisting device is copied to the specified map and a link to the preexisting device information is created. Required only if any one of [Regist Node] column, [Delete Node] column, [Login Setting] column, [License Setting] column, or [Monitoring-mode Setting] column is *"1"*.	
13	Icon Type	Specifies an icon type name that is registered with Network Manager appropriate to the device type. When [Regist Map] column is *"1"*, the icon types in map group can be specified. When [Regist Node] column is *"1"*, the icon types in node group can be specified. For the list of icon types, refer to "Appendix B. Icons (page 785)".	
14	Alias	Specifies an alias using up to 255 displayable characters. Enabled only when [Regist Node] column is *"1"*.	o
15	IPv6 Address	Specifies the IPv6 address for monitoring devices, using the format : "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx" (where x represents hexadecimal numbers that make up the IPv6 address). Only global unicast addresses are valid. To see the range for global unicast addresses, refer to "7.5.1 Using the IPv6 function (page 662)". Enabled only when [Regist Node] column is *"1"*.	o
16	SNMP Version	SNMP version is specified using the following settings. ***1*** **:** version 1 ***2C*** **:** version 2C ("C" is upper case) ***3*** **:** version 3 Enabled only when [Regist Node] column is *1*.	o
17	SNMP Community (get)	Specifies SNMP community name (get) using up to 255 characters. Enabled only when [Regist Node] column is *"1"*.	
18	SNMP Community (set)	Specifies SNMP community name (set) using up to 255 characters. Enabled only when [Regist Node] column is *"1"*.	o
19	SNMP User Name	Specifies a user name for SNMPv3 communication using up to 32 characters. You can use printable ASCII characters, in the range of 0x20 (space) to 0x7e (tilde (~)). It must be specified when the SNMP version property is set to 3. To receive SNMPv3-trap, this item should be set. Enabled only when [Regist Node] column is *"1"*.	o
20	SNMP EngineID	Specifies a unique ID of 32 octets or less, for identifying SNMPv3 agents. Specify in hexadecimal notation using any of the formats below. Valid characters are single-byte 0-9, single-byte a-f and x (either	o

No.	Item name	Description setting	Omit
		upper or lower case), single-byte colon (:), single-byte space. Single-byte alphabetical character of x can be specified at only "0x" of the beginning. For 0-f, specify as two hex digits (00-0f). • Format 1 Two hex digits separated with a colon (:). Insert 0x at the be ginning. Example: 0x12:04:0F:78:90:AA • Format 2 Two hex digits separated with a colon (:). Example: 12:04:0F:78:90:AA • Format 3 Two hex digits separated with a space. Example: 12 04 0F 78 90 AA Enabled only when [Regist Node] column is *"1"*.	
21	SNMP Security Level	Specifies a security levels for SNMPv3 communication. ***NoAuth/NoPriv* :** No authentication or encryption ***Auth/NoPriv* :** Authentication, but no encryption **Auth/Priv :** Authentication and encryption Leaving blank or entering invalid value have the same meaning as NoAuth/NoPriv. Enabled only when [Regist Node] column is *"1"*.	o
22	SNMP Authentication Protocol	Specifies an authentication protocol for SNMPv3 communication. • MD5 • SHA1 It must be specified when you have specified *"Auth/NoPriv"* or *"Auth/Priv"* in the SNMP security level. If any value other than *"Auth/NoPriv"* or *"Auth/Priv"* is specified in the security level, and the value is specified in this column, the value setting is configured as the property information, however, the set value is not used for SNMPv3 communication. Enabled only when [Regist Node] column is *"1"*.	o
23	SNMP Authentication Password	Specifies an authentication password for SNMPv3 communication, using 8 to 255 characters. You can specify printable ASCII characters, in the range of 0x20 (space) to 0x7e (tilde (~)). It must be specified when you have specified *"Auth/NoPriv"* or *"Auth/Priv"* in the SNMP security level. If any value other than *"Auth/NoPriv"* or *"Auth/Priv"* is specified in the security level, and the value is specified in this column, the value setting is configured as the property information, however, the set value is not used for SNMPv3 communication. Enabled only when [Regist Node] column is *"1"*.	o
24	SNMP Privacy Protocol	Specifies the following to encrypted protocol to be used for SNMPv3 communication. • DES It must be specified when you have specified *"Auth/Priv"* in the SNMP security level. If any value other than *"Auth/Priv"* is specified in the security level, and the value is specified in this column, the value	o

No.	Item name	Description setting	Omit
		setting is configured as the property information, however, the set value is not used for SNMPv3 communication. Enabled only when [Regist Node] column is *"1"*.	
25	SNMP Privacy Password	Specifies a privacy password for SNMPv3 communication, using 8 to 255 characters. You can specify printable ASCII characters, in the range of 0x20 (space) to 0x7e (tilde (~)). It must be specified when you have specified *"Auth/Priv"* in the SNMP security level. If any value other than *"Auth/Priv"* is specified in the security level, and the value is specified in this column, the value setting is configured as the property information, however, the set value is not used for SNMPv3 communication. Enabled only when [Regist Node] column is *"1"*.	o
26	SNMP Severity of Invalid EngineID	Specifies the alert severity to be published if the EngineID in a trap does not match the EngineID stored in Network Manager, when SNMPv3 trap is being received. • Warning • Major Fault • Minor Fault • Critical State • Blank If you specify blank, an alert will not be published. For the relation between the specified values and alert severities, refer to "4.9.2.1 About severity extension (page 237)" . Enabled only when [Regist Node] column is *"1"*.	o
27	Hardware Type	Specifies the device hardware type corresponding to [Icon Type] column using a character string of up to 255 characters. If you omit the row itself or specify a blank when newly registering a device, a hardware type appropriate to the icon type is automatically selected. Enabled only when [Regist Node] column is *"1"*.	o
28	Administrator	The device administrator name is specified using a character string of up to 255 characters. Enabled only when [Regist Node] column is *"1"*.	o
29	Location	The device's install location is specified using a character string of up to 255 characters. Enabled only when [Regist Node] column is *"1"*.	o
30	Map Name	Specifies the map name using up to 63 characters. Valid characters include alphanumeric characters, hyphen (-), underscore (_), and dot (.). • Registering Map Specify the map name to be registered. When registering a map, it cannot be omitted and multiple names cannot be specified. When a same map name exists in multiple records, the registration will overwrite the previous record. **When a specified map name does not exist:** create new map under the path specified in [Map Path] column. Set attribute information. **When a specified map name exists:** update attribute information for the existing map. If the map path for the existing map and [Map Path] column does not match, an error will result and registration will not be completed.	

No.	Item name	Description setting	Omit
		• Registering Node or Connection-line Specifies the map that devices identified in the [Device Name] column, and connection lines identified in the [Connection-Line] column, will be registered in. **When a map name is not specified:** nodes and connection-lines are generated subordinate to the map where the import process was launched. **When a specified map name does not exist:** a map with the specified map name is generated subordinate to the map where the import process was launched, and nodes and connection-lines subordinate to the new map are then generated. **When a specified map name exists:** nodes and connection-lines are generated subordinate to the preexisting map. • Deleting Node Specifies the map that the node of the device to be deleted is registered in. Use the same operations that were used when deleting a node icon using GUI commands. If all node icons corresponding with the devices have been deleted, all information associated with those devices is deleted. Enabled, only when [Regist Map] column, [Regist Node] column, [Delete Node] column, or [Regist Topology] column is *"1"*.	
31	SW Version	Specifies the device software version using a character string of up to 255 characters. For details, refer to "OS type and software version format (page 223)". [Software Version] must be set before the "login settings (page 189)" can be entered for device types that support RM licenses. The character string conventions for login settings are described in a later section. Enabled only when [Regist Node] column is *"1"*.	
32	OS Type	Specifies types to uniquely identify each device type. For details, refer to "OS type and software version format (page 223)". When newly registering a device, if a value of [OS Type] is omitted or incorrect value is entered, an appropriate OS type is set from an icon type. If the icon type is "cisco", since it is impossible to distinguish between "IOS" and "CatOS", it is registered as "IOS". To configure "Login Setting (page 189)", [OS Type] need to be registered in registration of device. Enabled only when [Regist Node] column is *"1"*.	
33	SysObjectID	Specifies system.sysObjectID with numbers and dots (.) in the SNMP MIB2 of the device. Specified using up to 255 characters. Enabled only when [Regist Node] column is *"1"*.	o
34	Local IP Address	Specifies the local IP address used when operating in NAT environments. This setting is used solely for displaying properties in Network Manager. Local IP address is specified in the x.x.x.x format (where x represents integers comprising the IP address). Enabled only when [Regist Node] column is *"1"*.	o
35	Default Port	Specifies the interface number used in data collection and state monitoring operations whenever the interface number is omitted. Specified using a character string of up to 4,090 characters.	o

No.	Item name	Description setting	Omit
		Enabled only when [Regist Node] column is *"1"*.	
36	Routing Information	Routing control information is specified as below. ***1* or *forwarding* :** perform IP forwarding ***2* or not *forwarding* :** do not perform IP forwarding ***Blank* :** not change current setting Enabled only when [Regist Node] column is *"1"*.	o
37	Memo	Memo information is entered using up to 255 characters (without linefeeds). Enabled only when [Regist Node] column is *"1"*.	o
38	Device Front Panel	Specifies the type of device front panel. Specified using a character string of up to 255 characters. If you omit the row itself when newly registering a device, select an appropriate **panel type** from **Icon Type**. If you specify a blank when newly registering a device, enter "NDEVICE". When exporting, if nothing is specified in this property, "NDEVICE" is output. "NDEVICE" indicates the same meaning that it is not set. Enabled only when [Regist Node] column is *"1"*.	o
39	Application Path	Specifies an application path to be launched from the node icons on the monitoring terminal, using up to 4,096 characters. Specify either an absolute path or a relative path. When specifying a relative path, the path for the current directory is: `<On the monitoring terminal, %installfolder%>\Svc\bin` There is one application path per one manager function. if you are accessing a single manager from multiple monitoring terminals, you will not be able to register an application path for each monitoring terminal. Enabled only when [Regist Node] column is *"1"*.	o
40	URL	Specifies URL of a web site to be launched from the node icons on the monitoring terminal, using up to 2,083 characters. There is one URL per one manager function. For this reason, if you are accessing a single manager from multiple monitoring terminals, you will not be able to register an URL for each monitoring terminal. Enabled only when [Regist Node] column is *"1"*.	o
41	Group Name	Specifies group names that the node belongs to. If the node belongs to multiple groups, specifies groups using single-byte colon (:) delimiter. The maximum length of group name is up to 63 characters. The maximum length including each group name and colon is up to 1000 characters. Valid characters include alphanumeric characters, multi-byte characters, hyphens (-), underscores (_), dots (.). 1. When [Group Name] column is omitted: not change current setting. 2. When a group name is not specified: clear all group settings of the node. 3. When a specified group name does not exist: create a group and make the node belong to the group. 4. When a specified group name exist:	o

No.	Item name	Description setting	Omit
		make the node belong to a group. 5. When a group to witch the node belongs is not specified: clear the group that was not specified. Enabled only when [Regist Node] column is *1*.	
42	Discovery Protocol	Specifies the type of the discovery protocol operating on the device. For details on the discovery protocol values corresponding to the device types, refer to "4.2.3.1 Discovery Protocol (page 148)". If you omit the row itself or specify a blank when newly registering or overwriting a device, enter "100", which indicates that it is not set. Enabled only when [Regist Node] column is *1*.	o
43	Administration Node Name	Specifies the name of the parent node, which manages this node, using 63 characters or less. In Cisco ASA 5500 multiple context mode, for example, the parent node would be the Admin context node of the general context node. Enabled only when [Regist Node] column is *1*.	o
44	sysName	Specifies sysName, which is the administrative name set on the device, using 255 characters or less. Enabled only when [Regist Node] column is *1*.	o
45	SNMP Character Code	Specifies the character code used to interpret non-ASCII characters contained in SNMP Get/Set or SNMP trap/inform data from the following. ***Unicode (UTF-8)*** **:** Non-ASCII characters are interpreted in UTF-8. ***Blank*** **:** Non-ASCII characters are not interpreted in any character encoding. Enabled only when [Regist Node] column is *1*.	o
46	Login Mode	Specifies the method to login to the device. Select below. ***0*** **:** use Telnet ***1*** **:** use SSH ***Blank*** **:** use Telnet (Interpreted as 0) Enabled only when [Login Setting] column is *"1"*.	o
47	Password 1	Password for telnet login is specified using up to 63 characters. If nothing is entered, there will be no password. Enabled only when [Lognin Setting] column is *"1"*, and [Login Mode] column is *"0"*.	
48	Password 2	Password for telnet login is specified using up to 63 characters. If nothing is entered, there will be no password. Enabled only when [Lognin Setting] column is *"1"*, and [Login Mode] column is *"0"*.	
49	Password 3	Password for telnet login is specified using up to 63 characters. If nothing is entered, there will be no password. This password will be ignored in the case of devices (models) that do not support a third password.	

No.	Item name	Description setting	Omit
		Enabled only when [Lognin Setting] column is *"1"*, and [Login Mode] column is *"0"*.	
50	Password 4	Password for telnet login is specified using up to 63 characters. If nothing is entered, there will be no password. This password will be ignored in the case of devices (models) that do not support a fourth password. Enabled only when [Lognin Setting] column is *"1"*, and [Login Mode] column is *"0"*.	o
51	Password 5	Password for telnet login is specified using up to 63 characters. If nothing is entered, there will be no password. This password will be ignored in the case of devices (models) that do not support a fifth password. Enabled only when [Lognin Setting] column is *"1"*, and [Login Mode] column is *"0"*.	o
52	Check Host Public Key	Specifies whether confirming the public host key or not for ssh login. ***0*** **:** do not confirm the public host key ***1*** **:** confirm the public host key ***Blank*** **:** confirm the public host key Enabled only when [Lognin Setting] column and [Login Mode] column are *"1"*.	o
53	SSH Login Name	Login name for ssh login is specified using up to 63 characters. If nothing is entered, there will be no login name. Enabled only when [Lognin Setting] column and [Login Mode] column are *"1"*.	o
54	SSH Password 1	Password for ssh login is specified using up to 63 characters. If nothing is entered, there will be no password. Enabled only when [Lognin Setting] column and [Login Mode] column are *"1"*.	o
55	SSH Password 2	Password for ssh login is specified using up to 63 characters. If nothing is entered, there will be no password. This password will be ignored in the case of devices (models) that do not support a second password. Enabled only when [Lognin Setting] column and [Login Mode] column are *"1"*.	o
56	SSH Password 3	Password for ssh login is specified using up to 63 characters. If nothing is entered, there will be no password. This password will be ignored in the case of devices (models) that do not support a third password. Enabled only when [Lognin Setting] column and [Login Mode] column are *"1"*.	o
57	SSH Password 4	Password for ssh login is specified using up to 63 characters. If nothing is entered, there will be no password. This password will be ignored in the case of devices (models) that do not support a fourth password. Enabled only when [Lognin Setting] column and [Login Mode] column are *"1"*.	o
58	File Transfer Protocol	The types of file transfer protocol used in resource management are specified using the following settings. ***0*** **:**	o

No.	Item name	Description setting	Omit
		detect automatically ***1*** **:** use TFTP ***2*** **:** use FTP ***Blank*** **:** detect automatically (interpreted as 0) If specified, file transfer protocol settings will be ignored in the case of devices (models) that do not support them. Enabled only when [Login Setting] column is *"1"*.	
59	TACACS+/RADIUS Login	The following settings are used to select whether to coordinate logins to network devices with TACACS+ and RADIUS. ***0*** **:** disable coordinating ***3*** **:** enable coordinating ***Blank*** **:** detect coordinating (interpreted as 0) If specified, TACACS+/RADIUS login settings will be ignored in the case of devices (models) that no not support them. Enabled only when [Login Setting] column is *"1"*.	o
60	TACACS+/RADIUS Login (user ID)	User name is specified using up to 63 characters. Enabled only when [Lognin Setting] column is *"1"* and [TACACS+/RADIUS Login] column is *"3"*.	o
61	TACACS+/RADIUS Login (user password)	Password is specified using up to 63 characters. If nothing is entered, there will be no password. Enabled only when [Lognin Setting] column is *"1"* and [TACACS+/RADIUS Login] column is *"3"*.	o
62	TACACS+/RADIUS Login (user ID for local)	Local authentication user name is specified using up to 63 characters. If nothing is entered, there will be no user ID. Enabled only when [Lognin Setting] column is *"1"* and [TACACS+/RADIUS Login] column is *"3"*.	o
63	TACACS+/RADIUS Login (user password for local)	Local authentication user password is specified using up to 63 characters. If nothing is entered, there will be no password. Enabled only when [Lognin Setting] column is *"1"* and [TACACS+/RADIUS Login] column is *"3"*.	o
64	TACACS+/RADIUS_ Enable	The following settings are used to select whether to switch to the enable mode with TACACS+ and RADIUS. ***0*** **:** disable switching ***1*** **:** enable switching ***Blank*** **:** desable switching (interpreted as 0) If specified, TACACS+/RADIUS enable settings will be ignored in the case of devices (models) that do not support them. Enabled only when [Login Setting] column is *"1"*.	o

No.	Item name	Description setting	Omit
65	TACACS+/RADIUS_ Enable (user ID)	User name for enable authentication is specified using up to 63 characters. Enabled only when [Lognin Setting] column and [TACACS+/RADIUS Enable] column are *"1"*.	o
66	TACACS+/RADIUS_ Enable (user password)	User password for enable authentication is specified using up to 63 characters. If nothing is entered, there will be no password. Enabled only when [Lognin Setting] column and [TACACS+/RADIUS Enable] column are *"1"*.	o
67	TACACS+/RADIUS_ Enable (user ID for local)	Local authentication user name for enable authentication is specified using up to 63 characters. If nothing is entered, there will be no password. Enabled only when [Lognin Setting] column and [TACACS+/RADIUS Enable] column are *"1"*.	o
68	TACACS+/RADIUS_ Enable (user password for local)	Local authentication password for enable authentication is specified using up to 63 characters. If nothing is entered, there will be no password. Enabled only when [Lognin Setting] column and [TACACS+/RADIUS Enable] column are *"1"*.	o
69	PortServer Setting	Port server usage states are specified as below. ***0*** **:** not use port server ***1*** **:** use port server, if attempt fails, failed to connect. ***3*** **:** use port server, if attempt fails, use device directly. ***Blank*** **:** not use server (interpreted as 0) If specified, these port server settings will be ignored in the case of devices (models) that do not support them. Enabled only when [Login Setting] column is *"1"*.	o
70	PortServer (IP)	Port server IP address is specified in the x.x.x.x format (where x represents integers comprising the IP address) with a maximum of 15 characters. When [Login Setting] column is *"1"* and [PortServer Setting] column is *"1"* or *"3"*, this item is required. Enabled only when [Login Setting] column is *"1"*.	o
71	PortServer (port)	Port number specifies the TCP/IP port number for the port server.Port number is specified using a value between 1 and 65535. When [Login Setting] column is *"1"* and [PortServer Setting] column is *"1"* or *"3"*, this item is required.	o
72	PortServer (sending message)	The message to send to the port server is specified using up to 511 characters. If you want to insert a linefeed, insert %0d%0a (all single-byte characters, 0 is a numeral). Enabled only when [Login Setting] column is *"1"* and [PortServer Setting] column is *"1"* or *"3"*.	o
73	File Transfer Server Setting	The following settings are used to specify the location of file transfer server. ***0*** **:** detect automatically	o

No.	Item name	Description setting	Omit
		1 **:** use Network Manager internal ***2*** **:** use external server ***Blank*** **:** interpreted as 0 File transfer server settings will be ignored in the case of devices (models) that do not support them. Enabled only when [Login Setting] column is *"1"*.	
74	File Transfer Server (IP for Device)	File transfer server IP address is specified (up to 15 characters) in the x.x.x.x format. When [Login Setting] column is *"1"* and [File Transfer Server Setting] column is *"1"* or *"2"*, this item is required,	o
75	File Transfer Server (IP for NetMgr)	File transfer server IP address referenced by Network Manager is specified (up to 15 characters) in the x.x.x.x format. When [Login Setting] column is *"1"* and [File Transfer Server Setting] column is *"2"*, this item is required.	o
76	File Transfer Server (FTP Login Name)	User names logging in to a file transfer server referenced by Network Manager are specified using up to 63 characters. Enabled only when [Lognin setting] is *"1"* and [File Transfer Server Setting] column is *"2"*.	o
77	File Transfer Server (FTP Password)	Passwords used for logging in to a file transfer server referenced by Network Manager are specified using up to 63 characters. If nothing is entered, there will be no password. Enabled only when [Lognin setting] is *"1"* and [File Transfer Server Setting] column is *"2"*.	o
78	File Transfer Server (TFTP root)	If a TFTP server provided on the same server as Network Manager will be used, the TFTP route path is specified using upto 255 bytes.Path name confirmation is not used, so it is important to specify the correct path name. Enabled only when [Lognin setting] is *"1"* and [File Transfer Server Setting] column is *"2"*.	o
79	Connection-Line	Names of connection-lines used to connect devices within the same map region are specified using up to 63 characters. In cases where a connection-line matching the device name and interface name of the connection source node and destination node already exists, the preexisting information is updated. Required when [Regist Topology] column is *"1"*.	
80	Source Device	Connection-line source node device name is specified using up to 63 characters. Specify component type as either a node or media component. The icon for the device must already be registered on the target map. Required when [Regist Topology] column is *"1"*.	
81	Source IP	Connection-line source node IP address is specified in the x.x.x.x format, up to 15 characters. Enabled only when [Regist Topology] column is *"1"*.	o
82	Source Port Name	Connection-line source node port name is specified using up to 255 characters. Enabled only when [Regist Topology] column is *"1"*.	o

No.	Item name	Description setting	Omit
83	Source Port ID	Specifies the port ID (ifIndex) for the connection-line's source-node port. Specified as a number from 1 to 2147483647. Enabled only when [Regist Topology] column is *"1"*.	o
84	Destination Device	Connection-line destination node device name is specified using up to 63 characters. Specify component type as either a node or media component. Required when [Regist Topology] column is *"1"*.	
85	Destination IP Address	Connection-line destination node IP address is specified in the x.x.x.x format, up to 15 characters. Enabled only when [Regist Topology] column is *"1"*.	o
86	Destination Port Name	Connection-line destination node port name is specified using up to 255 characters. Enabled only when [Regist Topology] column is *"1"*.	o
87	Destination Port ID	Specifies the port ID (ifIndex) of the connection-line's destination-node port.Specified as a number from 1 to 2147483647. Enabled only when [Regist Topology] column is *"1"*.	o
88	Link Speed	Connection-line link speeds are specified in Mbps. Specified as a number from 1 to 2147483647. Enabled only when [Regist Topology] column is *"1"*.	o
89	Duplex Mode	The connection-line full duplex mode is specified using the following settings. ***2*** **:** use half-duplex mode ***3*** **:** use full-duplex mode ***Blank*** **:** use full-duplex-mode (interpreted as 3) Enabled only when [Regist Topology] column is *"1"*.	o
90	Map Path	Specifies the registration path of the map specified in [Map Name] column. Specify the registration path using the path from [NetworkManagement] root icon with slash separators. All maps contained in paths need to exist when registering. (It is possible to include a map registered in the upper record in a map path of the lower record.) The maximum length is 1,023 characters. Valid characters include alphanumeric characters, multi-byte characters, hyphens (-), underscores (_), dots (.), and slashes (/). Specify a slash (/) at the beginning and end of the value. Do not include the map name that was specified in [Map Name] column, in the value. An example is shown below. Example: To create the maps below, Specify [Map Name] and [Map Path] as shown below. `[NetworkManagement]` `  |------ MapA` `  |------ MapB` `  |------ MapB-1` `[Map Name] [Map Path]` ` MapA /NetworkManagement/`	o

No.	Item name	Description setting	Omit
		MapB /NetworkManagement/ MapB-1 /NetworkManagement/MapB/ This item can be omitted. If it is omitted, perform the operations as below. • When map in [Map Name] does not exist The map specified in [Map Name] column are registered subordinate to the map where the import process was launched. • When map in [Map Name] already exists Update attribute information for the existing map, regardless of the map where the import process was launched. Enabled only when [Regist Map] column is *"1"*.	
91	Map Alias	Specifies a map alias name using up to 255 displayable characters. Enabled only when [Regist Map] column is *"1"*.	o
92	Network Address	Specifies the IPv4 network address of the map, using the "x.x.x.x" format (where x represents integers that make up the IP address). Enabled only when [Regist Map] column is *"1"*.	o
93	Network Mask	Specifies the IPv4 network mask of the map, using the "x.x.x.x" format (where x represents integers that make up the IP address). Enabled only when [Regist Map] column is *"1"*.	o
94	IPv6 Network Address	Specifies the IPv6 network address of the map, using the format: "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx" (where x represents hexadecimal numbers that make up the IPv6 address). Only global unicast addresses are valid. To see the range for global unicast addresses, refer to "7.5.1 Using the IPv6 function (page 662)". Enabled only when [Regist Map] column is *"1"*.	o
95	IPv6 Prefix Length	Specifies the length of the IPv6 prefix for the map component. Use a single-byte number from 0 to 128. Enabled only when [Regist Map] column is *"1"*.	o
96	Map Administrator	Specifies a map administrator name using up to 255 characters. Enabled only when [Regist Map] column is *"1"*.	o
97	Map Location	Specifies a location of the map using up to 255 characters. Enabled only when [Regist Map] column is *"1"*.	o
98	Map Application Path	Specifies an application path to be launched from the map icons on the monitoring terminal, using up to 4,096 characters. Specify either an absolute path or a relative path. When specifying a relative path, the path for the current directory is: *<On the monitoring terminal, %installfolder%>*\Svc\bin There is one application path per one manager function. For this reason, if you are accessing a single manager from multiple monitoring terminals, you will not be able to register an application path for each monitoring terminal. Enabled only when [Regist Map] column is *"1"*.	o
99	Map URL	Specifies URL of a web site to be launched from the map icons on the monitoring terminal, using up to 2,083 characters. There is one URL per one manager function.For this reason, if you are accessing a single manager from multiple monitoring terminals, you will not be able to register an URL for each monitoring terminal.	o

No.	Item name	Description setting	Omit
		Enabled only when [Regist Map] column is *"1"*.	

Save the import sample file and the file that explains the file format in the following directory:

<On the monitoring terminal, %installfolder%>\Svc\sg\NvPRO\NvPROCsvIOConfig\Sample\

Sample files

Files with a csv extension have standard OS multi-byte character encoding and comma separation. Files with a txt extension have Unicode (UTF-16) encoding and TAB separation.

Imported Contents	File Name
Register map information, device information, and topology information	Sample_AllFunctionImport.csv Sample_AllFunctionImport.txt
Register maps	Sample_RegisterMap.csv Sample_RegisterMap.txt
Register devices	Sample_RegisterComp.csv Sample_RegisterComp.txt
Configure login settings for devices	Sample_LoginSetting.csv Sample_LoginSetting.txt
Simultaneously register devices and configure login settings	Sample_RegisterComp_and_LoginSetting.csv Sample_RegisterComp_and_LoginSetting.txt
Set up licenses	Sample_LicenseSetting.csv Sample_LicenseSetting.txt
Set the monitoring mode	Sample_WatchModeSetting.csv Sample_WatchModeSetting.txt
Register topology information	Sample_RegisterTopology.csv Sample_RegisterTopology.txt

Format explanation file

The following file explains the import file format.

(Requires Microsoft Excel)

- ImportFileFormat.xls

OS type and software version format

The usable character strings and applicable software versions, both based on OS type, are listed below. When entering login settings, it is necessary that the SW version conditions and range already be entered as device information values.

When configuring login settings, be aware of the number of digits in the software version.

For example, to specify Version "05.0" of ServerIron, an error will occur if you enter "5".

Note that some tools used to create import files will have an automatic correction function that may save the version with a different number of digits. To stop the auto correction function from operating: Recommendation: write "#Format: [~OriginalItem]" in the first line of the file and add a tilde to the beginning of each item.

Character strings that can be specified to OS type and SW versions:

OS type	Software version		
	Sample	Requirements	Range
IP8800/S2400, S3600, S6300, S6700	10.0 build128	10.0 above	10.0 - 99.9
IP8800/SS1200	1.1.C	1.0 above	1.0 - 9.9
IP8800/S2500	3.1.A	1.0 above	1.0 - 9.9
IP8800/S8300	12.6.A	12.6 above	12.6 - 99.9
IP8800/S8600	12.7.C	12.7 above	12.7 - 99.9
QX-S	2.1.4	1.1 above	1.1 - 9.9
QX-S3400F	7.2.8	7.2 above	7.2 - 9.9
QX-S4100G	7.2.3	7.2 above	7.2 - 9.9
QX-S5200G	7.1.4	7.1 above	7.1 - 9.9
QX-S5500G	7.1.4	7.1 above	7.1 - 9.9
QX-S5900/PF5459	7.1.3	7.1 above	7.1 - 9.9
QX-S6600	7.1.3	7.1 above	7.1 - 9.9
IX1000/2000/3000	6.1.15	6.0 above	6.0 - 99.99
PF6800	V3.0.0.0 build80	V3.0 above	V3.0 - V9.9
PF5200	V2.0.0.0	V2.0 above	V2.0 - V9.9
PF5820	7.4.1.1	7.4a bove	7.4 - 99.9
WA	4.3.1	4.3.1 above	4.3.1 - 9.9.9
SIGMABLADE SwitchModule	1.0.0	1.0 above	1.0 - 9.9
SIGMABLADE SwitchModule(10G)	1.0.0	1.0 above	1.0 - 9.9
QX-R	1.2.2	1.0 above	1.0 - 9.9
UNIVERGE WL controller	No conditions		
IP8800/S	09-04-/A	09-04 above	09-04 - 09-99, 10-00 - 99-99
IP8800/R	09-04-/A	09-04 above	09-04 - 09-99, 10-00 - 99-99
IP8800/700	R7.3(ed17)	R6.0 above	R6.0 - R9.9
ES8800/1700	R7.1(ed34)	R6.0 above	R6.0 - R9.9
IP8800/620	R1.60(ed27)	R1.6 above	R1.6 - R1.9
IX5000	8.4.02	8.0 above	8.0 - 9.9, 10.0 - 99.9
IX5500	8.4.02	8.0 above	8.0 - 9.9, 10.0 - 99.9
CX	04.04.12	04.00.00 above, 06.00.00 above	04.00.00 - 04.99.99, 06.000.00 - 09.99.99
CX-Hammernet	1.3(N build 0014)	1.0 above	1.0 - 9.9
CX2600/220	03.01.12	03.0 above	03.0 - 09.9
Express5800/BladeServer	2.2.16	1.0 above	1.0 - 9.9
MAR	1.60(ed27)	R1.6 above	R1.6 - R1.9

OS type	Software version		
	Sample	Requirements	Range
IOS	12.3(1a)	11.0 above	11.0 - 99.9
IOS/IOS-XE	16.3	03.0 above	03.0 - 99.9
CatOS	5.5(1)	5.0 above	5.0 - 9.9
NX-OS	4.1(3)N2(1a)	4.1(3)N2(1a) above	4.1 - 9.9
Nexus7000	4.2	4 above	4 - 99
Nexus7000-VDC	5.1	4 above	4 - 99
ASR1000	No conditions		
ASA5500-ADMIN-CONTEXT	8.2(2)	8.0 above	8.0 - 99.9
ASA5500-CONTEXT	10.2(5)	8.0 above	8.0 - 99.9
ASA5500	8.2(1)	8 above	8 - 99
PIX Firewall	6.0(4)	6.0 above	6.0 - 9.9
Aironet	12.0	12.0 above	12.0 - 99.9
Brocade VDX 6720	v3.0.0a	v3.0.0 above	v3.0.0 - v9.9.9
Brocade ICX 6450	Version 07.4.00aT313	Version 07.4 above	Version 07.4 - Version 99.9
Brocade NetIron CES/CER2000	V5.4.0bT183	V5.4.0 above	V5.4.0 - V9.9.9
Brocade NetIron XMR/MLX/MLXe	V5.3.0T163	V5.3.0 above	V5.3.0 - V9.9.9
ServerIron	06.0.15	05.0 above	05.0 - 99.9
FastIronEdge	06.0.15	02.0 above	02.0 - 99.9
Foundry	06.0.15	05.0 above	05.0 - 99.9
BIG-IP_TMOS	11.4.1	11.0 above	11.0 - 99.9
BIG-IP_V9	9.1.2	9.0 above	9.0 - 99.9
BIG-IP	BIG-IP 4.0	BIG-IP 4.0 above	BIG-IP 4.0 - BIG-IP 9.9
A10AX	2.2.5	2 above	2 - 99
A10Thunder	2.7.1	2 above	2 - 99
Juniper EX4200	10.4R10.7	10.4R10.7 above	10.4 - 99.9
FortiGate	v4.0.10	v4.0	v4.0 - v9.9
APRESIA	7.12.01	7.11 above	7.1 - 9.9
NetScalerMPX	No conditions		
YAMAHA	Rev.6.00.22	Rev4.00.00 above, Rev6.00.00 above	Rev.4.00.00 - Rev. 4.99.99, Rev.6.00.00 - Rev. 999.99.99
Allied	2.2.2-21	2.0 above	2.0 - 9.9
HP ProCurve 2510	Y.11.12	Y.11.12 above	Y.11.12 - Y.99.99
HP ProCurve	No conditions		
HP A3100-8 v2 EI Switch	5.20	5.20 above	5.20 - 9.99
HP A3100-16 v2 SI Switch	5.20	5.20 above	5.20 - 9.99

OS type	Software version		
	Sample	Requirements	Range
HP A5120-24G SI Switch	5.20	5.20 above	5.20 - 9.99
HP	1.2.23	1.0 above	1.0 - 9.9
HP(Compaq)	2.0.1	2.0 above	2.0 - 9.9
Exentryeme	7.0.1b50	2.0 above	2.0 - 9.9 10.0 - 99.9
SII	2.0	1.0 above	1.0 - 9.9
Lucent(MAX)	7.2.4	6.0 above	6.0 - 9.9
Aruba 61, 70, 800	No conditions		
FX-DS540-AP	No conditions		
FX-DS540-APL	No conditions		
FX-DS540-APW	No conditions		
FX-DS540-APD	No conditions		
ORiNOCO AP	No conditions		
Inkra	No conditions		
ODN	1.0	1.0 above	1.0 only
Windows Server 2008	No conditions		
Windows Server 2003	No conditions		
Windows 7	No conditions		
Windows Vista	No conditions		
Windows XP	No conditions		
Windows 2000	No conditions		
Windows NT	No conditions		
Windows 95	No conditions		
MS-DOS/Windows	No conditions		
Windows	No conditions		
Linux	No conditions		
EWS-UX/V	No conditions		
UP-UX/V	No conditions		
OtherSwitch	No conditions		
OtherRouter	No conditions		
OtherServer	No conditions		
OtherHost	No conditions		

4.6.2 Importing a configuration information file

Import from the monitoring terminal GUI or by running commands on Manager.

- "4.6.2.1 Importing from the monitoring terminal (page 228)"
- "4.6.2.2 Importing using the manager command (page 228)"

Caution

1. Import operations place an extra load on the CPU of the manager machine, sometimes resulting in delayed response. Connections from other monitoring terminals during import operations are not recommended.
2. Import operations for devices can fail if scheduled operations are executed during the import operation. It is recommended that the monitoring mode be set to OFF prior to running the import operation.
3. In cases where an icon of the same name has already been registered, Network Manager assumes they are associated with the same device (the one in question being already registered) and will modify the attributes of both icons.
4. The Nexus 2000 icon type is not supported and cannot be imported.
5. Precautions Concerning Topology (Connection Line) Information

   For specifying rules of [Source Port Name] and [Destination Port Name], refer to "4.2.3.3.5 About port names in the topology information (page 158)" and "4.2.3.3.6 About map displays for the shared port (page 160)".

   a. In cases where an existing connection line is specified, but connection information (source/destination node, port name, port ID, IP address, link speed and duplex mode) is omitted, all current settings information will be cleared.

   b. It is necessary to register the devices to be specified (component type is node or media component) as the source and destination in advance. Even if one device is a node and the other media, the source node and destination node cannot have the same name.

   c. In cases where the specified map contains a node and a media component of the same name, if devices like the ones described above are specified as source/destination devices during an import operation, it will be determined that they were specified as node components.

   d. Despite the existence of multiple icons representing the same device component on the same map, the connection line can only be linked to one of them. In cases where a new connection line is specified and there are already multiple icons representing source- and destination-node device names on the same map, the line will be connected to icon(s) that have already been connected by a different connection line. If no icons have a connection line, the new line will be connected to the icon that was registered first.

   e. Existing information will be overwritten without warning in cases where the following types of connection line registration information are imported.

      - Regardless of connection line being new or preexisting, the registered port name will differ from the one specified, despite there being a line connecting a port that matches the specified port ID.
      - Regardless of connection-line being new or preexisting, the registered port ID will differ from the one specified, despite there being a line connecting a port that matches the specified port name.

   f. The topology check tool can be used to check correlation between port name and port ID by confirming if they are consistent with device information.

   g. In the case of devices that have icons in several maps, you cannot register a connection line for limited maps. In cases where the lines connecting devices specified as source and destination are registered on a different map, the lines created on the different map will be displayed when the connection lines are registered.

   h. In topology registration, the setting values of discovery protocol for the source device and destination device are checked. In MasterScope Network Manager 6.1 or later, if discovery protocol items are not specified, a setting of 100, which means "not specified", is specified. In MasterScope Network Manager 6.1 or before, if a file that was exported in the previous version is imported, 100 is specified in the discovery protocol and topology registration may fail. Execute topology registration after specifying a proper value in the discovery protocol.

4.6.2.1 Importing from the monitoring terminal

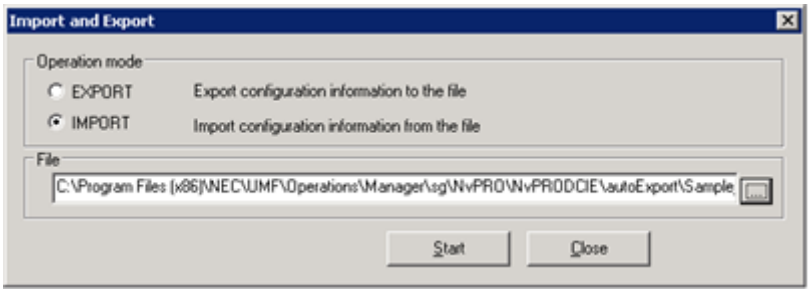
You must first change to the "configuration mode (page 27)".

1. Prepare a configuration information file.

   Note that you should specify the functions to be executed in columns from [Regist Map] to [Monitoring-mode Setting] of the configuration information file. For details, refer to "4.6.1.1 Configuration information file format (page 207)".

2. Open the Import and Export dialog box.

   Right-click the **NetworkView** icon, the **NetworkManagement** icon, or the map icon. Select **Configuration Management**>**Import and Export**.



3. In **Operation mode**, select **IMPORT**.
4. Specify the import file name with the absolute path in the **File** column.
5. Click **Start** button.

Tip

Hold down SHIFT and click **Cancel** button to avoid deleting all remaining devices without confirmation. (This dialog box will not appear again.)

6. In the completion dialog box, click **Operation Log** button and confirm the import results.

   For details, refer to "4.6.4 Operation log file (page 230)".

   Also, if there are rows that cannot be registered due to entry error, etc., these row are saved in another file as an "error record file". For details, refer to "4.6.5 Error record file (page 231)".

4.6.2.2 Importing using the manager command

1. Prepare a configuration information file.

   Note that you should specify the functions to be executed in columns from [Regist Map] to [Monitoring-mode Setting] of the configuration information file. For details, refer to "4.6.1.1 Configuration information file format (page 207)".

2. Run the configuration information batch registration command (`nvpnodeconf`).

```
> cd <%installfolder%>\Manager\bin
> nvpnodeconf import <import file name>
```

   For details, refer to "9.10.1 Configuration information batch registration command (nvpnodeconf) (page 722)".

3. Open the operation log file and confirm the import results.

The command result and the operation log file path are displayed in the standard output and standard error output. For details, refer to "4.6.4 Operation log file (page 230)".

Also, if there are rows that cannot be registered due to entry error, etc., these row are saved in another file as an "error record file". For details, refer to "4.6.5 Error record file (page 231)".

4.6.3 Exporting configuration information

Export configuration information from the monitoring terminal GUI or by running commands on Manager.

"#Format: [~OriginalItem]" is output to the first line and a tilde (~) is added to the beginning of the item. To export without adding a tilde (~) to the data, follow the steps below.

1. Change the names of the files below. Delete ".org" from the ends.

   For the Monitoring Terminal:

   <On the monitoring terminal, %installfolder%>/Svc/sg/NvPRO/IOFormat.ini.org

   For the Manager:

   <On the manager, %installfolder%>/Manager/sg/NvPRO/IOFormat.ini.org

2. Open the configuration file, replace "~OriginalItem=1" with "~OriginalItem=0" and save it.
3. Perform an export.

- "4.6.3.1 Exporting from the monitoring terminal (page 229)"
- "4.6.3.2 Exporting using the manager command (page 230)"

Caution

1. It is not possible to limit export of device connection lines to only certain maps in cases where a device possesses icons on multiple maps. In cases where the icons for devices specified as source and destination type are registered on a different map as well, the information associated with connection line icons will be exported even if the icons for the connection lines are deleted on one of the maps.
2. The Nexus 2000 icon type is not supported and cannot be exported.
3. The export may fail if there is a path name for the configuration information file location that includes "nul" (either uppercase or lowercase). Specify a path name that does not contain "nul" (either uppercase or lowercase).

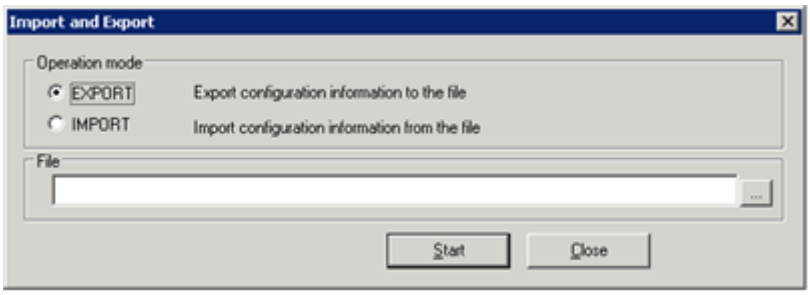
4.6.3.1 Exporting from the monitoring terminal

For exporting of device information, use the Import and Export dialog box.

You must first change to the "configuration mode (page 27)".

1. Open the Import and Export dialog box.

   Right-click the **NetworkView** icon, **NetworkManagement** icon, or the map icon. Select **Configuration Management**>**Import and Export**.



2. In **Operation mode**, select **EXPORT**.
3. Specify an export file name with the absolute path in the **File** column.
4. Click **Start** button.
5. In the completion dialog box, click **Operation Log** button and confirm the export results.

   For details, refer to "4.6.4 Operation log file (page 230)".

   For details of the exported file, refer to "4.6.1.1 Configuration information file format (page 207)".

4.6.3.2 Exporting using the manager command

You can also use the command for exporting device information.

1. Run the configuration information batch registration command (`nvpnodeconf`).

   ```
   > cd <%installfolder%>\Manager\bin
   > nvpnodeconf export <export file name>
   ```

   For details of command, refer to "9.10.1 Configuration information batch registration command (nvpnodeconf) (page 722)".

2. Open the operation log file and confirm the export results.

   The command result and the operation log file path are displayed in the standard output and standard error output. For details of operation log file, "4.6.4 Operation log file (page 230)".

   For details of the exported file, refer to "4.6.1.1 Configuration information file format (page 207)".

4.6.4 Operation log file

The following information is output to the operation log file.

- Import

  The result of checking the import file and import operation

- Export

  The results of the export operation

When operating from the monitoring terminal

The operation log backup file uses the name "*%incrementalnumber%*_ImportExportLog.txt". *%incrementalnumber%* starts at 000 and 1 is added each time. The maximum number is 099.

The operation log of activity, prior to the most recent operation, is saved as a backup.

In cases where the number of backup files has already reached 100, when operation commences, the message "Delete the backup operation log file" is displayed and the operation is not performed. Delete all unnecessary backup files and retry the operation.

- The log is stored in the following:

  <On the monitoring terminal, %installfolder%>\Svc\log\NvPROCsvIOConfig_ImportExportLog.txt

- The backup logs are stored in the following:

  <On the monitoring terminal, %installfolder%>\Svc\log\NvPROCsvIOConfig\ImportExportLog

When operating from the manager command

The operation log is created using the name "*%incrementalnumber%*_ImportExportLog.txt". It stores a maximum of 100 items. *%incrementalnumber%* is a number from 000 to 099. If -log *logfile* argument of the command is specified, the same contents of the operation log file is output to *logfile*.

- The log is stored in the following:

  <On the manager, %installfolder%>\Manager\log\nvpnodeconf*%incrementalnumber%*_ImportExportLog.txt

4.6.5 Error record file

Use the error record file to import only those records that could not be registered or deleted.

Correct the error record file according to the operation log before performing import.

Location of the error record file

Directory

Same directory as the import file

File Name

"TMP" + *import_file_name.extension*

4.7 Registering Routing Information for the Map between Two Nodes

Routing information is used for displaying the map between two points (point-to-point map). To display a point-to-point map, you must first register the routing information. For details of maps between two points, refer to "5.7.1 Displaying a point-to-point map (page 471)".

⚠ Caution

Route information is collected using SNMP to collect the following MIB from each router.

iso.org.dod.internet.mgmt.mib-2.ip.ipRouteTable

For this reason, route information not included in the above MIB will not be displayed in the point-to-point map.

You must first change to the "configuration mode (page 27)".

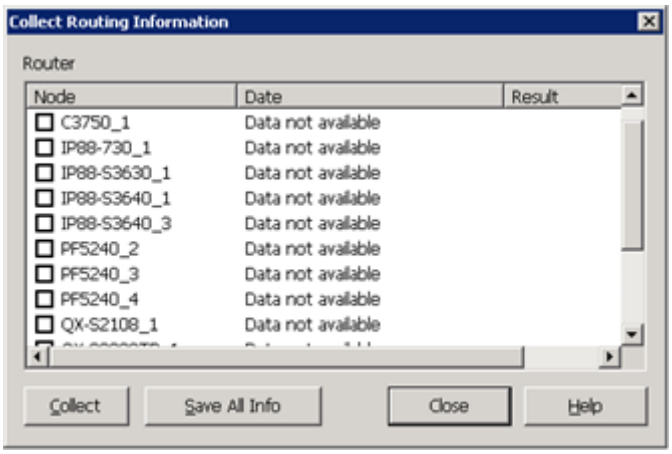
1. Open the "4.7.1 Collect Routing Information dialog box (page 232)".

Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Configuration Management**>**Collect Routing Information**.

2. Select the devices from which you want to collect route information and click **Collect** button.

4.7.1 Collect Routing Information dialog box

Collects L3 routing information to be used in plotting a point-to-point map. Collected routing information can be exported to an external file. You must change to "configuration mode (page 27)" before collecting routing information.



- **Node**

  Select the router for which you want to collect routing information. All L3 device names registered in Network Manager are displayed in the list.

- **Date**

  Displays the time that route information was collected from the device. (If there is no data, "Data not available" will be displayed.)

- **Result**

  Displays the collection results.

- **Collect** button

  Collects route information from the selected device.

- **Save All Info** button

  Outputs all route information collected from devices to an external file.

- **Close** button

  Closes the dialog box.

- **Help** button

  Displays Help.

The following right-click menus are displayed in the list.

- **List Routing Table** menu

  Displays collected route information for selected L3 devices.

- **Check ON** menu

  Selects the highlighted devices.

- **Check OFF** menu

  Deselects the highlighted devices.

4.8 Configuring the Operating Environment for the Fault Management

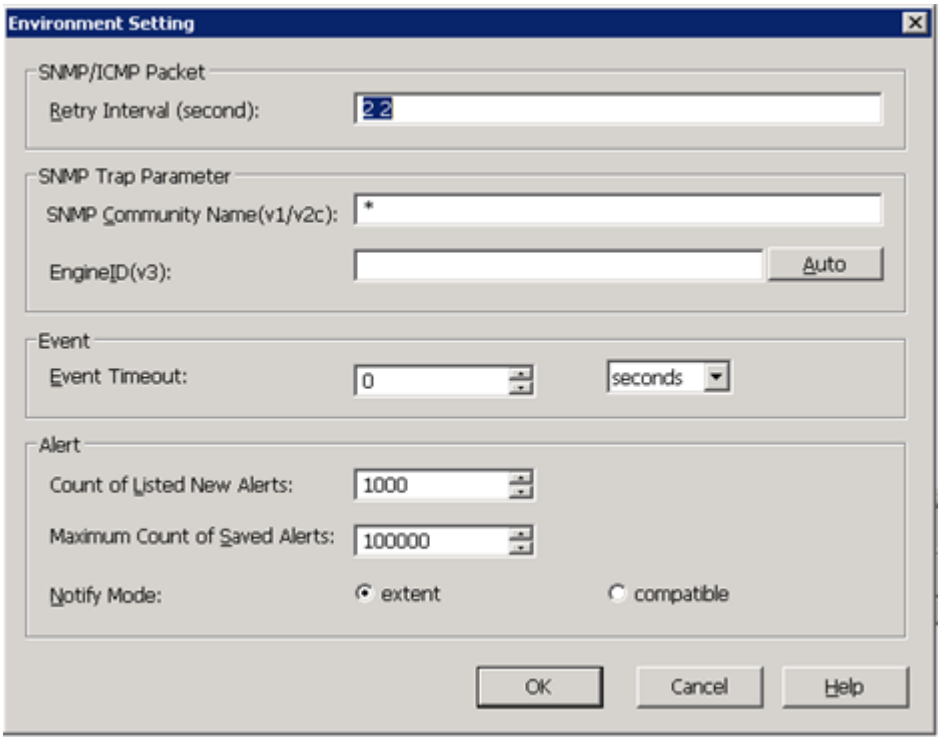
The Network Manager operating environment for the fault management is configured in the Environment Setting dialog box.

You must first change to the "configuration mode (page 27)".

1. Open the Environment Setting dialog box.

   Right-click the **NetworkView** icon and select **Environment Setting** menu.

2. Enter the necessary items.



- **SNMP/ICMP Packet**
  - **Retry Interval**

    Specify the retry interval for the target device when sending SNMP packets (for GET) or ICMP packets.

    Example:

    The retry interval "4 4 8" indicates the following behavior. Four seconds later from the first transmission, Network Manager retransmits packets, retransmits again 4 seconds later, and finally waits eight seconds. If there is no reply, Network Manager will time out.

    Format :

Include at least one single-byte space character between numbers. You can specify up to the 16th number. If 17 or more numbers are specified, the 17th-to-last character is/are ignored.

Numbers that can be specified:

1-3,600 (seconds)

- **SNMP Trap**
  - **SNMP Community**

Specify a community name for the SNMP v1/v2c traps to be received. SNMP v1/v2c traps that do not have the specified community name will be discarded. To specify multiple community names, separate the community names using a comma (,). If you do not specify anything, or you specify an asterisk (*), all SNMP traps will be received.

Maximum number of characters:

1,023 characters.

Available characters:

Single-byte alphabet and numbers, comma (,), or backslash (\). When using comma or backslash, specify additional backslash before comma or backslash, as escape sequence. (Example: abc\,def, abc\\def)

Maximum number of community names:

63 community names. If 64 or more community names are specified, all SNMP traps will be discarded.

  - **EngineID(v3)**

Specify the manager Engine ID of Network Manager. The specified value will be a remote engine ID that is required for transmitting the SNMPv3 inform from the monitored device.

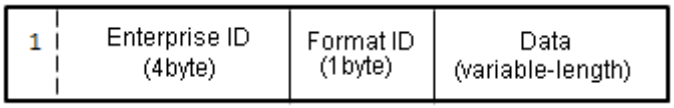
By specifying the value specified here in the monitored device as a manager Engine ID of Network Manager, Network Manager will be able to receive the SNMPv3 inform, which is transmitted from the monitored device.

Remove the SNMPv3 inform that does not match the Engine ID.

In order to determine Engine ID, click the **Auto** button to automatically create it or manually enter a value in accordance with the rules described below.

Available characters

It is possible to specify in hexadecimal notation separated by ":" or " " (space). Specify values in accordance with the following rules.



Specify 1 for the first 1 bit for the enterprise ID.

You can specify the following values for the format ID and data.

Format ID	Format	Data Length (in bytes)
1	IPv4 address	4
2	IPv6 address	16

Format ID	Format	Data Length (in bytes)
3	MAC address	6
4	Character string	1 to 27
5	Byte sequence	1 to 27
128 to 255	Optional information	1 to 27

For example, if the enterprise ID is NEC (119) and IPv4 address is 192.168.1.1, it will be 0x8000007701c0a80101.

Enterprise ID (4 bytes):	0x80000077
Format ID (1 byte):	0x01
Data (4 bytes):	c0a80101

If you click the **Auto** button, values in accordance with the rules are created.

- **Auto**

  The manager engine of Network Manager is created in a format in accordance with rules.

- **Event**
  - **Event Timeout**

    Specify the time until the icon color returns to its original status when an alert is generated indicating that a recovery event has not occurred (a manual recovery alert). If a zero is specified in this box, the icon will not be returned to its original color.

    Values that can be specified:

    0 - 3,600 (the default is 0)

    nits of time that can be specified:

    Seconds, Minutes, Hours

- **Alert**
  - **Count of Listed New Alerts**

    Specify how many alerts to display in the new alert window. (need to restart the monitoring window)

    Values that can be specified:

    1 - 1,000 (the default is 1,000)

- **Maximum Count of Saved Alerts**

  Specify the maximum number of alerts that will be saved in the database.

  Values that can be specified:

  1 - 100,000 (the default is 100,000)

- **Notify Mode**

  Specify the severity mode of the alert notification.
  - **extent**

    Manage severity as six levels ("NORMAL", "UNKNOWN", "WARNING", "MINOR", "MAJOR", "FATAL").

- **compatible**

  Manage severity as four levels ("NORMAL", "UNKNOWN", "WARNING", "FATAL").

- **OK** button

  Applies the settings.

- **Cancel** button

  Cancels the settings.

- **Help** button

  Displays Help.

3. Click **OK** button.

4.9 Error Monitoring

4.9.1 Monitoring items

In Network Manager, use the following methods to monitor for faulty devices on the network.

1. Ping monitoring using Internet Control Message Protocol (ICMP).

   Perform regular monitoring of the operating state of monitored devices by using ICMP echoes to check for responses. This monitoring method is also applicable to devices that do not support SNMP.

   For details, refer to "4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function) (page 241)" and "7.1.1 Rules for monitoring alive status (page 590)".

2. MIB monitoring using SNMP

   Perform regular monitoring of MIB state changes on monitored devices using SNMP.

   The monitoring rules below are by default.

   - Interface state monitoring
   - Threshold value monitoring
   - Host resource monitoring
   - Custom monitoring of specific device types
   - Monitoring for other errors

   It is also possible to create new monitoring rules to suit your operating environment.

   For details, refer to "4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function) (page 241)" and "7.1 State Monitoring Rules (page 590)".

3. Receiving SNMP traps

   Detect and then report faults occurring on devices in close to real-time. There is support for SNMP trap versions v1, v2c, and v3. There is also support for receiving and reporting vendor-defined traps.

   For details, refer to "4.11 Monitoring SNMP Traps (page 259)".

4. Receiving syslogs

Detect and report faults occurring on devices in close to real-time. Network Manager supports the receipt of syslogs in RFC3164 (the BSD syslog protocol) compliant formats. There is support for receive and report items with a severity level of "WARNING" or higher.

For details, refer to "4.12 Monitoring Syslogs (page 302)".

4.9.2 About alert severity and priority

4.9.2.1 About severity extension

Severity of an alert notification can be selected from the compatible mode (4 levels) or the extended mode (6 levels). The default is the extended mode. For details regarding changing mode, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

The following table shows the transformation rules from severity in each function setting to severity of an alert notification in the compatible mode and the extended mode.

Severity setting in each function		compatible mode	extended mode
Trap Definition (Severity)	n	NORMAL	NORMAL
	u	UNKNOWN	UNKNOWN
	w	WARNING	WARNING
	mi	FATAL	MINOR
	ma	FATAL	MAJOR
	f	FATAL	FATAL
State Monitoring	WARNING	WARNING	WARNING
	Minor	FATAL	MINOR
	Major	FATAL	MAJOR
	Critical	FATAL	FATAL
SYSLOG	WARNING(4)	WARNING	WARNING
	ERRORS(3)	WARNING	WARNING
	CRITICAL(2)	FATAL	FATAL
	ALERT(1)	FATAL	FATAL
	EMERGENCIES(0)	FATAL	FATAL
Alert Aggregation	NORMAL	NORMAL	NORMAL
	WARNING	WARNING	WARNING
	MINOR	FATAL	MINOR
	MAJOR	FATAL	MAJOR
	FATAL	FATAL	FATAL
SNMPv3 trap Invalid EngineID Alert	Warning	WARNING	WARNING
	Minor Fault	FATAL	MINOR
	Major Fault	FATAL	MAJOR
	Critical State	FATAL	FATAL
Device Config Management (Alert Sending Setting)	NORMAL	NORMAL	NORMAL
	WARNING	WARNING	WARNING

Severity setting in each function		compatible mode	extended mode
	MINOR	FATAL	MINOR
	MAJOR	FATAL	MAJOR
	FATAL	FATAL	FATAL

Caution

The extended mode is not supported in MasterScope Network Manager 2.0. If you want to use a monitoring console of MasterScope Network Manager 2.0 to connect the manager of MasterScope Network Manager 4.0 or later, you must select compatible mode.

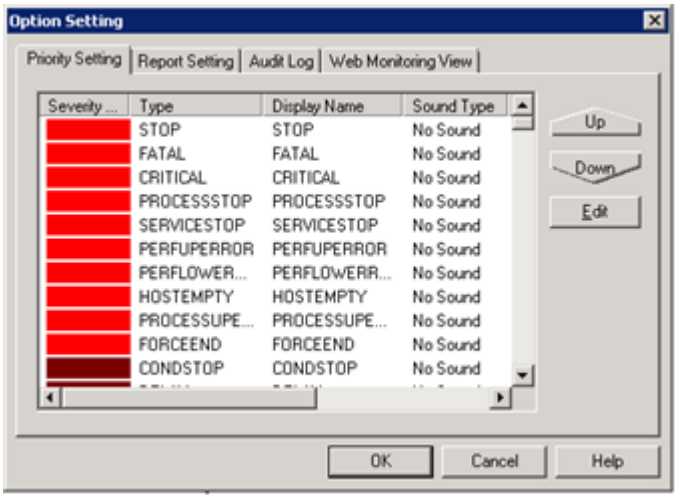
4.9.2.2 Changing priority level settings

Tip

- The **Priority Setting** tab is shared in MasterScope products. Settings that change affect the operations in all MasterScope products when combining the system is with MasterScope SystemManager G, etc.
- In Network Manager, only use the following types of system severity levels(display names).
  - FATAL
  - MAJOR
  - MINOR
  - WARNING
  - UNKNOWN
  - UNMANAGED
  - NORMAL

You must first change to the "configuration mode (page 27)".

1. In the main menu, select **Setting**>**Option**.
2. In the **Priority Setting** tab of the Option Setting dialog box, configure the priority settings.



This tab displays the **Severity Color**, **Type**, **Display Name**, **Sound Type**, **WAVE File**, and **Sound Count** for the severity levels.

- The priority of selected item can be changed by the **Up** button and **Down** button.

The severity levels displayed at the top of the window are higher for those positioned at the bottom.

3. Click **OK** button.

4.9.2.3 Changing severity level settings

Configure the severity level (system severity, user severity, on user mark) to be used in this system.

Tip

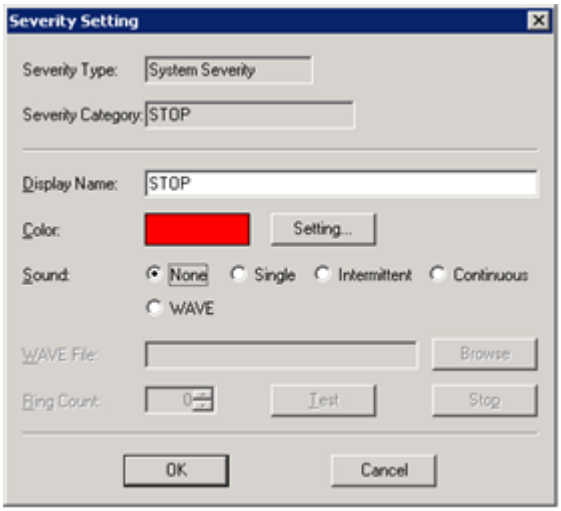
- The **Priority Setting** tab is shared in MasterScope products. Settings that change affect the operations in all MasterScope products when combining the system is with MasterScope SystemManager, etc.
- In Network Manager, only use the following types of system severity levels (display names).
  - FATAL
  - MAJOR
  - MINOR
  - WARNING
  - UNKNOWN
  - UNMANAGED
  - NORMAL

You must first change to the "configuration mode (page 27)".

1. Open the Option Setting dialog box.

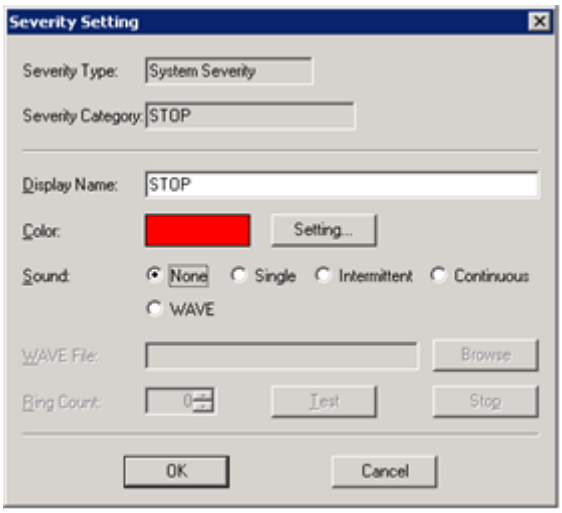
   In the main menu, select **Setting**>**Option**.

2. Select the **Priority Setting** tab.
3. Select the severity level or mark to edit, then click the **Edit** button or double-click the desired item.
4. In the "4.9.2.3.1 Severity Setting dialog box (page 239)", enter in each item.



5. Click **OK** button.

Severity Setting dialog box



- **Severity Type**

  Displays either the "System Severity", "User Severity", or "User Mark".

- **Severity Category**

  Displays the category for the severity level.

- **Display Name**

  Specify a name using up to 64 characters. The comma (,) and double quotation marks (") cannot be used in display names. If the **Severity Type** is "System Severity", the display name cannot be omitted. In cases where the display name for "User Severity" or "User Mark" is omitted, it will be deemed that the severity level will not use them.

- **Color**

  This field displays the color corresponding to the current severity level setting. To select the desired color: click the **Setting** button to displays the Color dialog box.

- **Sound**

  Select the sound type from **None**, **Single**, **Intermittent**, **Continuous**, and **WAVE**. Sound types can be specified for "System Severity" and "User Severity" levels. When an event of the designated severity occurs, the selected sounds go off as notification of the occurrence of a message. Sound notifications are limited to when the monitoring window is open, and occur at the monitoring terminal.

- **WAVE File**

  If selecting **WAVE** for **Sound**, enter the name of the WAVE file using up to 256 characters. Clicking the **Browse** button allows selection of a WAVE file. Environmental variables can be used in a file path name.

  Caution

  - In cases where an invalid WAVE file name was specified, the default continuous sound is heard for sound notifications.
  - WAVE file path name is a common setting in all monitoring terminals. It is necessary to put the WAVE file on the same path in all monitoring terminals.

- **Ring Count**

  Specify the ring count when selecting a **WAVE** sound as the sound type. Specify ring count in the 0 to 32767 range. 0 indicates unlimited ring count.

- **Test** button

  Conducts a test of the specified sound type.

- **Stop** button

  Stops the sound in the middle of a test.

4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function)

Network Manager is designed to monitor the states of registered devices and detect any status changes. For example, it is possible to detect heavily loaded segments and whether a device is up or down.

Caution

- The retry interval and timeout settings for SNMP packets and ICMP ECHO packets in the state monitoring are values set in the Environment Setting dialog box, under the **SNMP/ICMP Packet** settings, in the **Retry Interval** column. For details regarding the Environment Setting dialog box, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".
- There are several important points to consider when monitoring Nexus 5000 and 2000 series devices.

  For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".

4.10.1 State Monitoring window

The State Monitoring window is used to perform the following state monitoring operations.

To open the State Monitoring window, right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Fault Management**>**State Monitoring**.

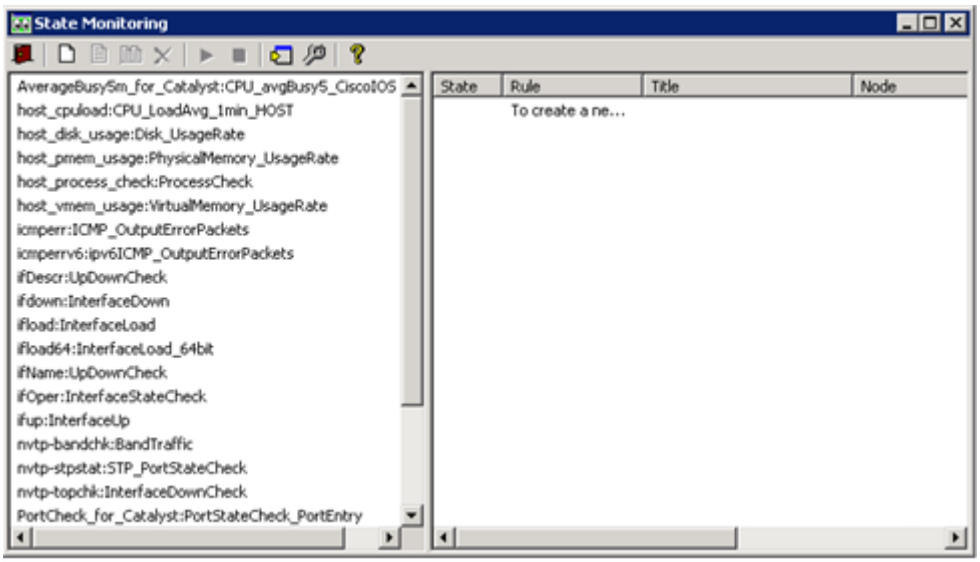
The State Monitoring window is used to perform the following state monitoring operation.

- Registering, viewing, and deleting monitoring rule entries.
- Executing and stopping execution of monitoring rule entries.
- Importing or exporting monitoring rules entries.
- Embedding or removing rule files.

Monitoring is usually performed using the following two steps.

1. Registering monitoring rule entries.
2. Executing monitoring rule entries.

The State Monitoring window is comprised of the rules list (left screen) and the rule entries list (right screen).



- Rules list

  A list of state monitoring rules. Rules used in operations are selected from this list. Any rule entries associated with a selected rule are displayed to the right. To display all rule entries, select all the rules. (Multiple rules can be selected by clicking them while holding down the CTRL or SHIFT key.)

  For details regarding embedded rules, refer to "7.1 State Monitoring Rules (page 590)".

- Rule entries list

  A list of the rule entries that have been set. Rules entries are added whenever a new rule is created.

  - **State**

    Indicates the status ("Started", or "Stopped") of the rule entry.

  - **Rule**

    Displays the names of rules to be executed.

  - **Title**

    Displays the titles of rule entries.

  - **Node**

    Displays the name of the managed node to which the monitoring rule will be applied.

  - **Interval**

    Displays the interval time for which the rule entry will be executed. (Indicated in seconds for all rules.)

  - **EntryName**

    Displays the names of rule entries.

- Tool Bar

  - **Quit** button

    Closes the State Monitoring window.

  - **Create a new rule entry** button

Opens the Rule Entry Settings dialog box used to create new rule entries. For details, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

- **Update** button

  Opens the Rule Entry Settings dialog box used to modify information for a selected rule entry. For details, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

- **Copy rule entries** button

  Creates a copy of the selected rule entry.

- **Delete rule entries** button

  Deletes the selected rule entries.

- **Start rule entries** button

  Executes a monitoring operation using the selected rule entry.

- **Stop rule entries** button

  Stops the selected rule entry's monitoring operation.

- **Import/Export** button

  Imports/exports monitoring rule entries.

- **Embedded rule files** button

  Embeds and removes rule files.

- **Help** button

  Displays Help.

4.10.2 Creating new state monitoring rule entries

You must first change to the "configuration mode (page 27)".

1. Open the "4.10.1 State Monitoring window (page 241)".

   Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Fault Management**>**State Monitoring**.

2. Select a new rule to create from the rules list.

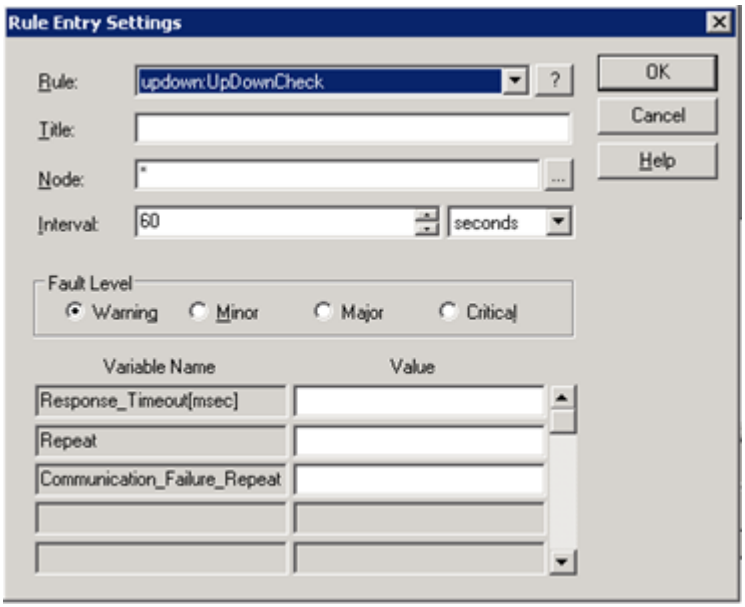
   The top rule is the target when more than one rule is selected.

3. Click the **Create a new rule entry** button.

   Tip

   You can double-click the blank row in the **rule entries list**.

4. Set a value in each field of "4.10.2.1 Rule Entry Settings dialog box (page 244)", and then click **OK** button.



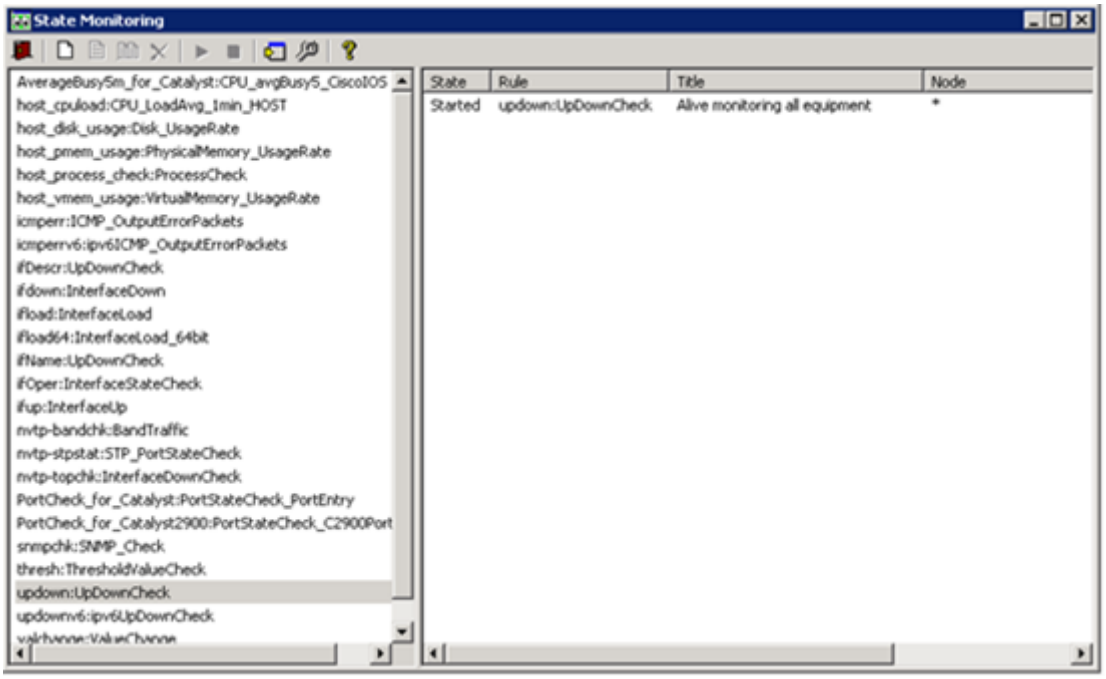
Entering invalid settings may cause monitoring to perform poorly.

5. To execute the newly created entry, select the entry and then click the **Start rule entries** button.

Caution

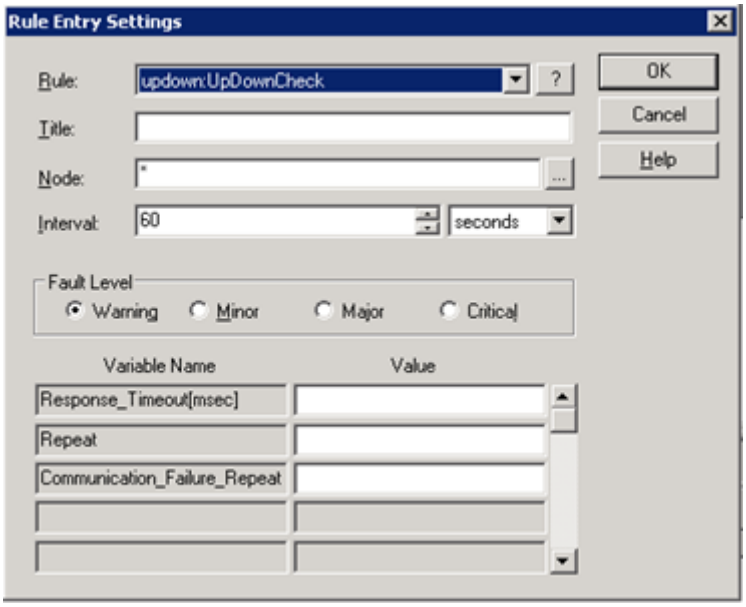
State monitoring rules can be set and started for devices with monitoring mode OFF, but monitoring itself will not be conducted. The state monitoring for the device will begin once its monitoring mode returns to ON.

Starts monitoring.



4.10.2.1 Rule Entry Settings dialog box

Use to enter the various parameter settings for rule entries. If rule entries are being executed, the dialog box can be displayed but values cannot be changed.



- **Rule**

  Selects the rule to be executed. Click the ? button to display a description of the rule. Help information cannot be displayed for rules that users customized.

- **Title**

  Enter the title of the rule entry.

- **Node**

  Specify the node or group name to be monitored. By specifying a group name, the monitoring for this entry can be performed for all devices that belong to the specified group. The format of specification complies with the "Standard Component Name Specification Format", and the component of node/group type can be specified. For multiple devices, specify using comma (,) separation. To specify group name, specify in the format of "grp:*group name*". For details of the standard component name specification format, refer to "7.3.3 Standard Component Name Specification Format (page 645)".

  Click the ... button to display the Node List dialog box. For details, refer to "4.10.2.2 Node List dialog box (page 246)".

  Caution

  Even if a node or group name of the monitored device is changed, the **Node** fields in rule entries will not be changed automatically. For this reason, if a node or group name is changed, devices may be excluded from the monitoring targets. Also, if the device is excluded from the monitored target while the "auto recovery type alerts" have been issued, these alerts will be recovered.

  To continue monitoring after a node or group name has changed, review **Node** column in the Rule Entry Settings dialog box.

- **Interval**

  Enter the time interval for which the rule will be executed. Specify for any unit of measurement up to a value of 32,767.

- **Fault Level**

Specify the level of the failure alert which will be issued when a rule discovers a failure. For example, alerts can be set to issue at lower levels of severity on standard client machines but at higher levels on server machines.

Refer to the table below for the relationship between **Fault Level**, fault severity, and alert types.

Fault Level	Severity	Alert Type
Warning	WARNING	Warning
Minor	MINOR	Minor
Major	MAJOR	Major
Critical	FATAL	Critical

Caution

In the compatible mode, the severity level of MINOR/MAJOR will become FATAL. For details, refer to "4.9.2.1 About severity extension (page 237)".

- **Variable Name**

  Displays names of variables dependent on rules. The names of variables cannot be changed.

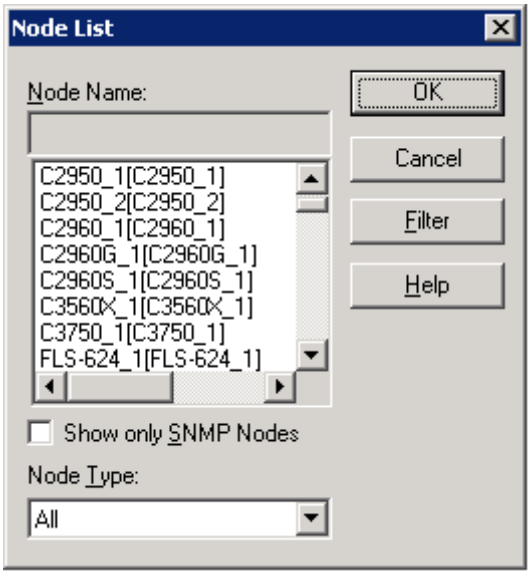
- **Value**

  Specify the values to be set for each variable. For details, refer to "7.1 State Monitoring Rules (page 590)".

  Depending on rules,  buttons are displayed for input items. For details, refer to "4.10.2.3 Variable setting dialog box (page 247)".

4.10.2.2 Node List dialog box

Select devices from information registered with Network Manager.



- **Node Name**

  Select a device from a list of devices registered with Network Manager.

- **Show only SNMP Nodes**

In the **Property** menu of the icon, displays only nodes with SNMP community name or **SNMPv3** user name in the icon properties.

- **Node Type**

  All:

  Displays all nodes registered on the map.

  Router Only:

  Displays only those nodes registered with icon types showing routers such as "router" "ip45", "ip48", "CiscoRouter".

  Catalyst Device:

  Displays only those nodes registered with icon types showing Catalyst devices such as "C2950-12", "C2950-24", "C3550-12T", "C3550-12G".

  Only IPv4 nodes:

  Displays only those nodes registered with IPv4 address. This item is only displayed in certain functions.

  Only IPv6 nodes:

  Displays only those nodes registered with IPv6 address. This item is only displayed in certain functions.

- **Filter** button

  It is possible to refine the list of devices registered with Network Manager using standard matching specification format. For the standard matching specification format, refer to "7.3.2 Standard Matching Specification Format (page 644)".

4.10.2.3 Variable setting dialog box

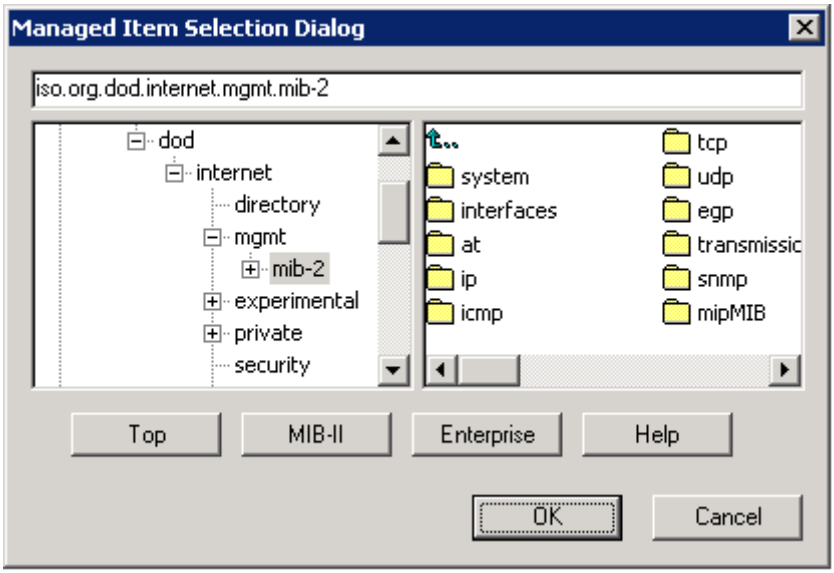
The … button is displayed to the right of the input column, depending on the combination of rules and variable names. The dialog boxes that are displayed when the … button is clicked are shown below.

Rule Name	Variable Name	Displayed Dialog Box
thresh:ThresholdValueCheck	MIB_Name	Refer to "4.10.2.3.1 Managed Item Selection Dialog dialog box (single MIB selection) (page 248)".
valchange:ValueChange		Refer to "4.10.2.3.2 Managed Item Selection Dialog dialog box (multiple MIBs selection) (page 248)".
ifDescr:UpDownCheck	Interface_Number	Refer to "4.10.2.3.3 Interface Number Select dialog box (page 249)".
ifdown:InterfaceDown		
ifload:InterfaceLoad		
ifload64:InterfaceLoad_64bit		
ifName:UpDownCheck		
ifOper:InterfaceStateCheck		
ifup:InterfaceUp		
nvtp-bandchk:BandTraffic		

Rule Name	Variable Name	Displayed Dialog Box
nvtp-topchk:InterfaceDownCheck		

Managed Item Selection Dialog dialog box (single MIB selection)

In this dialog box, it is not possible to select multiple MIBs.



- **Top** button

  Moves to the "iso" at the top of the MIB tree.

- **MIB-II** button

  Moves to the "iso.org.dod.internet.mgmt.mib-2" that is at the top of the location where MIB-II is defined.

- **Enterprise** button

  Moves to the "iso.org.dod.internet.private.enterprises" that is at the top of the location in which the enterprise MIB is defined.

- **Help** button

  Displays the MIB Description dialog box for the currently selected MIB.

- **OK** button

  If you select the MIB that you want to monitor and click this button, the Managed Item Selection Dialog dialog box for setting up managed items is closed and "full AMIB name" is displayed in the column for the **Management Item Name**.

- **Cancel** button

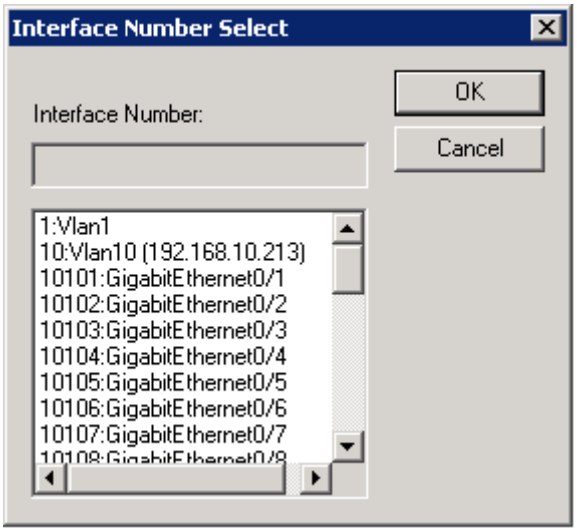
  Closes the Managed Item Selection Dialog dialog box. The **Management Item Name** column remains the same as before the dialog box was opened.

Managed Item Selection Dialog dialog box (multiple MIBs selection)

In this dialog box, it is possible to select multiple MIBs.

For details on how this is used, refer to "4.10.2.3.1 Managed Item Selection Dialog dialog box (single MIB selection) (page 248)".

Interface Number Select dialog box



- **OK** button

  If you select the interface number that you want to monitor and click this button, this dialog box for selecting interface numbers is closed and the interface number is displayed in the interface number column.

- **Cancel** button

  Closes this dialog box. The interface number column remains the same as before the dialog box was opened.

Caution

- If multiple nodes are specified in the **Node** column, this dialog box will not be displayed. If a component other than node (group name, etc.) is specified in the **Node** column, this dialog box will not be displayed.
- This dialog box displays interface numbers based on the interface information already registered in Network Manager. If a node has been manually registered or if the interface configuration has been changed, select **Update Property** to update the interface information to be registered to Network Manager in advance.

4.10.3 Modifying state monitoring rule entries

You must first change to the "configuration mode (page 27)".

1. Open the "4.10.1 State Monitoring window (page 241)".

   Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Fault Management**>**State Monitoring**.

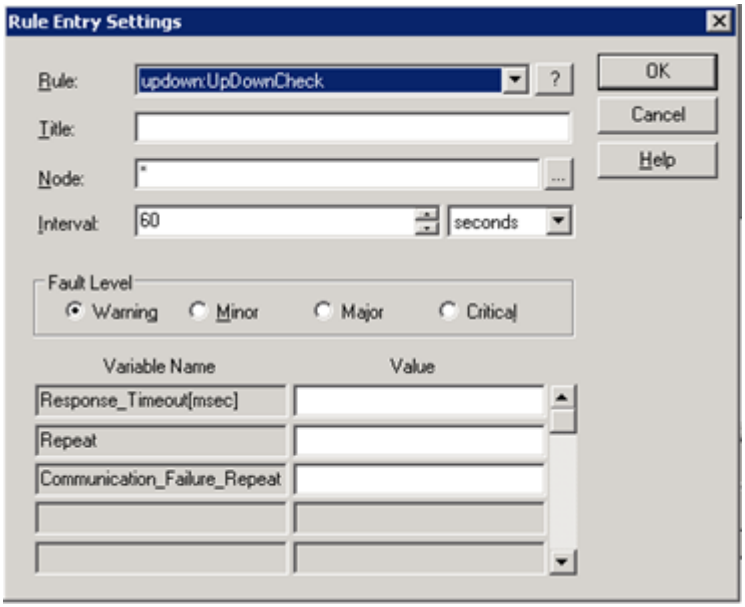
2. If the rule entry that you want to modify is currently being executed, click **Stop rule entries** button to stop execution.

3. Select the rule entry that you want to modify and click **Edit a rule entry** button.

Tip

Yuo can double-click the rule entry that you want to modify.

4. When the "4.10.2.1 Rule Entry Settings dialog box (page 244)" is displayed, change values for the desired fields.



5. Click **OK** button.

4.10.4 Copying state monitoring rule entries

You must first change to the "configuration mode (page 27)".

1. Open the "4.10.1 State Monitoring window (page 241)".

   Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Fault Management**>**State Monitoring**.

2. Select the rule entry to be copied and click **Copy rule entries** button.

The status of the newly copied and added rule entry will be "Stopped", and "(Copy)" will be added at the end of its title.

4.10.5 Deleting state monitoring rule entries

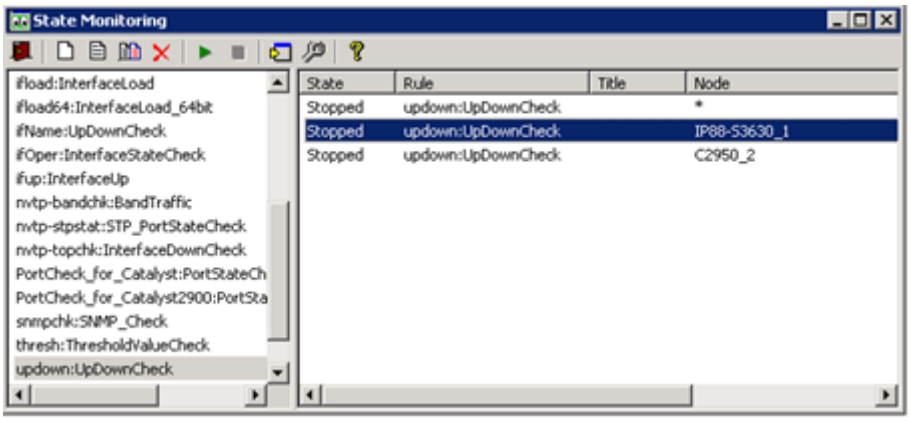
You must first change to the "configuration mode (page 27)".

1. Open the "4.10.1 State Monitoring window (page 241)".

   Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Fault Management**>**State Monitoring**.

2. If the rule entry that you want to delete is currently being executed, press **Stop rule entries** button to stop execution.

3. Select the rule entry to be deleted and click **Delete rule entries** button.



4.10.6 Batch registering state monitoring settings

The rule entry import/export function performs the following operations.

- Reads from the file and registers, updates, and deletes rule entry settings.
- Outputs completed rule-entry settings information to a file.

This function can be executed from the monitoring terminal and the command on the manager.

4.10.6.1 State monitoring setting file format

The conventions used for descriptions of information contained in the files are outlined below.

- There is support for the following file formats:

  When importing or exporting from the monitoring terminal:

OS	Encoding	BOM	Separator Characters	File Name Extension
Windows	OS multi-byte character encoding	-	Comma	.csv
	Unicode (UTF-16LE)	Yes	TAB	.txt

  When importing or exporting using the Manager command:

Manager OS	Encoding	BOM	Separator Characters	File Name Extension
Windows	OS multi-byte character encoding	-	Comma	.csv
	Unicode (UTF-16LE)	Yes	TAB	.txt
Linux	UTF-8	No	TAB	.txt

- Lines beginning with the "#" symbol are treated as comment lines.
- Write the item name in the first line (excluding comment lines).
- Each line shows one monitoring entry.
- If the first line contains "#Format: [~OriginalItem]", the tilde (~) at the beginning of each item is ignored. When exporting, "#Format: [~OriginalItem]" is exported to the first row and a tilde is added to the beginning of each item.

Some tools used to verify an export file or create an import file have an automatic correction function and some output values (input values) will be displayed (inputted) as a different value. You can stop the auto correction of data by adding a tilde (~) to the beginning of each item.

- How to create a file in Windows for importing to Linux Manager

  When a command on Linux Manager to import a file created in Windows, convert the encoding because the file encoding and line breaks vary depending on the OS. Convert the encoding using the file conversion command (`nvpfileconv`); included in the Monitoring Terminal function. For details, refer to "9.13 File Code Conversion Command (nvpfileconv) (page 739)".

Description Format

The following is the Information specified for each item in a state monitoring settings file:

Column Name	Description of Setting	Omission
State Monitoring Rule	Specifies rule name (included in the rules list on the left side of the State Monitoring window). If the specified rule is not embedded, its rule file will be embedded.	
Target Node	Specifies the names of target nodes. Multiple node names are delimited using a comma, and item data is enclosed in double quotation marks. Entering the "*" setting specifies all nodes. Example 1: "deviceA,deviceB" Example 2: "grp:groupA"	
Interval	Specifies the interval using numbers and units. Specify an interval number between 0 and 32,767. Specify the following units: Seconds: S or s Minutes: M or m Hours: H or h Example: five minutes = 5M, 5m, 300S, or 300s. Cannot use a combination of S, M, H, s, m, and h.	
Fault Level	Specifies the level of failure severity using one of the following values or character strings. 1 : Warning 2 : Minor Fault 3 : Major Fault 4 : Critical State	
Arguments	Specifies the arguments used for rules. Make sure to check the rule descriptions ("7.1 State Monitoring Rules (page 590)") and confirm the types of arguments and specification conventions defined for each rule type when specifying arguments. This can be omitted. If specified, errors result if the number of arguments exceeds the rule definition or when invalid symbols are used for quotation marks. Arguments are enclosed in single quotation marks ('), with a space inserted between if there are multiple arguments. The colon (:) is specified when there are arguments that are not specified. Use double quotation marks (") in cases where the argument itself contains single quotation marks ('). Example 1: First argument: "10"; when 10 is specified in the second argument: '10'_'10'. ("_" represents the single space character). Example 2: No first argument, second argument is specified as 10; ':'_'10'("_" represents the single space character).	o

Column Name	Description of Setting	Omission
	Caution Specifying invalid "Arguments" may cause rules to function poorly. Make sure to check the rule descriptions ("7.1 State Monitoring Rules (page 590)") and confirm the types of arguments and specification conventions defined for each rule type when specifying. Special attention is required when specifying "1" (execute) for the "Execution Flag".	
Title	Specifies the title of the rule entry. Can be omitted if not required to be set. In cases where it is unnecessary to set this item for any data file records, the row definition of the row name line can also be omitted.	o
Execution Flag	When executing an imported rule entry, specifies the value "0" or "1". "0" stops execution and "1" enables execution. Both the item and row definition may be omitted. Omission is interpreted as the "0" (stop) setting, in which case the imported rule entry is not executed. **Caution** Importing numerous rule entries and setting the "Execution Flag" to "1" (execute) for numerous import records is not recommended, as it places significant load on system machines.	o
Rule Entry Name	Specifies rule entry name. The rule entry name cannot be specified for first time registrations of rule entries. Rule entry names can be specified only when intending to overwrite existing rule entry settings. An error will occur in the record if the specified rule entry name does not exist. **Caution** 1. When registering a new rule entry refrain from entering any information for the "Rule Entry Name" item in the data file. When making a data file output by the export function the import data file format when registering new rule entries, the "Rule Entry Name" column in the data file should be deleted. 2. To update an existing rule entry setting by overwriting it, enter its name in the "Rule Entry Name" item in the data file. A dialog box confirming overwriting and registration will then be displayed.	o
Delete Flag	Delete a rule entry that have the specified entry name. "0" means not deleting, "1" means deleting. Both the item and row definition may be omitted. Omission is interpreted as the "0" (not delete) setting. When "1" (delete) is specified, the item **Rule Entry Name** must be specified. (Items except "Rule Entry Name" are ignored.) An error will occur if "Rule Entry Name" is not specified or an entry specified by "Rule Entry Name" is not exist. If specify "1" for both the remove and delete flag simultaneously, the line is treated as a remove.	o
Remove Flag	"0" means not removing, "1" means removing. When not specified (the line is not defined or it is not entered), it is assumed to be "0". (rule is not removed.) When specifying "1" (remove), entries for items other than "State Monitoring Rule" are ignored. If there are rule entries for the specified "State Monitoring Rule", a removing process will fail.	o

Caution

The following procedure is used for overwriting such existing rule entry information as row definition, and the "Argument", "Title", and "Execution Flag" items for which settings can be entered.

- When the column name line does not contain a column definition, settings for "Argument" and "Title" in the current rule entry information will not be updated. In the case of the "Execution Flag" item, if the rule entry is being executed, the information is updated and the interrupted rule entry operation restarted.
- When the column name line contains column definition but information is omitted, "Arguments" and "Title" will be interpreted as being blank. As a result, any setting entered for "Title" in the existing rule entry will be cleared. The "Execution Flag" will be interpreted as having the "0" (stop) setting. The operation will not be retried after rule entry update, even if an existing rule is executing.

4.10.6.2 Importing state monitoring rule entries

Reading data files and making Network Manager state monitoring rule entry settings are performed as a batch operation.

As required, use the following preparation procedures.

- Registering target components

  Registers any unregistered managed nodes to which rules will be applied.

- Stopping target rule entries

  When modifying existing rule entries, use the State Monitoring window to first stop execution of any targeted rule entries that are running. Settings for rule entries cannot be modified while they are being executed.

Importing from the monitoring terminal

If necessary, conduct the preparation procedures described in "4.10.6.2 Importing state monitoring rule entries (page 254)".

You must first change to the "configuration mode (page 27)".

1. Prepare an import data file.

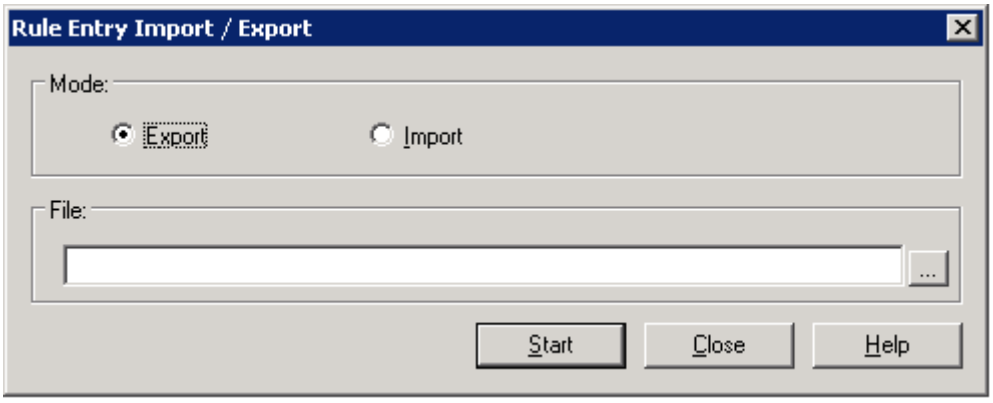
   In accordance with "4.10.6.1 State monitoring setting file format (page 251)", specify the information of rule entries to be registered.

2. Open the "4.10.1 State Monitoring window (page 241)".

   Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Fault Management**>**State Monitoring**.

3. Open the Rule Entry Import / Export dialog box.

   Click **Import / Export** button.



4. Select **Import** in **Mode**.
5. Specify the import file name with the absolute path in the **File** column.
6. Click **Start** button.

Caution

When the target rule entry to be updated is being executed, it is suspended while updating the information.

Tip

When a dialog box appears to confirm overwriting or deleting or removing the rule, hold down SHIFT and click **Cancel** button to process all remaining rows without confirmation. (This dialog box will not appear again.)

7. In the completion dialog box, click **Operation Log** button and confirm the import results.

   For details, refer to "4.10.6.4 Operation log file (page 257)".

   Also, if there are rows that cannot be registered due to entry error, etc., these row are saved in another file as an "error record file". For details, refer to "4.10.6.5 Error record file (page 257)".

Importing using the manager command

If necessary, conduct the preparation procedures described in "4.10.6.2 Importing state monitoring rule entries (page 254)".

1. Prepare an import data file.

   In accordance with "4.10.6.1 State monitoring setting file format (page 251)", specify the information of rule entries to be registered.

2. Run the status monitoring setting batch register command (`nvpstsmonconf`).

```
> cd <%installfolder%>\Manager\bin
> nvpstsmonconf import <import file name>
```

   For details, refer to "9.11 Status Monitoring Config Command (nvpstsmonconf) (page 731)".

3. Open the operation log file, and confirm the import results.

   The command result and the operation log file path are displayed in the standard output and standard error output. For details, refer to "4.10.6.4 Operation log file (page 257)".

   Also, if there are rows that cannot be registered due to entry error, etc., these row are saved in another file as an "error record file". For details, refer to "4.10.6.5 Error record file (page 257)".

4.10.6.3 Exporting state monitoring rule entries

Currently registered Network Manager state monitoring rule entry information will be output to a CSV-format file.

Caution

1. The "Delete Flag" column is always empty when exported.
2. The "Interval" column is always exported in seconds.

Exporting from the monitoring terminal

You must first change to the "configuration mode (page 27)".

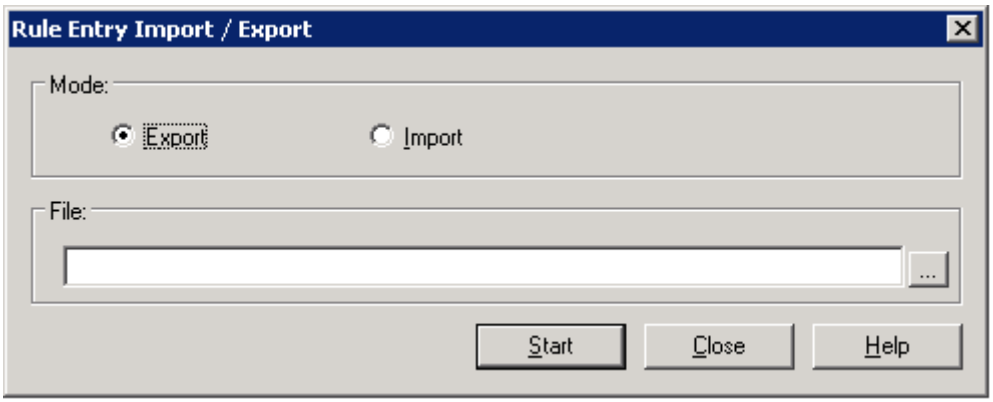
1. Open the "4.10.1 State Monitoring window (page 241)".

   Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Fault Management**>**State Monitoring**.

2. Specify output targets.

   The output targets are the rule entries selected in the rules list (screen left) of the State Monitoring window. Rules are selected by clicking a rule item in the rules list. Clicking highlights the selected item. Multiple items in the rules list can be selected by holding down the CTRL key while clicking. To select all items of rule entry information as targets for output, either select all rules or click on a blank space in the window away from the rules list to deselect all items (no rules in the rules list are highlighted).

3. Click **Import / Export** button, and open Rule Entry Import / Export dialog box.



4. Select **Export** in **Mode**.
5. Specify an export file name with the absolute path in the **File** column.

   Caution

   The export may fail if there is a path name for the destination file location that includes "nul" (either uppercase or lowercase). Specify a path name that does not contain "nul" (either uppercase or lowercase).

6. Click **Start** button.
7. In the completion dialog box, click **Operation Log** button and confirm the export results.

   For details, refer to "4.10.6.4 Operation log file (page 257)".

   For details of the exported file, refer to "4.10.6.1 State monitoring setting file format (page 251)".

Exporting using the manager command

Exporting state monitoring rule entries can be performed by using the manager command.

1. Run the status monitoring setting batch register command (`nvpstsmonconf`).

```
> cd <%installfolder%>\Manager\bin
> nvpstsmonconf export <export file name>
```

For details, refer to "9.11 Status Monitoring Config Command (nvpstsmonconf) (page 731)".

2. Open the operation log file, and confirm the export results.

   The command result and the operation log file path are displayed in the standard output and standard error output. For details, refer to "4.10.6.4 Operation log file (page 257)".

   For details of the exported file, refer to "4.10.6.1 State monitoring setting file format (page 251)".

4.10.6.4 Operation log file

The following information is output in the operation log file.

- Import

  The result of checking the import file and import operation

- Export

  The results of the export operation

When operating from the monitoring terminal

The operation log backup file uses the name "*%incrementalnumber%*_ImportExportLog.txt". *%incrementalnumber%* starts at 000 and 1 is added each time. The maximum number is 099.

The operation log of activity, prior to the most recent operation, is saved as a backup.

In cases where the number of backup files has already reached 100, when operation commences, the message "`Delete the backup operation log file`" is displayed and the operation is not performed. Delete all unnecessary backup files and retry the operation.

- The log is stored in the following:

  <On the monitoring terminal, %installfolder%>`\Svc\log\NvPROCsvIOConfig\_ImportExportLog.txt`

- The backup logs are stored in the following:

  <On the monitoring terminal, %installfolder%>`\Svc\log\NvPROCsvIOConfig\ImportExportLog`

When operating from the manager command

The operation log is created using the name "*%incrementalnumber%*_nvpstsmonconf.txt". It stores a maximum of 100 items. *%incrementalnumber%* is a number from 000 to 099. If -log *logfile* argument of the command is specified, the same contents of the operation log file is output to *logfile*.

- The log is stored in the following:

  <On the manager, %installfolder%>`\Manager\log\nvpstsmonconf\`*`%incrementalnumber%`*`_nvpstsmonconf.txt`

4.10.6.5 Error record file

Use the error record file to import only those records that could not be registered or deleted.

Correct the error record file according to the operation log before performing import.

Location of the error record file

Directory

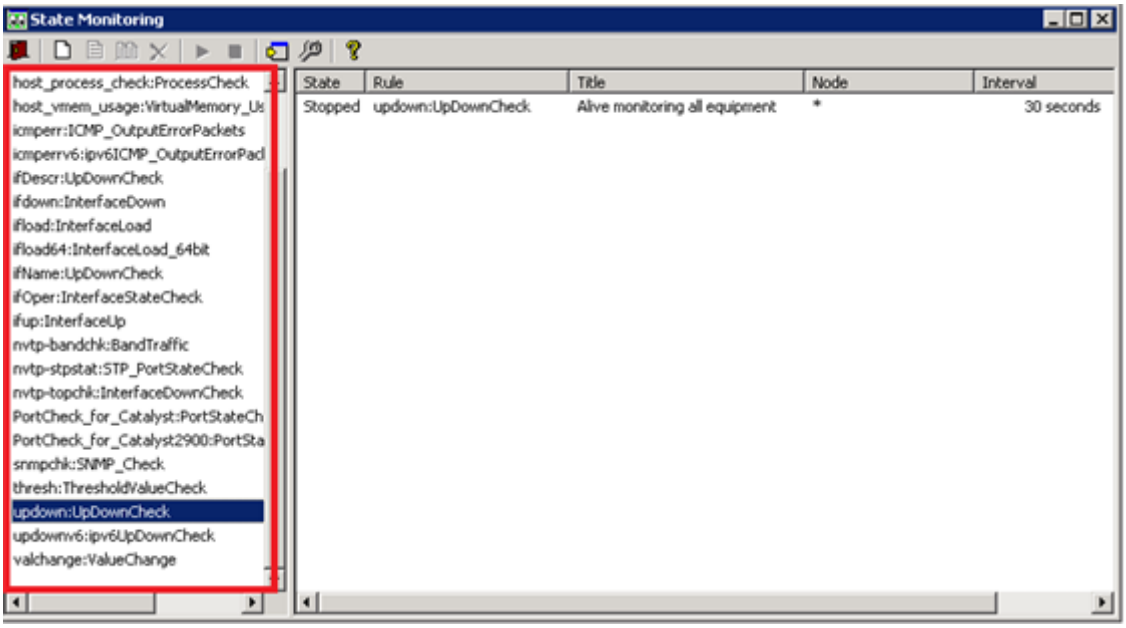
Same directory as the import file

File Name

import_file_name + "TMP" + *.extension*

4.10.7 Embedding rule files

The rule file embedding process involves adding (embedding), and deleting (removing) rules displayed in the rules list of the State Monitoring window.



You must first change to the "configuration mode (page 27)".

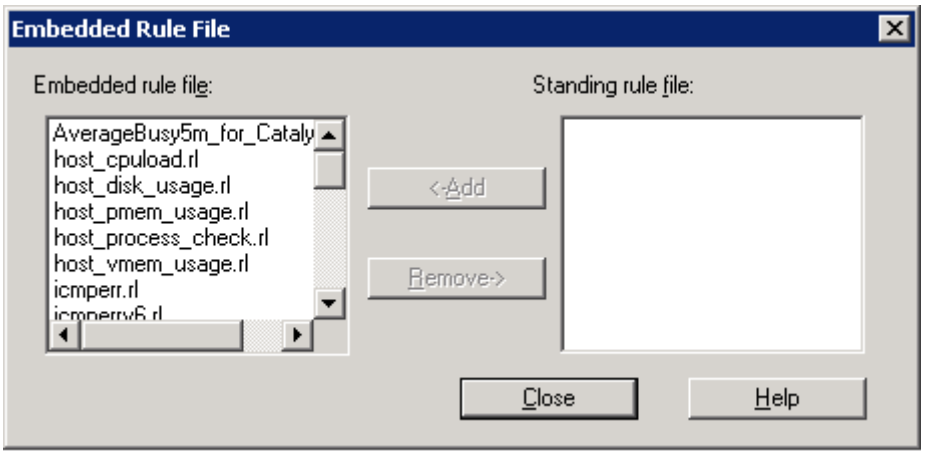
1. Open the "4.10.1 State Monitoring window (page 241)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Fault Management**>**State Monitoring**.

2. Click the **Embedded rule files** button.

3. In the Embedded Rule File dialog box, add a rule file.

   Select a target from the **Standing rule file**, click **<- Add** button to add to the **Embedded rule file** list.



- **Embedded rule file**

  This list displays the embedded rule files. The correlation between rule name and rule file name is described below.

  <Rule name> = <Rule file name without extension>:<Rule ID>

  Example: For rule name "icmperr:ICMP_OutputErrorPacket", the rule file name is "`icmperr.rl`".

- **Standing rule file**

  Displays the non-embedded rule files.

- **<- Add** button

  Moves a selected rule from the **Standing rule file** list to the **Embedded rule file** list.

- **Remove- >** button

  Moves a rule selected in the **Embedded rule file** list to the **Standing rule file** list. If there are rule entries using the target rule file, a removing process will fail.

- **Close** button

  Closes the dialog box.

- **Help** button

  Displays Help.

4. Click **Close** button.

4.11 Monitoring SNMP Traps

4.11.1 Settings for monitoring SNMP traps/informs

By monitoring the SNMP traps/informs (hereinafter referred to as SNMP Trap), the status abnormality of the monitored devices can be detected almost in real time. In order to monitor SNMP Trap by Network Manager, it is necessary to specify the following settings.

- In the settings on the monitored device side, set the SNMP trap send destination to the Manager IP address for Network Manager.
- In the Map View, register the monitored device information.

  For details, refer to "4.2 Creating Network Configuration Map (page 127)".

- When using SNMP v1 or SNMP v2c, in the Environment Setting dialog box, set **SNMP Community Name(v1/v2c)** of **SNMP Trap Parameter** to an appropriate value.

  For details, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

- In order to receive the SNMP inform from SNMPv3, properly specify **EngineID(v3)** of **SNMP Trap Parameter** in the Environment Setting dialog box.

  For details, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

- When using SNMP v3, in the Properties dialog box, register the relevant SNMP v3 information.

  For details, refer to "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)".

- To interpret non-ASCII characters contained in SNMP traps/informs, register an appropriate **SNMP Character Code** in the Properties dialog box.

  For details, refer to "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)".

- Turn the monitoring mode ON.

  For details, refer to "5.13 Starting or Stopping Monitoring by the Monitoring Mode (page 505)".

- When you create a trap definition, you can report SNMP traps/informs with easy-to-understand contents. For details, refer to "4.11.2 Trap definitions (page 260)".

⚠ Caution

If monitoring SNMP traps, there are important points below to consider.

1. Although SNMP inform communication uses UDP as well as SNMP trap communication, it requests a response from an SNMP manager.

   Therefore, the arrival of SNMP inform can be confirmed by the existence of a response, and a resending can also be made. For this reason, relative to SNMP traps, it reduces the possibility of a transmission not being received. It has the advantage of reducing the possibility of a transmission failing to be received.

2. On servers with Network Manager installed, if the SNMP trap receive port (162/udp) conflicts with another product, you will not be able to receive SNMP traps properly.

   On a Windows OS, Network Manager SNMP trap monitoring can coexist with other products using an SNMP trap service if set the system to use the SNMP trap service that comes with the OS.

   For details, refer to "11.4.1 Using the Windows SNMP Trap service (page 776)".

   However, if SNMP Trap Service is used, SNMP informs cannot be received. In order to receive SNMP informs, make sure SNMP trap reception port (162/udp) does not conflict with other products.

4.11.2 Trap definitions

In Network Manager, you can create a "trap definition", which defines the information to be reported when an SNMP trap/inform (hereinafter referred to as an SNMP trap) is received. This allows a received SNMP trap to be reported with easy-to-understand contents.

Trap definitions for some RFC or device vendors are provided by default with the product. If a definition is missing, you can create it based on an MIB file obtained from the device vendor or detailed information on an SNMP trap. You can also edit the notification content, including the definitions provided with the product.

Tip

When an SNMP trap that is not defined in Network Manager is received, an alert is reported as a "enterpriseSpecificTrap" (severity "UNKNOWN").

The Trap Definition Management window is used to perform trap definition operations. The following trap definition operations are available in the Trap Definition Management window.

- Referring to trap definitions

  You can refer to all the trap definitions registered in Network Manager. You can also filter the displayed contents by the parameter values specified in the trap definition. For details, refer to "4.11.3 Referring to trap definitions (page 265)".

- Searching for trap definitions

  Using the Search Matching Definitions window, which can be launched from the Trap Definition Management window, you can search for the trap definition that is applied when an SNMP trap is received. For details, refer to "4.11.4 Searching for trap definitions (page 275)".

- Adding trap definitions

  You can create new trap definitions and also copy and edit built-in trap definitions provided by default. For details, refer to "4.11.5.2 Adding a trap definition (page 290)".

  In addition, trap definitions can be automatically created from MIB files published by the RFC or device vendors. For details, refer to "4.11.6 Creating a trap definition from an MIB file (page 292)".

- Editing trap definitions

  You can edit existing trap definition settings to change the alert notification contents. For details, refer to "4.11.5.3 Editing a trap definition (page 291)".

- Deleting trap definitions

  You can also delete unnecessary trap definitions. For details, refer to "4.11.5.4 Deleting a trap definition (page 291)".

Network Manager select a trap definition for alert notification using the "Enterprise", "SpecificCode", and "GenericCode" values, which are contained in the PDU (Protocol Data Unit) of an SNMP trap, as well as the send source node name. The Trap Definition Management window is used to define and manage alert notification contents for each combination of the "Enterprise", "SpecificCode", "GenericCode", and node.

Tip

- The PDU of SNMPv2c/v3 traps has no "Enterprise", "SpecificCode", or "GenericCode" areas. In Network Manager, when an SNMPv2c/v3 trap is received, the "Value" of "snmpTrapOID.0" in the PDU is converted using a unique method into the same "Enterprise", "SpecificCode", and "GenericCode" formats as for SNMPv1. For details, refer to "7.6 SNMP Trap Identification Method (page 664)".
- In Network Manager, "Enterprise", "SpecificCode", and "GenericCode" are referenced as follows.

Enterprise :	Enterprise ID
SpecificCode :	Specific Trap Code
GenericCode :	Generic Trap Code

4.11.2.1 Trap definition categories

In Network Manager, trap definitions are grouped into the following four categories for management.

- User Definition

  Indicates that the definition was created by a user. You can freely edit or delete trap definitions in this category.

- System Definition

  Indicates that the trap definition was provided by default with Network Manager. You cannot manually edit or delete trap definitions in this category. To modify the information, you need "add by quoting" operation for the definition so as to copy it in the "User Definition" category, and then edit its content.

- MIB Original Definition

  Indicates that the trap definition was automatically created from an MIB file. You cannot manually edit trap definitions in this category. To modify the information, you need "add by quoting" operation for the definition so as to copy it in the "User Definition" category, and then edit its content.

- Incomplete Definition

  Indicates that the trap definition has an incomplete **Enterprise ID**. When a trap definition is automatically created from an MIB file, if the MIB file is missing or has a syntax error, the trap definition may be incomplete because the OID of the Enterprise ID cannot be determined correctly. In such a case, it is registered as a trap definition in the "Incomplete Definition" category.

  Trap definitions in this category do not function as trap definitions unless the OID of **Enterprise ID** is edited correctly. Obtain an appropriate MIB file from the device vendor and automatically create a definition again. Otherwise, determine the correct OID of the Enterprise ID and manually edit the value accordingly.

Tip

- You can register only one trap definition with the same combination of **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** in each category.

  If a trap definition with the same combination already exists in the User Definition category when editing, you must either overwrite it or cancel the editing.

- If a trap definition with the same combination of **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** exists in multiple categories, a trap definition to be applied in alert notification is selected according to the category priority levels. For details on the priority levels, refer to "4.11.2.2 Trap definition priority levels (page 262)".

4.11.2.2 Trap definition priority levels

A trap definition to be applied upon alert notification is selected according to the category priority levels and the priority levels by the **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings.

Priority levels by category

If a trap definition with the same combination of **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** exists in multiple categories, a trap definition to be applied in alert notification is selected according to the category priority levels.

The priority levels by category are set in the following order.

1. User Definition (highest priority)
2. System Definition
3. MIB Original Definition (lowest priority)

Example:

If "Trap definition A" and "Trap definition B" shown below are registered, "Trap definition A" is given higher priority in alert notification.

Parameter	Trap definition A	Trap definition B
Enterprise ID:	*	*
Specific Trap Code:	*	*
Generic Trap Code:	2	2
Node Name:	*	*
Summary:	Interface %1% Down	Interface Down
Category:	User Definition	System Definition
The definition setting of other parameters is not explained in this example.		

Tip

"*" in a trap definition example indicates that any value is allowed.

Priority levels by specified item setting

In Network Manager, you can create trap definitions even with a different combination of **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** for a given SNMP trap.

Example:

To create trap definitions for the necStormRising trap (1.3.6.1.4.1.119.2.3.126.10.2.66.3.1), you can describe them as follows.

Parameter	Trap definition A	Trap definition B
Enterprise ID:	~119.2.3.126.10.2.66.3	~119.2.3.126.10.2.66.3
Specific Trap Code:	1	1
Generic Trap Code:	6	*
Node Name:	*	router01
The definition setting of other parameters is not explained in this example.		

Tip

In the above example, the tilde (~) in **Enterprise ID** represents *"1.3.6.1.4.1"*.

The following describes which definition is given higher priority in an alert notification when both "Trap definition A" and "Trap definition B", shown above, are created.

When an SNMP trap is received, Network Manager checks each trap definition item in the following order.

1. Enterprise ID
2. Generic Trap Code
3. Specific Trap Code

4. Node

In the above check, therefore, a trap definition expressing the target without using "*" is given higher priority.

Example:

When the following trap definitions are created, if an SNMP trap with Enterprise ID: 1.3.6.1.4.1.119.1.84, Specific Trap Code: 3, and Generic Trap Code: 6 is received, "Trap definition A" is selected.

Parameter	Trap definition A	Trap definition B	Trap definition C
Enterprise ID:	~119.1.84	~119.1.84	*
Specific Trap Code:	3	3	3
Generic Trap Code:	6	*	6
Node Name:	*	Router*	Router01
The definition setting of other parameters is not explained in this example.			
Priority:	High	Medium	Low

Specifically, the process is executed as follows.

1. After checking the Enterprise ID, "Trap definition A" and "Trap definition B" are selected as trap definition candidates for alert notification.
2. After checking the Generic Trap Code, only "Trap definition A" remains as a candidate.
3. Since no other candidates are found by other checks, "Trap definition A" remains selected.

Caution

When trap definitions with the same combination of **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Category** but a different **Node** setting exist, and the same node name matches multiple **Node** settings, it may not be possible to determine which definition should be given higher priority.

Example:

When a node called "Router01", belonging to both groups "GrpA" and "GrpB", exists and the following trap definitions are created, it is not possible to determine which definition should be given higher priority for SNMP traps from Router01 only by looking at the parameter settings.

Parameter	Trap definition A	Trap definition B
Enterprise ID:	~119.1.84	~119.1.84
Specific Trap Code:	3	3
Generic Trap Code:	6	6
Node Name:	grp:GrpA	grp:GrpB
Category:	User Definition	User Definition
The definition setting of other parameters is not explained in this example.		

For operational reasons, the creation of the trap definitions shown above is not recommended. Always strive to create trap definitions that are easy to understand.

If the trap definitions shown above are created, Network Manager will determine the priority level based on how they were created. The priority level status determined by Network Manager can be checked in the Search Matching Definitions window. For details, refer to "4.11.4.1 Search Matching Definitions window (page 276)".

4.11.3 Referring to trap definitions

You can refer to all the trap definitions incorporated into Network Manager in the Trap Definition Management window. This section describes the details of the Trap Definition Management window and the trap definition reference operations.

4.11.3.1 Trap Definition Management window

The Trap Definition Management window is the main window used to manage trap definitions.

The Trap Definition Management window is used to perform the following operations.

- Referring to trap definitions
- Adding, editing, and deleting trap definitions
- Searching for trap definitions applied when SNMP traps are received

  (Search Matching Definitions window display)

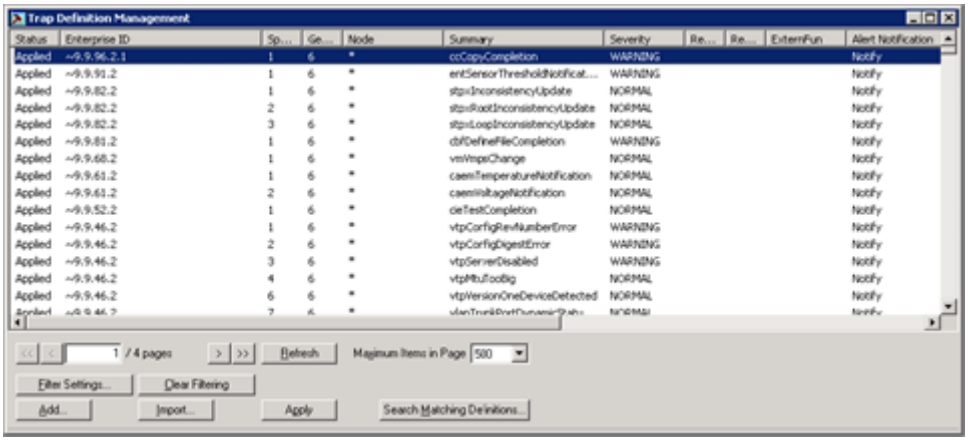
To open the Trap Definition Management window, right-click the **Network View** icon or **Map Management** icon, and select **Fault Management**>**Trap Definition Management** menu.

Immediately after you start the Trap Definition Management window, only the trap definitions defined in Network Manager that satisfy the following conditions are listed.

- Trap definitions for which **Category** is set to a definition other than "Incomplete Definition"
- Trap definitions with a unique setting combination of **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node**
- Trap definitions with a duplicate setting combination of **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** and which are the highest in the "Priority levels by category (page 262)"

Tip

In Network Manager, trap definitions that satisfy the above conditions are referred to as "effective definitions". Trap definitions that do not satisfy the above conditions are referred to as "ineffective definitions".



Items displayed in the trap definition list

- **Status**

  Shows the trap definition application state.

- Applied

  Indicates that the definition has been reflected onto the Network Manager operations.

- Not Applied

  Indicates that the definition has not yet been reflected onto the Network Manager operations and will be applied.

- Deleting

  Indicates that the definition has been reflected onto the Network Manager operations and will be deleted.

- **Enterprise ID**

  Shows the definition setting corresponding to the "Enterprise" value (OID) of the SNMP traps in the complete numerical string type.

  "1.3.6.1.4.1." is replaced by a tilde (~). For example, *"1.3.6.1.4.1.119"* is displayed as *"~119"*.

  "1.3.6.1.2.1." is replaced by a dot (.). For example, *"1.3.6.1.2.1.14.16"* is displayed as *". 14.16"*.

  Characters after 260th character are omitted.

- **Specific Trap Code**

  Shows the definition setting corresponding to the "SpecificCode" value of the SNMP traps.

- **Generic Trap Code**

  Shows the definition setting corresponding to the "GenericCode" value of the SNMP traps.

  The value is 0 to 5 for standard traps.

  It is always 6 for vendor-extended traps.

- **Node**

  Shows the definition setting for a specific node or group to which the trap definition is applied. If the definition is applied to all the nodes, it is displayed as "*".

- **Summary**

  Shows the definition setting of the summary text of an alert to be reported when the target SNMP trap is received.

- **Severity**

  Shows the definition setting of the severity level of an alert to be reported when the target SNMP trap is received.

- **RecoveryNo**

  Shows the definition setting of the number used to identify a trap definition pairing with the auto recovery control definition.

- **RecoveryCondition**

  Shows the definition setting of the varBindList number condition used to identify whether an SNMP trap is the automatic recovery control target.

- **ExternFun**

  Shows the definition setting of the model-specific alert notification control.

Tip

With the current version, one of the following can be defined in **ExternFun** for the trap definition.

- Blank

  Special alert notification control is not performed.

- ChangeCompByIfIndex

  This is a parameter for monitoring Nexus 2000 and reporting an alert to the target Nexus 2000 icon when a linkDown or linkUp trap is received.

- **Alert Notification**

  Shows the definition setting of whether to receive or discard the target SNMP trap.

  - Notify

    Indicates that it receives an SNMP trap that matches the **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings and performs an alert notification process.

  - Not Notify

    Indicates that it does not receive but discards an SNMP trap that matches the **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code** and **Node** definition settings and does not perform any alert notification process.

- **Category**

  Shows the trap definition category. In Network Manager, trap definitions are grouped into the following four categories for management.

  - User Definition

    Indicates that the definition was created by a user.

  - System Definition

    Indicates that the trap definition was provided by default with Network Manager.

  - MIB Original Definition

    Indicates that the trap definition was automatically created from an MIB file.

  - Incomplete Definition

    Indicates that the trap definition has an incomplete **Enterprise ID**.

  For details on the trap definition categories, refer to "4.11.2.1 Trap definition categories (page 261)".

- **Last Modified Date**

  Shows the date on which the trap definition was last modified.

- **Import Date**

  Shows the date on which the trap definition was automatically created from an imported MIB file.

- **MIB File Name**

  Shows the name of the MIB file in which the target SNMP trap is defined. This information is registered when a trap definition is automatically created from an imported MIB file.

- **MIB Module Name**

  Shows the name of the MIB module in which the target SNMP trap is defined. This information is registered when a trap definition is automatically created from an imported MIB file.

Right-click menu in the trap definition list

- **Select All**

  Selects all the trap definitions displayed in the trap definition list (one page).

- **Add by Quoting**

  Displays the Add Trap Definition dialog box in the case of "Configuration mode (page 27)". You can add a new trap definition by copying and editing the selected trap definition setting.

  However, if you select multiple trap definitions, this menu item cannot be selected.

- **Delete**

  Deletes the selected trap definition in the case of "Configuration mode (page 27)". You can select multiple trap definitions.

  If the selection includes a trap definition that cannot be deleted, a confirmation message appears.

  However, if the category of the selected trap definition is "Product Definition", this menu item cannot be selected.

- **Properties**

  If you select multiple trap definitions, this menu item cannot be selected.

  - In the case of "Normal mode (page 27)"

    Displays the Trap Definition Properties dialog box. You can check the detailed information on the selected trap definition.

  - In the case of "Configuration mode (page 27)"

    Displays the Edit Trap Definition dialog box when a trap definition that satisfies all the following conditions is selected. You can edit the selected trap definition setting.

    * When **Category** is "User Definition" or "Incomplete Definition"
    * When **Status** is a state other than "Deleting"

    Displays the Trap Definition Properties dialog box when a trap definition that does not satisfy all the above conditions is selected.

  Tip

  Double-clicking a trap definition performs the same operation as selecting this menu item.

Tip

- If you do "Add by Quoting" for a trap definition, the **Import Date**, **MIB File Name**, **MIB Module Name**, and **MIB File Last Updated** information added to the copied trap definition is also inherited.
- Even when a trap definition is added by quoting, edited, or deleted, it will not be immediately reflected onto the Network Manager operations. To reflect it onto the Network Manager operations, click the **Apply** button to change the trap definition state to "Applied".

Operation button

- **<<** button

  Displays the first page of the trap definition list. When the first page is displayed, this button is disabled.

- **<** button

Displays the previous page of the trap definition list. When the first page is displayed, this button is disabled.

- Page number field

  Displays the page information of the trap definition list. When you specify the page number and then click the **Refresh** button, the contents of the specified page are displayed.

- **>** button

  Displays the next page of the trap definition list. When the last page is displayed, this button is disabled.

- **>>** button

  Displays the last page of the trap definition list. When the last page is displayed, this button is disabled.

- **Refresh** button

  Refreshes the displayed information of the trap definition list.

- **Maximum Items in Page**

  Specify the number of trap definitions displayed in one page of the trap definition list. You can select 50, 100, 250, or 500. The default value is 500.

- **Filter Settings...** button

  Displays the Filter Settings dialog box to filter trap definitions displayed in the trap definition list. For details, refer to "4.11.3.2 Filter Settings dialog box (page 270)".

- **Clear Filtering** button

  Clears the applied filter settings and resets the displayed contents of the trap definition list to the default.

- **Add...** button

  Displays the Add Trap Definition dialog box to add a new trap definition in the case of "Configuration mode (page 27)". For details, refer to "4.11.5.1 Add/Edit/Properties of Trap Definition dialog box (page 282)".

- **Import...** button

  Displays the Import dialog box in the case of "Configuration mode (page 27)". Trap definitions can be automatically created from the MIB files provided by device vendors. For details, refer to "4.11.6.1 Import dialog box (page 293)".

- **Apply** button

  Reflects trap definitions for which **Status** is set to "Not Applied" or "Deleting" onto the Network Manager operations in the case of "Configuration mode (page 27)". If a trap definition that has not been reflected onto the Network Manager operations exists, even when the target SNMP trap is received, the trap definition is not reflected onto the alert notification.

  Caution

  When you click the **Apply** button, all the trap definitions for which **Status** is set to "Not Applied" or "Deleting" are reflected onto the Network Manager operations, and the **Status** changes to "Applied". Check the definitions carefully before clicking the **Apply** button because even those definitions not displayed in the trap definition list may be reflected, depending on the filter settings.

- **Search Matching Definitions...** button

Displays the Search Matching Definitions window to search for the trap definition that is applied when an SNMP trap is received. For details, refer to "4.11.4.1 Search Matching Definitions window (page 276)".

Caution

- When a trap definition is added, edited, or deleted, it is not immediately reflected onto the Network Manager operations but instead is saved with **Status** set to "Not Applied" or "Deleting".

  Check the action of the added, edited, or deleted trap definition in the Search Matching Definitions window and then click the **Apply** button to reflect it onto the actual Network Manager operations.

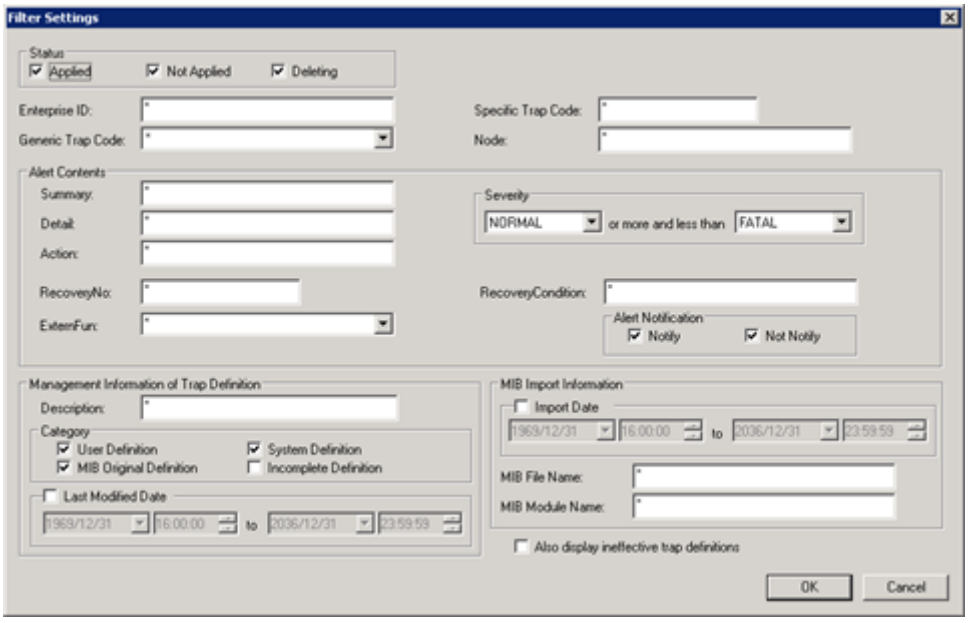
  When you click the **Apply** button, all the trap definitions for which **Status** is set to "Not Applied" or "Deleting" and saved in Network Manager are reflected onto the Network Manager operations. Be sure to check the settings of all the trap definitions for which **Status** is set to "Not Applied" or "Deleting" before clicking the **Apply** button.
- The input values in the Filter Settings dialog box, which is displayed by clicking the **Filter Settings...** button, are retained until you click the **Clear Filtering** button or close the Trap Definition Management window.

  If the displayed information of the trap definition list after making the filter settings is not as you expected, click the **Filter Settings...** button to display the Filter Settings dialog box again and check the validity of the input values.

4.11.3.2 Filter Settings dialog box

This dialog box is used to filter the displayed contents of the trap definition list in the **Trap Definition Management** window by specifying conditions.

To open the Filter Settings dialog box, click the **Filter Settings...** button in the Trap Definition Management window.



Trap definitions that satisfy all the specified item conditions are displayed in the trap definition list of the **Trap Definition Management** window.

- **Status**

  Specify a condition for the State setting of the trap definitions to be displayed.

  - **Applied** checkbox

Displays trap definitions that have been reflected onto the Network Manager operations.

- **Not Applied** checkbox

  Indicates that the definition has not yet been reflected onto the Network Manager operations and will be applied.

- **Deleting** checkbox

  Displays trap definitions that have been reflected onto the Network Manager operations and will be deleted.

When multiple checkboxes are checked, trap definitions that satisfy any of the selected conditions are to be displayed.

- **Enterprise ID**

  Specify a condition for the Enterprise ID setting of the trap definitions to be displayed in the "complete numerical string type (page 646)". The maximum number of characters is 600, and "*" and "?" can be used as wildcards.

  If a tilde (~) is used at the beginning, it is treated as *"1.3.6.1.4.1."* For example, if *"~119"* is specified, it is converted to *"1.3.6.1.4.1.119."*

  If a dot (.) is used at the beginning, it is treated as *"1.3.6.1.2.1."* For example, if *".14.16"* is specified, it is converted to *"1.3.6.1.2.1.14.16."*

- **Specific Trap Code**

  Specify a condition for the Specific Trap Code setting of the trap definitions to be displayed. You can use "*" as a wildcard, which allows all the settings.

- **Generic Trap Code**

  Specify a condition for the Generic Trap Code setting of the trap definitions to be displayed from the following list.

  - *
  - 0 (coldStart)
  - 1 (warmStart)
  - 2 (linkDown)
  - 3 (linkUp)
  - 4 (authentificationFailure)
  - 5 (egpNeighborLoss)
  - 6 (enterpriseSpecific)
  - *

  You can use "*" to allow all the definition settings. To display only those trap definitions for which "*" is set, specify "*".

- **Node**

  Specify a condition for the Node setting of the trap definitions to be displayed. The maximum number of characters is 128, and "*" and "?" can be used as wildcards.

Tip

In the **Node** trap definition, the node component type (node:) is omitted during registration. Therefore, when you specify a condition for the node component, omit the node component type (node:).

- Alert Contents
  - **Summary**

    Specify a condition for the Summary setting of the trap definitions to be displayed. The maximum number of characters is 128, and "*" and "?" can be used as wildcards.
  - **Severity**

    Specify a condition range for the Severity setting of the trap definitions to be displayed.

    Select one of the following from the list.
    * NORMAL
    * UNKNOWN
    * WARNING
    * MINOR
    * MAJOR
    * FATAL
  - **Detail**

    Specify a condition for the Detail setting of the trap definitions to be displayed. The maximum number of characters is 2,000, and "*" and "?" can be used as wildcards.
  - **Action**

    Specify a condition for the Action setting of the trap definitions to be displayed. The maximum number of characters is 1,280, and "*" and "?" can be used as wildcards.
  - **RecoveryNo**

    Specify a condition for the RecoveryNo setting of the trap definitions to be displayed. You can use "*" as a wildcard, which allows all the settings.
  - **RecoveryCondition**

    Specify a condition for the RecoveryCondition setting of the trap definitions to be displayed. The maximum number of characters is 2,000, and "*" and "?" can be used as wildcards.
  - **ExternFun**

    Specify a condition for the ExternFun setting of the trap definitions to be displayed. The maximum number of characters is 2,000, and "*" and "?" can be used as wildcards.

    Tip

    With the current version, one of the following can be defined in **ExternFun** for the trap definition.
    * Blank

      Special alert notification control is not performed.
    * ChangeCompByIfIndex

      This is a parameter for monitoring Nexus 2000 and reporting an alert to the target Nexus 2000 icon when a linkDown or linkUp SNMP trap is received.
  - **Alert Notification**

    Specify a condition for the Receive/Discard SNMP Trap setting of the trap definitions to be displayed.

* **Notify** checkbox

  Displays trap definitions set to notify of an SNMP trap that matches the **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings.

* **Not Notify** checkbox

  Displays trap definitions set not to notify but instead discard an SNMP trap that matches the **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings.

When multiple checkboxes are checked, trap definitions that satisfy any of the selected conditions are to be displayed.

- Management Information of Trap Definition
  - **Description**

    Specify a condition for the Description setting of the trap definitions to be displayed. The maximum number of characters is 4,000, and "*" and "?" can be used as wildcards.

  - **Category**

    Specify a condition for the Category setting of the trap definitions to be displayed.

    * **User Definition** checkbox

      Displays trap definitions created by a user.

    * **System Definition** checkbox

      Displays trap definitions provided by default with Network Manager.

    * **MIB Original Definition** checkbox

      Displays trap definitions automatically created from an MIB file.

    * **Incomplete Definition** checkbox

      Displays trap definitions that have an incomplete **Enterprise ID**.

    When multiple checkboxes are checked, trap definitions that satisfy any of the selected conditions are to be displayed.

  - **Last Modified Date** checkbox

    The condition for the Last Modified Date is enabled when this checkbox is checked.

    Specify a condition range for the Last Modified Date setting of the trap definitions to be displayed in the *YYYY/MM/DD HH:MM:SS* format.

- MIB Import Information
  - **Import Date** checkbox

    The condition for the Import Date is enabled when this checkbox is checked.

    Specify a condition range for the Import Date setting of the trap definitions to be displayed in the *YYYY/MM/DD HH:MM:SS* format.

  - **MIB File Name**

    Specify a condition for the additional information of the MIB File Name setting of the trap definitions to be displayed. The maximum number of characters is 256, and "*" and "?" can be used as wildcards.

  - **MIB Module Name**

Specify a condition for the additional information of the MIB Module Name setting of the trap definitions to be displayed. The maximum number of characters is 256, and "*" and "?" can be used as wildcards.

- **Also display ineffective definitions** checkbox

  Displays trap definitions, including ineffective ones, when this checkbox is checked.

  Tip

  "Ineffective definitions" refer to any of the following trap definitions.

  - Trap definitions with a duplicate setting combination of **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** but which are not the highest in the "priority levels by category (page 262)"
  - Trap definitions for which **Category** is set to "Incomplete Definition"

Tip

- Wildcards can be used as follows.
  - Example: Specify *"1.3.6.1.4.1.119.* "* in **Enterprise ID**.

    In this case, all those trap definitions with the OID starting with *"1.3.6.1.4.1.119. "* In **Enterprise ID** are to be displayed.
  - Example: Specify *"grp:Grp\?"* In **Node**.

    In this case, all those trap definitions with a text string such as *"grp:GrpA "* or *"grp:Grp"* (+ one character) in **Node** are to be displayed.
- To specify "*", "?", or "\" as a text character, use "\" to escape.
  - Example: Specify *"*"* in **Enterprise ID**.

    In this case, all those trap definitions for which **Enterprise ID** is set to *"*"* are to be displayed.
  - Example: Specify *" grp:Grp\?"* In **Node**.

    In this case, all those trap definitions for which **Node** is set to *"grp:Grp?"* are to be displayed.
  - Example: Specify *"*C:*"* in **Action**

    In this case, all those trap definitions for which **Action** contains text string *"C:*"*are to be displayed.

Caution

At least one of the **Status**, **Alert Notification**, and **Category** checkboxes must be checked.

4.11.3.3 Filtering trap definitions to display

You can filter the trap definitions displayed in the trap definition list in the Trap Definition Management window by specifying conditions. The steps are shown below.

1. Open the **Filter Settings** dialog box.

   Click the **Filter Settings** button in the **Trap Definition Management** window.

2. In the **Filter Settings** dialog box, specify the conditions for filtering the trap definitions to be displayed.

   Trap definitions that satisfy all the conditions specified in the **Filter Settings** dialog box are to be displayed.

   For details on the **Filter Settings** dialog box, refer to "4.11.3.2 Filter Settings dialog box (page 270)".

3. Click the **OK** button.

After the above steps have been performed, the displayed contents of the trap definition list in the Trap Definition Management window are filtered.

Tip

If the results of the filtering are not as you expected, click the **Filter Settings** button in the **Trap Definition Management** window again and check the filter conditions specified in the **Filter Settings** dialog box.

The filter conditions specified in the **Filter Settings** dialog box are retained until you click the **Clear Filtering** button or close the Trap Definition Management window.

Operation example

The following shows an operation example of displaying all the trap definitions for which **Status** is set to "Not Applied" or "Deleting".

Tip

Use the following steps to check the status of those trap definitions for which status is set to "Not Applied" or "Deleting", and then click the **Apply** button in the Trap Definition Management window.

1. In the Filter Settings dialog box, specify the filter conditions for the trap definition list.

Parameter	Setting details
Status	Check the **Not Applied** and **Deleting** checkboxes. Uncheck the **Applied** checkbox.
Enterprise ID	Specify "*" to allow all values.
Specific Trap Code	Specify "*" to allow all values.
Generic Trap Code	Specify "*" to allow all values.
Node	Specify "*" to allow all values.
Alert Contents	Specify "*" in **Summary**, **Detail**, **Action**, **RecoveryNo**, **RecoveryCondition**, and **ExternFun** to allow all values. **Severity** should be "NORMAL" or higher and "FATAL" or lower. Also, check both the **Notify** and **Not Notify** checkboxes in **Alert Notification**.
Management Information of Trap Definition	Specify "*" in **Description** to allow all values. Check all the checkboxes in **Category**. Uncheck the **Last Modified Date** checkbox to exclude the last modified date from the filter conditions.
MIB Import Information	Uncheck the **Import Date** checkbox to exclude the import date from the filter conditions. Specify "*" in **MIB File Name** and **MIB Module Name** to allow all values.
Also display ineffective definitions	Check the checkbox.

2. Click the **OK** button.

4.11.4 Searching for trap definitions

In Network Manager, you can create different trap definitions for a given SNMP trap. In an environment in which such trap definitions are created, the Search Matching Definitions window can be used to check the trap definition that is applied when the target SNMP trap is received.

4.11.4.1 Search Matching Definitions window

The Search Matching Definitions window is used to perform the following operations.

- Searching for/referring to trap definitions to be applied when SNMP traps are received

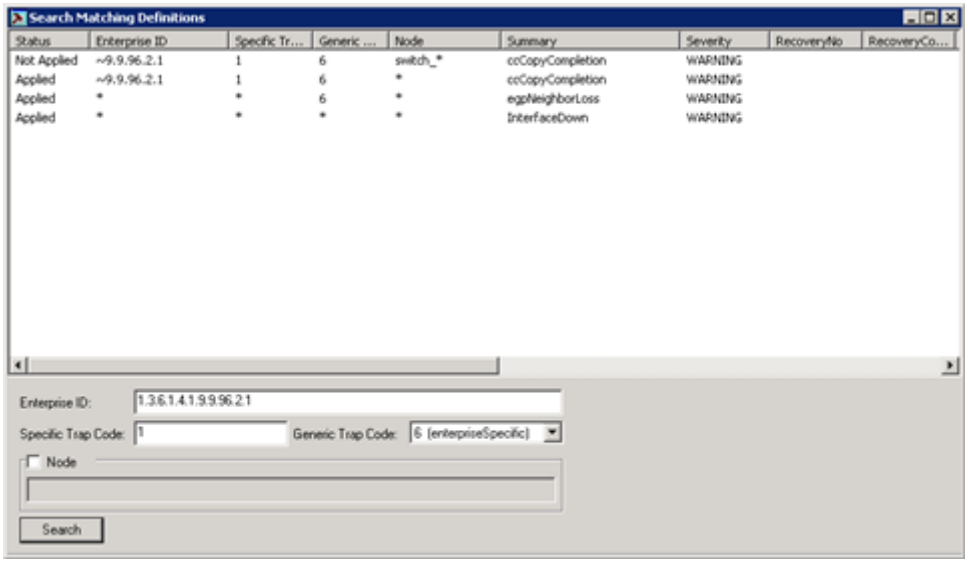
  By specifying the information on the Enterprise ID, Specific Trap Code, Generic Trap Code, and send source node of an SNMP trap, you can search for trap definitions to be applied when the target SNMP trap is received. The search results are displayed in the trap definition list.

- Adding, editing, and deleting trap definitions

  You can add (add by quoting), edit, or delete trap definitions based on the searched trap definition information.

The Search Matching Definitions window can be opened by one of the following operations.

- Click the **Search Matching Definitions** button in the Trap Definition Management window.
- Right-click an alert in the **Alert Management** tab (new alerts list) or **Alert Management** window, and select **Search trap definition**.
- Click the **Search trap definition** button in the **Alert Detail** dialog box.



Tip

The search results show not only the highest-priority trap definition to be applied when the SNMP trap is received but also trap definition candidates in order starting from that with the highest priority. They also include those trap definitions for which **Status** is set to "Not Applied" or "Deleting". Using this search function, you can also determine the effects on the Network Manager operations before clicking the **Apply** button in the Trap Definition Management window.

Operation range

- **Enterprise ID**

  Specify the "Enterprise" value (OID) of an SNMP trap assumed to be received in the complete numerical string type. Up to 600 characters can be specified.

If a value other than "6 (enterpriseSpecific)" is specified in the **Generic Trap Code** field, this parameter can be omitted. When omitted, the OID "1.3.6.1.6.3.1.1.5" of an SNMPv2c/v3 standard trap is specified for the search.

If a tilde (~) is used at the beginning, it is treated as *"1.3.6.1.4.1."* For example, if *"~119 "*is specified, it is converted into *"1.3.6.1.4.1.119"* for the search.

If a dot (.) is used at the beginning, it is treated as 1.3.6.1.2.1. For example, if *".14.16"* is specified, it is converted into *"1.3.6.1.2.1.14.16"* for the search.

Characters after 260th character are omitted.

- **Specific Trap Code**

  Specify the "SpecificCode" of an SNMP trap assumed to be received with a number between *"-2147483648"* and *"2147483647"*.

  If a value other than "6 (enterpriseSpecific)" is specified in the **Generic Trap Code** field, this parameter can be omitted. When omitted, "0" is specified for the search.

- **Generic Trap Code**

  Specify the "GenericCode" of an SNMP trap assumed to be received from the list. The selectable values are shown below.

  - 0 (coldStart)
  - 1 (warmStart)
  - 2 (linkDown)
  - 3 (linkUp)
  - 4 (authentificationFailure)
  - 5 (egpNeighborLoss)
  - 6 (enterpriseSpecific)

  This parameter cannot be omitted.

- **Node** checkbox

  Check this checkbox if you want to search for trap definitions to be applied by assuming a specific node that sends a specified SNMP trap. If unchecked, this condition is disabled.

  You can specify only one node name with a value containing up to 63 characters in the input field.

- **Search** button

  Searches for trap definitions to be applied when the target SNMP trap is received based on the specified SNMP trap conditions and shows them in the trap definition list.

Tip

- The PDU of SNMPv2c/v3 traps has no "Enterprise", "SpecificCode", or "GenericCode" areas. For SNMPv2c/v3 traps, convert the value of "snmpTrapOID.0" into the same "Enterprise", "SpecificCode", and "GenericCode" formats as for SNMPv1, using Network Manager identification method. For details, refer to "7.6 SNMP Trap Identification Method (page 664)".
- When you search for standard traps for which the **Generic Trap Code** is set to 0 to 5, normally use the following values for "Enterprise" and "SpecificCode" of SNMP traps.
  - Enterprise:

For SNMPv1 traps, specify the sysObjectId (1.3.6.1.2.1.1.2.0) value of the send source device. For standard traps from IP8800/S3830, for example, the value would be "1.3.6.1.4.1.21839.1.2.17".

For SNMPv2c/v3 traps, it is "1.3.6.1.6.3.1.1.5".

- SpecificCode:

  For SNMPv1 traps, the value would be "0".

  For SNMPv2c/v3 traps, it is treated as "0" by Network Manager.

Since the value may be different from those above depending on the specification of each monitored device model, if you do not know the value that you should specify in **Enterprise ID** or **Specific Trap Code**, contact the help desk for the device model to determine the value.

Items displayed in the trap definition list

- **Status**

  Shows the trap definition application state.

  - Applied

    Indicates that the definition has been reflected onto the Network Manager operations.

  - Not Applied

    Indicates that the definition has not yet been reflected onto the Network Manager operations and will be applied.

  - Deleting

    Indicates that the definition has been reflected onto the Network Manager operations and will be deleted.

- **Enterprise ID**

  Shows the definition setting corresponding to the "Enterprise" value (OID) of the SNMP traps in the complete numerical string type.

  "1.3.6.1.4.1. " is replaced by a tilde (~). For example, *"1.3.6.1.4.1.119 "* is displayed as *"~119"*.

  "1.3.6.1.2.1." is replaced by a dot (.). For example, *"1.3.6.1.2.1.14.16"* is displayed as *". 14.16."*

- **Specific Trap Code**

  Shows the definition setting corresponding to the "SpecificCode" value of the SNMP traps.

- **Generic Trap Code**

  Shows the definition setting corresponding to the "GenericCode" value of the SNMP traps.

  The value is 0 to 5 for standard traps.

  It is always 6 for vendor-extended traps.

- **Node**

  Shows the definition setting for a specific node or group to which the trap definition is applied. If the definition is applied to all the nodes, it is displayed as "*".

- **Summary**

  Shows the definition setting of the summary text of an alert to be reported when the target SNMP trap is received.

- **Severity**

  Shows the definition setting of the severity level of an alert to be reported when the target SNMP trap is received.

- **RecoveryNo**

  Shows the definition setting of the number used to identify a trap definition pairing with the auto recovery control definition.

- **RecoveryCondition**

  Shows the definition setting of the varBindList number condition used to identify whether an SNMP trap is the automatic recovery control target.

- **ExternFun**

  Shows the definition setting of the model-specific alert notification control.

  Tip

  The current version only supports the display of whether the setting (ChangeCompByIfIndex) to report a linkDown or linkUp trap alert to the Nexus 2000 icon is available.

- **Alert Notification**

  Shows the definition setting of whether to receive or discard the target SNMP trap.

  - Notify

    Indicates that it receives an SNMP trap that matches the **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings and performs an alert notification process.

  - Not Notify

    Indicates that it does not receive but discards an SNMP trap that matches the **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code** and **Node** definition settings and does not perform any alert notification process.

- **Category**

  Shows the trap definition category. In Network Manager, trap definitions are grouped into the following four categories for management.

  - User Definition

    Indicates that the definition was created by a user.

  - System Definition

    Indicates that the trap definition was provided by default with Network Manager.

  - MIB Original Definition

    Indicates that the trap definition was automatically created from an MIB file.

  - Incomplete Definition

    Indicates that the trap definition has an incomplete **Enterprise ID**.

  For details on the trap definition categories, refer to "4.11.2.1 Trap definition categories (page 261)".

- **Last Modified Date**

  Shows the date on which the trap definition was last modified.

- **Import Date**

Shows the date on which the trap definition was automatically created from an imported MIB file.

- **MIB File Name**

  Shows the name of the MIB file in which the target SNMP trap is defined. This information is registered when a trap definition is automatically created from an imported MIB file.

- **MIB Module Name**

  Shows the name of the MIB module in which the target SNMP trap is defined. This information is registered when a trap definition is automatically created from an imported MIB file.

Right-click menu in the trap definition list

- **Select All**

  Selects all the trap definitions displayed in the trap definition list.

- **Add by Quoting**

  Displays the Add Trap Definition dialog box in the case of "Configuration mode (page 27)". You can add a new trap definition by copying and editing the selected trap definition setting.

  However, if you select multiple trap definitions, this menu item cannot be selected.

- **Delete**

  Deletes the selected trap definition in the case of "Configuration mode (page 27)". You can select multiple trap definitions.

  If the selection includes a trap definition that cannot be deleted, a confirmation message appears.

  However, if the category of the selected trap definition is "Product Definition", this menu item cannot be selected.

- **Properties**

  If you select multiple trap definitions, this menu item cannot be selected.

  - In the case of "Normal mode (page 27)"

    Displays the Trap Definition Properties dialog box. You can check the detailed information on the selected trap definition.

  - In the case of "Configuration mode (page 27)"

    Displays the Edit Trap Definition dialog box when a trap definition that satisfies all the following conditions is selected. You can edit the selected trap definition setting.

    * When **Category** is "User Definition" or "Incomplete Definition"
    * When **Status** is a state other than "Deleting"

    Displays the Trap Definition Properties dialog box when a trap definition that does not satisfy all the above conditions is selected.

  Tip

  Double-clicking a trap definition performs the same operation as selecting this menu item.

Tip

- If you do "Add by Quoting" for a trap definition, the **Import Date**, **MIB File Name**, **MIB Module Name**, and **MIB File Last Updated** information added to the copied trap definition is also inherited.

- Even when a trap definition is added by quoting, edited, or deleted, it will not be immediately reflected onto the Network Manager operations. To reflect it onto the Network Manager operations, click the **Apply** button in the Trap Definition Management window to change the trap definition state to "Applied."

4.11.4.2 Searching for trap definitions to be applied when SNMP traps are received

Check which trap definition is used by Network Manager to report an alert when an SNMP trap is received.

1. Display the **Trap Definition Management** window.

   Right-click the **Network View** icon or **Map Management** icon, and select **Fault Management**>**Trap Definition Management** menu.

2. In the Trap Definition Management window, click the **Search Matching Definitions** button to display the Search Matching Definitions window.

3. In the Search Matching Definitions window, specify the SNMP trap parameters.

   Specify the Enterprise ID, Specific Trap Code, and Generic Trap Code parameters of the SNMP trap.

4. Specify **Node**, which is the SNMP trap send source, as necessary.

   a. Check the **Node** checkbox.

   b. Specify the send source node in the **Node** input field.

5. Click the **Search** button.

Tip

If the Search Matching Definitions window is displayed using the following steps, the trap definition list shows the search results obtained with the target alert SNMP information specified.

- Right-click an alert in the **Alert Management** tab (new alerts list) or the **Alert Management** window, and select **Search trap definition**.
- Click the **Search trap definition** button in the **Alert Detail** dialog box.

Operation example

The following shows an operation example of searching for trap definitions applied by Network Manager when the SNMPv2c trap *"ciscoEnvMonFanNotification (1.3.6.1.4.1.9.9.13.3.0.4)"*, which indicates a fan fault, is sent from a node called *"Cisco001"*.

1. In the Search Matching Definitions window, specify the information for the ciscoEnvMonFanNotification trap.

   Enterprise ID 1.3.6.1.4.1.9.9.13.3

   Specific Trap Code 4

   Generic Trap Code 6

   ### Tip

   You can also specify *"~9.9.13.3"* using a tilde (~) in **Enterprise ID**.

2. Specify *"Cisco001"* for the node.

a. Check the **Node** checkbox.

b. Specify *"Cisco001"* in the **Node** input field.

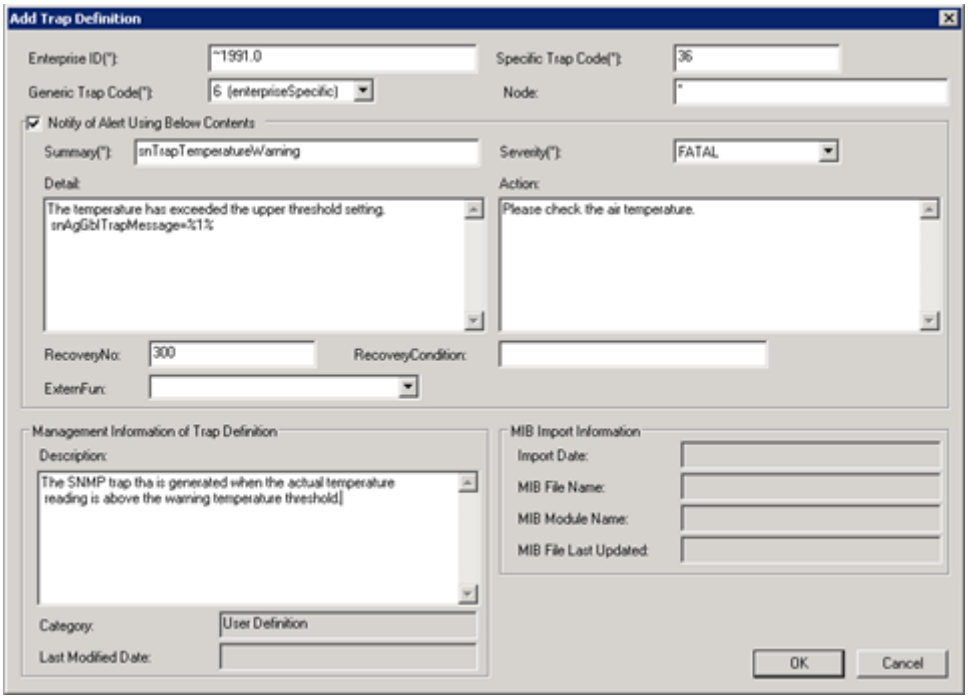
3. Click the **Search** button.

4.11.5 Adding, editing, or deleting trap definitions

In Network Manager, trap definitions for some RFC or device vendors are provided by default with the product. Any other required trap definitions can be freely added during operation. You can also modify a built-in trap definition or delete a trap definition that has become unnecessary due to a change in the models being monitored.

4.11.5.1 Add/Edit/Properties of Trap Definition dialog box

In the Add/Edit/Properties of Trap Definition dialog box, which can be displayed from the Trap Definition Management or Search Matching Definitions window, you can add or edit trap definitions or refer to detailed information.



- SNMP trap identification information:

  - **Enterprise ID**

    Shows the definition setting corresponding to the "Enterprise" value (OID) of SNMP traps in the "complete numerical string type (page 646)" or with "*" which corresponds to any character.

    * Input operation

      Specify a value containing up to 598 characters in the "complete numerical string type (page 646)" or "*" which can correspond to any character.

      If a tilde (~) is used at the beginning, it is treated as *"1.3.6.1.4.1."*. For example, if *"~119"* is specified, it is registered as *"1.3.6.1.4.1.119."*

If a dot (.) is used at the beginning, it is treated as *"1.3.6.1.2.1."*. For example, if *". 14.16"* is specified, it is registered as *"1.3.6.1.2.1.14.16"*.

Tip

* If a tilde (~) or dot (.) is used at the beginning, it is counted not as one character but as the number of characters of *"1.3.6.1.4.1."* or *"1.3.6.1.2.1."* after expansion.
* If the end of an input value is ".0", the maximum number of characters that can be registered is 598, excluding ".0".
* If this dialog box is displayed from the **Add by Quoting** menu or **Properties** menu, a tilde (~) or dot (.) at the beginning is not displayed but is expanded to *"1.3.6.1.4.1."* or *"1.3.6.1.2.1."*.

- **Specific Trap Code**

Shows the definition setting corresponding to the "SpecificCode" value of SNMP traps with a numerical value or "*" which can correspond to any character.

* Input operation

  Specify a number between *"-2147483648"* and *"2147483647"* or "*" which can correspond to any character.

- **Generic Trap Code**

Shows the definition setting corresponding to the "GenericCode" value of SNMP traps.

* Input operation

  Select one of the following from the list.

  + *
  + 0 (coldStart)
  + 1 (warmStart)
  + 2 (linkDown)
  + 3 (linkUp)
  + 4 (authentificationFailure)
  + 5 (egpNeighborLoss)
  + 6 (enterpriseSpecific)

- **Node**

Shows the definition setting for a specific node or group to which the target trap definition is applied in the "standard component name specification format (page 645)".

* Input operation

  Specify a value containing up to 128 characters in the "standard component name specification format (page 645)". If omitted, "*" which can correspond to any node, is specified.

  Caution

  + In this parameter, you cannot specify multiple components combined with a comma (,), which are supported in the "standard component name specification format (page 645)".
  + Even if a value is specified with the node component type (node:) expressly added, the node component type is omitted when a trap definition is registered.

- **Notify of Alert Using Below Contents** checkbox

  Shows the definition setting as to whether to receive the SNMP trap and report an alert or not to receive but discard it when an SNMP trap that matches the specified **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings is received.

  Uncheck this checkbox when you do not want to receive the SNMP trap and instead want to discard it.

  ### Tip

  If this checkbox is unchecked, Network Manager does not perform any alert process including recording and reporting of the target SNMP trap. In addition, the items in the frame are disabled.

  - **Summary**

    Shows the text string indicating the summary information of an alert to be reported when an SNMP trap that matches the specified **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings is received.

    * Input operation

      The maximum number of input characters is 128. A Unicode surrogate pair character is counted as two characters.

      You can specify a substitute string to display the varBindList values of a received SNMP trap individually. For details on the substitute strings, refer to "Display of varBindList information (page 288)".

      #### Tip

      + If you specify a substitute string, you must define it so that the number of characters in the string after substitution in the alert message does not exceed 128.
      + Any white space characters after an input value will be deleted during registration.

  - **Severity**

    Shows the severity level of an alert to be reported when an SNMP trap that matches the specified **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings is received.

    * Input operation

      Select one of the following from the list.

      + NORMAL
      + UNKNOWN
      + WARNING
      + MINOR
      + MAJOR
      + FATAL

  - **Detail**

    Shows the text string indicating the detailed information of an alert to be issued when an SNMP trap matching the definitions specified for **Enterprise ID**, **GenericCode**, **SpecificCode**, and **Node** is received.

    * Input operation

The maximum number of input characters is 2,000. A Unicode surrogate pair character is counted as two characters.

Notification contents can include line breaks and tabs. A line break is counted as two characters, and a tab is counted as one character.

You can specify a substitute string to display the varBindList values of a received SNMP trap individually or display all the varBindList values in order. For details on the substitute strings, refer to "Display of varBindList information (page 288)".

Tip

+ When you specify a substitute string, you must define it so that the number of characters in the string after expansion does not exceed 2,000 upon alert notification.
+ To input a line break, press the Enter key while holding down the Ctrl key.
+ To input a tab, press the Tab key while holding down the Ctrl key.
+ Any white space characters after an input value will be deleted during registration.

- **Action**

Shows the text string indicating the action information of an alert to be reported when an SNMP trap that matches the specified **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings is received.

* Input operation

The maximum number of input characters is 1,280. A Unicode surrogate pair character is counted as two characters.

Notification contents can include line breaks and tabs. A line break is counted as two characters, and a tab is counted as one character.

You can also specify a substitute string to display the varBindList values of a received SNMP trap individually. For details on the substitute strings, refer to "Display of varBindList information (page 288)".

Tip

+ When you specify a substitute string, you must define it so that the number of characters in the substitute string after expansion does not exceed 1,280 upon alert notification.
+ To input a line break, press the Enter key while holding down the Ctrl key.
+ To input a tab, press the Tab key while holding down the Ctrl key.
+ Any white space characters after an input value will be deleted during registration.

- **RecoveryNo**

Shows the definition setting of the number used to identify a trap definition pairing with the auto recovery control definition. Network Manager performs auto recovery control with a pair of two trap definitions, each having the same number.

For trap definitions having the same **RecoveryNo**, the one with a severity of "NORMAL" is regarded as the definition for recovery alert notification, while the other with a severity other than "NORMAL" is regarded as the definition for abnormal alert notification. If an abnormal alert is reported and then followed by a recovery alert with the same **RecoveryNo**, the alert is automatically recovered.

* Input operation

Specify a single-byte number between *"1"* and *"4,294,967,295"*. Set the same **RecoveryNo** for those trap definitions that correspond to alert and recovery SNMP traps for the same incident.

⚠ Caution

If **RecoveryNo** or **RecoveryCondition** is changed during an operation, an alert reported before the change cannot be automatically recovered. In such a case, recover it manually.

- **RecoveryCondition**

  Shows the definition setting of the varBindList number condition used to identify whether an SNMP trap is the automatic recovery control target. This is used when it cannot be determined, with **RecoveryNo** alone, that an SNMP trap to form a pair has been received.

  In the case of a linkDown or linkUp SNMP trap, "ifIndex", which is contained in the first information of varBindList, indicates the interface on which the incident occurred. Therefore, in this case, the first value in varBindList is used to determine if the SNMP trap forms a pair. You can use this parameter to automatically recover from such an SNMP trap alert.

  * Input operation

    Specify the n-th value of varBindList with a single-byte number to determine if the trap forms a pair. To determine the other part of the pair using multiple varBindList values, delimit them with a comma (,).

    Example: 1,3

    If **RecoveryNo** is not set, this parameter value is ignored.

- **ExternFun**

  Shows the definition setting of the model-specific alert notification control.

  * Input operation

    Select one of the following. Normally, specify nothing.

    + Blank (Nothing specified)

      Special alert notification control is not performed.

    + ChangeCompByIfIndex

      This is a parameter to monitor Nexus 2000 and report an alert to the target Nexus 2000 icon when a linkDown or linkUp trap is received.

• Management Information of Trap Definition:

- **Description**

  Shows the description of an SNMP trap that matches the specified **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings.

  If a trap definition is automatically created from an imported MIB file, the DESCRIPTION of an SNMP trap defined in the MIB file is output.

  * Input operation

    The maximum number of input characters is 4,000. A Unicode surrogate pair character is counted as two characters.

    Description contents can include line breaks and tabs. A line break is counted as two characters, and a tab is counted as one character.

Tip

+ To input a line break, press the Enter key while holding down the Ctrl key.
+ To input a tab, press the Tab key while holding down the Ctrl key.
+ Any white space characters after an input value will be deleted during registration.

- **Category**

  Shows the trap definition category. In Network Manager, trap definitions are grouped into the following four categories for management.

  * User Definition

    Indicates that the definition was created by a user.

  * System Definition

    Indicates that the trap definition was provided by default with Network Manager.

  * MIB Original Definition

    Indicates that the trap definition was automatically created from an MIB file.

  * Incomplete Definition

    Indicates that the trap definition has an incomplete **Enterprise ID**.

  For details on the trap definition categories, refer to "4.11.2.1 Trap definition categories (page 261)".

  This parameter cannot be edited.

- **Last Modified Date**

  Shows the date when the trap definition was last modified.

  This parameter cannot be edited.

• MIB Import Information:

- **Import Date**

  Shows the date when the trap definition was automatically created from an imported MIB file.

  This parameter cannot be edited.

- **MIB File Name**

  Shows the name of an MIB file in which the target SNMP trap is defined. This information is registered when a trap definition is automatically created from an imported MIB file.

  This parameter cannot be edited.

- **MIB Module Name**

  Shows the name of an MIB module in which the target SNMP trap is defined. This information is registered when a trap definition is automatically created from an imported MIB file.

  This parameter cannot be edited.

- **MIB File Last Updated**

  Shows the date on which an MIB file, in which the target SNMP trap is defined, was last updated. This information is registered if the "LAST-UPDATED" definition of the

"MODULE-IDENTITY" macro is defined in the target MIB file when a trap definition is automatically created from an imported MIB file.

This parameter cannot be edited.

- **OK** button

  Registers the set value.

  If, however, the **Receive This SNMP Trap** checkbox is unchecked, the following is registered.

  - Adding a trap definition (including "adding by quoting") with the checkbox unchecked:

    Blank (only with severity NORMAL) is registered.

  - Editing a trap definition with the checkbox unchecked:

    The contents before editing are registered.

- **Cancel** button

  Cancels the registration.

Display of varBindList information

Trap definitions use the following substitute strings to display varBindList information.

- Substitute string to display individually:

  The following three methods can be used to specify this string.

  - %<*value-order*>%

    Replaces the string with a value specified in <*value-order*> in varBindList to report an alert.

  - %D<*value-order*>%

    Regards a value specified in <*value-order*> in varBindList as ifIndex, and replaces the string with the interface name (ifDescr setting) corresponding to the ifIndex to report an alert.

    Tip

    The interface property information of the target node is used to replace the string with the interface name. Therefore, you must register the interface property information before starting operation.

  - %<*value-order*>:<*type*>%

    Regards a value specified in <*value-order*> in varBindList as a data type specified in <*type*> when the value is a text string, and replaces the string to report an alert.

    The following data types can be specified in <*type*>.

    * NetworkAddress
    * PhysAddress
    * Ipv6Address
    * Ipv6AddressPrefix
    * Ipv6AddressIfIdentifier
    * OctetString

Tip

* If the varBindList value is a text string, the alert notification text may be corrupted because the varBindList data type cannot be correctly determined only from information contained in a received SNMP trap. To prevent this text corruption, you must specify the correct <*type*>.
* If the varBindList value is a text string and <*type*> is not specified in the varBindList display definition of the trap definition, the data type is determined to be "DisplayString".

Caution

The varBindList format varies depending on the SNMP version. The method of specifying the order for each SNMP version in Network Manager is shown below.

SNMP version	varBindList order and description method during reference				
	First	Second	Third	Fourth	Fifth
v1	%1%	%2%	%3%	%4%	%5%
V2c and v3	sysUpTime.0 (Not displayed)	snmpTrapOID.0 (Not displayed)	%1%	%2%	%3%

- Substitute string to display all in order:

  The following two methods can be used to specify this string.

  - %all

    Displays all the values contained in varBindList, in order, in the following format.

    ```
    <1st-MIB-name-in-varBindList>=<1st-value-in-varBindList>
    <2nd-MIB-name-in-varBindList>=<2nd-value-in-varBindList>
     :
    ```

    Example:

    ```
    iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.
    ifEntry.ifIndex=10001
    iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.
    ifEntry.ifDescr=FastEthernet0/1
    ```

  - %allleaf

    Displays all the values contained in varBindList, in order, in the following format.

    ```
    [1]<1st-MIB-leaf-name-in-varBindList>=<1st-value-in-varBindList>
    [2]<2nd-MIB-leaf-name-in-varBindList>=<2nd-value-in-varBindList>
     :
    ```

    Example:

    ```
    [1]ifIndex=10001
    [2]ifDescr=FastEthernet0/1
    ```

    If an MIB required to solve an MIB name contained in varBindList is not incorporated into Network Manager, the value is represented by a combination of a solvable MIB name and numbers.

    Example:

    ```
    [1]ciscoMgmt.106.1.2.1.1.15=6
    ```

Tip

If varBindList contains text string information, alert notification text may be corrupted unless an MIB definition (data type definition) related to this item is incorporated into Network Manager in advance. For details on incorporating MIB definitions, refer to "7.4 Adding MIBs (page 648)".

Caution

1. If varBindList may contain a non-ASCII text string, you must set **SNMP Character Code** in the Properties dialog box for the node in advance. For details, refer to "4.2.2.1 Manual Register dialog box and Properties dialog box (page 140)".
2. If varBindList contains information that should be displayed in hexadecimal format, the alert notification text may be corrupted unless the data type is expressly specified as "OctetString". Specify "%<*value-order*>:OctetString%", or refer to "7.4.1.4 MIB Definition hexadecimal notation setting procedure (page 655)" and set it to be displayed in hexadecimal format.

4.11.5.2 Adding a trap definition

The following two methods can be used to manually create a trap definition.

- Creating a new trap definition
- Quoting an existing trap definition and editing it as a new trap definition

The method used to display the Add Trap Definition dialog box is different for each. The detailed steps are shown below.

You must first change to "configuration mode (page 27)".

1. Open the **Add Trap Definition** dialog box.
   - To create a new trap definition, click the **Add** button in the Trap Definition Management window.
   - To copy an existing trap definition and edit it as a new trap definition, right-click a trap definition in the trap definition list in the Trap Definition Management or Matching Definition Search window and then select the **Add by Quoting** menu.
   - When you click the **Add trap definition** button in the Alert Detail dialog box or right-click an alert in the alert list and then select the **Add trap definition** menu, the Add Trap Definition dialog box appears with the "Enterprise ID", "Specific Trap Code", "Generic Trap Code", and "Node" values set for the alert.
2. Specify the trap definition parameters in the **Add Trap Definition** dialog box.

   For details on the Add Trap Definition dialog box, refer to "4.11.5.1 Add/Edit/Properties of Trap Definition dialog box (page 282)".
3. Click the **OK** button in the **Add Trap Definition** dialog box.

   The trap definition is saved with the state "Not Applied".

   ### Tip

   The Search Matching Definitions window can be used to check whether the target trap definition is applied as expected when an SNMP trap is received. For details, refer to "4.11.4.2 Searching for trap definitions to be applied when SNMP traps are received (page 281)".
4. Click the **Apply** button in the **Trap Definition Management** window.

   The apply operation will reflect the target trap definition to the Network Manager operations.

Caution

When you click the **Apply** button, all those trap definitions for which **Status** is set to "Not Applied" or "Deleting" are reflected onto the Network Manager operations, and the **Status** changes to "Applied". Check the definitions carefully before clicking the **Apply** button because even those definitions that are not displayed in the trap definition list may be reflected depending on the filter settings.

4.11.5.3 Editing a trap definition

Edit an existing trap definition.

Tip

If, for a trap definition, **Category** is set to "System Definition" or "MIB Original Definition", you cannot edit the trap definition.

You must first change to "configuration mode (page 27)".

1. Open the Edit Trap Definition dialog box.

   Right-click a trap definition in the trap definition list in the Trap Definition Management or Search Matching Definitions window and then select the **Properties** menu.

2. Edit the trap definition parameters in the **Edit Trap Definition** dialog box.

   For details on the Edit Trap Definition dialog box, refer to "4.11.5.1 Add/Edit/Properties of Trap Definition dialog box (page 282)".

3. Click the **OK** button in the **Edit Trap Definition** dialog box.

   The trap definition is saved with the state "Not Applied".

   Tip

   The Search Matching Definitions window can be used to check whether the target trap definition is applied as expected when an SNMP trap is received. For details, refer to "4.11.4.2 Searching for trap definitions to be applied when SNMP traps are received (page 281)".

4. Click the **Apply** button in the **Trap Definition Management** window.

   The apply operation will reflect the target trap definition to the Network Manager operations.

   Caution

   When you click the **Apply** button, all those trap definitions for which **Status** is set to "Not Applied" or "Deleting" are reflected onto the Network Manager operations, and the **Status** changes to "Applied". Check the definitions carefully before clicking the **Apply** button because even those definitions that are not displayed in the trap definition list may be reflected depending on the filter settings.

4.11.5.4 Deleting a trap definition

Delete an existing trap definition.

Tip

- If, for a trap definition, **Category** is set to "System Definition", you cannot delete the trap definition.
- This section describes how to delete a trap definition in the Trap Definition Management window although it can also be deleted in the Search Matching Definitions window.

You must first change to "configuration mode (page 27)".

1. Open the **Trap Definition Management** window.

   Right-click the **Network View** or **Map Management** icon, and then select **Fault Management**>**Trap Definition Management** menu.

2. Display the trap definition you want to delete in the trap definition list.

   a. Open the **Filter Settings** dialog box.

      Click the **Filter Settings...** button in the **Trap Definition Management** window.

   b. Specify the conditions for the trap definition you want to delete in the **Filter Settings** dialog box.

      For example, specify the conditions for the work period in the **Last Modified Date** or **Import Date** parameter and for the model in the **Enterprise ID** or **MIB Module Name** parameter.

      For details on the **Filter Settings** dialog box, refer to "4.11.3.2 Filter Settings dialog box (page 270)".

   c. Click the **OK** button in the **Filter Settings** dialog box.

3. Right-click the trap definition you want to delete in the trap list and then select the **Delete** menu.

   Tip

   You can also select all of the displayed trap definitions by selecting the **Select All** menu.

   The trap definition is saved with the state "Deleting".

4. Click the **Apply** button in the **Trap Definition Management** window.

   The deletion of the target trap definition will be reflected onto the Network Manager operations.

   Caution

   When you click the **Apply** button, all those trap definitions for which **Status** is set to "Not Applied" or "Deleting" are reflected onto the Network Manager operations, and the **Status** changes to "Applied". Check the definitions carefully before clicking the **Apply** button because even those definitions that are not displayed in the trap definition list may be reflected depending on the filter settings.

4.11.5.5 Adding, updating, or deleting all trap definitions at once

You can perform an operation on all the trap definitions at once from an external file using the commands on the manager.

For details on the commands, refer to "9.6 Trap Definition Operation Commands (page 700)".

4.11.6 Creating a trap definition from an MIB file

A trap definition can be automatically created from an imported MIB file that is published by an RFC or device vendor.

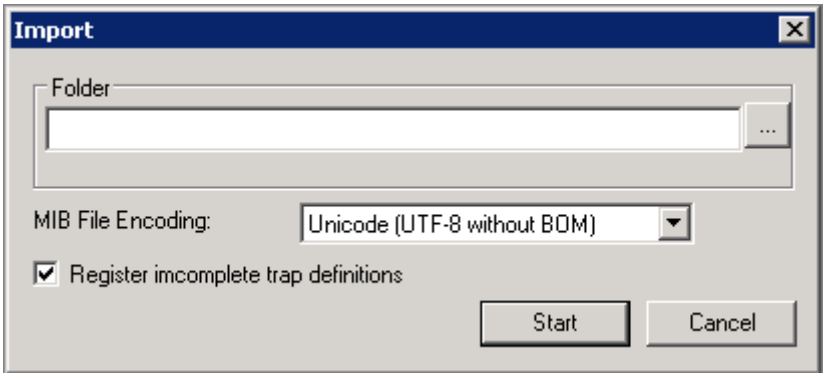
You can import MIB files using the Import dialog box.

You can also import them by using "9.6.2 Trap definition auto generation command (nvpmib2trapdef) (page 710)".

4.11.6.1 Import dialog box

The Import dialog box is used to read MIB files contained in a specified folder and automatically create a Network Manager trap definition from the SNMP trap information defined in the target MIB file.

The Import dialog box appears when you click the **Import...** button in the Trap Definition Management window.



- **Folder**

  Specify a folder containing the MIB files to be imported.

  Manually enter a folder path in the input field or click the **...** button and then select a folder.

  Caution

  - Do not place files other than MIB files in the specified folder. If a file is found to be a non-MIB file, analysis is stopped for that file and moves to the next file. However, depending on the file contents, the entire process may be affected.
  - Files under subfolders in the specified folder are not imported.

    File names in the specified folder that satisfy any of the following conditions are also not imported.

    * File names starting with a dot (.)
    * File names starting or ending with the "#" symbol
    * File names ending with a tilde (~)
  - Only ASCII or standard OS multi-byte character code are acceptable for a folder name containing imported MIB files and MIB file names.

- **MIB File Encoding**

  Select the character code used to encode imported MIB files from the list. The following can be specified for the character code.

  - Unicode (UTF-8 without BOM)

- **Register incomplete trap definitions** checkbox

  If the MIB file is missing or has a syntactically incorrect definition, the trap definition may be incomplete because the OID of the Enterprise ID cannot be determined correctly. In such a case, specify whether to register an incomplete trap definition.

  When this checkbox is checked, a trap definition is registered even if it is incomplete.

Tip

- Normally, when a trap definition is automatically created from an MIB file, it is registered with the category "MIB Original Definition". If a trap definition is incomplete, it is registered with the category "Incomplete Definition".
- Trap definitions registered with the category "Incomplete Definition" do not function as trap definitions unless the OID of the Enterprise ID is edited correctly. Obtain an appropriate MIB file from the device vendor and automatically create the definition again. Otherwise, determine the correct OID of the Enterprise ID and manually edit the value accordingly.

- **Start** button

  Reads all the MIB files contained in the specified folder and creates trap definitions from the SNMP trap information defined in the target MIB files.

- **Cancel** button

  Closes the dialog box and cancels the analysis of the specified MIB files.

Caution

- In the Import dialog box, trap definitions are registered after all the MIB files under the specified folder have been analyzed. When you click the **Start** button to start the process, you can cancel the process with the **Cancel** button while MIB files are being analyzed. You cannot, however, cancel it while trap definitions are being registered. Even if you close the Import dialog box, trap definition registration continues.
- When trap definition registration starts after MIB file analysis, the process for any operation to update the Trap Definition Management window or search operation in the Search Matching Definitions window is temporarily halted. Once trap definition registration completes, the halted process will restart.
- If you store MIB files from many models in the same folder and import all of them at once, MIB file analysis and trap definition registration may take a long time to complete. If a timeout message appears during import, store the MIB files in different folders for each model and import them again.
- The following MIB files cannot be correctly analyzed.
  - When the line break code in the file description is other than CRLF or LF

    In this case, the target file analysis is skipped because the file is not recognized as being an MIB file. You must, in this case, convert the line break code to a CRLF or LF in advance, using a text editor.
  - When multiple MIB modules are defined in one file

    In this case, the second and subsequent MIB modules cannot be analyzed. You must, therefore, separate the file for each MIB module in advance.

    Example: When MIB file *"AB-MIB.txt"* has the following description

```
A-MIB DEFINITIONS ::= BEGIN
:
END
B-MIB DEFINITIONS ::= BEGIN
:
END
```

    Separate it into the following two files.

    A-MIB.txt:

```
A-MIB DEFINITIONS ::= BEGIN
:
END
```

    B-MIB.txt:

```
B-MIB DEFINITIONS ::= BEGIN
:
END
```

4.11.6.2 Automatically creating a trap definition from an MIB file

Import MIB files and automatically create trap definitions.

Tip

- Prepare all the MIB files related to the monitored device in advance. If any MIB file is missing, trap definitions may not be created correctly.
- Do not place unnecessary files such as non-MIB files in the folder containing the MIB files to be imported.

You must first change to "configuration mode (page 27)".

1. Display the **Trap Definition Management** window.

   Right-click the **Network View** or **Map Management** icon, and then select **Fault Management**>**Trap Definition Management** menu.

2. Click the **Import** button in the **Trap Definition Management** window.

3. In the Import dialog box, specify a folder in which to store imported MIB files.

   Click the **...** button and then select a folder in which to store imported MIB files.

4. In the Import dialog box, specify a character code in **MIB File Encoding**.

   The default value is "Unicode (UTF-8 without BOM)".

5. Check the **Register incomplete trap definitions** checkbox as necessary.

   When checked, even if an MIB file is missing or has a syntax error, a trap definition is created based on the results of the MIB analysis.

6. Click the **Start** button.

7. Check the messages output during MIB analysis.

   When a message is output during MIB analysis, check whether it indicates any problems.

   If an error is output, contact the device vendor providing the MIB file depending on the error description.

8. Display a trap definition automatically created from the MIB file in the **Trap Definition Management** window.

   a. Display the Filter Settings dialog box.

      Click the **Filter Settings** button.

   b. Specify the parameters.

      Set **Status** to "Not Applied", **Category** to "MIB Original Definition", and other conditions to allow all values, and then click the **OK** button.

9. Check the details of the trap definition automatically created from the MIB files.

   Double-clicking a trap definition in the trap definition list displays the Trap Definition Properties dialog box.

Select the **Add by Quoting** menu and then edit the definition as necessary. For details, refer to "4.11.5.2 Adding a trap definition (page 290)".

10. Click the **Apply** button.

    Reflect the created trap definition onto the Network Manager operations.

⚠ Caution

When you click the **Apply** button, all those trap definitions for which **Status** is set to "Not Applied" or "Deleting" are reflected onto the Network Manager operations, and the **Status** changes to "Applied". Check the definitions carefully before clicking the **Apply** button because even those definitions that are not displayed in the trap definition list may be reflected depending on the filter settings.

4.11.6.3 Description of a trap definition automatically created from an MIB file

When a trap definition is automatically created from an MIB file, it is registered as follows.

Parameter	Description of setting
Enterprise ID	An OID value is set based on the MIB file analysis results. If the Enterprise ID is not correctly determined, the value would be as follows. `<Unknown :%unsolved-identifier%>.%solved-OID%` Example: `<Unknown :panCommonMib>.3.2` In the above case, you must check the OID corresponding to panCommonMib and then manually modify the value.
Specific Trap Code	A numerical value is set based on the MIB file analysis results.
Generic Trap Code	Normally, "6" is set.
Node	"*" is set.
Summary	An SNMP trap name is set based on the MIB file analysis results. The value would be the object name defined in TRAP-TYPE or NOTIFICATIONTYPE in the MIB file.
Severity	"NORMAL" is set. You must change the setting manually, as necessary.
Detail	An object name and a substitute string in varBindList contained in the target SNMP trap are set based on the MIB file analysis results, as follows. `%first-MIB-leaf-name-in-varBindList%=%1%` `%second-MIB-leaf-name-in-varBindList%=%2%` `:` If the MIB data in varBindList is a text string, a substitute string matching that data type is set. Example: `ifPhysAddress=%1:PhysAddress%`
Action	No value is set.
RecoveryNo	No value is set.

Parameter	Description of setting
RecoveryCondition	No value is set.
ExternFun	No value is set.
Alert Notification	"Notify" is set.
Category	"MIB Original Definition" is set.
Last Modified Date	The date on which the file was imported is set.
Description	The text string of the DESCRIPTION definition for the target SNMP trap is set. If the DESCRIPTION definition in the MIB file contains more than 4,000 characters, the text string of the DESCRIPTION definition is not set.
Import Date	The date on which the file was imported is set.
MIB File Name	The name of the MIB file in which the target SNMP trap was defined during import is set.
MIB Module Name	The name of the MIB module in which the target SNMP trap was defined during import is set.
MIB File Last Updated	The LAST-UPDATED definition value in an MIB file in which the target SNMP trap was defined during import is set. If there is no LAST-UPDATED definition, or if the LAST-UPDATED definition is syntactically incorrect, no value is set.

Tip

If you import an MIB file and then automatically create trap definitions, the MIB enumeration type definition information corresponding to the created trap definitions is also registered. This allows numerical value-type MIB values to be converted into symbol names in the varBindList display.

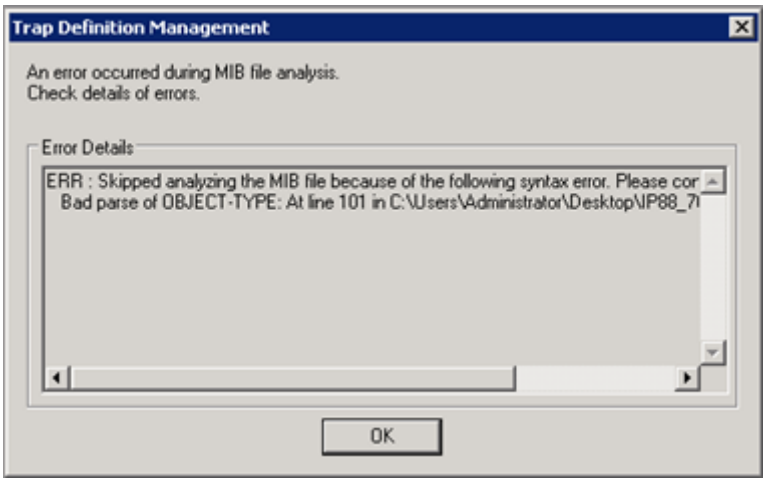
The above enumeration type definitions are enabled only in an alert notification when an SNMP trap is received. To convert numerical value-type MIB values obtained by the `NvPROAmibGetSvc`/`NvPROAmibGetMgr` command into symbol names, you also need to incorporate an AMIB numeration file. For details, refer to "7.4.1.3 Procedure for incorporating an AMIB enumeration (page 655)".

Caution

If you import an MIB file and automatically create a trap definition, be sure to check the created definition setting and review (add by quoting) it according to the operation you are performing. In particular, **Severity** often needs to be reviewed because it is set to "NORMAL". For details on changing the definition setting, refer to "4.11.5.2 Adding a trap definition (page 290)".

4.11.6.4 Messages output during MIB file analysis

When you start importing trap definitions from MIB files, if an incident requiring a check of the validity of the process or an error occurs, a dialog box appears to display the details of the process.



Tip

When it is imported using the `nvpmib2trapdef` command, messages are output to the log file.

Check the displayed messages. If there is any problem, contact NEC Customer Support Center or the help desk of the device vendor providing the MIB file.

Each message is displayed in a two-line format, as follows.

```
Severity: Summary message
   Detailed message
```

Example:

```
INFO: Skipped analyzing the following file because it is not a MIB file.
   Faild to parse MIB file D:\MIB/MIB_Reference.txt
```

The details of the displayed message format are shown below.

- Severity

  Shows the severity level of the output message. Each message is output with one of the following three severity levels.

  - ERR

    If the target file analysis is skipped during the process due to a read failure of a file under the specified folder or a syntax error in the MIB file, a message is output with this severity.

  - WARN

    When MIB file analysis partially fails because the MIB file or MIB definition is missing or the Network Manager process specification limit is exceeded, a message is output with this severity.

  - INFO

    When the read file is not an MIB file or the last update date of the MIB file cannot be obtained, it does not affect the trap definition creation. If, however, it needs to be checked for precautionary purposes, a message is output with this severity.

- Summary message

  Outputs the summary information of an incident that has occurred while the MIB was being analyzed.

- Detailed message

Outputs the detailed information of an incident that has occurred while the MIB was being analyzed. It includes detailed information, such as an incident description, the detected file name, and line number.

The messages output by Network Manager and their causes and solutions are given below.

Severity	Summary message	Cause and solution
ERR	Failed to read the file. Check the file status.	The process failed because the file shown in the detailed message could not be opened. Using an editor, check whether the file can be opened. If the file was opened in another application during import, close it. Provided you can confirm that the file can be opened, import it again.
	Skipped analyzing the MIB file because of the following syntax error. Please contact the MIB file vendor.	The process failed because a syntax error about MIB definitions was found in the file at the line number shown in the detailed message. Contact the supplier of the MIB file to obtain a syntactically correct MIB file, and then import it again.
	Skipped analyzing the MIB file because of unsupported definitions.	The process failed because the file contains an MIB definition that cannot be analyzed in Network Manager. Contact NEC Customer Support Center and provide this output message and the MIB file.
WARN	Trap definitions or MIB enum type definitions could not be created properly because of the following reason. Please contact the MIB file vendor.	The process failed because an MIB file describing a definition for the read MIB file is not found in the specified folder. Contact the supplier of the MIB file to obtain an MIB file defining the MIB module shown in the detailed message, and then import it again.
	Trap definitions or MIB enum type definitions could not be created properly because of the following reason. Please contact the MIB file vendor.	The process failed because the read MIB file has a missing MIB definition (symbol, parent object, or type). Contact the supplier of the MIB file about the detailed message to obtain an MIB file containing the missing definition, and then import it again.
	Trap definitions could not be created properly because of the following reason.	The process failed because the data size limit that can be handled by Network Manager was exceeded. Contact NEC Customer Support Center and provide this output message and the MIB file.
	Failed to acquire additional information of the trap because of the following reason.	The process failed because the data size limit that can be handled by Network Manager was exceeded. Contact NEC Customer Support Center and provide this output message and the MIB file.
	MIB enum type definitions could not be created properly because of the following reason.	The process failed because the data size limit that can be handled by Network Manager was exceeded. Contact NEC Customer Support Center and provide this output message and the MIB file.
INFO	Skipped analyzing the following file because it is not a MIB file.	This indicates that the file shown in the detailed message was determined to be a non-MIB file. Confirm that the file is not an MIB file, for precautionary purposes.
	There is no MIB definition.	This indicates that the file shown in the detailed message contains no MIB definition.

Severity	Summary message	Cause and solution
		If an ERR or WARN message is output together with this message, contact the supplier of the MIB file to check the relationship with the ERR or WARN message. If an ERR or WARN message is not output together with this message, no action is required.
	Failed to acquire the last updated information of MIB file because of MIB file syntax error.	This indicates that the last update date of the MIB file shown in the detailed message could not be obtained because a syntax error about the MIB definition was found. No action is required, but if you want to record the last update date of the MIB file, contact the supplier of the MIB file to obtain a syntactically correct MIB file, and then import it again.
	Failed to acquire the last updated information of MIB file.	This indicates that the last update date of the MIB file shown in the detailed message could not be obtained because an illegal value, which cannot be handled by Network Manager (such as 1969 or earlier, or 2038 or later), is specified. No action is required.

4.11.7 Priority order for alert conversion using trap definition files

This section shows examples of trap definitions.

Example 1: Recovering automatically from an alert when linkDown or linkUp trap is receive

The following shows a description example of a trap definition to automatically recover from an alert when a linkDown or linkUp trap with the same interface on the same node is received.

Parameter	linkDown trap setting value	linkUp trap setting value
Enterprise ID	*	*
Specific Trap Code	*	*
Generic Trap Code	2	3
Node	*	*
Summary	Interface Down (%D1%)	Interface Up (%D1%)
Severity	FATAL	NORMAL
Detail	Interface is down. ifname=%D1% ifIndex=%1%	Interface is up. ifname=%D1% ifIndex=%1%
Action	Check the impact.	
RecoveryNo	100	100
RecoveryCondition	1	1
ExternFun	ChangeCompByIfIndex	ChangeCompByIfIndex
Description	An SNMP trap to report that the interface is down.	An SNMP trap to report that the interface is up.

Tip

Specify the same numerical value in **RecoveryNo** for a trap definition pair of fault and recovery. Also, specify the first information of varBindList, containing "ifIndex" used to identify the interface, in **RecoveryCondition**.

Example 2: Changing the notification contents of a linkDown trap from a specific node

The following shows a description example of a trap definition to change the alert contents reported when a linkDown trap from specific nodes (specific group) is received. This example uses nodes belonging to the "CoreSwitch" group and other nodes.

Parameter	"Core Switch" group setting value	Other node setting value
Enterprise ID	*	*
Specific Trap Code	*	*
Generic Trap Code	2	2
Node	grp:CoreSwitch	*
Summary	Core Switch Interface Down (%D1%)	Interface Down (%D1%)
Severity	FATAL	WARNING
Detail	Core Switch interface is down. ifname=%D1% ifIndex=%1%	Interface is down. ifname=%D1% ifIndex=%1%
Action	Check the impact.	
RecoveryNo		
RecoveryCondition		
ExternFun	ChangeCompByIfIndex	ChangeCompByIfIndex
Description	An SNMP trap to report that the interface of a switch belonging to the core switch group is down.	An SNMP trap to report that the interface is down.

Tip

Only when the **Node** matches a group specified in Node, "Core Switch Interface Down" is reported. Specify a description in **Node** so that a node to which the trap definition is applied can be clearly identified.

Example 3: Changing the notification contents for an undefined vendor extended trap

The following shows a description example of a trap definition for changing the alert contents reported when an undefined SNMP trap is received.

Parameter	Setting value after change	Default setting value
Enterprise ID	*	*
Specific Trap Code	*	*
Generic Trap Code	*	*
Node	*	*
Summary	Undefined Trap	Vendor-defined Trap

Parameter	Setting value after change	Default setting value
Severity	UNKNOWN	UNKNOWN
Detail	%allleaf	%all
Action	Check the details of the received SNMP trap and identify the impact. Also, create a trap definition.	
RecoveryNo		
RecoveryCondition		
ExternFun		
Description	An undefined SNMP trap.	

Tip

Specify "*" representing the lowest priority in all of the **Enterprise ID**, **Specific Trap Code**, **Generic Trap Code**, and **Node** definition settings for an undefined SNMP trap. By this setting, this trap definition is applied when an SNMP trap does not match any of the registered trap definitions.

4.12 Monitoring Syslogs

In Network Manager, when syslogs with a severity of WARNING or higher are received, a fault is reported.

Settings for monitoring syslogs

Detect faults in monitored devices in close to real-time by monitoring syslogs. To monitor syslogs in Network Manager configure the following settings.

- In the settings on the monitored device side, set the syslog send destination to the Manager IP address for Network Manager.
- In the Map View, register the monitored device information. For details, refer to "4.2.1 Automatically detecting devices and networks (page 127)". It is important that the IP address value specified in the **IP Address** column in the properties are the same as the syslog source address.
- Turn the monitoring mode on. For details, refer to "5.13 Starting or Stopping Monitoring by the Monitoring Mode (page 505)".

Caution

1. Syslog communication uses UDP. For this reason, syslogs might get lost on networks with poor communication quality and might not be received.
2. On servers with Network Manager installed, if the syslog receive port (514/udp) conflicts with another product, syslogs will not be received properly. For information on measures for avoiding conflicts, refer to "11.4.2 Sharing the SYSLOG port with other software (page 778)".

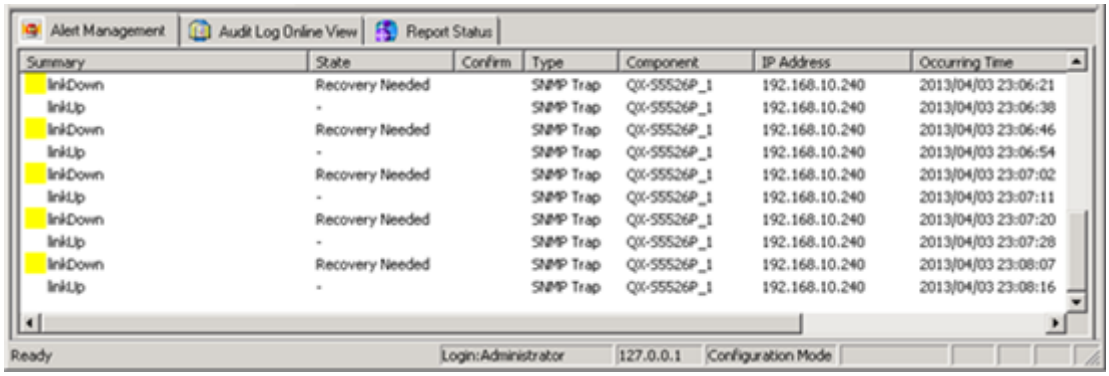
4.13 Controlling Alerts (Aggregating, Discarding, and Converting Contents)

4.13.1 Controlling alerts

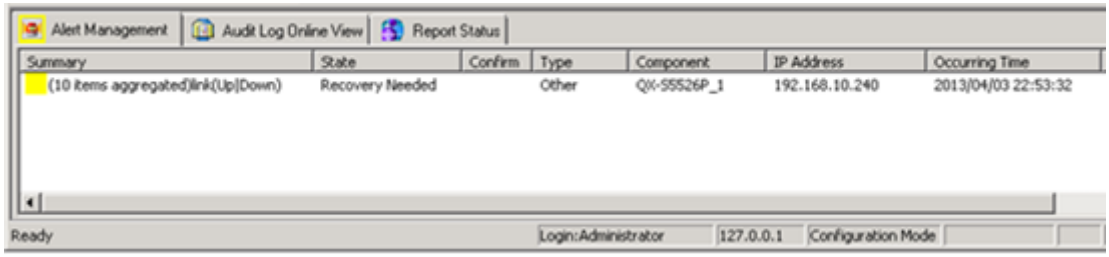
Control (aggregate, discard, or change alert content for) the alert notifications for SNMP traps or syslogs that are sent from monitored devices when a fault occurs or when a status changes.

This makes it easier to identify critical alerts, such as faults or status changes, and to analyze the problem.

- Example of alerts with no aggregation



- Example of alerts with aggregation



Caution

1. SNMP traps and syslogs are the only alerts that can be controlled.

   Other alerts (such as alerts based on status monitoring rules) will not be controlled, even if you set them up to control. In addition, the SNMP traps below will not be controlled, even if the alert type is SNMP trap.

Source Column	Alert Occurrence Conditions
Topology Check Tool	If an inconsistency was detected when running a command from the **Check Topology** menu.
Physical Topology Autodiscover	An inconsistency was detected when running a command from the **Physical Topology** menu.

   To avoid controlling of these alerts, do not set the keywords in the [Summary] or [Detail] section in the following file to the control condition such as [CorrelationSummary], [CorrelationDetail], [ConversionSummary], or [ConversionDetail].

   <On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\public\trap_backup*YYYYMMDDhhmmss*\nvtp.def

   - *YYYY*: Year
   - *MM*: Month
   - *DD*: Day
   - *hh*: Hour
   - *mm*: Minute

- *ss*: Second

If the relevant control setting is configured, alert are not issued, even if inconsistencies are detected in the menu operation above.

2. The coldStart and warmStart SNMP traps sent by monitored devices are monitored using the Resource Manager software distribution function. If an A10 Networks AX series or Thunder ADC series device is being managed, the axSystemRestart SNMP traps are monitored. Therefore, when this function is being used, do not set it to control the coldStart, warmStart, and axSystemRestart SNMP trap alert notification.

4.13.2 Setting controlling conditions

In the folder below, create a new definition file to specify controlling conditions.

```
<On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\public
\exdll\correlation
```

Specify one controlling condition per file and use the file naming convention "*any_name*.def". Character encoding for the file is UTF-16LE with BOM for Windows, and UTF-8 without BOM for Linux.

It is recommended to copy the sample file and use this to create the definition file. For details, refer to "4.13.4 Control condition sample files (page 308)".

Example of definition file: interfaceUpDown.def.sample

```
[Alert Analyzer]
Component=*
Summary=link(Up|Down)
Detail=Interface <ifindex> was link-(up|down).
Priority=10
TimeRange=60
NumberRange=10
Mode=1
ShowFirstAlert=0
CorrelationSummary=
CorrelationDetail=
CorrelationSeverity=3
```

Explanation of parameters

Controlling Condition Parameter Name	Description
Component	Specifies the name of the component to be controlled. This is a mandatory item. Multiple components can be specified using the standard matching specification format. The component of node type can be specified. To specify all components, specify "*". (Even if you specify "*", aggregation alerts will still be published per component.)
Summary	Specifies the summary text for control targets using the same wording that is used in the **Summary** column in the alert list, and with a maximum of 128 characters (excluding regular expression special characters). This is a mandatory item.

Controlling Condition Parameter Name	Description
	You can specify regular expressions. If you want to use the same special characters as a regular expression, use "\" to escape.
Detail	Specifies the details text for control targets using the same wording that is used in the **Detail** column in the alert details, and with a maximum of 2,000 characters (excluding regular expression special characters). This is optional. You can specify regular expressions. If you want to use the same special characters as a regular expression, use "\" to escape.
Priority	Specifies a priority for the control condition from 1 to 3,000. The highest is 1. This is optional. The default value is 1000. Specify a different priority for each definition file so that all the files have a unique value.
TimeRange	This setting will be valid when the operating mode is Aggregate (Mode=1). Specifies an aggregation time in units of single-byte seconds from 5 to 3,600. This is optional. The default value is 60 (seconds).
NumberRange	This setting will be valid when the operating mode is Aggregate (Mode=1). Specifies the number of aggregation items in single-byte numerals from 2 to 1,000. This is optional. The default value is 100 (items).
Mode	Specifies one of the operating modes below (in single-byte numerals). ***1*** **:** Aggregate ***2*** **:** Discard ***3*** **:** Convert This is optional. The default value is 1 (aggregation).
CorrelationSummary	This setting will be valid when the operating mode is Aggregate (Mode=1). Specifies the summary text for aggregation alerts using up to 128 characters. This is optional. If omitted, the summary is displayed in the format below. (X items aggregated) "Summary"
CorrelationDetail	This setting will be valid when the operating mode is Aggregate (Mode=1). Specifies the details text for aggregation alerts using up to 2,000 characters. If specified, only the ["Summary" were aggregated. (X items)] row is replaced. This is optional. If omitted, the detail is displayed in the format below. "Summary" were aggregated. (X items) Last alert detail: "last alert details" CorrelationFile: "definition file name" TimeRange: from YYYY/MM/DD HH:MM:SS to YYYY/MM/DD HH:MM:SS
CorrelationSeverity	This setting will be valid when the operating mode is Aggregate (Mode=1).

Controlling Condition Parameter Name	Description
	Specifies one of the aggregation alert severities below (in single-byte numerals, or MINOR or MAJOR). ***2*** **:** NORMAL ***3*** **:** WARNING ***MINOR*** **:** MINOR (in extended mode) or FATAL (in compatible mode) ***MAJOR*** **:** MAJOR (in extended mode) or FATAL (in compatible mode) ***4*** **:** FATAL This is optional. The default value is 3 (WARNING).
ShowFirstAlert	This setting will be valid when the operating mode is Aggregate (Mode=1). Specifies whether to show the first alert to be aggregated. Select below. ***0*** **:** Do not show the first alert. ***1*** **:** Show the first alert. This is optional. The default value is 0 (do not show the first alert).
ConversionSummary	This setting will be valid when the operating mode is Convert (Mode=3). Specifies the summary text for conversion alerts using the format below. ***{0}*** **:** Displays the summary text for the conversion source alert without performing processing ***Any text string*** **:** Displays the specified text. ***Omitted*** **:** Same as specifying {0}
ConversionDetail	This setting will be valid when the operating mode is Convert (Mode=3). Specifies the detailed text for conversion alerts using the format below. ***{0}*** **:** Displays the detailed text of the conversion source alert without performing processing. ***{n}*** **:** When the nth line of detailed text for the conversion source alert has the <string>=<value> format, only the <value> of the nth line is displayed. This parameter can be used to extract the varBind value of an SNMP trap by using %all or %allleaf. For example, when the detailed text of the conversion source alert is as follows, {1} displays "10101" and {2} displays "GigabitEthernet1/0/1". `[1]ifIndex.10101=10101` `[2]ifDescr.10101=GigabitEthernet1/0/1`

Controlling Condition Parameter Name	Description
	Any text string **:** Displays the specified text. ***Omitted*** **:** Same as specifying {0} Specify a combination of any text string and "{0}" or "{n}". The maximum length is 2,000 characters. To include "{}" (single-byte braces) in the text string, use "\" as an escape sequence.
ConversionSeverity	This setting will be valid when the operating mode is Convert (Mode=3). Specifies one of the severity levels (one-byte numeral character or MINOR, MAJOR) below for the conversion alert. ***{0}*** **:** Display the severity level of the conversion source alert without performing processing. ***2*** **:** NORMAL ***3*** **:** WARNING ***MINOR*** **:** MINOR (in extended mode) or FATAL (in compatible mode) ***MAJOR*** **:** MAJOR (in extended mode) or FATAL (in compatible mode) ***4*** **:** FATAL ***Omitted*** **:** Same as specifying {0}
ConversionSender	This setting will be valid when the operating mode is Convert (Mode=3). Specifies the source for conversion alerts using the format below. ***{0}*** **:** Displays the source for the conversion source alert without performing processing. ***Any text string*** **:** Displays the specified text ***Omitted*** **:** Same as specifying {0} Specify a combination of any text string and "{0}". The maximum length is 64 characters. Cannot specify "{}" (single-byte braces) in any text string.

Explanation of regular expression special characters

Special Character	Description
[^ -]	Matches a single character contained in the brackets. For example, *[abc]* matches "a", "b", and "c". *[a-z]* matches all lower case characters. *[^abc]* matches any character other than "a", "b", "c".
(|)	Parentheses are used to define the scope and the priority order of operators. A vertical line separates options. For example, *(gray|grey)* matches "gray" or "grey".

Special Character	Description
*	Matches any character string of zero or more characters. For example, *ab** matches "ab", "abc", "abcd".
?	Matches any single character. For example, *ab?* matches "abc", "abd", and "abe".
<Any character string>	This is used to aggregate identical alerts. When *<Any character string>* is specified multiple times, alerts are aggregated if each part matches in the alerts. Example: Alert summary text : The syslog (Warning) occurred. Definition method : The syslog \(<Severity>\) occurred. Description: The <Severity> will be replaced any character strings.

4.13.3 Enabling controlling conditions

Enable the control settings.

1. Create a definition file to specify the control conditions.

   For details, refer to "4.13.2 Setting controlling conditions (page 304)".

2. Run the `NvPROReloadDllMgr` command.

   For details, refer to "9.5.3 NvPROReloadDllMgr (page 698)".

4.13.4 Control condition sample files

Control condition sample files (extension: .sample) are provided in the folder below.

<On the manager, %sharedfolder%>`\Manager\sg\NvPRO\NVWORK\public\exdll\correlation`

The following describes usage cases of each sample file.

1. interfaceUpDown.def.sample

   This sample aggregates alerts for interface up/down alerts. When this sample is applied, interface up/down traps from all devices are displayed as aggregation alerts (a maximum of 10 items or after 60 seconds).

```
[Alert Analyzer]
Component=*
Summary=link(up|down)
Detail=Interface <ifindex>; was link-(up|down)
Priority=10
TimeRange=60
NumberRange=10
Mode=1
ShowFirstAlert=0
CorrelationSummary=
CorrelationDetail=
CorrelationSeverity=3
```

2. discard.def.sample

   This sample discards all SNMP trap or syslog alerts. Apply in conjunction with the alert settings for an aggregation target and use if you do not want to display anything else.

```
[Alert Analyzer]
Component=*
Summary=*
Detail=*
Priority=3000
TimeRange=
NumberRange=
Mode=2
CorrelationSummary=
CorrelationDetail=
CorrelationSeverity=
```

3. conversion.def.sample

   This sample shows how to change the severity level and displayed information for an alert using keywords in the Detail field as conditions.

   If applying this sample, when receiving an alert that contains the "0-C [MN]" text string in the Detail field, the summary alert information converts to "RESET INTERRUPT" and the severity level is converted to the Warning level.

```
[Alert Analyzer]
Component=*
Summary=*
Detail=*0-C*\[MN\]*
Priority=10
Mode=3

ConversionSummary=RESET INTERRUPT
ConversionDetail={0}
ConversionSeverity=3
ConversionSender={0}
```

4. Sample for NEC ESMPRO Agent management

   This is a sample to display NEC ESMPRO Agent alerts in an easily understandable form, as well as NEC ESMPRO Manager. There are four files because the settings varies depending on the alert severity. The control condition parameters does not need to be changed in principle. Only the setting of [Priority] in each file should be changed in accordance with the other definitions, if needed.

   - ESM_MAJOR.def

```
[Alert Analyzer]
Component=*
Summary=*
Detail=Level: major\(4\)*
Priority=14
Mode=3

ConversionSummary={0}
ConversionDetail={0}
ConversionSeverity=4
ConversionSender={0}
```

   - ESM_MINOR.def

```
[Alert Analyzer]
Component=*
```

```
Summary=*
Detail=Level: minor\(3\)*
Priority=13
Mode=3

ConversionSummary={0}
ConversionDetail={0}
ConversionSeverity=3
ConversionSender={0}
```

- ESM_NORMAL.def

```
[Alert Analyzer]
Component=*
Summary=*
Detail=Level: normal\(2\)*
Priority=12
Mode=3

ConversionSummary={0}
ConversionDetail={0}
ConversionSeverity=2
ConversionSender={0}
```

- ESM_UNKNOWN.def

```
[Alert Analyzer]
Component=*
Summary=*
Detail=Level: unknown\(1\)*
Priority=11
Mode=3

ConversionSummary={0}
ConversionDetail={0}
ConversionSeverity=3
ConversionSender={0}
```

4.13.5 Important points to consider when massive alerts are rushed

If massive alert are rushed, the occurrence time of the aggregation alert, based on the time conditions (time range), is shown as being more recent than other alerts before and after that alert.

This happens if the alert receive speed exceeds the display speed.

In such cases, it is recommended to remove the cause of the alert rush. The actual timeline of aggregations is displayed as **TimeRange** in the **Detail** column in the Alert Detail dialog box. Check here to confirm.

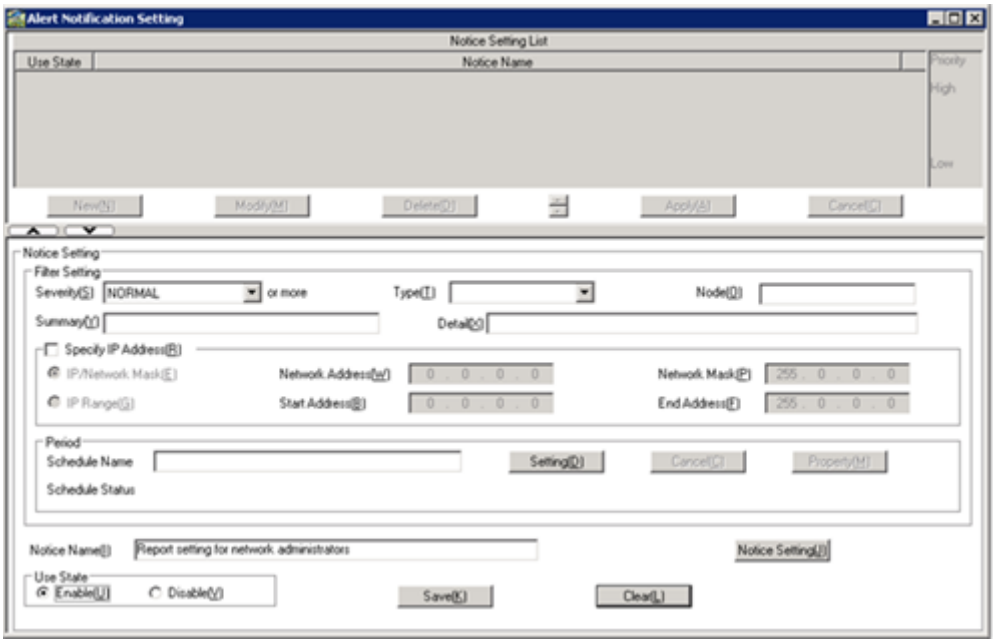
4.14 Settings for Sending Alert Reports

Network Manager can be configured to issue a report when each alert occurs.

In addition to being displayed on monitoring windows, alerts can be reported using Patlite, e-mail notifications and notifications by registered commands (action report).

4.14.1 Alert Notification Setting window

To open the Alert Notification Setting window, right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Fault Management**>**Alert Notification Setting**.



Notice Setting List pane

- **Use State**

  Indicates whether the notification setting displayed by the notification setting name is enabled or disabled.

- **Notice Name**

  Displays the name that the notification setting is identified with.

- **New** button

  Creates a new notification setting.

- **Modify** button

  Modifies the selected notification setting.

- **Delete** button

  Deletes the selected notification setting.

- button

  Change the priority assigned to notification settings. Notification settings that match the details of the generated alert are searched for in the order of highest priority in the settings list, and a notification is sent based on the matching notification settings. A notification is only sent if matching notification settings are found. If they are found, no further searching for notification settings is performed.

- **Apply** button

  Applies the priority setting that was changed using the button.

- **Cancel** button

Cancels the priority setting change made using the  button.

Notice Setting pane

- **Filter Setting**
  - **Severity**

    Specify the level of alert severity for which to send notification.
  - **Type**

    Specify the types of alerts (examples: SNMP trap, and system log) for which to send notification. Leaving this field blank selects all types of alerts.
  - **Node**

    Specify one or more node or group names for which reports will be issued. The maximum length of each node and group name is up to 63 characters. The total length is up to 1023 characters.

    Leaving this field blank selects all nodes.

    You can use the extended standard component name specification format. You can specify node or group type components. For details regarding the standard component name specification format, refer to "7.3.3 Standard Component Name Specification Format (page 645)".

    The extended points from the standard component specification format are as follows:

    * Component name (node or group name) can be searched by partial matching.
    * Some regular expression operators can be used for a part of component name (node or group name).

    Available regular expression operators are as follows:

    Hut (^):

    Hut (^) represents the beginning position of the character string.

    Specifying `^Switch` matches "Switch" or "Switch1", but it does not match "ASwitch" or "B-Switch".

    Dollar ($):

    Dollar ($) represents the ending position of the character string.

    Specifying `Switch$` matches "Switch" or "ASwitch", but it does not match "Switch1" or "SwitchABC".

    Plus (+):

    Plus (+) represents one or more repetition of the preceding character.

    Specifying `Switch1+` matches "Switch11" or "Switch111".

    Parentheses ("()") and vertical bar (|):

    By combining of parentheses ("()") and vertical bar (|), multiple character strings can be specified.

    Specifying `(Switch1|SwitchABC)` matches "Switch1" and "SwitchABC".
  - **Summary**

Specifies the summary text for notification target alerts using the same wording that is used in the **Summary** column in the alert list, and with a maximum of 128 characters(excluding special characters in regular expressions).

When no settings are selected for this item, all alert notifications are treated as notification targets.

You can specify regular expressions. For explanations of special characters that can be specified as regular expressions, refer to "4.13.2 Setting controlling conditions (page 304)". If the summary contains the same special characters used in the regular expression, use "\" to escape.

- **Detail**

  Specify the details text for notification target alerts using the same wording that is used in the **Details** column in the alert details, and with a maximum of 2,000 characters (excluding special characters in regular expressions).

  When no settings are selected for this item, all alert notifications are treated as notification targets.

  You can specify regular expressions. For explanations of special characters that can be specified as regular expressions, refer to "4.13.2 Setting controlling conditions (page 304)". If the detail contains the same special characters used in the regular expression, use "\" to escape.

  If linefeed or tab could be included in the alert detail string of the target notification, specify asterisk (*) or the necessary number of question mark (?) so that linefeed or tab would not be included in the comparison conditions.

- **Specify IP Address**

  Specifies the IP address range for nodes for which notifications will be issued.

  When no settings are selected for this item all IP addresses will create notifications.

  The range of nodes for which notifications will be issued can be limited by selecting the **Specify IP Address** check box, then entering either information for either of the **IP/ Network Mask** or **IP Range** options.

- **Period**

  Specifies the schedule of the period in which the alert notification is enabled.

  When no settings are specified for this item, alert notifications are always enabled.

  * **Schedule Name**

    Displays the schedule name being set.

    In the case of the upgrade from MasterScope Network Manager 4.0 or earlier and occur time was specified in the previous version, occur time information is displayed in this field.

    For example, "start: 2010/08/01 00:00:00, end: 2011/12/31 23:59:59" was specified in **Occur Time**, after upgrading, "2010/08/01 00:00:00 - 2011/12/31 23:59:59" is displayed in this field and alert notifications are enabled in the displayed duration.

  * **Schedule Status**

    Displays the state of the schedule if the schedule is defined.

For example, if the schedule that is available between 8:30 and 17:00 was defined, "Inside of a period" is displayed between 8:30 and 17:00 and "Outside of a period" is displayed between 17:01 and 8:29.

* **Setting** button

  Displays the schedule setting dialog box.

  By clicking this button, a window used to create, delete and set a schedule appears. For how to set up the schedules, refer to "4.22 Scheduling (page 426)".

* **Cancel** button

  Cancels the configured schedule.

* **Property** button

  Displays the configured schedule.

For example of schedule setting, refer to "4.14.2.1 Setting example that switches report settings depending on the date and time (page 316)".

- **Notice Name**

  Specify a name to identify the notification setting to be registered using a character string of up to 256 bytes.

- **Notice Setting** button

  By clicking this button, a window used to enter settings for Patlite notifications, e-mail notifications and action notifications is displayed. For how to set, refer to "4.14.3 Defining report settings (page 318)". The report status will be normal even if no setting is configured in the Report Setting dialog box.

- **Use State**

  Specify whether to enable or disable the notification settings that you are entering.

- **Save** button

  Saves entered notification settings.

- **Clear** button

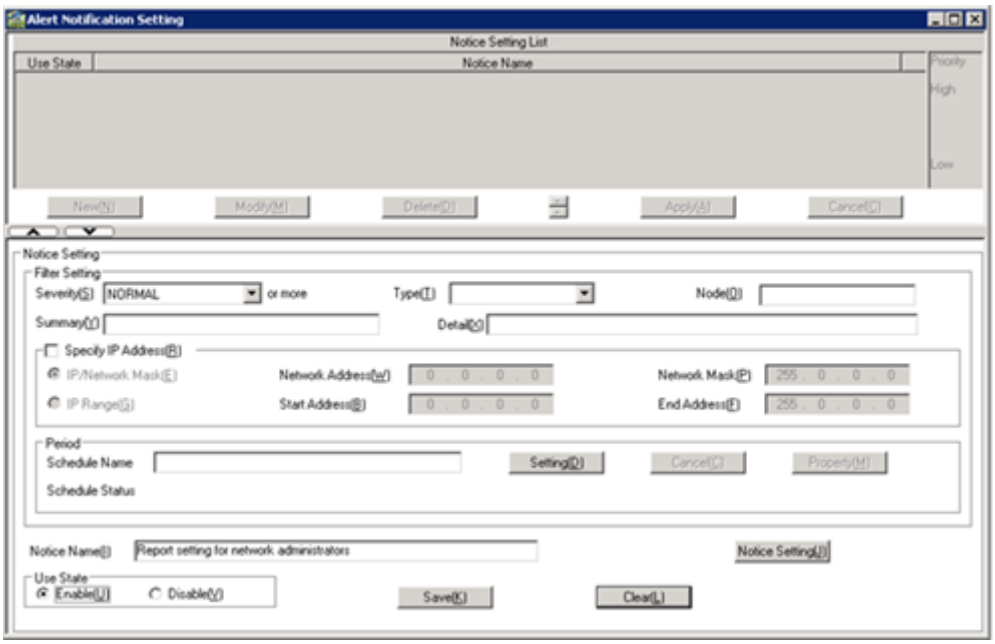
  Discards entered notification settings.

4.14.2 Configuring report settings

You must first change to the "configuration mode (page 27)".

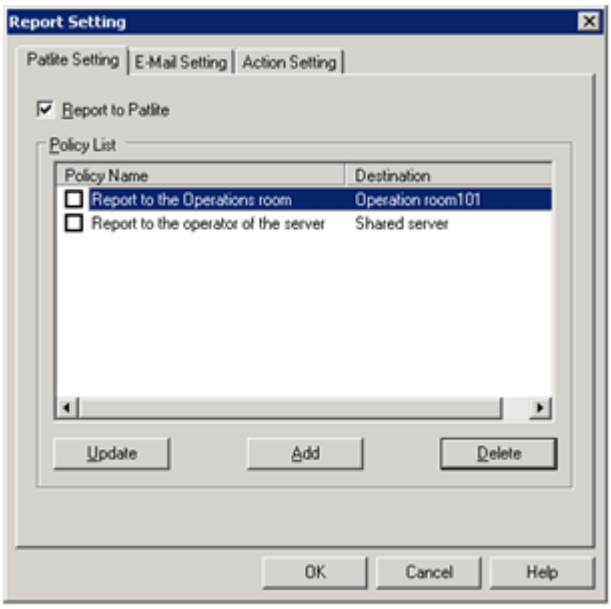
1. Open the "4.14.1 Alert Notification Setting window (page 311)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Fault Management**>**Alert Notification Setting**.



2. In the Notice Setting List pane, click **New** button.
3. Enter **Notice Name** of the Notice Setting pane.
4. Click **Notice Setting** button.

   The Report Setting dialog box is displayed.



5. Specify report settings in the Report Setting dialog box.

   For details, refer to "4.14.3 Defining report settings (page 318)".
6. Specify notification conditions in the Alert Notification Setting window.

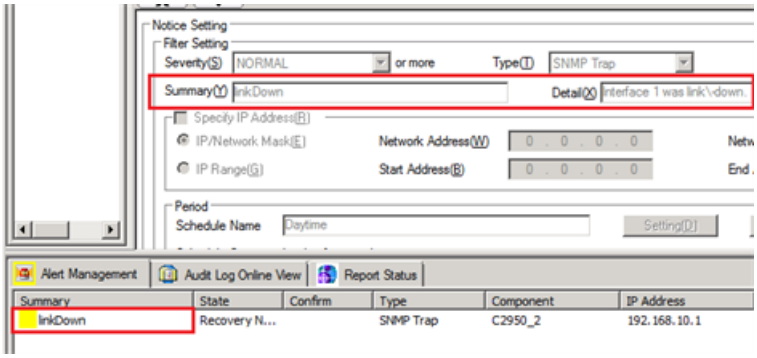
   Entering notification condition settings is unnecessary if the user wishes to issue notifications for all alerts. Notification settings include severity level (NORMAL, UNKNOWN, WARNING, MINOR, MAJOR, and FATAL), type (system event, system log, and SNMP trap), node name, IP address, and notification timeframe.

For example, settings can specify that notifications be issued for warning-level severity and above alerts that occur in devices in the 192.168.1.10 to 192.168.20.254 IP address range.

7. Click **Save** button.

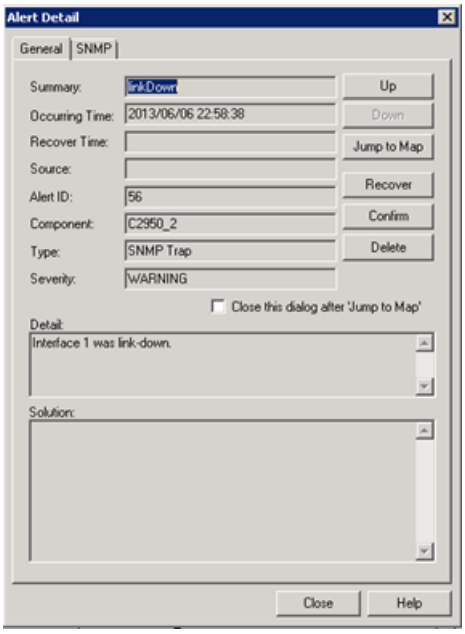
Example Settings

This example shows that the manager monitors link down SNMP traps for the interface 1 and report them.



Based on the settings above, notifications are not issued for link down SNMP traps for interfaces other than interface 1.

The detailed issued window:



4.14.2.1 Setting example that switches report settings depending on the date and time

By combing the report setting with the schedule, the contents of reports can be switched depending on time of day or the day of week. This section describes two representative setting pattern.

For details, refer to "4.14.2 Configuring report settings (page 314)".

Setting Example1: Reports by Patlite at daytime, Reports by e-mail at nighttime

Create the report setting for daytime "Report Setting (Daytime)" and the report setting "Report Setting (Nighttime)" for nighttime, and set the schedule "Daytime" and "Nighttime" that specify respective periods of time.

The setting is configured under the following conditions.

Notice Name	Report Setting (Daytime)	Report Setting (Nighttime)
Schedule Name	Daytime	Nighttime
Calendar Name	All operation dates	All operation dates
Time	08:30-17:00	17:01-08:29
Application period	**Start Date**: Today **End Date**: Not defined	**Start Date**: Today **End Date**: Not defined
Report Method	Patlite	E-Mail

Setting Example 2: Reports by Patlite on weekday, Reports by e-mail on Saturday, Sunday and Holiday

Create the report setting for weekday "Report Setting (Weekday)" and the report setting for Saturday, Sunday and holiday "Report Setting (Holiday)", and set the schedule "Schedule (Weekday)" and "Schedule (Holiday)" that specify respective dates. Additionally, By combing "Calendar Rule A" and "Calendar Rule B", create calenders "Weekday" and "Holiday".

In the following example, 2013/1/1 (Tue) falls in holiday.

The setting is configured under the following conditions.

Notice Name	Report Setting (Weekday)	Report Setting (Holiday)
Schedule Name	Schedule (Weekday)	Schedule (Holiday)
Calendar Name (Calender Rules)	Weekday	Holiday
	• Calender Rule A **Schedule Rule** Operation date, Weekly **Week** Mon, Tue, Wed, Thu, Fri **Application period** **Start Date**: Today **End Date**: Not defined • Calendar Rule B **Type** Non-operation date, Specified day **Date** 2013/01/01	• Calender Rule A **Schedule Rule** Operation date, Weekly **Week** Sat, Sun **Application period** **Start Date**: Today **End Date**: Not defined • Calendar Rule B **Type** Non-operation date, Specified day **Date** 2013/01/01
Time	08:30-17:00	00:00-23:59
Application period	**Start Date**: Today **End Date**: Not defined	**Start Date**: Today **End Date**: Not defined
Report Method	Patlite	E-Mail

Caution

Since "Calendar Rule B" is a rule when dates conflict with "Calendar Rule A", "Calender Rule B" should be placed in the top of the calender rules list so that "Calendar Rule B" would be given higher priority than "Calender Rule A".

4.14.3 Defining report settings

Network Manager uses registered settings to issue reports and notify operators of specific types of alerts as they occur. The types of reports are described in the following section.

- Patlite warning-light report

  Report by Patlite warning light is given when specific messages or status changes occur.

  Patlite reports are defined using the following procedure.

  1. Define Patlite report.
  2. Define Patlite report policy.
  3. Define the Patlite report destination.

  For details, refer to "4.14.3.1 Defining Patlite reports (page 318)".

- E-Mail report

  Report by e-mail is given when specific messages or status changes occur.

  E-Mail reports are defined using the following procedures.

  1. Define e-mail report.
  2. Define policy for e-mail report.
  3. Edit message of the e-mail.
  4. Define the mail server.

  For details, refer to "4.14.3.2 Defining e-mail reports (page 322)".

- Action report

  Report by action command is given when specific messages or status changes occur.

  Reports by action command are defined using the following procedures.

  1. Define action report.
  2. Define policy for action report.

  For details, refer to "4.14.3.3 Defining action reports (page 326)".

When a report is issued, report history is displayed in the **Report Status** tab at the bottom of the window. For details of the **Report Status** tab, "5.4 Managing Alert Report Status (page 463)".

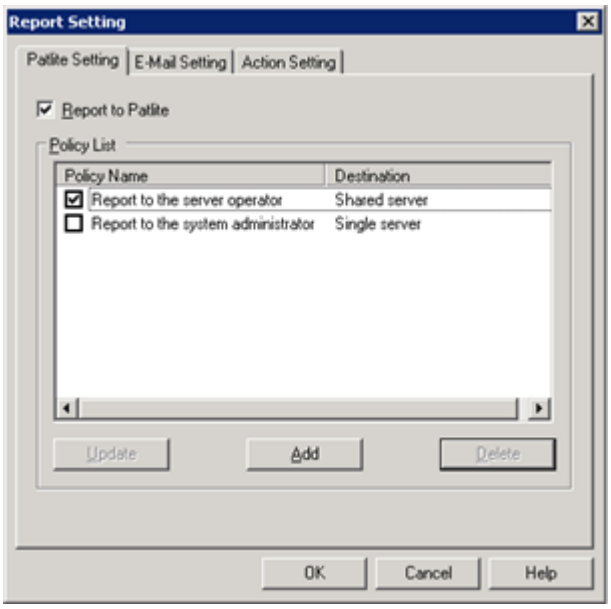
4.14.3.1 Defining Patlite reports

As a report method in the report setting, define the Patlite report. For the entire report setting, refer to "4.14.2 Configuring report settings (page 314)".

You must first change to the "configuration mode (page 27)".

1. In the Report Setting dialog box, select **Patlite Setting** tab.
2. In the "4.14.1 Alert Notification Setting window (page 311)", display the Report Setting dialog box.

3. Enter each of the items



- **Report to Patlite**

  Patlite reports are issued when the checkbox is checked. The checkbox is not checked by default.

- **Policy List**

  Select a predefined report policy. The policy is active if the checkbox is checked.

  - **Update** button

    Edit the selected policy.

  - **Add** button

    Define a new policy.

  - **Delete** button

    Delete the selected policy.

    Caution

    A policy can be used from multiple report settings. If you delete a policy, it affects all the report settings using that policy. Confirm that the policy is not used before deleting it.

  For details, refer to "4.14.3.1.1 Defining a Patlite report policy (page 319)".

4. Click **OK** button.

Defining a Patlite report policy

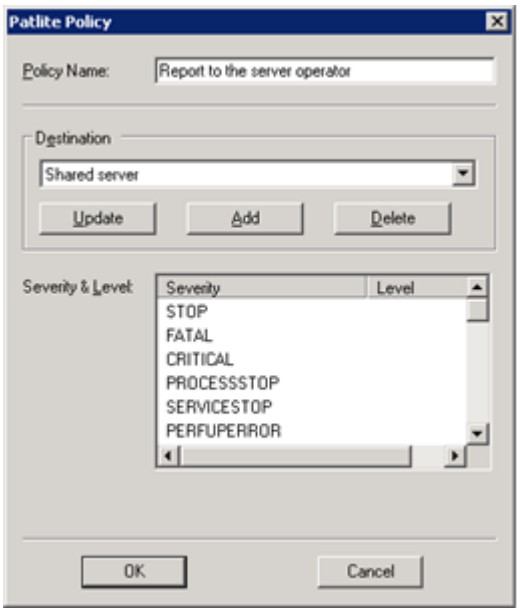
This procedure is used to define the policy (notification level and destination) used for Patlite report.

Defined policies can be used commonly within the manager.

You must first change to the "configuration mode (page 27)".

1. Open the Patlite Policy dialog box in one of the following ways.
   - In the Report Setting dialog box (**Patlite Setting** tab), click **Add** button.
   - Select a predefined policy and click **Update** button.

2. Enter each item.



- **Policy Name**

  Specify a policy name using up to 64 characters.

- **Destination**

  Select the defined destination setting.

  - **Update** button

    Edit the selected destination.

  - **Add** button

    Define a new destination.

  - **Delete** button

    Delete the selected destination.

    Caution

    A destination can be used from multiple Patlite policies. If you delete a destination, it affects all the Patlite policies using that destination. Confirm that a destination is not being used before deleting it.

  For details of the report destination setting, refer to "4.14.3.1.2 Defining a Patlite report destination (page 321)".

- **Severity & Level**

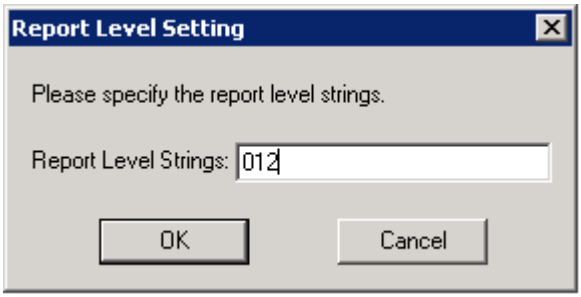
  Specify the reports for various severity levels. Double-click **Severity** to display the Report Level Setting window, then specify the report-level character string using up to 16 characters and click **OK** button to finish.

  Severity level settings are the same as the levels of severity for Network Manager alerts, including only "NORMAL", "UNKNOWN", "WARNING", "MINOR", "MAJOR", and "FATAL". Any severity level settings outside of this are invalid.

  - When using the serial-controlled type

    Specify the level set for the Patlite service setting (Relay Settings window).

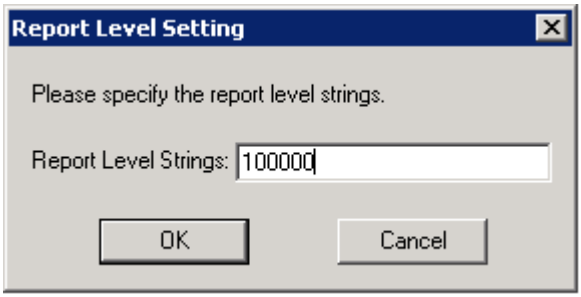
"0" indicates light-off in the Patlite service (the "012" setting below specifies blinking-light at the level 1 and level 2 settings after light-off).



- When using the network type

  Specify the type of illumination. For details about types of illumination, refer to the Patlite manuals.

  The "100000" setting below specifies that the red light blinks (the default setting for the Patlite).



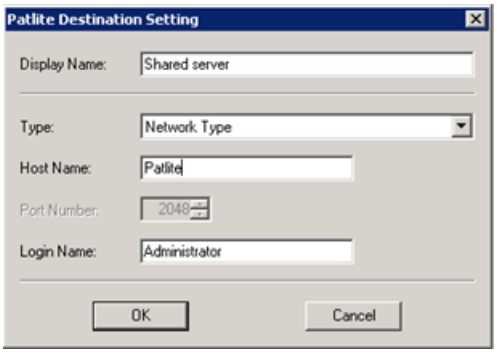
3. Click **OK** button.

Defining a Patlite report destination

Define a report destination of Patlite report policies.

You must first change to the "configuration mode (page 27)".

1. Open the Patlite Destination Setting dialog box in one of the following ways.
   - In the Patlite Policy dialog box, click **Add** button.
   - Select a predefined destination and click **Update** button.
2. Enter each of the items.



- **Display Name**

  Specify a destination setting name using up to 64 characters.

- **Type**

  Specify the type of Patlite product to be used.

  Select either "Serial-controlled Type" or "Network Type". Each type supports the following the following Patlite products.

  Serial-controlled Type :

  PHE-3FB-RYG, PHE-3FBE1-RYG ,PHC-100A

  Network Type :

  NHE-3FB-RYG, NHC-3FB-RYG, NHM-3FB-RYG, NHS-3FB1-RYG, NHP-3FB1-RYG, NHL-3FB1-RYG

- **Host Name**

  Specify destination host name (host name or IP address of which address resolution is possible.) for the Patlite report using up to 64 characters. The system will attempt to send reports even to host names that have errors, so it is important to enter the name correctly.

- **Port Number**

  If "Serial-controlled Type" is selected in **Type**, specify the port number to be used for Patlite reports with a value from the 1 to 32767 range.

- **Login Name**

  If "Network Type" is selected in **Type**, log in with the name of a user with rsh command execution rights.

3. Click **OK** button.

4.14.3.2 Defining e-mail reports

As a report method in the report setting, define the E-Mail report. For the entire report setting, refer to "4.14.2 Configuring report settings (page 314)".

⚠ Caution

Some security monitoring software and antivirus programs are designed to monitor e-mail applications. If not properly configured beforehand, some applications may limit the sending of e-mails.

If these security monitoring applications are installed through the manager, their settings must be changed to permit mail sent from Network Manager. For instructions on changing settings, refer to the manual of the software in use.

For how to configure the settings, refer to the manual of software that you are using actually.

Example:

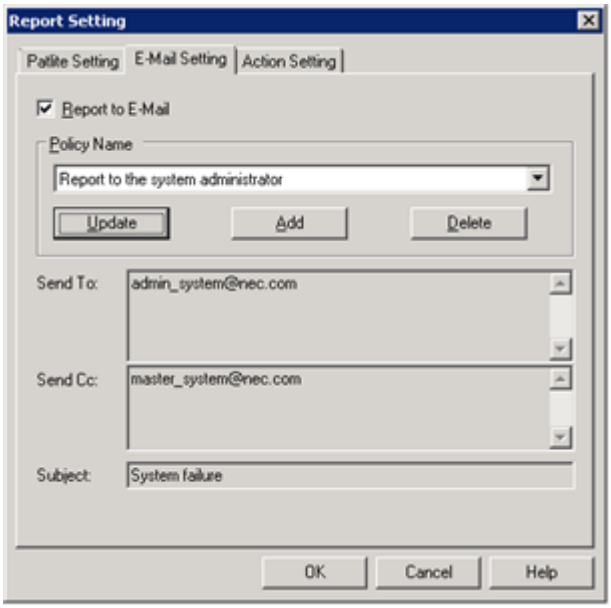
McAfee's VirusScan Enterprise 8.0, for example, has a default setting that prevents the sending of mail from applications that have not been registered with the program. Use the following procedures to register Network Manager and ensure that mail can be sent.

1. Go to the VirusScan Console, select and double-click on **Access Protection**.
2. When the Access Protection Properties window is displayed, go to **Blocked Ports** and select "Prevent mass mailing worms from sending mail". Then click the **Edit** button.
3. When the Add to or Edit Blocked Port Range dialog box appears, add the following information to **Excluded Processes** in the lower portion of the dialog box.

   ```
   SysMonMgr.exe
   ```

You must first change to the "configuration mode (page 27)".

1. In the Report Setting dialog box, select **E-Mail Setting** tab.
2. Enter each of the items.



- **Report to E-mail**

  E-mail reports are issued when this checkbox is checked. The default setting is the checkbox is not checked.

- **Policy Name**

  Select a predefined report policy.

  - **Update** button

    Edit the selected policy.

  - **Add** button

    Define a new policy.

  - **Delete** button

    Delete the selected policy.

    Caution

    A policy can be used from multiple report settings. If you delete a policy, it affects all the report settings using that policy. Confirm that the policy is not used before deleting it.

  For details, refer to "4.14.3.2.1 Defining an e-mail report policy (page 323)".

3. Click **OK** button.

Defining an e-mail report policy

Define the policy (mail sending destination and mail server to use) for e-mail reports.

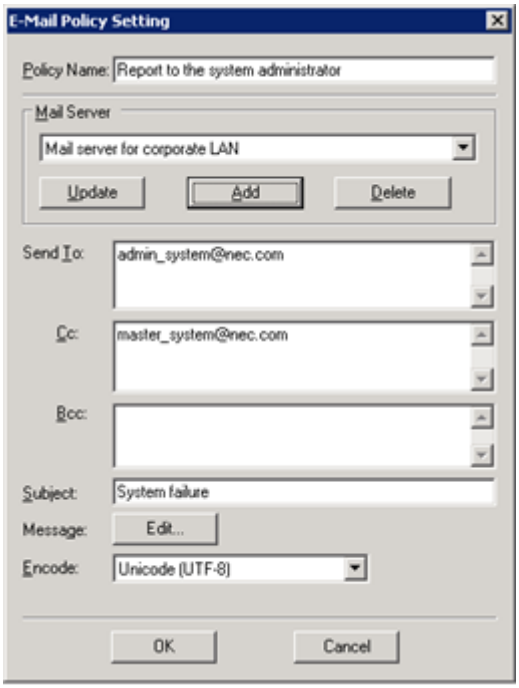
Defined policies can be used commonly within the manager.

You must first change to the "configuration mode (page 27)".

1. Open the E-Mail Policy Setting dialog box in one of the following ways.
   - In the Report Setting dialog box (**E-Mail Setting** tab), click **Add** button.

- Select a predefined policy and click **Update** button.

2. Enter each of the items.



- **Policy Name**

  Specify a policy name using up to 64 characters.

- **Mail Server**

  Select the defined mail server.

  - **Update** button

    Edit the selected mail server.

  - **Add** button

    Define a new mail server.

  - **Delete** button

    Delete the selected mail server.

    ⚠ Caution

    A mail server can be used from multiple e-mail policies. If you delete a mail server, it affects all e-mail policies using the mail server. Confirm that the mail server is not used before deleting it.

  For details, refer to "4.14.3.2.2 Defining a mail server (page 325)".

- **Send To (To)**, **(Cc)**, **(Bcc)**

  Specify the send TO, CC, and BCC e-mail destinations. Insert line breaks when specifying multiple destinations.

  Send destinations can be specified using up to 256 characters per line, up to an overall total of 768 characters, including line break characters.

- **Subject**

Specify the mail subject using up to 128 characters. Substitute character strings can also be specified for e-mail subjects. For details, refer to "4.14.3.4 List of substitute strings (page 329)".

- **Message**

  Click **Edit** button, and edit the message text of the e-mail using up to 2048 characters. You can specify substitute stings in the message text. For details, refer to "4.14.3.4 List of substitute strings (page 329)".

- **Encode**

  Specify the character code used for the encoding.

  Select the appropriate character code from those listed in the table below.

Encoding	Description
Chinese Simplified (GB18030)	This selects GB18030 encoding.
Chinese Simplified (GB2312)	This selects GB2312 encoding.
Chinese Traditional (Big5)	This selects Big5 encoding.
Japanese (JIS)	This selects JIS encoding.
Japanese (Shift-JIS) 1)	This selects Shift-JIS encoding.
Unicode (UTF-8)	This selects UTF-8 encoding.

1) When Shift-JIS encode is selected in the Linux manager, if characters that are not defined in JIS X 0208 (Roman numerals, etc.) are used in the subject or message text, they will get garbled.

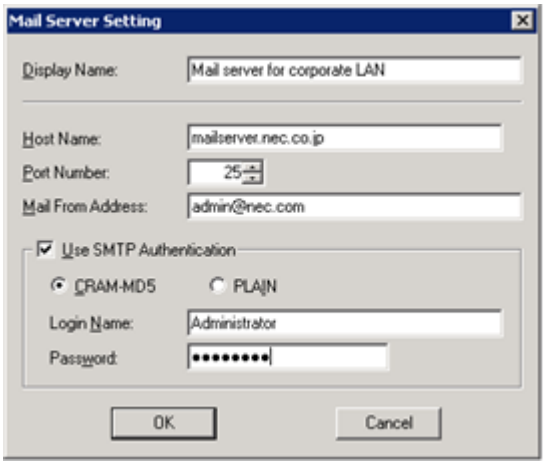
3. Click **OK** button.

Defining a mail server

Define the mail server used when issuing e-mail reports. The defined mail server can be used within managers in common.

You must first change to the "configuration mode (page 27)".

1. Open the Mail Server Setting dialog box in one of the following ways.
   - In the E-Mail Policy Setting dialog box, click **Add** button.
   - Select a predefined mail server and click **Update** button.
2. Enter each of the items.



- **Display Name**

  Specify the mail server setting name using up to 64 characters.

- **Host Name**

  Specify the mail server name used for e-mail notifications using up to 64 characters.

- **Port Number**

  Specify the port number used for issuing e-mail notifications within the 1 to 32767 range.

- **Mail From Address**

  Specify the sending address for e-mail notifications using up to 128 characters.

- **Use SMTP Authentication**

  Specifies that SMTP authentication be used for accessing the mail server. When the checkbox is checked, select the authentication method and specify the login name and password used for authentication using up to 128 characters for each.

  Caution

  Passwords of 32 or more characters in length are recommended to ensure security.

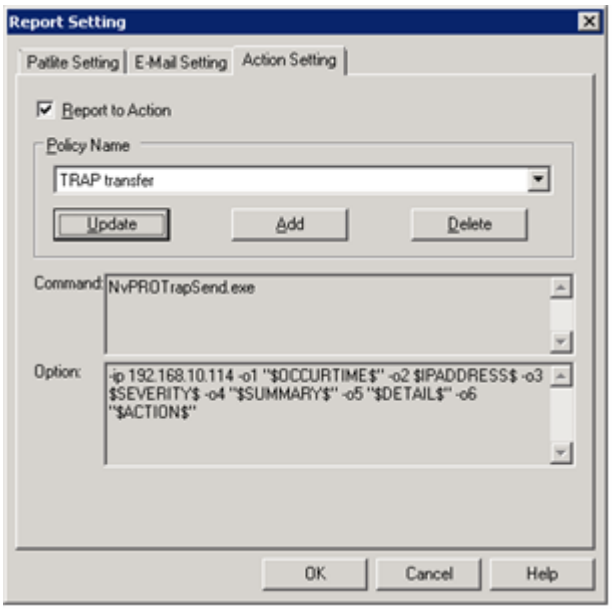
3. Click **OK** button.

4.14.3.3 Defining action reports

As a report method in the report setting, define the action report. For the entire report setting, refer to "4.14.2 Configuring report settings (page 314)".

You must first change to the "configuration mode (page 27)".

1. In the Report Setting dialog box, select **Action Setting** tab.
2. Enter each of the items.



- **Report to Action**

  Action reports are issued when this checkbox is checked. The checkbox is not checked by default.

- **Policy Name**

  Select a predefined report policy.

  - **Update** button

    Edit the selected policy.

  - **Add** button

    Define a new policy.

  - **Delete** button

    Delete the selected policy.

    Caution

    A policy can be used from multiple report settings. If you delete a policy, it affects all the report settings using that policy. Confirm that the policy is not used before deleting it.

  For details, refer to "4.14.3.3.1 Defining an action report policy (page 327)".

- **Command**

  Displays the command which is executed when specific messages or status changes occur.

- **Option**

  Displays the arguments passed to the command.

3. Click **OK** button.

Defining an action report policy

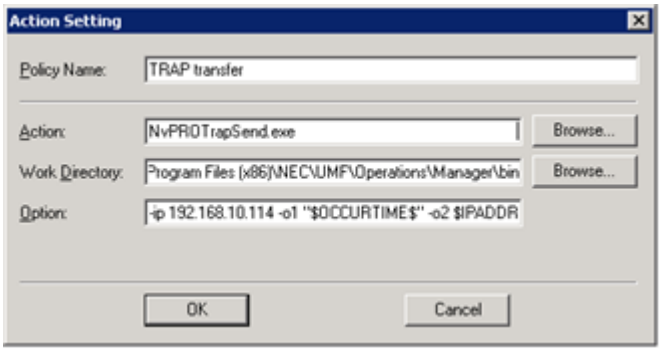
Define the policy (a command or program on the manager) for action reports.

Defined policies can be used commonly within the manager.

You must first change to the "configuration mode (page 27)".

1. Open the Action Setting dialog box in one of the following ways.
   - In the Report Setting dialog box (**Action Setting** tab), click **Add** button.
   - Select a predefined policy and click **Update** button.
2. Enter each item.

   Defined policies can be used commonly within the manager.



- **Policy Name**

  Specify a policy name using up to 64 characters.

- **Action**

  Specify a path name of the command using up to 256 characters.

  Click **Browse** button to open the Directory in Manager dialog box. You can select a file on the manager.

  You can use appropriate environment variables for the path name to the command. If the path name includes a space, enclose it in quotation marks ("").

- **Work Directory**

  Specify a working directory in which to run the command, using up to 256 characters.

  Click **Browse** button to open the Directory in Manage dialog box. You can select a directory on the manger.

  You can use appropriate environment variables for the path name of the working directory. Even if a blank is included in the path, you do not need to put double quotation marks (""). If using double quotation marks, command executions will be failed.

- **Option**

  Specify arguments passed to the command, using up to 2048 characters.

  You can use appropriate environment variables for the arguments. In addition, the following substitute strings can be specified. For details, refer to "4.14.3.4 List of substitute strings (page 329)".

  In addition, a specified argument is interpreted in the command line as is.

  - Character strings separated by spaces are interpreted as separate individual arguments.
  - Character strings enclosed in double quotations (") are interpreted as one argument even if they contain spaces.
  - For other specific operations, refer to the specifications of each OS.

    (In the case of Windows, refer to http://msdn.microsoft.com/en-US/library/a1y7w461%28v=vs.71%29.aspx)

  Substitution is made before the entered strings are interpreted as the command. Note that the spaces and double quotation marks contained in the substitution strings may not be interpreted as you intended.

⚠ Caution

a. In the Linux manager, the command is executed under the UTF-8 locale.

   If the command does not support UTF-8, create a shell script that sets a locale and converts output results to the UTF-8 code, and specify the shell script for the command.

   You cannot directly specify a pipe in Action and Option. Be sure to create a shell.

   Example: If you must run a command that only supports the SJIS locale in Linux.

   ```
   env LC_ALL=ja_JP.SJIS $1 | iconv -f sjis -t utf8
   ```

b. A command is executed by authority of the manager process (SYSTEM user authority in Windows, or root user authority in Linux). Confirm what authority can execute the command.

   Example: **Action**: `sh` , **Option**: `-c "ls /home/*"`

c. A command is executed by authority of the manager process (SYSTEM user authority in Windows, or root user authority in Linux). Confirm what authority can execute the command.

d. If there is a linefeed in the substitute strings, it will be converted into a single-byte space.

e. When you specify a substitute string for the command and the option (in addition, the environment variables if the OS type of the manager is Windows), you must define it so that the number of characters in the string after expansion does not exceed 1,700. If the number of characters exceeds this value, shorten the length of the option using batch files.

3. Click **OK** button.

Limiting the number of commands execution

In the action report function, a thread is generated per one alert notification in order to invoke the command, and a generated thread will be finished without waiting for the command finishing.

So, when a large number of action report requests occur at the same time, a large number of commands will running at the same time and the manager resources (memory, file descriptors, etc.) may be exhausted.

By the following procedure, you can suppress the number of commands that run at the same time, and reduce the manager resource consumption.

1. Stop the manager function.

   For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

2. Create the configuration file below and store it in the specified location.

   File name:

   <On the manager, %installfolder%>\Manager\sg\CommandMgr.ini

   Example:

```
[Passage]
CommandLimit=100
ReserveLimit=1000
```

   CommandLimit:

   Number of command starting threads that can be started simultaneously (0=no limit)

   ReserveLimit :

   Number of command starting requests that can be retained in excess of the [CommandLimit] value.

   Commands in excess of the [ReserveLimit] will not be started.

3. Start the manager function.

   For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

4.14.3.4 List of substitute strings

The following substitute strings can be specified in the subject or message text of e-mail report, or the option of the action report policy.

$SEVERITY$	Substituted for alert severity level.
$GENERATEDDATE$	Substituted for date of the alert.
$GENERATEDTIME$	Substituted for occurrence time of the alert.
$RECEIVEDATE$	Substituted for reception date of the alert .
$RECEIVETIME$	Substituted for reception time alert.

$OCCURTIME$	Substituted for Occurrence date and time of the alert.
$NODE$	Substituted for alert node name.
$GROUP$	Substituted for alert group name.
$APPLICATION$	Substituted for alert application name.
$OBJECT$	Substituted for alert object name.
$MESSAGEID$	Substituted for alert ID.
$MESSAGETEXT$	Substituted for alert text.
$IPADDRESS$	Substituted for IPv4 address of the alert.
$IPV6ADDRESS$	Substituted for IPv6 address of the alert.
$LOCATION$	Substituted for alert node location.
$SUMMARY$	Substituted for alert summary.
$DETAIL$	Substituted for alert detail.
$ACTION$	Substituted for alert solution.
$ENTERPRISE$	Substituted for Enterprise code if the alert is generated by SNMP trap.
$GENERIC$	Substituted for Generic trap type code if the alert is generated by SNMP trap.
$SPECIFIC$	Substituted for Specific code if the alert is generated by SNMP trap.

4.14.4 Linking with other SNMP manager software using SNMP traps

Network Manager can convert the alert information detected by each Network Manager function into SNMP traps, and sends them to other network management systems (SNMP managers). The function enables linkages with other SNMP managers.

SNMP traps sent from Network Manager can contain each information displayed in the alerts.

4.14.4.1 Configuring settings for sending SNMP traps

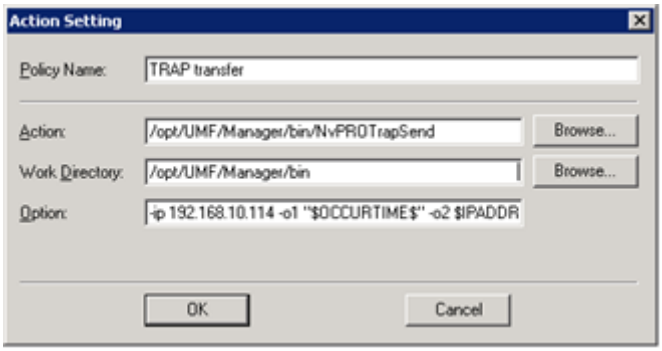
By specifying the `NvPROTrapSend` command in an alert report (action report), you can send SNMP traps that correspond with alerts detected by Network Manager. For details of `NvPROTrapSend` command, refer to "9.8 Command for Sending SNMP Traps (page 717)".

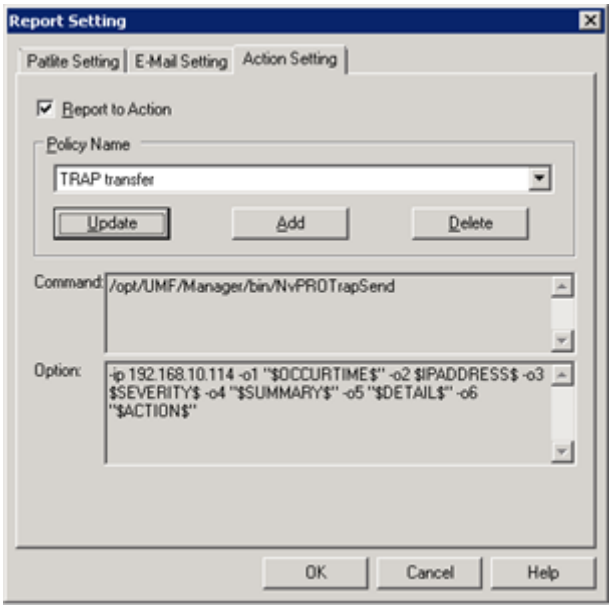
Parameter of Action Report	Description of Setting
Action	*<On the manager, %installfolder%>*\Manager\bin\NvPROTrapSend
Work Directory	*<On the manager, %installfolder%>*\Manager\bin
Option	-ip *x.x.x.x* -o1 "$OCCURTIME$" -o2 $IPADDRESS$ -o3 $SEVERITY$ -o4 "$SUMMARY$" -o5 "$DETAIL$" -o6 "$ACTION$" (enter on one line without line breaks)

Caution

A space might be included in the character strings after replacement of the alternate strings $OCCURTIME$, $SUMMARY, $DETAIL$, and $ACTION$. For this reason, they need to be enclosed in double quotation marks("").

A screen shots of the action setting (for Linux) are shown below. For details, refer to "4.14.3 Defining report settings (page 318)".





4.14.4.2 Important points when sending SNMP traps

1. In the conditions for the alert monitor settings, be particularly careful that all or most alerts are not set as targets. When all alerts are set as targets, if the alerts are rushed, the equivalent number of SNMP traps are sent to the specified SNMP manager and may result in a DoS (Denial of Service). We strongly recommend the settings below.

   Example:

   a. Only alerts with a severity of Error are targets. This avoids the problem of SNMP traps containing important alerts being buried among many alerts.

   b. Send the results of unnecessary alert aggregation as an SNMP trap using the alert aggregation function.

2. Do not specify manager's own address as the send destination of SNMP traps. If it is specified, SNMP traps might be repeatedly sent to manager itself under some conditions, and operations cannot be guaranteed.

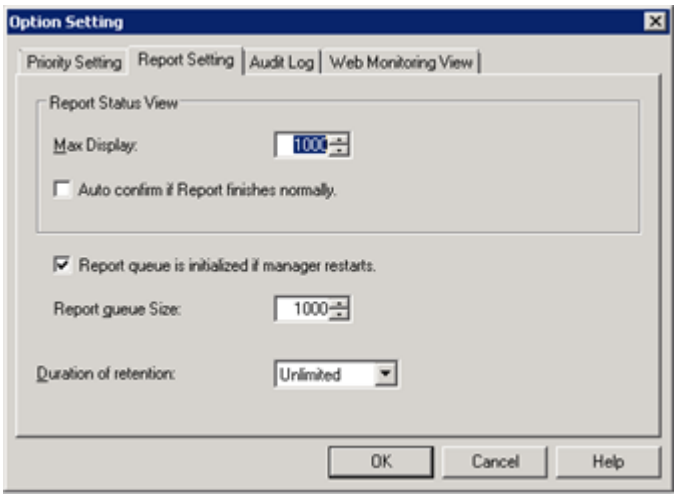
4.14.5 Setting report options

You must first change to the "configuration mode (page 27)".

1. Open the Option Setting dialog box.

In the main menu, select **Setting**>**Option**.

2. Click the **Report Setting** tab.
3. Change the settings.



- **Report Status View**
  - **Max Display**

    Specify the maximum number of entries displayed in the **Report Status** tab. Specify in the 100 to 20000 range. The default value is 1000.
  - **Auto confirm if Report finishes normally**

    If the checkbox is checked, the notification is automatically removed from display when it finishes normally.
- **Report queue is initialized if manager restarts**

  If the checkbox is checked, the notifications in the report queue will be removed without being issued when the manager is started next time. The report queue is used for storing the backlog of the notifications temporarily. When a notification in the report queue is issued successfully, it is removed from the report queue.
- **Report queue Size**

  Specify the maximum number of entries stored in the report queue. Specify in the 1000 to 10000 range. If the number of entries in the report queue exceeds Report queue Size, the latest notifications are removed.
- **Duration of retention**

  Select the period for which notification history is retained (choices are "unlimited", "1 week", "2 weeks", "1 month", "2 months", "3 months", "6 months", "9 months", and "1 year"). The default value is "Unlimited". Notification history older than the specified period will be automatically deleted.

  ⚠ Caution

  Notification history is not automatically deleted when the "Unlimited" setting is selected. Delete using either initialize or swap.

4. Click **OK** button.

4.15 Settings for Executing Device Commands When Alerts Occur

Network Manager can be configured to perform a login and execute commands on network devices where alerts originate when SNMP trap events occur.

This function permits the gathering of maintenance information for specific types of alerts and the initializing of network devices. It also stores command execution results and character-string output by network devices as files in the Network Manager manager.

Caution

1. To use this function, login settings for target devices should be registered in advance. For details, refer to "4.3 Registering Login Information (page 189)".

4.15.1 Executing commands when SNMP traps are received

To define commands that are automatically executed for network devices whenever an SNMP trap is received, create the trap definition file.

1. Create a trap command definition file.

   Create a trap command definition file by using a text editor, and register the node and command pair in the following format, and then save it as "*any_name*.def".

   ```
   Component:<node name>
   ActionCmd:<command line>
   ```

   Tip

   You can use the following sample file.

   <On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\public\exdll\TRAPCMD\TrapCmd.sample

   When the same alert occurs frequently, by specifying the following format, command executions on identical alerts from the same node are suspended for the specified interval of seconds.

   ```
   ActionInterruptTm:<number of seconds>
   ```

   Caution

   Since the suspension starts at the end time of the preceding command execution, the following command execution will not be suspended until the preceding command execution will have been completed.

2. Store the trap command definition file in the following directory.

   <On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\public\exdll\TRAPCMD

3. After updating the trap definition file, enable by executing the `NvPROReloadDllMgr` command.

   ```
   > cd <On the manager, %installfolder%>\Manager\bin\
   > NvPROReloadDllMgr
   ```

For details, refer to "9.5.3 NvPROReloadDllMgr (page 698)".

For the method to confirm the result of command execution, refer to "5.2 Checking Results of Device Commands Executed When Alerts Occurred (page 461)".

4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices

Network Manager can periodically collect and store performance information (MIB) from registered devices. For example, it can periodically collect the traffic and CPU usage rate of devices to display graphs or create reports. It also monitors whether the collected data exceeds the threshold.

The "4.16.1 Data Collecting Setting window (page 334)" is used for making settings of entries for data collection, displaying graphs, and compiling reports.

When Network Manager and other MasterScope products are installed on the same service, the MasterScope products can use performance data (MIB data) collected by the data collect function of Network Manager via the performance management service.

For details, refer to "4.16.8 Filtering function for performance data passed to other MasterScope products (page 369)".

4.16.1 Data Collecting Setting window

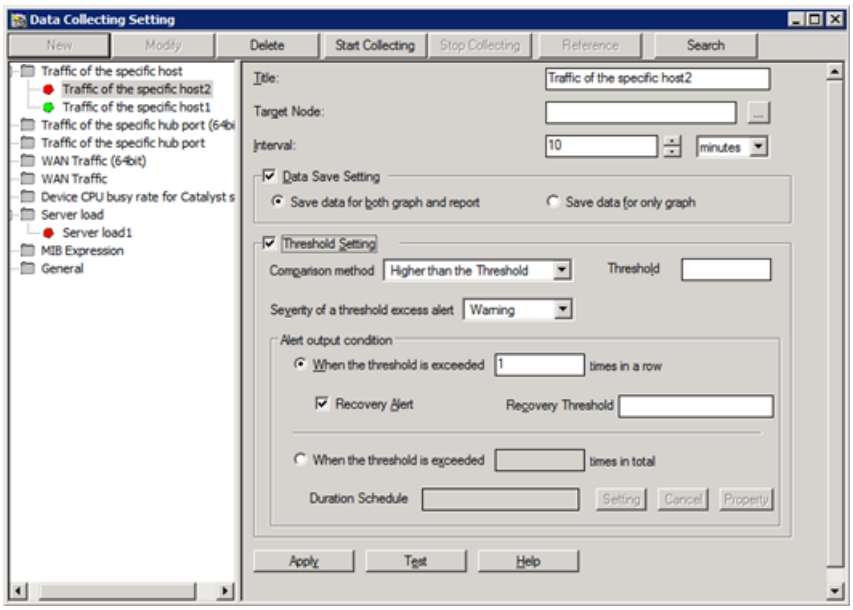
Go to the Data Collecting Setting window and perform the following operations for collecting data.

- Registering, viewing and deleting data collection entries.
- Opening and closing data collection entries.

To open the Data Collecting Setting window, right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.

Data collection is normally performed using the following two steps.

1. Registering data collection entries.
2. Starting gathering of data collection entries.



The Data Collecting Setting window is comprised of the list of data collection entries (left pane) and the collection entry settings pane (right pane). The list of data collection entries (left pane) is configured in the directory tree format and displays data collection rules and data collection entries.

Tool bar

- **New** button

  Creates new data collection entry based on selected data collection rule.

- **Modify** button

  Changes the settings for selected collection entry.

- **Delete** button

  Deletes the selected collection entries. The **Delete** button cannot be used if the **Start Collecting** button has already been clicked. You first need to click **Stop Collecting** button.

- **Start Collecting** button

  Begins collection of data for the selected collection entry.

- **Stop Collecting** button

  Terminates collection of data for the selected collection entry.

- **Reference** button

  Displays a list of nodes and list of created reports for the selected collection entry.

- **Search** button

  Searches for the corresponding collection entry using the collection entry settings information as a key.

Tree icons for list of data collection items (left pane)

- 

  Represents the data collection entry is currently stopped.

- 

Represents the data collection entry is in progress.

Data collection entry settings pane (right pane)

Displays detailed properties of data collection entries. (Displayed content varies according to the type of collection rule.)

This pane has three kinds of items; "Basic settings", "Data collection rule specific settings", and "Threshold monitoring specific settings". The following describes the items in common with all data collection rules.

For details regarding each of data collection rules, refer to "7.2 Data Collection Rules (page 622)".

- **Title**

  Enter the title of the data collection entry. In this item, there is no differentiation between uppercase and lowercase. Unicode surrogate pair characters and some symbolic characters (\ / : ? " < > | .) cannot be used.

  Caution

  If the title is set to "nul" (either uppercase or lowercase), some data collection functions may work incorrectly. Be sure not to specify "nul".

- **Target Node**

  Specify the target node or group name for data collection. By specifying a group name, data collection for this entry can be performed for all devices that belong to the same group. The format of specification complies with the "Standard Component Name Specification Format", and the component of node/group type can be specified. For multiple devices, specify using comma (,) separation. To specify group name, specify in the format of "grp:*group name*". For details of the standard component name specification format, refer to "7.3.3 Standard Component Name Specification Format (page 645)".

  Click  button to open the Node List dialog box. For details, refer to "4.10.2.2 Node List dialog box (page 246)". If multiple nodes are specified in the Node List dialog box, or if multiple nodes are specified directly using comma separation, the maximum overall length that can be specified is the equivalent of 1,024 single-byte characters. You cannot exceed this limit. If you want to specify nodes in excess of this limit, use "*" or separate the nodes into multiple settings and specify them that way. In this item, there is no differentiation between uppercase and lowercase. The surrogate pair characters cannot be specified.

  Caution

  If a node or group name of the data collection target is changed, the **Target Node** field in entries will not be changed automatically. For this reason, if a node or group name is changed, devices may be excluded from the data collection targets. To continue collecting after node or group name was changed, review this setting. Additionally, when monitoring threshold is configured and if the device is excluded from the collection targets before the change while the "auto recovery type alerts" have been issued, these alerts will be recovered.

- **Interval**

  Specifies the length of the data collection interval using numerical values (1 to 999). Seconds, minutes, and hours can be specified as units.

  Intervals cannot be set for longer than 24 hours. If the interval is short, there is a limit to the number of items that can be collected within the given time.

The limit varies between systems so you need to confirm in advance that there are no problems with the method below.

[Method for checking whether the interval is appropriate]

In the data collection function, a data collection processing log is output to the file below. Start data collection and confirm that the following log is not output to the file.

File:

<On the manager, %installfolder%>\Manager\sg\NvPRO\DataCollect\log\DataCollect.log

Log:

1. NOTE [YY/MM/DD HH:MM:SS] Delay unexecuted collection.
   (LogEntryName=[collection entry title],
   device=[device node name],
   collectTime=[collection time])
2. NOTE [YY/MM/DD HH:MM:SS] Skip unexecuted collection.
   (LogEntryName=[collection entry title],
   device=[device node name],
   collectTime=[collection time])

- **Data Save Setting** checkbox

To save the collected data, check this checkbox. In this case, the data for graph must be saved, however, whether the data for report is saved or not is optional.

1. **Save data for both graph and report**

   By selecting this item, you can display a graph or report.

2. **Save data for only graph**

   If this item is selected, only a graph can be displayed. A report cannot be created, nor be displayed.

Tip

To display the collected data on the Web Console provided by the IMS component, check this checkbox. However, the data that can be displayed on the Web Console is only the data collected with the following rules.

- **Device CPU busy rate for Catalyst series** rule
- The built-in rules of **MIB Expression**
- MIB expression rules newly created and specified a **Type of data**

- **Threshold Setting** checkbox

To monitor the threshold, check this checkbox.

Caution

The data collection rule "Server load" does not support the operation of monitoring threshold. For details, refer to "7.2.6 Server load (page 630)".

- **Comparison method**

  In respect of the relation between the threshold and the collected value, select either one of the following two options.

  1. Detect that the collected value is over the threshold value

2. Detect that the collected value is below the threshold value

- **Threshold**

  Enter a threshold for monitoring.

- **Severity of a threshold excess alert**

  Select the severity for a threshold excess alert to be notified from the following list.

  * **FATAL**
  * **MAJOR**
  * **MINOR**
  * **WARNING**
  * **NORMAL**

- **Alert output condition**

  * **When the threshold is exceeded *n* times in a row**

    When data exceeds the threshold value specified number of times in a row, an alert indicating the threshold excess will be issued.

    + **Recovery Alert**

      If performance data exceeds the threshold value and then data falls below the recovery value, an alert indicating recovery of threshold excess will be issued. When this item is specified, once a threshold excess alert was issued, even if the threshold excess has continued, a threshold excess alert will not be issued again until the recovery alert is issued.

    + **Recovery Threshold**

      Enter a value to determine recovery after the threshold excess.

  * **When the threshold is exceeded *n* times in total**

    + If data exceeds the threshold value specified number of times or more in total within the period specified in the **Duration Schedule**, an alert indicating the threshold excess will be issued at the end of specified period.

    + **Duration Schedule**

      • **Setting**

        Set a period to monitor **When the threshold is exceeded *n* times in total**. Click this button to open the window to set schedule. For details, refer to "4.22 Scheduling (page 426)".

      • **Cancel**

        Cancels the settings.

      • **Property**

        Displays the settings.

- **Apply** button

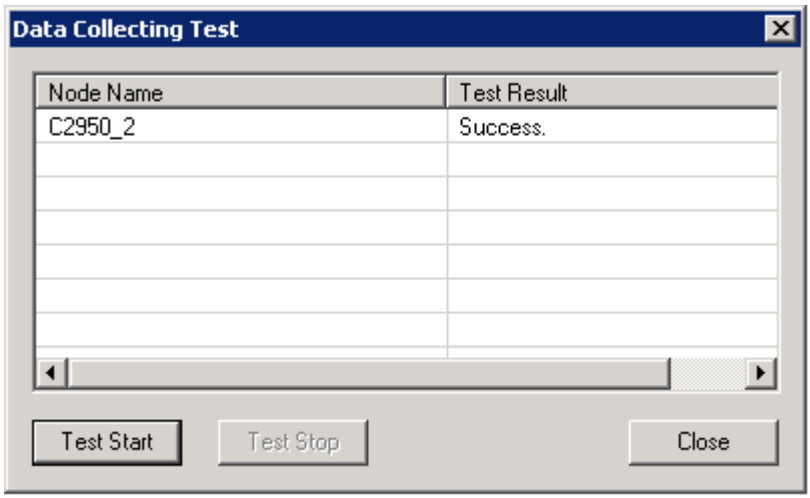
  Registers the data collection entry.

- **Test** button

  Used to confirm that data can be gathered from the target node.

Click **Test** button to open the Data Collecting Test dialog box.

In this dialog box, click the **Test Start** button to start the test and then display the test results in the **Test Result** column. To stop a test that is in progress, click the **Test Stop** button. It may take a long time to complete testing of target nodes if there is a large quantity of target nodes.

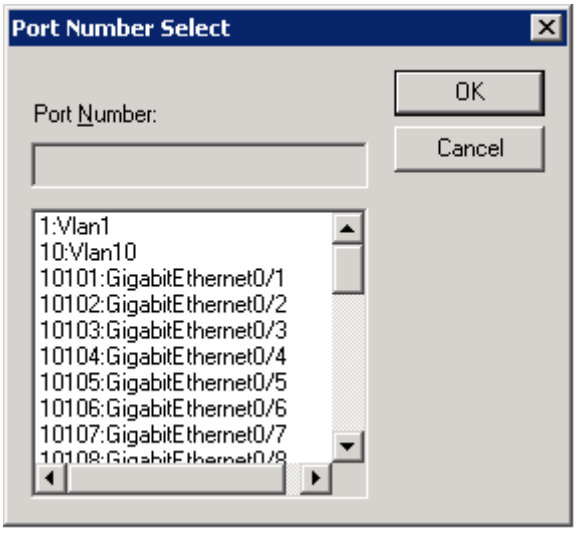


- **Help** button

  Displays Help.

4.16.1.1 Port Number Select dialog box

When creating collection entries of "Traffic of the specific hub port" or "Traffic of the specific hub port(64bit)" in the "4.16.1 Data Collecting Setting window (page 334)", click ... button of **Port Number** to open this dialog box. Select the device port number. If a group is specified in the **Target Node**, if multiple nodes are specified, or if the manager function cannot communicate with the specified node, this dialog box cannot be used.



- **Port Number**

  Select the port number from a list of device ports.

- **OK** button

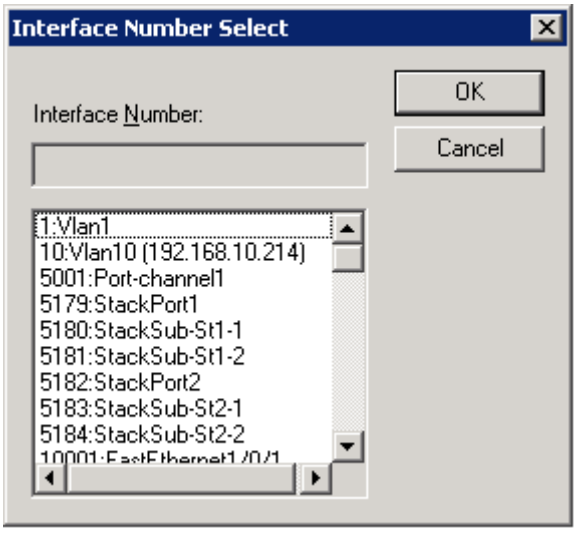
  Applies the set values.

- **Cancel** button

  Cancels selection of the setting.

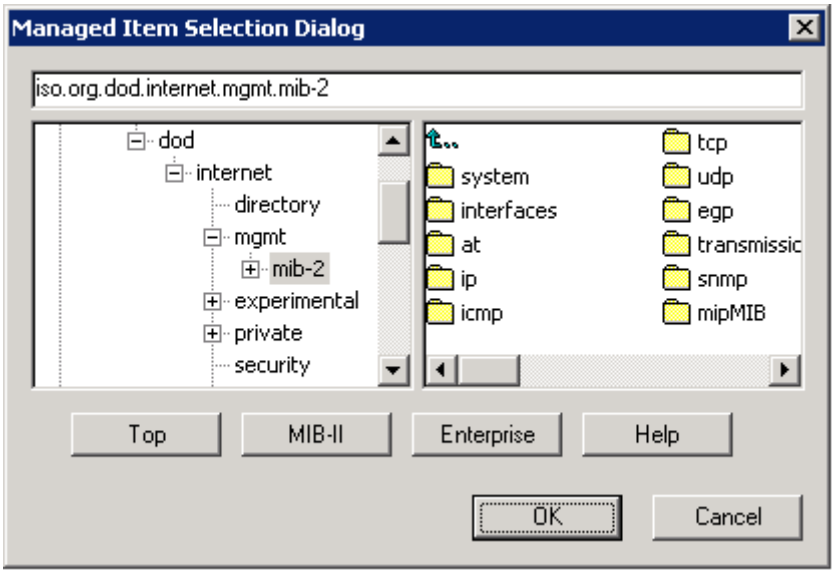
4.16.1.2 Interface Number Select dialog box

When creating "WAN Traffic" and "WAN Traffic (64bit)" rule entries in the "4.16.1 Data Collecting Setting window (page 334)", click ... button of **Interface_Number** to open this dialog box. Select interface numbers. If a group is specified in the **Target Node**, if multiple nodes are specified, or if the manager function cannot communicate with the specified node, this dialog box cannot be used.



4.16.1.3 Managed Item Selection Dialog dialog box

When creating "General" rule entries in the "4.16.1 Data Collecting Setting window (page 334)" click ... button of **Management Item Name** to open this dialog box. Select MIB objects to be collected.



- **Top** button

  Moves operation to the top (iso) of the MIB tree.

- **MIB-II** button

  Moves operation to the top (iso.org.dod.internet.mgmt.mib-2) of MIB-II.

- **Enterprise** button

  Moves operation to the top (iso.org.dod.internet.private.enterprises) of the Enterprise MIB.

- **Help** button

  Displays a description of the selected MIB object in the "4.16.1.4 MIB Description dialog box (page 341)".

- **OK** button

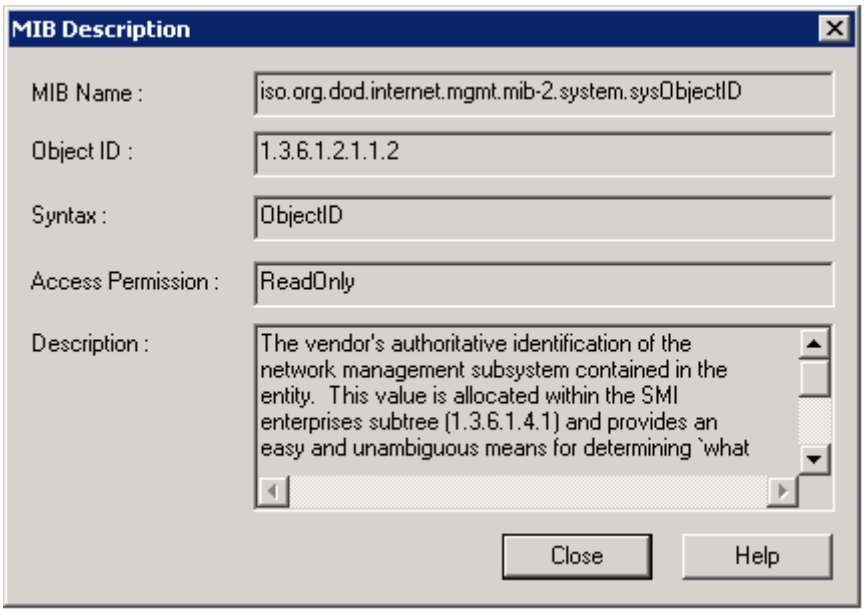
  Applies the settings.

- **Cancel** button

  Cancels selection of the setting.

4.16.1.4 MIB Description dialog box

Select a MIB in the "4.16.1.3 Managed Item Selection Dialog dialog box (page 340)", and then click **Help** button to display the information of the selected MIB.



- **MIB Name**

  Displays the name of the selected MIB as a symbol name.

- **ObjectID**

  Displays the object ID for the selected MIB as a series of numbers.

- **Syntax**

  Displays the type of value that will be used for the selected MIB.

- **Access Permission**

  Displays the rights (Examples: "NotAccessible", "ReadOnly", and "ReadWrite") for the MIB. It may not be possible to perform read and write operations due to settings restrictions on the device side, even if "ReadWrite" is displayed as the access right.

- **Description**

  Displays a description of the contents of the MIB. Depending on MIB, description is written in English, or description may be omitted.

- **Close** button

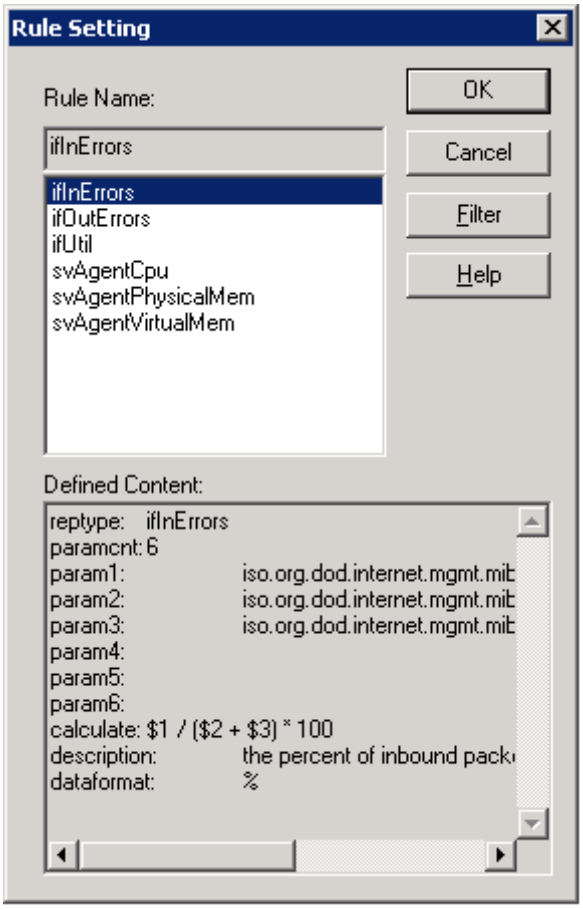
  Closes the dialog box.

- **Help** button

  Displays Help.

4.16.1.5 Rule Setting dialog box

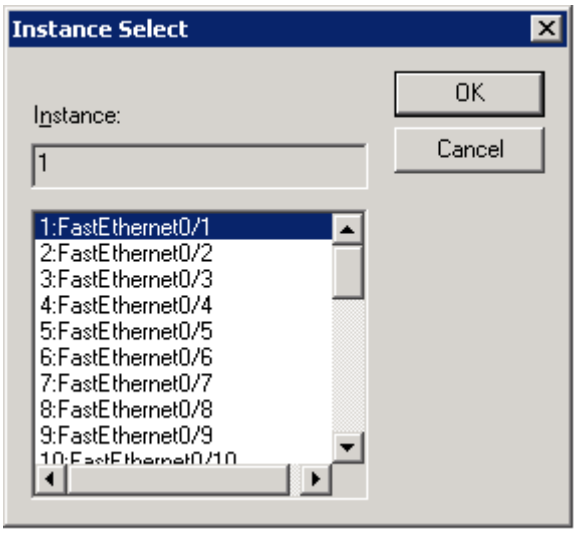
When creating "MIB Expression" rule entries in the "4.16.1 Data Collecting Setting window (page 334)", click ... button of **Rule** to open this dialog box. Select a MIB expression rule.



4.16.1.6 Instance Select dialog box

When creating "MIB Expression" rule entries in the "4.16.1 Data Collecting Setting window (page 334)", click ... button of **Instance** to open this dialog box.

The interface list of the target node is displayed in the Instance Select dialog box. MIB can be selected out of the list when the last element of OID is the interface number. If a group is specified in the **Target Node**, if multiple nodes are specified, and if the manager function cannot communicate with the specified node, this dialog box cannot be used.



4.16.2 Configuring threshold monitoring

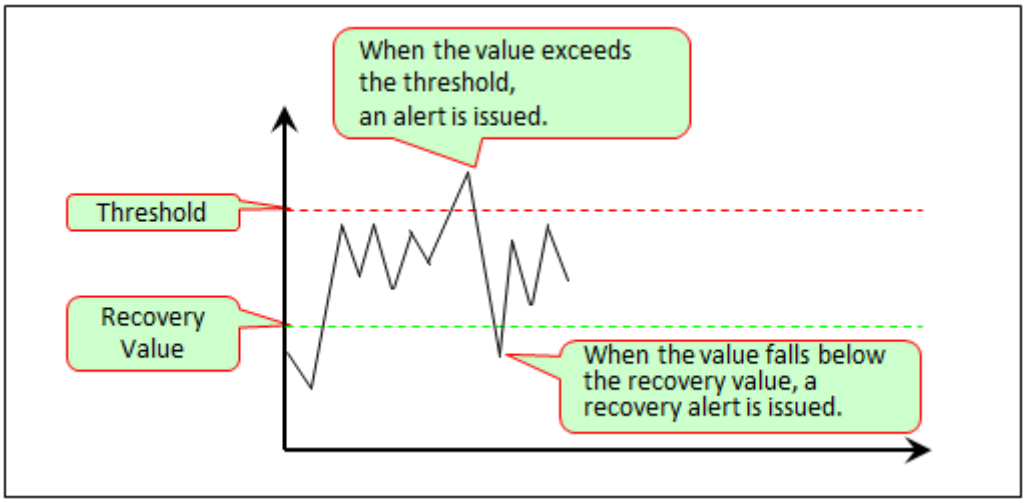
When the threshold monitoring setting is configured, if the obtained value exceeds the threshold value, an alert indicating the threshold excess can be issued.

The threshold monitoring setting is configured for each entry in the collection entry setting pane. Depending on the settings, you can monitor the threshold excess as described below.

Example 1: Basic monitoring of the threshold excess

The conditions to issue an alert is as follows:

- An alert is issued when the obtained value exceeds the threshold "1" time.
- Recovery alert: ON
- Recovery value: Specified

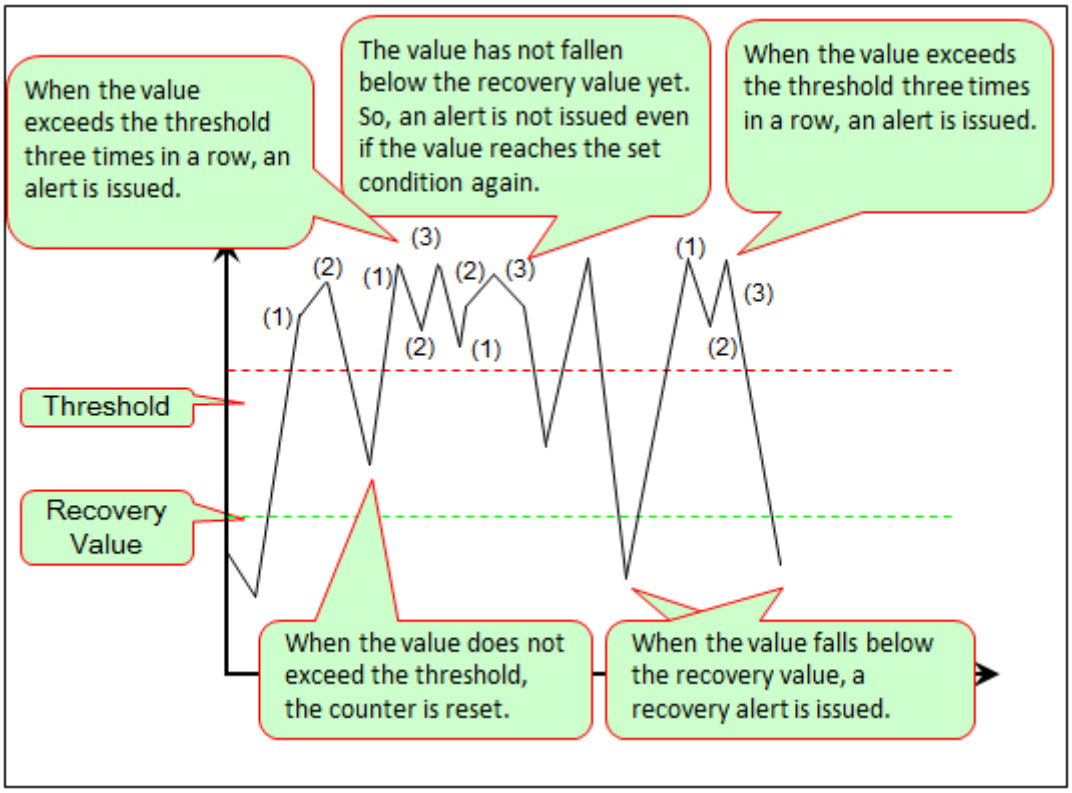


Example 2: Detect the continuous threshold excess

The conditions to issue an alert is as follows:

- An alert is issued when the obtained value exceeds the threshold "3" times in a row.

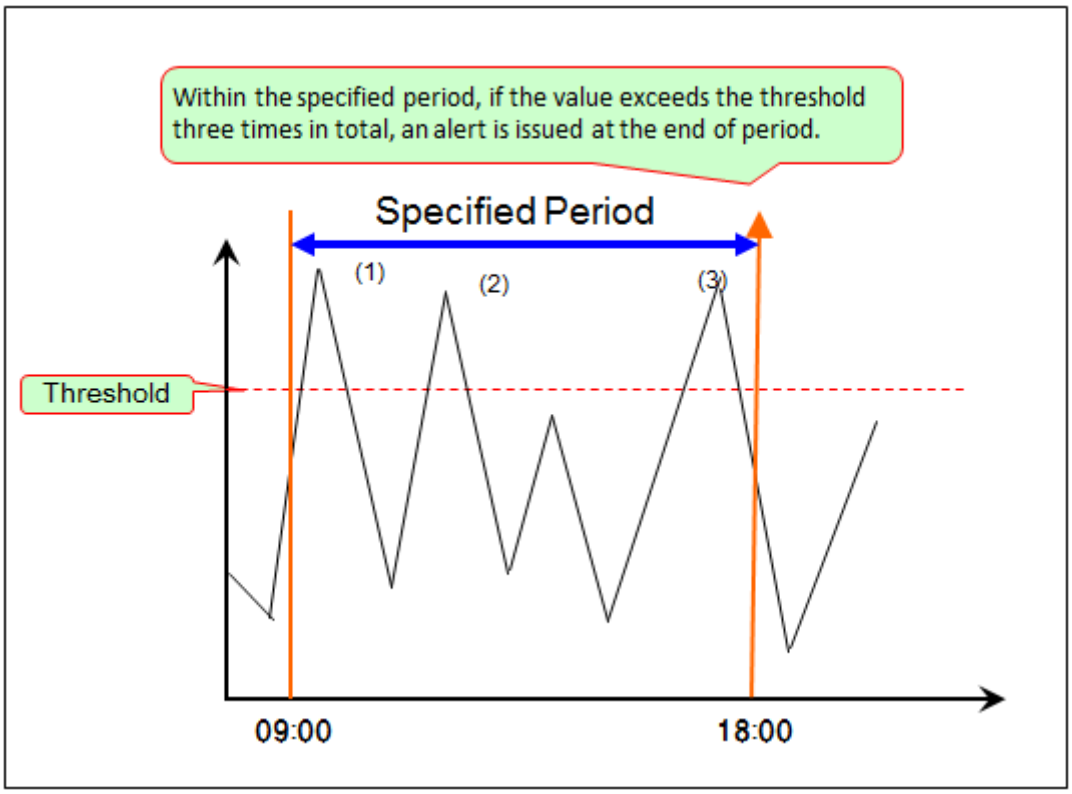
- Recovery alert: ON
- Recovery value: Specified



Example 3: Detect that the threshold excess is occurred specified number of times (or more) within the specified period

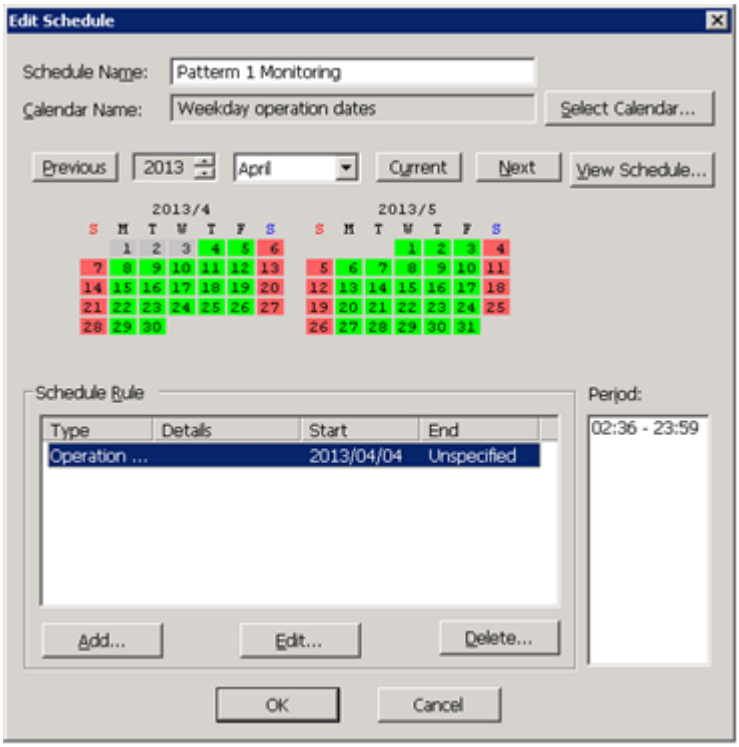
The conditions to issue an alert is as follows:

- An alert is issued when the obtained value exceeds the threshold "3" times in total.
- Duration Schedule: 9:00 to 18:00 on weekday

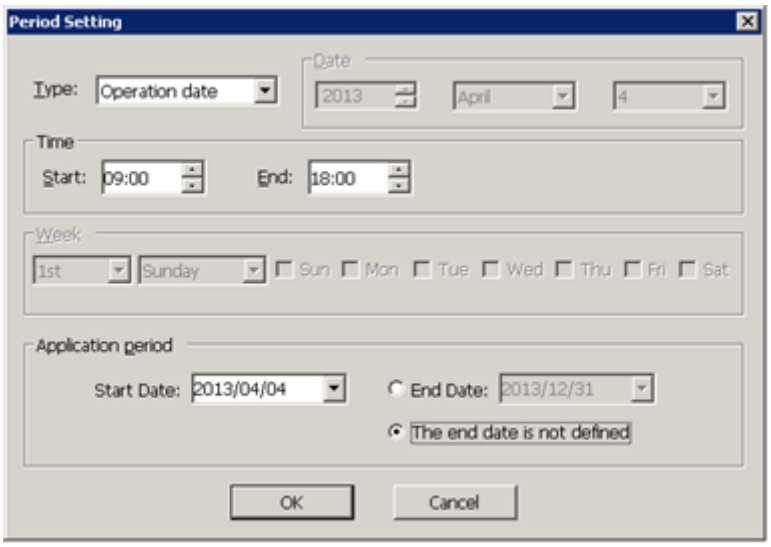


An example of the schedule setting for the above conditions:

1. As a calender, select a calender of weekday operation dates.



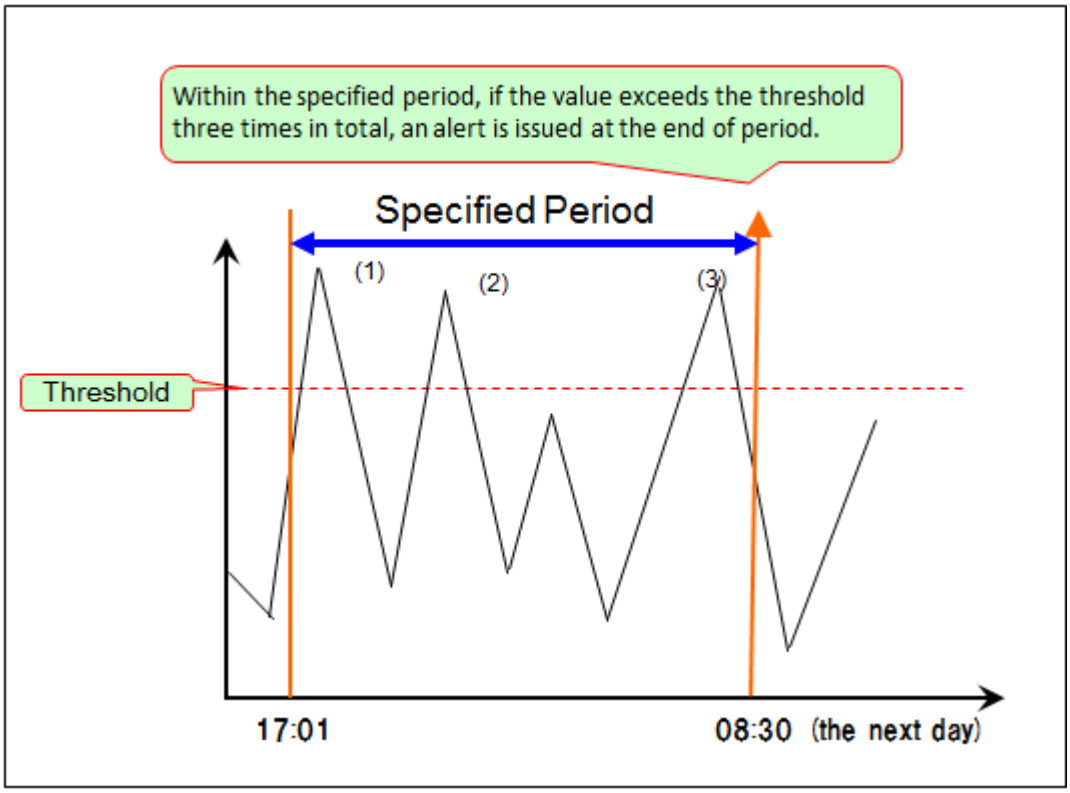
2. As a schedule rule, create a rule enabling 9:00 to 18:00 of the operation dates.



Example 4: Detect that the threshold excess is occurred specified number of times (or more) within the specified period (nighttime)

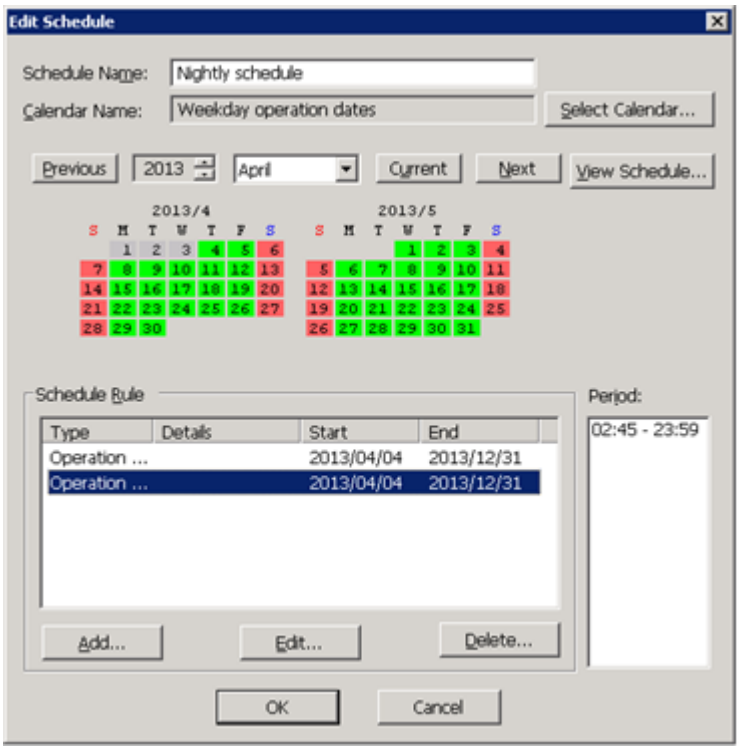
The setting of conditions to output an alert is as follows:

- An alert is issued when the obtained value exceeds the threshold "3" times in total.
- Duration Schedule: 17:01 to 08:30 (next day) on weekday



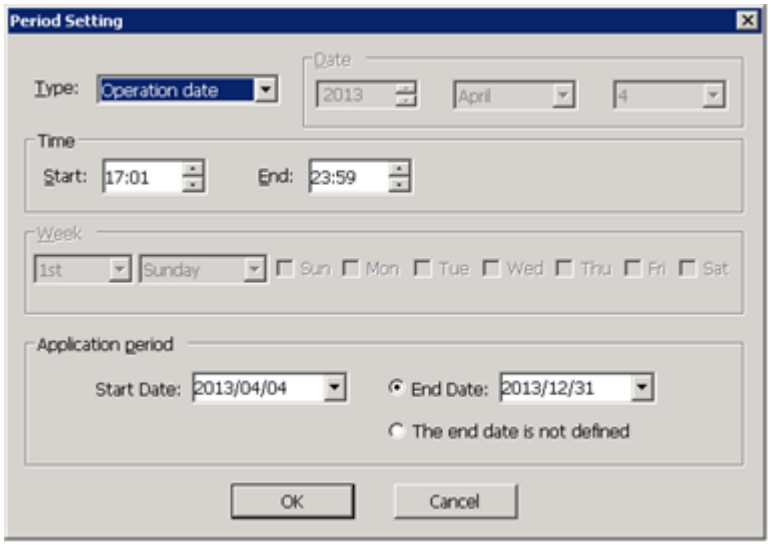
An example of the schedule setting for the above conditions:

1. As a calender, select a calender of weekday operation dates.

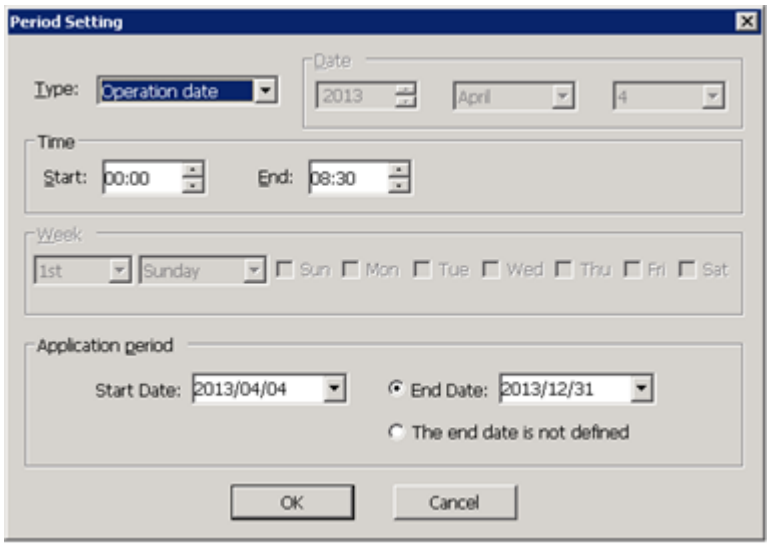


2. As a schedule rule, create a rule enabling the following.

   - 17:01 to 23:59 of the operation date



   - 00:00 to 08:30 of the operation date



⚠ Caution

1. The "Server load" rule does not support the operation of the threshold monitoring. For details, refer to "7.2.6 Server load (page 630)".
2. When the collection targets are multiple expressions or MIB items in "MIB Expression" or "General" rule, expressions and MIB items that are the collection targets are all monitored based on the specified threshold value. If you want to monitor based on the different threshold value, divide the targets into multiple entries. For details of "MIB Expression" rule, refer to "7.2.8 MIB Expression (page 632)". For details of "General" rule, refer to "7.2.9 General (page 634)".
3. In the schedule setting, if the specified end time succeeds to the next start time such as 0:00 to 23:59 and the operation dates are successive, the manager considers the schedule period as the entire successive operation dates.

   For example, under the following conditions, the start time is 0:00 every Monday, and the end time is 23:59 every Friday. Therefore, 23:59 from Tuesday through Thursday is not considered as the end of period.

   - As a calender, select a calender of weekday operation dates.
   - As a schedule rule, create a rule enabling 0:00 - 23:59 of the operation dates.

   If you want to reset the accumulation time of the over threshold on a day-to-day basis, set the specified time so that the end time would not succeed to the start time such as 0:01 to 23:59.

4.16.2.1 Customizing the contents of threshold excess alerts and recovery alerts

For threshold excess alerts and recovery alerts of threshold excess, you can customize the alert summary, details, and sender.

Change the following definition file on the manager.

Use a file "dcconfig.ini.org" placed in the same folder as a base file.

- file: *<On the manager, %sharedfolder%>*\Manager\sg\NvPRO\DataCollect\config\dcconfig.ini

- Default setting of the dcconfig.ini file

```
...
[ThresholdWatch]
ThresholdSummary=Threshold Exceeded(%title%)
ThresholdDetail=The rule[%title%] exceeded the threshold [%overtimes%]
times(Item=[%item%], Threshold=[%tsh%], Recovery Threshold=[%rec%], Set
 Times=[%settimes%]).
RecoverySummary=Threshold Recovered(%title%)
RecoveryDetail=The rule [%title%] recovered from the threshold excess(I
tem=[%item%], Recovery Threshold=[%rec%]).
ThresholdSender=Threshold Watch(%type%)
```

- Detailed explanation of the setting items:

Item name	Description	Variables
ThresholdSummary	The summary text of the threshold excess alert Maximum of 128 characters Default setting: Threshold Exceeded(%title%)	%title%: Collection entry title
ThresholdDetail	The detail text of the threshold excess alert Maximum of 2000 characters Default setting: The rule[%title%] exceeded the threshold [%overtimes%] times(Item=[%item%], Threshold=[%tsh%], Recovery=[%rec%], Set Times=[%settimes%]).	%title%: Collection entry title %overtimes%: Actual number of excess times %item%: MIB name (including index numbers), same as the column name of the corresponding CSV file %tsh%: threshold value %rec%: recovery threshold %settimes%: Times of the over specified threshold
RecoverySummary	The summary text of the recovery alert Maximum of 128 characters Default setting: Threshold Recovered(%title%)	%title%: Collection entry title
RecoveryDetail	The detail text of the recovery alert Maximum of 2000 characters Default setting: The rule[%title%] recovered from the threshold excess(Item=[%item%], Recovery Threshold=[%rec%]).	%title%: Collection entry title %item%: MIB name (including index numbers), same as the column name of the corresponding CSV file %rec%: recovery threshold
ThresholdSender	The sender of an alert of the over threshold value and an alert of recovery from the over threshold. Maximum of 64 characters Default setting: Threshold Watch(%type%)	%type%: Collection rule type

This setting will be valid after the manager function is restarted. For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

4.16.3 Configuring MIB expressions

Use MIB expressions to record and graphically display information that can only be obtained from multiple MIB value calculations.

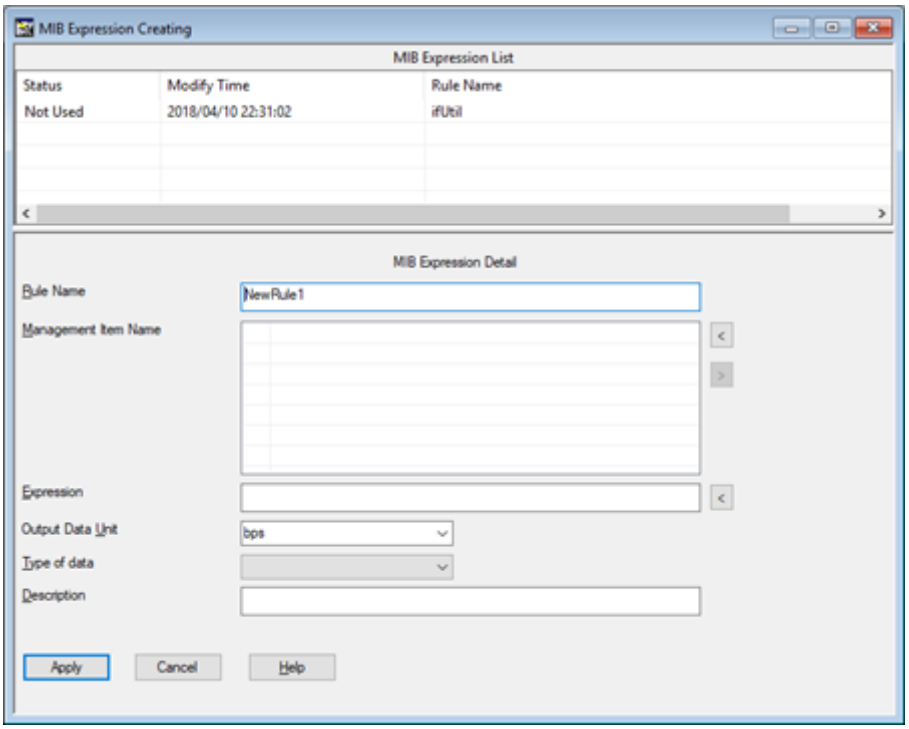
For example, use to calculate the error rate from MIBs that show the overall number of packets and MIBs that show the number of error packets, or to calculate the line usage rate from MIBs that show the line speed and MIBs that show the volume of communication.

To set up MIB expressions, go to the MIB Expression Creating window.

Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**MIB Expression Creating**. For details, refer to "4.16.3.1 MIB Expression Creating window (page 350)".

4.16.3.1 MIB Expression Creating window

To open the MIB Expression Creating window, right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**MIB Expression Creating**.



Tip

- Several rules are standard built in Network Manager. However, those rules are not displayed in the list. For details of the built-in rules, Refer to "7.2.10 Built-in MIB Expression rules (page 636)".
- As an example of MIB expression definition, **ifUtil** rule is provided. Refer to it when creating a new MIB expression rule.

The following describes the items of MIB Expression Detail window.

- **Rule Name**

  Specify a name of the MIB expression. You can specify up to 127 characters. Unicode surrogate pair characters cannot be specified.

- **Management Item Name**

  Specify MIB objects that are the operands of the MIB expression. You can specify up to 20 MIB objects.

  Click **<** button to select MIB object from the "4.16.1.3 Managed Item Selection Dialog dialog box (page 340)".

  If the specified item is the counter-type MIB, an average value per second is used for calculation instead of a raw MIB value. In addition, there are notes for collecting counter-type MIBs. For details, refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

  To specify an MIB object that does not come with Network Manager, first add the MIB to Network Manager. Refer to "7.4 Adding MIBs (page 648)".

  ## Tip

  When instance numbers are not specified in the management items (Example 1), data is collected from the instances specified in the "4.16.1 Data Collecting Setting window (page 334)". When instance numbers are specified in the management items (Example 2), the specified instances are assigned to the operands and data is collected from the specified instances.

  - Example 1: When instance numbers are not specified in the management items
    * Settings in MIB Expression Creating window

      Management Item Name:

      1: iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets

      2: iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets

      Expression: $1 + $2
    * Settings in Data Collecting Setting window

      Instance: 1,2,3,4
    * Data to be collected

      ifInOctets.1 + ifOutOctets.1

      ifInOctets.2 + ifOutOctets.2

      ifInOctets.3 + ifOutOctets.3

      ifInOctets.4 + ifOutOctets.4
  - Example 2: When instance numbers are specified in the management items
    * Settings in MIB Expression Creating window

      Management Item Name:

      1: iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets.3

      2: iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets.4

      Expression: $1 + $2
    * Settings in Data Collecting Setting window

      Instance: empty (not specified)
    * Data to be collected

      ifInOctets.3 + ifOutOctets.4

  If instance numbers are specified in the management items, do not specify instance numbers in "4.16.1 Data Collecting Setting window (page 334)". If you specify instance numbers redundantly, data will not be collected correctly.

Caution

1. If a counter-type or counter64-type MIB, such as the number of packets, is specified in the management items, an average value per unit time (second) is applied to an MIB object specified in "$n" format, such as $1, for calculation instead of a raw MIB value obtained by the SNMP.
2. "Default Ports", specified in the icon properties, is enabled only when an MIB under the following MIBs is selected.
   - iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable (1.3.6.1.2.1.2.2)
   - iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable (1.3.6.1.2.1.31.1.1)

- **Expression**

  Specify a MIB expression. You can specify up to 1023 characters.

  Specify MIB objects in the "$n" format.

  Specify the "+", "-", "*", or "/" operators (all single-byte only). Also can specify "(" or ")".

  Example: $1 * ($2 + $3)

  Specify more than one MIB expression (up to eight). If specifying more than one expression, use a comma "," to separate the expressions.

- **CSV Output Data Unit**

  Specify the collection data unit that is displayed in the report.

  If multiple expressions are specified in the Expression field, specify the same number of units. To specify more than one unit, use a comma "," to separate the units.

  You can specify up to 63 characters in total.

- **Type of data**

  Specify information to identify the data type in the Web Console. In the Web Console, based on the **Type of data**, the collected data is identified, aggregated and analyzed.

  For the **Type of data**, specify one of the following character strings.

Type of data	Description
ifInUtil	Interface Utilization (IN)
ifOutUtil	Interface Utilization (OUT)
ifInDiscards	Packet Loss Rate (IN)
ifOutDiscards	Packet Loss Rate (OUT)
ifInErrors	Packet Error Rate (IN)
ifOutErrors	Packet Error Rate (OUT)
cpuUtil	CPU Utilization
memoryUtil	Memory Utilization

Tip

If you do not specify the **Type of data**, the collected data is not displayed on the Web Console.

- **Description**

  Write a description of the MIB expression. Specify up to 255 characters.

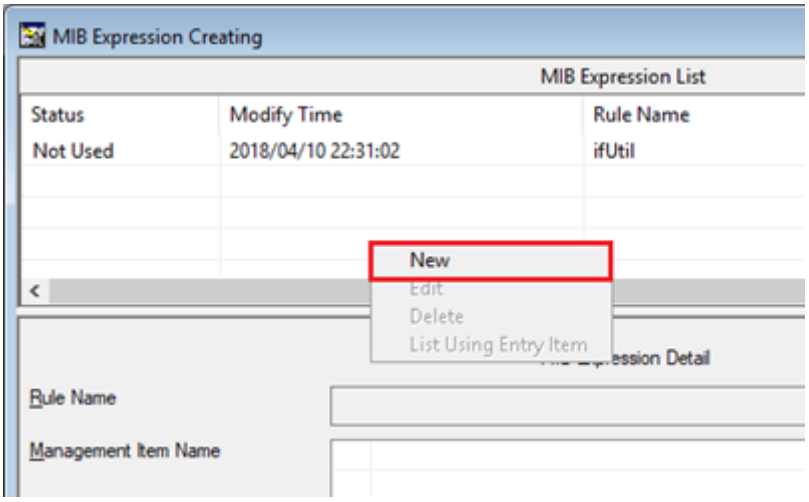
4.16.3.2 Creating a new MIB expression

You must first change to the "configuration mode (page 27)".

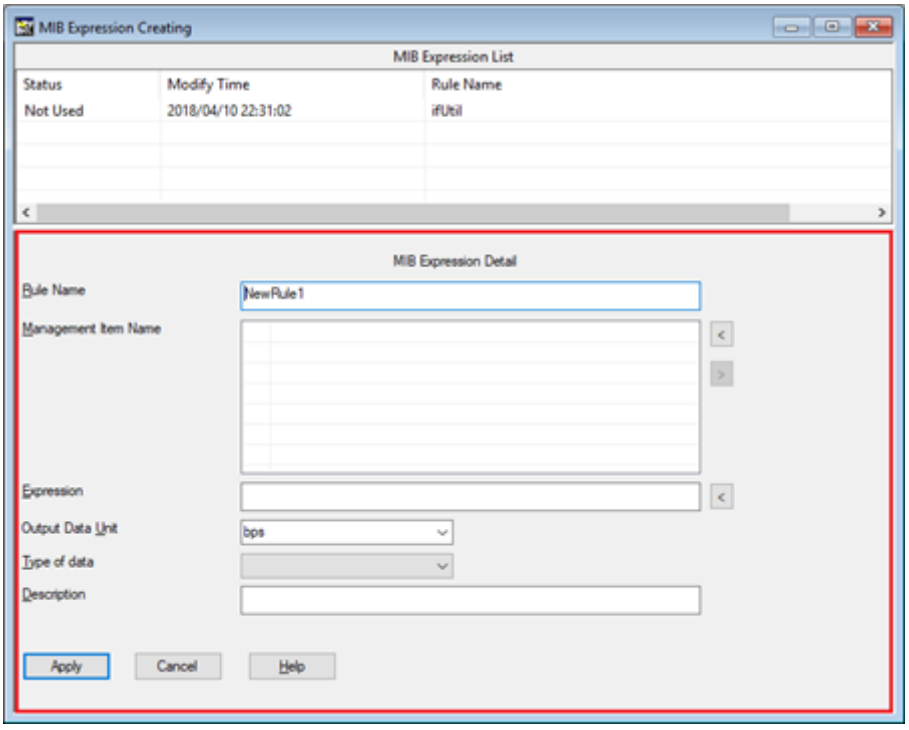
1. Open the "4.16.3.1 MIB Expression Creating window (page 350)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**MIB Expression Creating**.

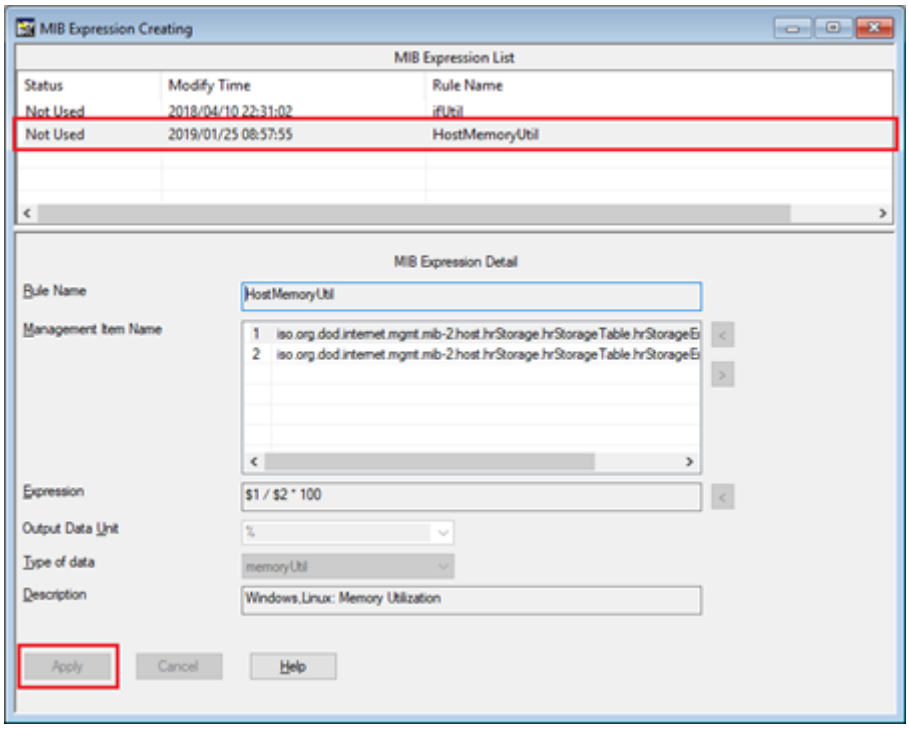
2. Right-click the MIB Expression List pane and select **New** menu.



3. Enter each of the parameters for the MIB expression.



4. To add the MIB expression, click the **Apply** button.



4.16.3.3 Editing a MIB expression

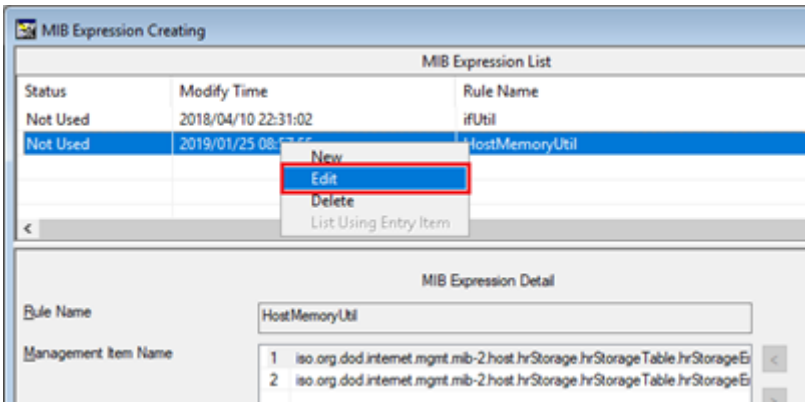
Refer to "4.16.3.5 Checking for entries that are using expressions (page 355)", and check that the MIB expression is not in use.

You must first change to the "configuration mode (page 27)".

1. Open the "4.16.3.1 MIB Expression Creating window (page 350)".

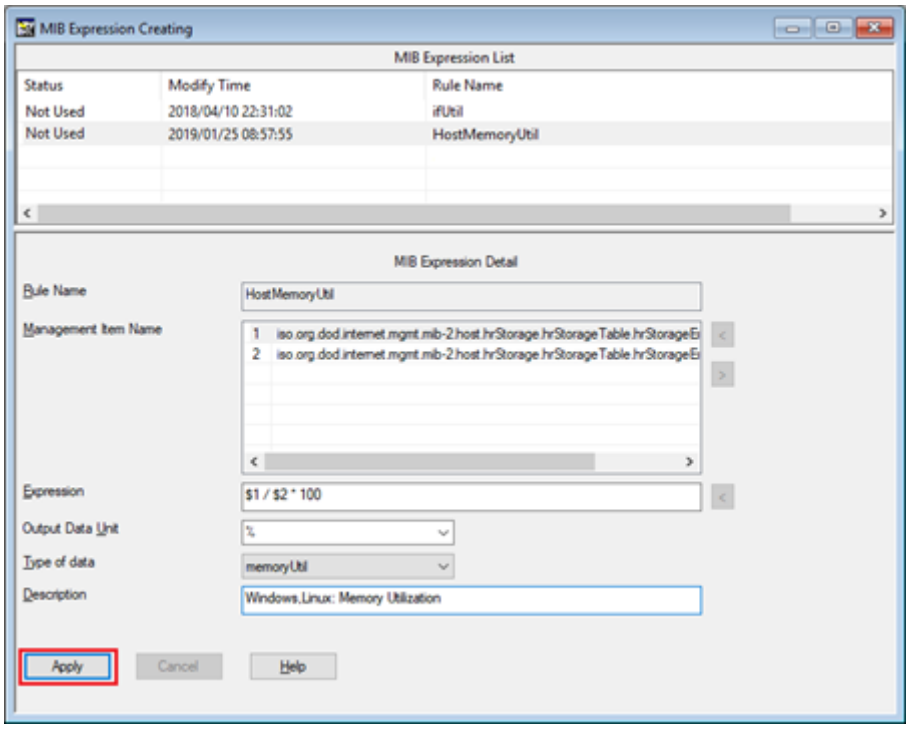
   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**MIB Expression Creating**.

2. Right-click the MIB expression to be edit in the MIB Expression List pane, and select **Edit** menu.



3. Edit each of the MIB expression parameters.

   It is not possible to change the rule name.



4. To apply the changes, click **Apply** button.

4.16.3.4 Deleting a MIB expression

You must first change to the "configuration mode (page 27)".

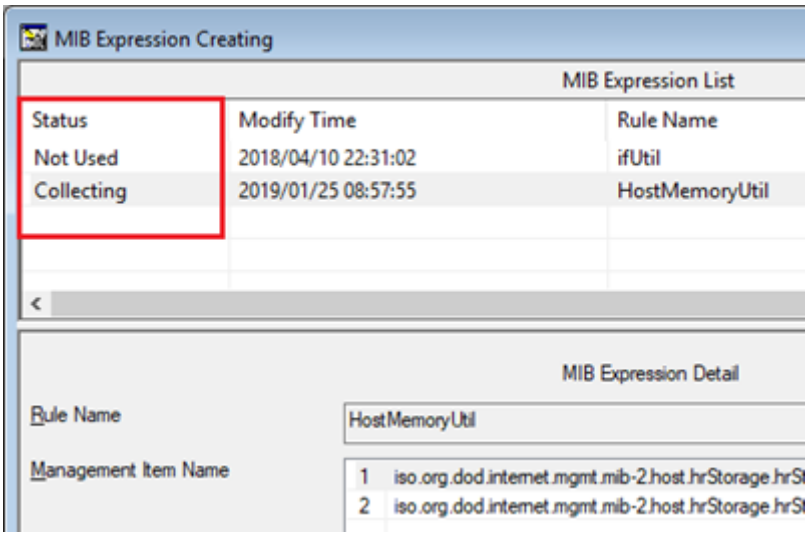
1. Open the "4.16.3.1 MIB Expression Creating window (page 350)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**MIB Expression Creating**.

2. In the MIB Expression List pane, right-click the MIB expressions and click **Delete** button.
3. The confirmation dialog box is displayed. To delete the specified MIB expression, click **Yes** button.

4.16.3.5 Checking for entries that are using expressions

If there are collection entries that are using that MIB expression, it is not possible to edit or delete. Check which expressions are in use by looking at the MIB Expression List pane and seeing whether "Collecting" is displayed in the **Status** column.



To edit or delete a MIB expression that is in use, follow the steps below to stop collecting entries that are using the MIB expression.

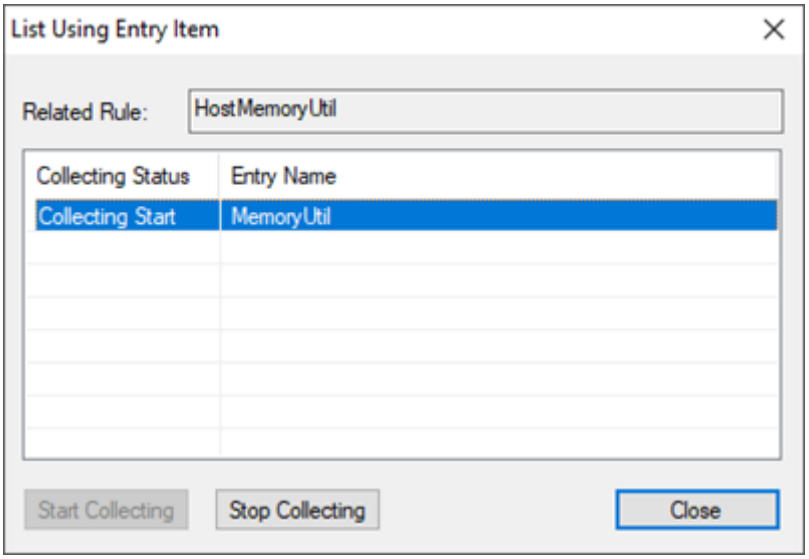
You must first change to the "configuration mode (page 27)".

1. Open the "4.16.3.1 MIB Expression Creating window (page 350)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**MIB Expression Creating**.

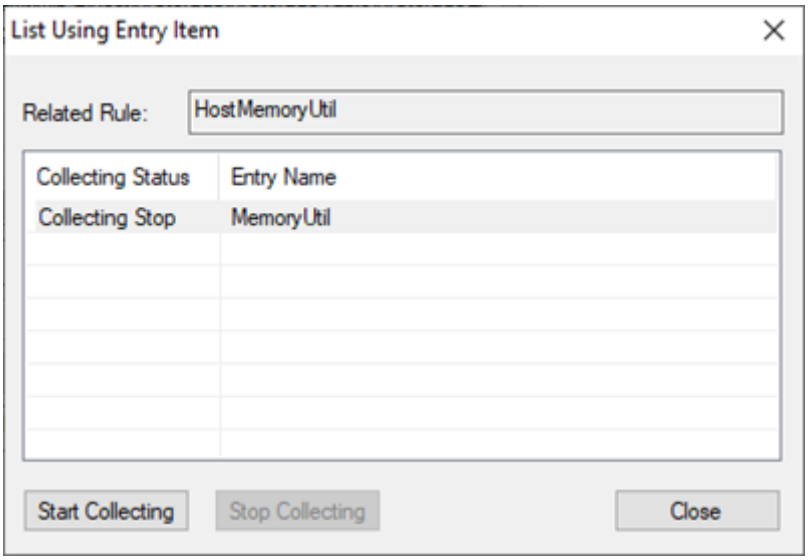
2. In the MIB Expression List pane, right-click the MIB expression and select **List Using Entry Item** menu.

3. In the List Using Entry Item dialog box, stop entry collection by selecting entries with "Collecting Start" status and clicking the **Stop Collecting** button.



4. Restart collecting the entries.

   To start collecting the entries again after editing the MIB expression, open the List Using Entry Item dialog box again and start collecting by selecting entries with "Collecting Stop" status and clicking the **Start Collecting** button.



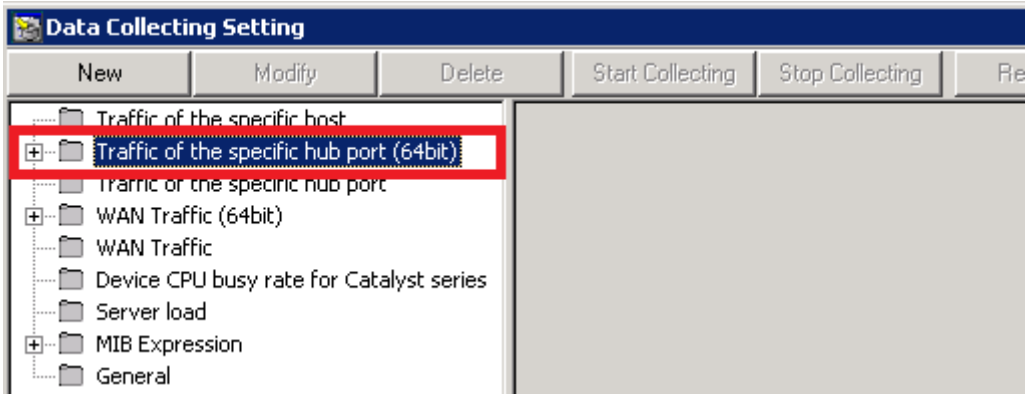
4.16.4 Executing data collection

You must first change to the "configuration mode (page 27)".

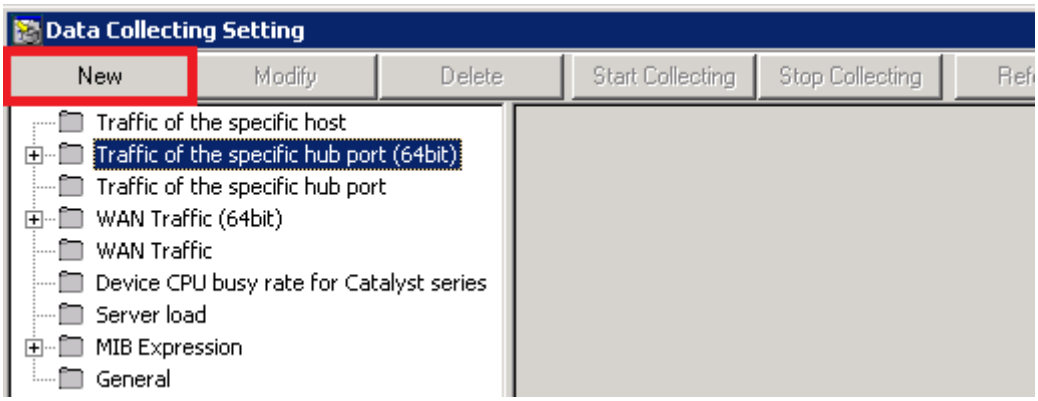
1. Open the "4.16.1 Data Collecting Setting window (page 334)"

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.

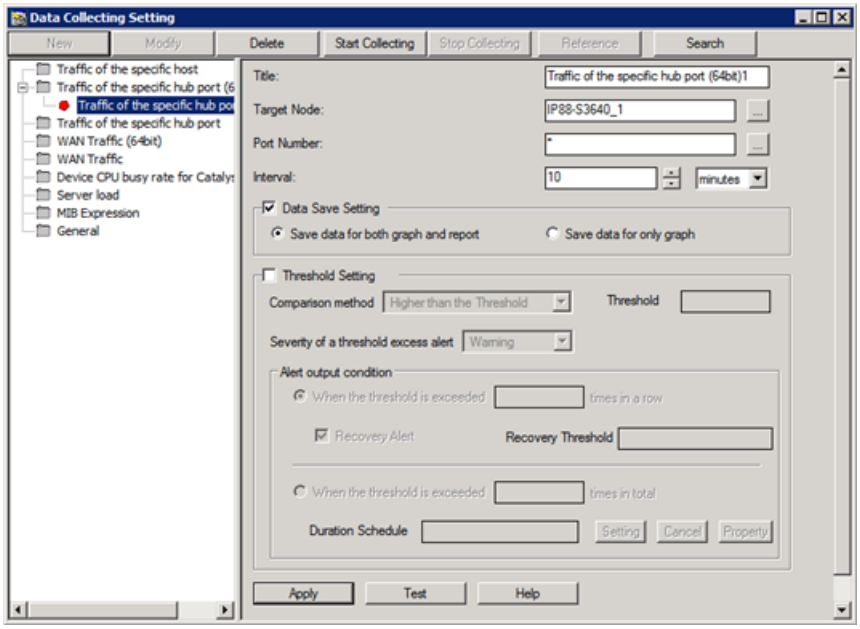
2. Select a data collection rule to execute from the list of collection rules.



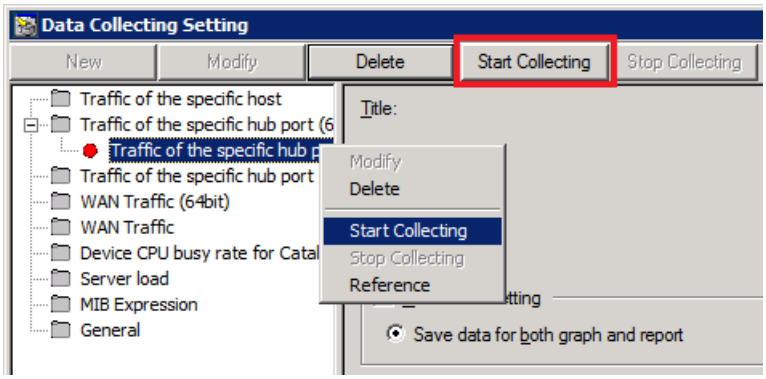
3. Click **New** button on the tool bar.



4. Enter settings in the various fields in the data collection settings entry pane, and then click **Apply** button.



5. Select the collection entry for which values have been entered, and then click the **Start Collecting** button on the tool bar.



Caution

Although the data collection settings can be entered and the start of collection enabled for devices with monitoring mode OFF, the data collection itself will not start. The data collection for that device will begin once monitoring mode changes to ON.

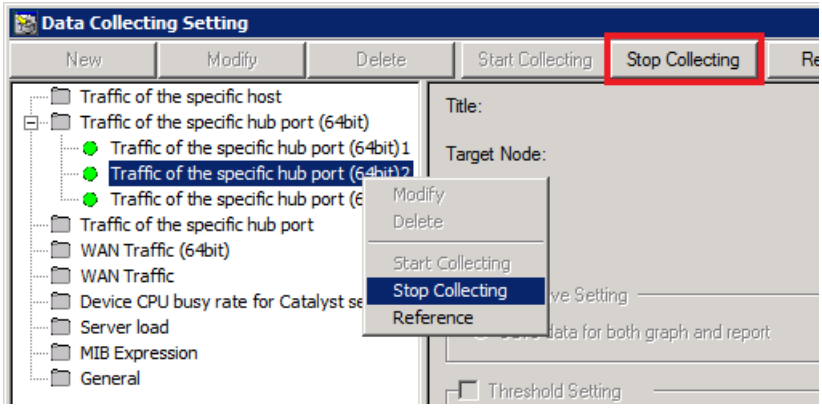
4.16.5 Deleting a data collection entry

You must first change to the "configuration mode (page 27)".

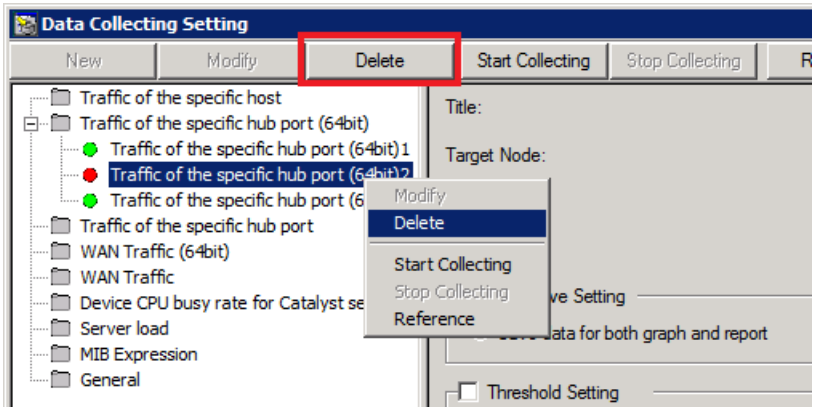
1. Open the "4.16.1 Data Collecting Setting window (page 334)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.

2. If the data collection entry to be deleted is currently executing, click the **Stop Collecting** button to stop execution.



3. Select the data collection entry to be deleted and click the **Delete** button.



4.16.6 Batch registering data collection settings

Data collection settings can be batch registered in Network Manager by importing the information from an external file.

Batch update and delete settings already registered in Network Manager by exporting them to an external file, making the changes, and then importing the file.

4.16.6.1 Data collection settings file format

The rules for writing data collection settings files are outlined below.

- There is support for the following file formats.

  When importing or exporting from the monitoring terminal:

OS	Encoding	BOM	Separator Characters	File Name Extension
Windows	OS multi-byte character encoding	-	Comma	.csv
	Unicode (UTF-16LE)	Yes	TAB	.txt

  When importing or exporting using the Manager command:

Manager OS	Encoding	BOM	Separator Characters	File Name Extension
Windows	OS multi-byte character encoding	-	Comm	.csv

Manager OS	Encoding	BOM	Separator Characters	File Name Extension
	Unicode (UTF-16LE)	Yes	TAB	.txt
Linux	UTF-8	No	TAB	.txt

- Lines beginning with the "#" symbol are treated as comment lines.
- Write the item names in the first line (excluding comment lines).
- Each line shows one collection entry.
- If registering and deleting using the same file, the deletions are performed first, regardless of the order of lines in the file.
- If there are entries with the same "Title" in multiple lines, a latter row is valid.
- If the first line contains "#Format: [~OriginalItem]", the tilde (~) at the beginning of each item is ignored. When exporting, "#Format: [~OriginalItem]" is exported to the first row and a tilde is added to the beginning of each item.

  Some tools used to verify an export file or create an import file have an automatic correction function and some output values (input values) will be displayed (inputted) as a different value. You can stop the auto correction of data by adding a tilde (~) to the beginning of each item.

Description Format

The description format of the data collection setting information is as follows:

Column Name	Description of Setting	For Reg.	For Del.
Register Entry	To register, specify *"1"*. To delete, do not specify anything.	Yes	
Delete Entry	To delete, specify *"1"*. To register, do not specify anything.		Yes
Start Collect	To start collecting immediately when registering, specify *"1"*. If do not want to start collecting, specify *"0"*.	Yes	
Report Type	Specify the string that corresponds to the data collection rule. The following are the strings that correspond to each data collection rule. ***host_trf*** **:** Traffic of the specific host ***64hub_trf*** **:** Traffic of the specific hub port(64bit) ***hub_trf*** **:** Traffic of the specific hub port ***64wan_trf*** **:** WAN Traffic(64bit) ***wan_trf*** **:** WAN Traffic ***sv_sys*** **:** Server load ***_repType1*** **:** Device CPU busy rate for Catalyst series ***_mib*** **:** MIB Expression	Yes	

Column Name	Description of Setting	For Reg.	For Del.
	***(Nothing specified)*:** General		
Title	Specify the title of the collection entry. The format for the title is the same as when setting it using the GUI.	Yes	Yes
Object Device	Specify the name of the target node. The format for the name is the same as when setting it using the GUI.	Yes	
Port/Interface/Instance	Specify the port number, interface number, or instance number, depending on the rule. **Traffic of the specific hub port(64bit):** *Port number* **Traffic of the specific host:** *Port number* **WAN Traffic(64bit):** *Interface number* **WAN Traffic:** *Interface number* **MIB Expression:** *Interface number* **Rules other than the above:** *(Blank)* The format for these items is the same as when setting them using the GUI.	Yes	
Manage Item	Only specify the MIB OID for "General" rules. In all other cases, do not need to specify anything.	Yes	
Interval	Specify the collection interval. The format is "number + unit". The unit is seconds: S or s; minutes: M or m; hour: H or h. **Examples:** 30s, 10m, 1h The specified ranges for each of the units are as follows: **Seconds:** 1 - 999 seconds **Minutes:** 1 - 999 minutes **Time:** 1 - 23 hours This column can be omitted. If omitted in a new entry, the default value: 10 minutes is set. If omitted in an existing entry, the predefined setting remains as it is.	Yes	
CSV File Output	To write collected data to a CSV file, specify *"1"*. If do not want to write the data to a CSV file, specify *"0"*. If do not save to a CSV file, will only be able to display graphs; will not be able to create reports. If a value other than *"0"* or *"1"* is set, or nothing is set, the following value is set. For a new entry, *"1"* is set.	Yes	

Column Name	Description of Setting	For Reg.	For Del.
	For an existing entry, the existing setting remains as it is.		
Output Data Process/MIB Expression Rule Name	• If the collection rule is "General": This specified the method of processing output data. The strings to specify are the following. *bps*: Processing method is "bps" *pps*: Processing method is "pps" *perc*: Processing method is "%" (percentage) *diff*: Processing method is "Differential" *abs*: No processing • If the collection rule is "MIB Expression": This specifies the MIB expression. The format for the expression is the same as when setting it using the GUI. • Other than the above: Do not need to specify anything.	Yes	
Operation mode	Specify the operation mode to execute the data collection or the threshold monitoring. ***1*** **:** Data collection mode ***2*** **:** Threshold monitoring mode ***3*** **:** Data collection + threshold monitoring mode	Yes	
Threshold	Specify a threshold value to be monitored in the range of 0 to (2^{64} - 1).	Yes	
Severity	Specify the severity level of alerts indicating the threshold excess. ***0*** **:** FATAL ***1*** **:** MAJOR ***2*** **:** MINOR ***3*** **:** WARNING ***4*** **:** NORMAL If any value other than the above is set, see below: • When *"1"* (data collection mode) is set to [Operation mode]: Despite the specified value, *"3"* (WARNING) is set. • When *"2"* (threshold monitoring mode) or *"3"* (data collection + threshold monitoring mode) is set to [Operation mode]: - If any value other than the above is set, or if no value is set in the newly registered entry, *"3"* (WARNING) is set. - If no value is set in the existing entry, the existing setting remains as it is. If any value other than the above is set, 3 (WARNING) is set.	Yes	

Column Name	Description of Setting	For Reg.	For Del.
	If no value is set in the newly registered entry, 3 (WARNING) is set. If no value is set in the existing entry, the existing setting remains as is.		
Compare	As a method to compare threshold value, specify one of the following options. ***0*** **:** Detect that the obtained value exceeds the threshold ***1*** **:** Detect that the obtained value falls below the threshold If no value or any value other than the above is set, *"0"* is set .	Yes	
Alert Output Condition	As a condition to issue an alert indicating the threshold excess, specify one of the following options. ***0*** **:** Consecutive ***1*** **:** Cumulative If no value or any value other than the above is set, *"0"* is set .	Yes	
Continuous Times	When [Alert Output Condition] is set to consecutive, specify the number of times that is used for issuing a threshold excess alert. Specify a value in the range of 1 to 10000. • When *"2"* (threshold monitoring mode) or *"3"* (data collection + threshold monitoring mode) is set to [Operation mode]: - When *"0"* (Consecutive) is set to [Alert Output Condition], importing fails if no value or a value with the invalid range is set. - When *"1"* (Cumulative) is set to [Alert Output Condition], *"1"* is set despite the setting value. • When *"1"* (data collection mode) is set to [Operation mode]: Despite the setting value, *"1"* is set.	Yes	
Recovery Alert	Specify whether a recovery alert is issued or not. ***0*** **:** Not issued ***1*** **:** Issued If no value or any value other than the above is set, *"0"* is set .	Yes	
Recovery Threshold	Specify a value used for determining the recovery from the the threshold excess. Specify a value in the range of 0 to (2^{64} - 1). It must be less than the threshold value when [Compare] is set to *"0"*, and must be grater than the threshold value when [Compare] is set to *"1"*. • When *"2"* (threshold monitoring mode) or *"3"* (data collection + threshold monitoring mode) is set to [Operation mode]: - When *"0"* (Not issued) is set to [Recovery Alert]: no value is set despite the setting value. - When *"1"* (Issued) is set to [Recovery Alert]:	Yes	

Column Name	Description of Setting	For Reg.	For Del.
	importing fails if no value or a value with the invalid range is set. • When *"1"* (data collection mode) is set to [Operation mode]: Despite the setting value, no value is set.		
Total Times	When [Alert Output Condition] is set to *"1"* (Cumulative), specify the number of times that is used for issuing a threshold excess alert. Specify a value in the range of 1 to 10000. • When *"2"* (threshold monitoring mode) or *"3"* (data collection + threshold monitoring mode) is set to [Operation mode]: - When *"1"* (Cumulative) is set to [Alert Output Condition], importing fails if no value or a value with the invalid range is set. - When *"0"* (Consecutive) is set to [Alert Output Condition], *"1"* is set despite the setting value. • When *"1"* (data collection mode) is set to [Operation mode]: Despite the setting value, *"1"* is set.	Yes	
Schedule Name	When [Schedule Import Export File] is specified, specify a schedule name defined in the file. When [Schedule Import Export File] is not specified, specify the existing schedule name configured for the data collection function.	Yes	
Schedule Import Export File	Specify a schedule import/export file name using an absolute path. The schedule import/export file is output with a file name "SchImport_*YYYYMMDDhhmmss*.txt" in the same folder as the schedule information configuration file. This item is valid only when batch registration is performed from the monitoring terminal. When batch registration is performed by `nvpdatacolconf` command on the manager, this column is treated as omitted.	Yes	

Sample file

The import sample files are stored in the following directory:

<On the monitoring terminal, %installfolder%>\Svc\sg\NvPRO\ DataCollect\Sample\

<On the manager, %installfolder%>\Manager\sg\NvPRO\DataCollect\Sample\

The file with a "csv" extension uses OS multi-byte character encoding, and commas as delimiters.

The file with a "txt" extension uses Unicode (UTF-16) character encoding, and TAB as delimiters.

Import Content	File Name
Register data collection settings.	Sample_DataEntryImport.csv Sample_DataEntryImport.txt

4.16.6.2 Importing data collection settings

Import a data collection settings file from the monitoring terminal GUI or by running commands on Manager.

- "4.16.6.2.1 Importing from the monitoring terminal (page 365)"
- "4.16.6.2.2 Importing using the manager command (page 366)"

⚠ Caution

Import operations place an extra load on the CPU of the manager machine, sometimes resulting in delayed response. Connections from other monitoring terminals during import operations are not recommended.

Importing from the monitoring terminal

Importing of the data collection settings is executed in the Data Collenting Information Import and Export dialog box.

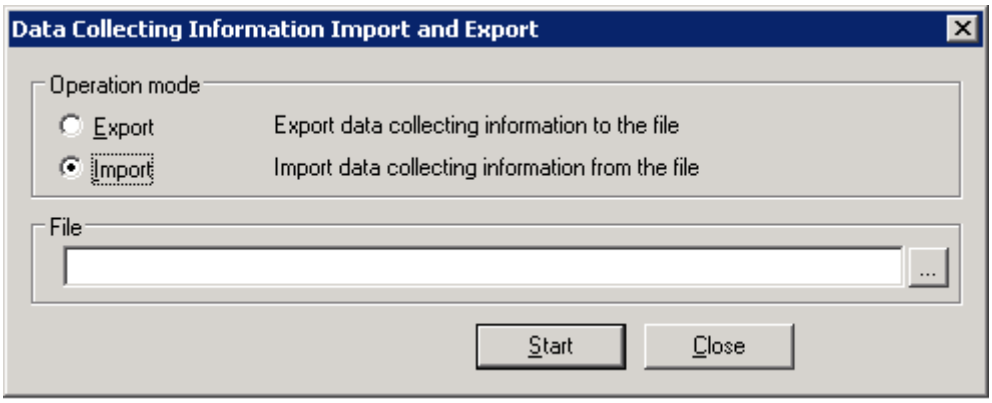
You must first change to the "configuration mode (page 27)".

1. Prepare the data collection setting information file.

   For details, refer to "4.16.6.1 Data collection settings file format (page 359)".

2. Open the Data Collenting Information Import and Export dialog box.

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**Entry Information Import and Export**.



3. In **Operation mode**, select **Import**.
4. Specify the import file with the absolute path in the **File** column.
5. Click **Start** button.

   Tip

   When a dialog box appears to confirm of overwriting or deletion, hold down SHIFT and click **Cancel** button to process all remaining rows without confirmation. (This dialog box will not appear again.)

6. In the completion dialog box, click **Operation Log** button and confirm the import results.

   For details, refer to "4.16.6.4 Operation log file (page 367)".

   Also, if there are rows that cannot be registered due to entry error, etc., these row are saved in another file as an "error record file". For details, refer to "4.16.6.5 Error record file (page 368)".

Importing using the manager command

1. Prepare configuration information file.

   For details, refer to "4.16.6.1 Data collection settings file format (page 359)".

2. Run the data collection settings batch registration command (`nvpdatacolconf`).

   ```
   > cd <%installfolder%>\Manager\bin
   > nvpdatacolconf import <import file name>
   ```

   For details, refer to "9.12.1 Data Collection Config Command (nvpdatacolconf) (page 734)".

3. Open the operation log file and confirm the import results.

   The command result and the operation log file path are displayed in the standard output and standard error output. For details, refer to "4.16.6.4 Operation log file (page 367)".

   Also, if there are rows that cannot be registered due to entry error, etc., these row are saved in another file as an "error record file". For details, refer to "4.16.6.5 Error record file (page 368)".

4.16.6.3 Exporting data collection settings

Export data collection settings from the monitoring terminal GUI or by running commands on Manager.

⚠ Caution

The export may fail if specifying a path name for the data collection settings file location that includes "nul" (either uppercase or lowercase).

Specify a path name that does not contain "nul" (either uppercase or lowercase).

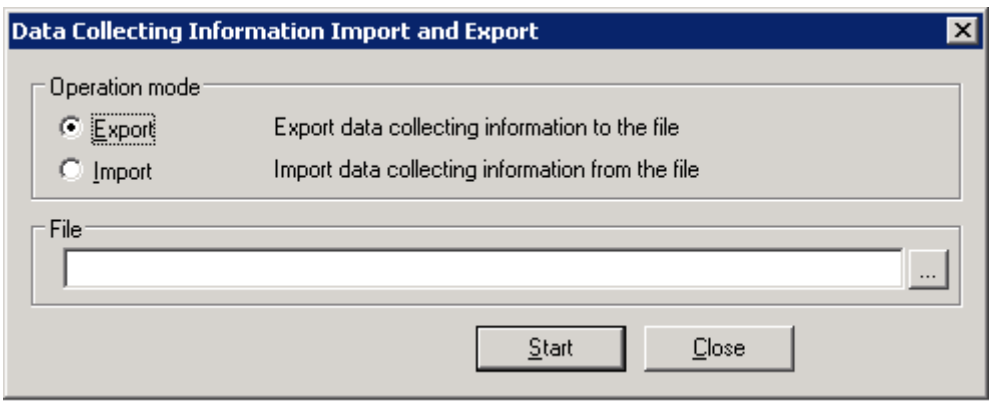
Exporting from the monitoring terminal

Exporting of the data collection settings is executed in the Data Collenting Information Import and Export dialog box.

You must first change to the "configuration mode (page 27)".

1. Open the Data Collenting Information Import and Export dialog box.

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**Entry Information Import and Export**.



2. Select **Export** in the **Operation mode**.

3. Specify an export file name with the absolute path in the **File** column.
4. Click **Start** button.
5. In the completion dialog box, click **Operation Log** button and confirm the export results.

   For details, refer to "4.16.6.4 Operation log file (page 367)".

   For details of the exported file, refer to "4.16.6.1 Data collection settings file format (page 359)".

Exporting from the manager command

You can also use the command for exporting the information of data collection rule entries.

1. Run the data collection setting batch registration command (`nvpdatacolconf`).

   ```
   > cd <%installfolder%>\Manager\bin
   > nvpdatacolconf export <Export file name>
   ```

   For details, refer to "9.12.1 Data Collection Config Command (nvpdatacolconf) (page 734)".

2. Open the operation log file and confirm the export results.

   The command result and the operation log file path are displayed in the standard output and standard error output. For details, refer to "4.16.6.4 Operation log file (page 367)".

   For details of the exported file, refer to "4.16.6.1 Data collection settings file format (page 359)".

4.16.6.4 Operation log file

The following information is output to the operation log file.

- Import

  The result of checking the import file and import operation

- Export

  The results of the export operation

When operating from the monitoring terminal

The operation log backup file uses the name "*%incrementalnumber%*_ImportExportLog.txt". *%incrementalnumber%* starts at 000 and 1 is added each time. The maximum number is 099.

The operation log of activity, prior to the most recent operation, is saved as a backup.

In cases where the number of backup files has already reached 100, when operation commences, the message "`Delete the backup operation log file`" is displayed and the operation is not performed. Delete all unnecessary backup files and retry the operation.

- The log is stored in the following:

  <On the monitoring terminal, %installfolder%>`\Svc\log\NvPROCsvIOConfig\_ImportExportLog.txt`

- The backup logs are stored in the following:

  <On the monitoring terminal, %installfolder%>`\Svc\log\NvPROCsvIOConfig\ImportExportLog`

When operating from the manager command

The operation log is created using the name "*%incrementalnumber%*_ImportExportLog.txt". It stores a maximum of 100 items. *%incrementalnumber%* is a number from 000 to 099. If -log *logfile* argument of the command is specified, the same contents of the operation log file is output to *logfile*.

- The log is stored in the following:

  <On the manager, %installfolder%>\Manager\log\nvpdatacolconf*%incrementalnumber%*_ImportExportLog.txt

4.16.6.5 Error record file

Use the error record file to import only those records that could not be registered or deleted.

Correct the error record file according to the operation log before performing import.

Location of the error record file

Directory

Same directory as the import file

File Name

"TMP_" + *import_file_name.extension*

4.16.7 Maintaining performance data (CSV files, report files)

4.16.7.1 Storage folder and format for performance data (CSV files)

In Network Manager, CSV files are created per 1 day based on performance data collected by the data collection function.

Performance data (CSV file format) and report files are automatically deleted once the period specified in the below definition has passed. This setting can be changed to allow for the requirements and disk capacity of each system.

- File

  <On the manager, %sharedfolder%>\Manager\sg\NvPRO\DataCollect\config\dcconfig.ini

- Setting format

  ```
  Savedays=550
  ```

  (n: days, available range: 0 - 550)

  The default value is 550 days. If "0" is specified, data and report files are not deleted automatically.

When the manger is restarted, the setting will be reflected. For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

4.16.7.2 Automatic generation and automatic deletion of reports

Reports can be automatically generated when dates change, or automatically deleted according to specified retention periods (the same as CSV data file).

Automatically generating reports

The report files are not generated automatically by default. To generate automatically, change the setting as follows.

- File:

  <On the manager, %sharedfolder%>\Manager\sg\NvPRO\DataCollect\config\dcconfig.ini

- Setting format:

  ```
  AutoReport=1
  ```

  (1:automatic generation, 0: no automatic generation)

  If you specify AutoReport=1 for the report files in the definition above, report files will be generated automatically when the date changes. Weekly reports are generated for Sunday to Saturday, monthly reports are generated for the first day until the last day of each month, and annual reports are generated for January 1st until December 31st of each year.

  Default value is 0. If "0" is specified, report files will not be generated automatically.

When the manager is restarted, the setting will be reflected. For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

Automatically deleting reports

Performance data (CSV file format) and report files are automatically deleted once the period specified in the below definition has passed. This setting can be changed to allow for the requirements and disk capacity of each system. If you specify "0", reports will not be deleted automatically as Version 2.0.

- File:

  <On the manager, %sharedfolder%>\Manager\sg\NvPRO\DataCollect\config\dcconfig.ini

- Setting format:

  ```
  Savedays=550
  ```

  (n: days, available range: 0 - 550)

  Default value is 550 days. If 0 is specified, data and report files are not deleted automatically.

When the manager is restarted, the setting will be reflected. For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

4.16.8 Filtering function for performance data passed to other MasterScope products

Cooperation with other MasterScope products

When Network Manager and following MasterScope products, such as MasterScope SystemManager G, are installed on the same service, each MasterScope products can use performance data (MIB data) collected by the data collect function of Network Manager.

The following functions are available.

- MasterScope SystemManager G Invariant Analyzer Option

  On-line analytical function of Invariant Analyzer Option can analyze the performance data collected by Network Manager.

- Displaying performance data on the multi-graph view

  Multi-graph view of other MasterScope products can display performance data collected by Network Manager.

Filtering performance data passed to other MasterScope products

By default, Network Manager passes all performance data to other products.

If it is not necessary to pass all performance data, you can filter unnecessary data. Filtering unnecessary data can reduce a load of other MasterScope products and save the disk space. When Network Manager collects a great deal of performance data, configure the filter settings as necessary.

4.16.8.1 Filtering performance data passed to other MasterScope products

To filter performance data passed to other MasterScope products, you need to create a data filter settings file and import it. By default, the filtering function is disabled, so you also need to enable the function after importing settings.

1. Create a data filter settings file.

   For details, refer to "4.16.8.5 File format of the data filter settings (page 372)".

   A quick and easy way to create a filter settings file is exporting data collection settings to a file and editing it. Edit an exported file of data collection settings as follows.

   - Delete columns unnecessary for a filter settings file.
   - Specify the filter conditions to the items such as "Target device" and "Port number/ Interface number/Instance number".

   For details of exporting data collection settings, refer to "4.16.6.3 Exporting data collection settings (page 366)".

2. Import the data filter settings file.

   To import the created file, execute the following command.

   ```
   > cd <On the manager, %installfolder%>\Manager\bin
   > nvpdatacolfilter import <import file name>
   ```

   For details, refer to "9.12.2 Data Collection Filter Operation Command (nvpdatacolfilter) (page 736)".

   The filter function is disabled by default after Network Manager has been installed. Enable this function in the next step.

3. Enable the data filter function.

   To enable the data filter function, execute the following command.

   ```
   > cd <On the manager, %installfolder%>\Manager\bin
   > nvpdatacolfilter enable
   ```

   For details, refer to"9.12.2 Data Collection Filter Operation Command (nvpdatacolfilter) (page 736)".

   Note that when the data filter function is enabled with no filter settings imported, no data is passed to other MasterScope products.

4.16.8.2 Changing the data filter settings

To change the data filter settings, export the data filter settings to a file, edit the settings file, and import it again.

1. Export the data filter settings to a file.

   ```
   > cd <On the manager, %installfolder%>\Manager\bin
   > nvpdatacolfilter export <export file name>
   ```

   For details, refer to "9.12.2 Data Collection Filter Operation Command (nvpdatacolfilter) (page 736)".

2. Edit the exported settings file.

   Refer to "4.16.8.5 File format of the data filter settings (page 372)", and edit the data filter settings file.

3. Import the data filter settings file.

   ```
   > cd <On the manager%, installfolder%>\Manager\bin
   > nvpdatacolfilter import <import file name>
   ```

   For details, refer to "9.12.2 Data Collection Filter Operation Command (nvpdatacolfilter) (page 736)".

4.16.8.3 Confirming status of the data filter function

To confirm whether the data filter function is enabled or not, execute the command as follows.

1. Execute the command to confirm status of the data filter function.

   ```
   > cd <On the manager, %installfolder%>\Manager\bin
   > nvpdatacolfilter status
   ```

   For details, refer to "9.12.2 Data Collection Filter Operation Command (nvpdatacolfilter) (page 736)".

   The operation status of the data filter function is displayed.

   - When "enabled" is displayed, the data filter function works.
   - When "disabled" is displayed, the data filter function does not work.

4.16.8.4 Stopping and resuming the data filter function

To stop the data filter, disable the filter function. To resume the data filter, enable the filter function.

Even if the data filter function status is changed the data filter settings remain. Thus it is not necessary to import settings again.

- Stopping the data filter function.

```
> cd <On the manager, %installfolder%>\Manager\bin
> nvpdatacolfilter disable
```

For details, refer to "9.12.2 Data Collection Filter Operation Command (nvpdatacolfilter) (page 736)".

- Resuming the data filter function.

```
> cd <On the manager, %installfolder%>\Manager\bin
> nvpdatacolfilter enable
```

For details, refer to "9.12.2 Data Collection Filter Operation Command (nvpdatacolfilter) (page 736)".

When the data filter function is enabled with no filter settings (in case settings have never been imported, or all settings are deleted), no data is passed to other MasterScope products.

4.16.8.5 File format of the data filter settings

The detailed file format of the filter setting is described below.

- The following file formats are supported. (These formats are the same as the data collection settings information file).

Manager OS	Encoding	BOM	Separator Characters	File Name Extension
Windows	OS multi-byte character encoding	-	Comma	.csv
	Unicode(UTF-16LE)	Yes	TAB	.txt
Linux	UTF-8	No	TAB	.txt

- Lines beginning with the "#" symbol are treated as comment lines.
- Write the item names in the first line (excluding comment lines).
- Each line shows one filter setting.
- If registering and deleting using the same file, the deletions are performed first, regardless of the order of lines in the file.
- If there are entries with the same "Title" in multiple lines, a latter row is valid.
- If the first line contains "#Format: [~OriginalItem]", the tilde (~) at the beginning of each item is ignored.

  When exporting, "#Format: [~OriginalItem]" is exported to the first row and a tilde is added to the beginning of each item.

  Some tools used to verify an export file or create an import file have an automatic correction function and some output values (input values) will be displayed (inputted) as a different value.

  You can stop the auto correction of data by adding a tilde (~) to the beginning of each item.

Description Format

The description format of the filter settings file is as follows:

Column Name	Description of Setting	For Reg.	For Del.
Register Filter	To register filter settings, specify "1". When deleting settings, do not specify anything.	Yes	
Delete Filter	To delete filter settings, specify "1". When registering settings, do not specify anything.		Yes
Title	Specify the title of the collection entry. The format for the title is the same as when setting it using the GUI.	Yes	Yes
Object Device	Specify the name of the target node. The format for the name is the same as when setting it using the GUI.	Yes	
Port/Interface/Instance	Specify the port number, interface number, or instance number, depending on the rule. **Traffic of the specific hub port(64bit) :** *Port number* **Traffic of the specific hub port :** *Port number* **WAN Traffic(64bit) :** *Interface number* **WAN Traffic :** *Interface number* **MIB Expression :** *Instance number* **Rules other than the above :** *(Blank)* The format for these items is the same as when setting them using the GUI.	Yes	

4.17 Collecting Traffic Flow (sFlow) Information

Network Manager receives traffic flow (sFlow) information from specified devices and stores it. Analyze and verify detailed traffic states from the stored traffic flow information.

For example, check which servers are receiving a large amount of communication from which services (protocols).

4.17.1 Registering sFlow agents

To receive and store traffic flow information, register the sFlow agent devices in the sFlow Agent List window.

A maximum of 10 sFlow agents can be set.

sFlow agents with identical IP addresses set cannot be registered.

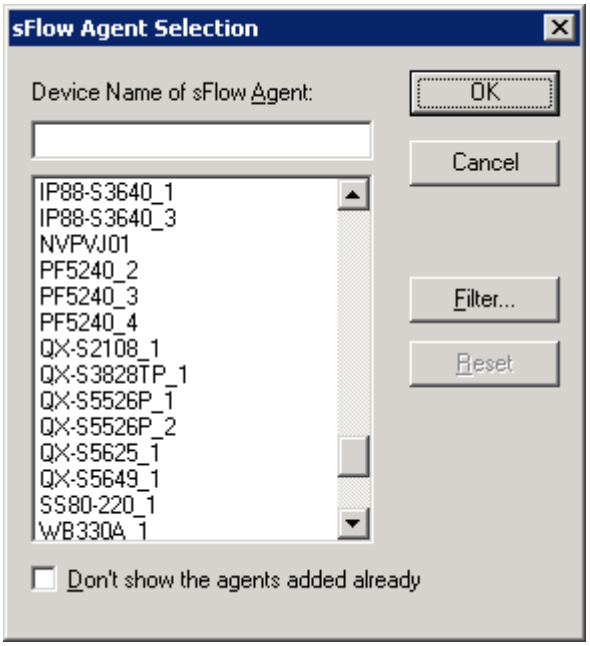
Set a device installed with Network Manager (sFlow collector) beforehand as the sFlow packet destination IP address for sFlow agent devices.

You must first change to the "configuration mode (page 27)".

1. Open the "4.17.1.1 sFlow Agent List window (page 374)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**sFlow Setting**>**sFlow Agent List**.

2. Click **Add** button.
3. In the sFlow Agent Selection dialog box, select the target device, and click **OK** button.

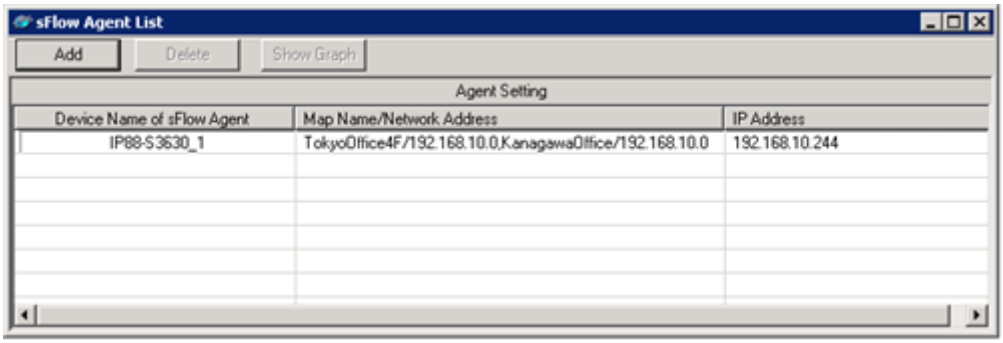


The sFlow Agent Selection dialog box displays all devices registered in Network Manager.

Use the refine function, etc., to select sFlow agents from the displayed devices.

4.17.1.1 sFlow Agent List window

To open the sFlow Agent List window, right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**sFlow Setting**>**sFlow Agent List**.



- **Add** button

  Adds devices to the sFlow agent list. Display the sFlow Agent Selection dialog box, and select the device to be added.

- **Delete** button

  Deletes devices from the sFlow agent list.

- **Show Graph**

  Displays a traffic flow information graph based on information received from selected sFlow agents.

- **Agent Setting**

- **Device Name of sFlow Agent**

  Displays the device name of sFlow agent.

- **Map Name/Network Address**

  Displays the map name with which the sFlow agent is affiliated (only directly above) and network address. If the device is affiliated with multiple maps, map names will be displayed separated by commas.

- **IP Address**

  Displays the IP address of the sFlow agent.

⚠ Caution

If the following operations are performed while this window is opened, the device list in this window is not updated immediately. When you perform one of the following operations, open this window again from the right-click menu.

- Add and delete a device icon.
- Change a device.
- Move an icon to another map.

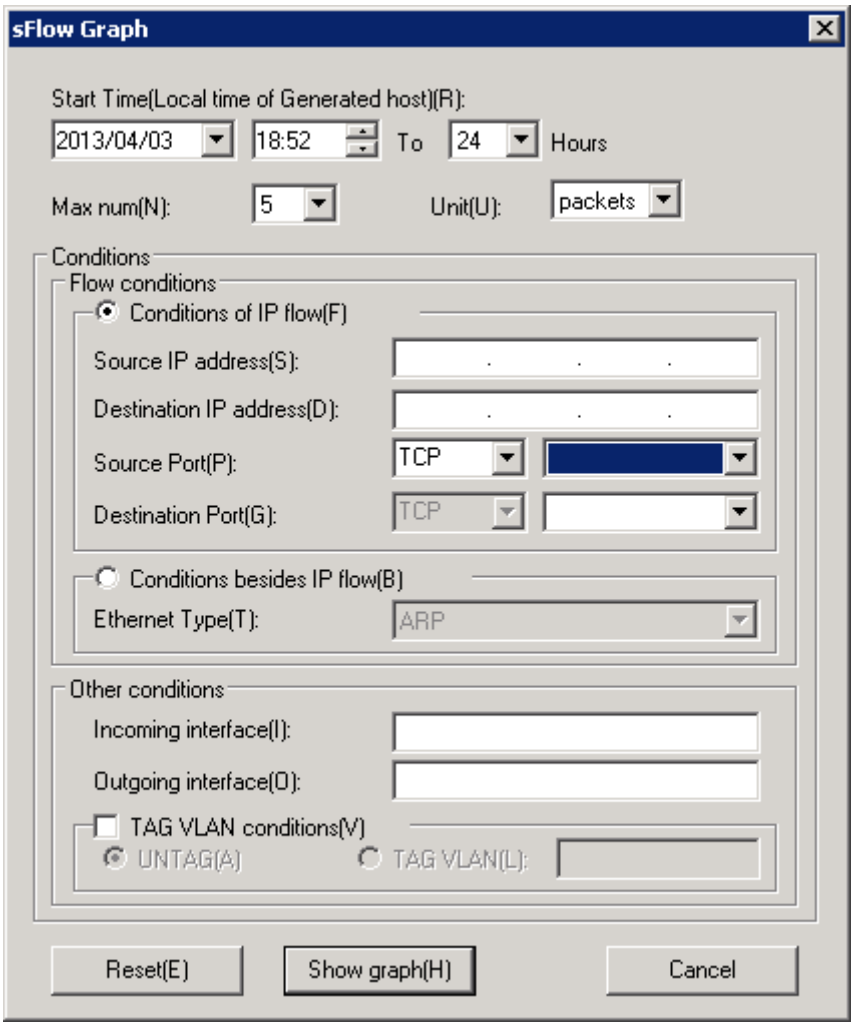
4.17.2 Customizing search conditions

In the sFlow graph display conditions, the port number in the **Conditions of IP flow** can be added. An example of adding "2049/nfsd" to the TCP port numbers list is explained below.

1. Open the *<On the manager, %sharedfolder%>*\Manager\sg\NvPRO\SFlowAnalyzer\portno.ini file using a text editor, add "2049=nfsd" to the [TCP] section, and then overwrite and save.

```
[TCP]
20=ftp
22=ssh
23=telnet
25=smtp
80=http
110=pop3
111=sunrpc
179=bgp
443=https
2049=nfsd

[UDP]
67=bootps
68=bootpc
69=tftp
161=snmp
162=snmptrap
514=syslog
```

2. Restarting the sFlow Graph dialog box will reflect the results of the addition.



4.17.3 Setting duration of flow data retention

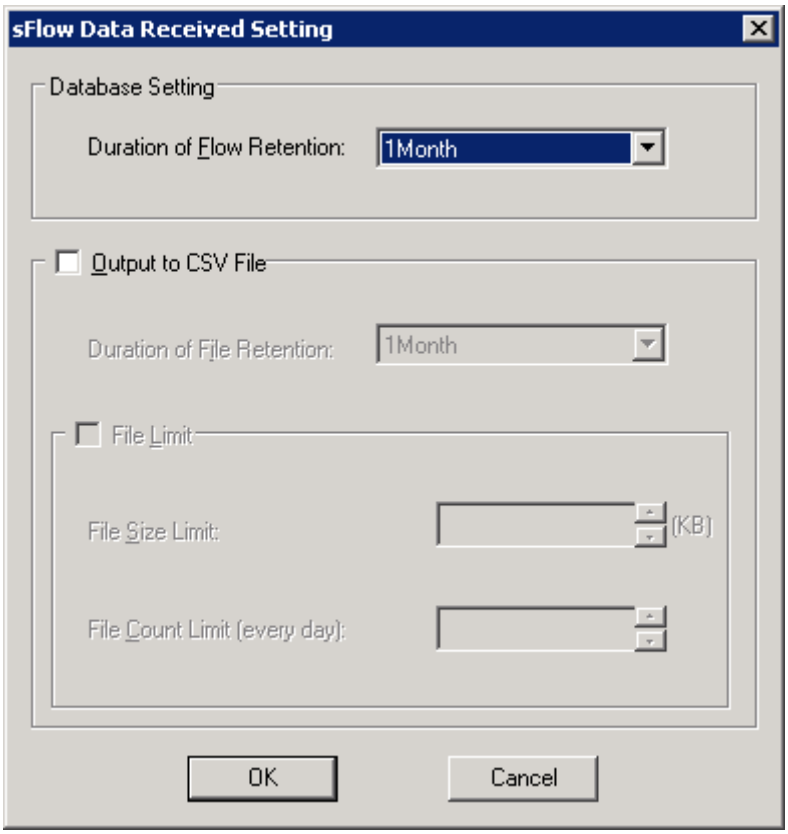
Users can set the collection method for flow data received from sFlow agents.

You must first change to the "configuration mode (page 27)".

1. Open the sFlow Data Received Setting dialog box.

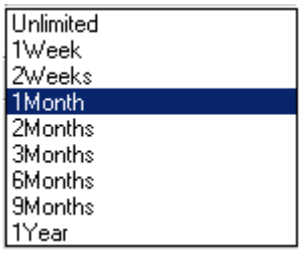
   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**sFlow Setting**>**sFlow Data Setting**.

2. Open the sFlow Data Received Setting dialog box.



- **Database Settings (Duration of Flow Retention)**

  Select the period for which to retain flow data in the database from the drop-down list below. The default value is one month.



Caution

a. When using the database which has the capacity limitation, select an appropriate duration (1 month or less is recommended) so that the database capacity is not depleted.

b. When traffic flow data is accumulated and the database capacity has been exhausted, the oldest data in the database is deleted.

- **Output to CSV File**

  Users can export flow data as a CSV-format file. Default settings are not exported.

- **Duration of File Retention**

  Select the retention period for the CSV file in which flow data is stored from a selection dialog. The default value is one month.

- **File Limit**

  Specify limits for the size and number of CSV files in which flow data is stored. The default maximum file size is 4096 KB. The default maximum number of files is 10.

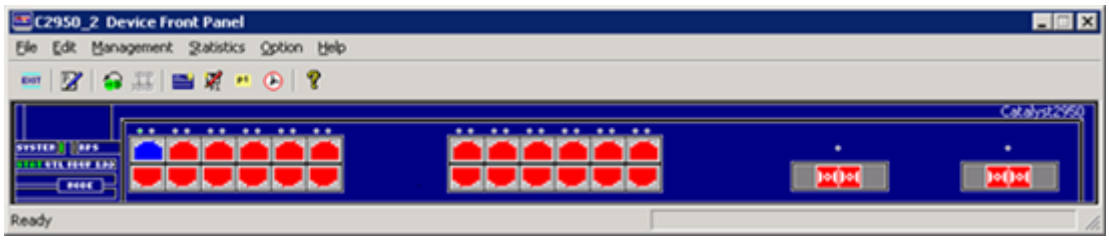
3. Click **OK** button.

4.18 Settings for Displaying Device Front Panel

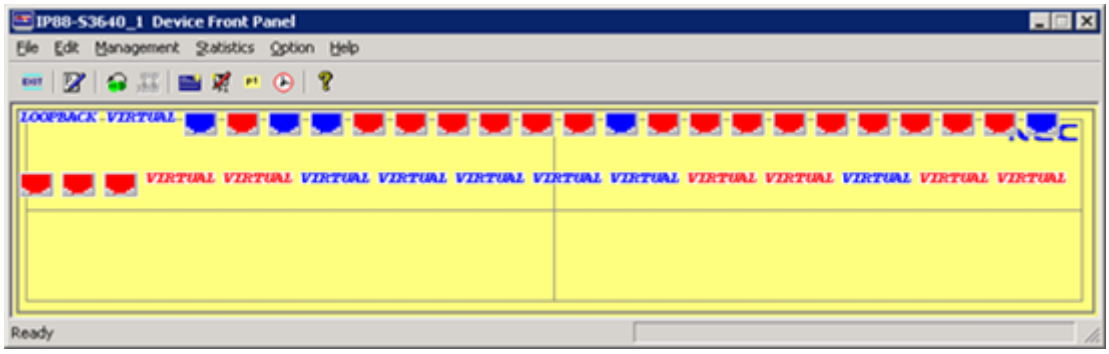
Network Manager can display the front panel image of the device in the window (panel window). In the panel window, you can check port status and various types of information.

The device front panel is displayed either as a supported device specific panel or as a general-purpose panel.

- Example of a supported device front panel:



- Example of a general-purpose device front panel:



The models listed below are supported in displaying the device front panel in a stack configuration. The model supporting the stuck configuration are as follows:

Series Name	Panel window type
PF5459 series	PF5459-48GT-4X2Q, PF5459-48XP-4Q, PF5459-48XT-4Q
Cisco Systems Catalyst3750 series	Catalyst3750-24PS, Catalyst3750-24TS, Catalyst3750G-16TD, Catalyst3750G-12S, Catalyst3750G-24T, Catalyst3750G-24TS, Catalyst3750G-24TS1U
Cisco Systems Catalyst2960 series	Catalyst2960-24TC, Catalyst2960-24TT, Catalyst2960-48TC, Catalyst2960-48TT

A panel window can be displayed per node icon.

For settings for displaying a panel window, refer to "4.18.1 Setting for displaying device front panel (page 379)".

Menus and display of a panel window can be customized per node icon. For information about panel customizing, refer to "4.18.2 Customizing a device front panel (page 380)".

Customized panel window image can be saved as new definition of the panel window (new panel window type). New panel window type can be applied to other node icons which are the same model.

Also, new panel window type definition can be copied into the different monitoring terminals. For details, refer to "4.18.3 Using a customized device front panel for multiple icons (page 389)" and "4.18.4 Using a customized device front panel in other monitoring terminals (page 390)".

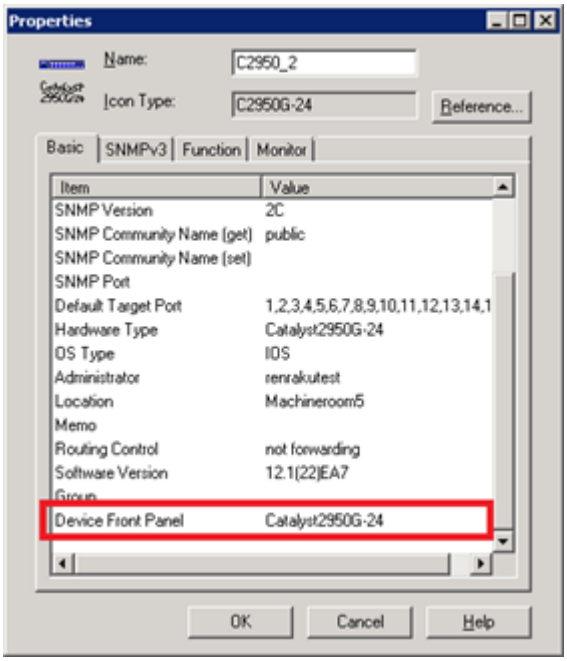
4.18.1 Setting for displaying device front panel

To display the device front panel, set the icon properties shown below and assign NM license to a node icon. The following setting should be configured for SNMP communication in an icon property of node.

- IPv4 address or IPv6 address
- SNMP community name (get) or SNMPv3 information

You must first change to the "configuration mode (page 27)".

1. Right-click the icon and select **Property** menu.
2. The type of displayed front panel window is specified in the icon property **Device Front Panel** for the node.



- When the target node is supported by the Node Manager function, the **Device Front Panel** may be automatically input based on the icon type.

  If the panel window type is empty or not appropriate, specify the appropriate type manually.

- If **Device Front Panel** is empty or set to "NDEVICE", general-purpose device front panel is displayed.

  When the target node is not supported by the Node Manager function, specify "NDEVICE" or leave blank.

Tip

The panel window types, that are newly created according to "4.18.3 Using a customized device front panel for multiple icons (page 389)", are not listed in the **Device Front Panel** field. Specify the name of the panel window type directly.

The list of panel window types newly created can be confirmed in the file below. The name of new panel window type starts with "exp_".

<On the monitoring terminal, %installfolder%>\Svc\sg\NvPRO\NodeManager\export\ PanelList*<new panel type name>*.IMP

3. Click **OK** button.

4.18.2 Customizing a device front panel

The panel windows for supported models can normally be displayed without editing if an appropriate panel window type is selected. If devices have slots for expansion modules (modular-type device) or you select "NDEVICE" (general-purpose device front panel) as the panel window type, it is recommended to edit the device front panel image in order to adjust the panel window to the real device image.

For the panel window for supported models, the following customizations are available.

- "Module port setting (page 380)" (Only for the models that are supported in module port settings)
- "Customizing port displays (page 382)"
- "Editing port positions (page 385)"
- "Editing polling interval (page 388)"

For the general-purpose panel window, the following customizations are available.

- "Editing device front panel background (page 382)"
- "Customizing port displays (page 382)"
- "Editing port positions (page 385)"
- "Editing management and statistics menus (page 385)"
- "Editing MIBs for port status decision (page 388)"
- "Editing polling interval (page 388)"

To clear the customizations and return the panel window to its original state, refer to "4.18.2.8 Clearing panel window customizations (page 389)".

⚠ Caution

1. Panel window editing must be performed on an individual node basis. To apply the same customization for another node which is the same model, refer to "4.18.3 Using a customized device front panel for multiple icons (page 389)" and "4.18.4 Using a customized device front panel in other monitoring terminals (page 390)".
2. Only one of the following windows can start at a time for each node. To start a new dialog box, close the active window before starting another window.
   - Device Front Panel
   - Module Port Settings
   - Customizer

4.18.2.1 Setting module ports

In some cases, it is not possible to display port information at the correct location for devices that have slots for expansion modules. Port information can be displayed at the correct position for

devices compatible with module port settings by using the Module Port Setting dialog box to specify slot No. and module type.

For the models supported by the module port setting, refer to "4.18.2.1.1 List of supported models in the module port setting (page 382)".

⚠ Caution

1. If the module port setting is not set, ports on a module are displayed in an incorrect position on the device front panel.
2. If the model is not supported by the module port setting, set the port positions manually. For editing the port positions, refer to "4.18.2.4 Editing port positions (page 385)".

You must first change to the "configuration mode (page 27)".

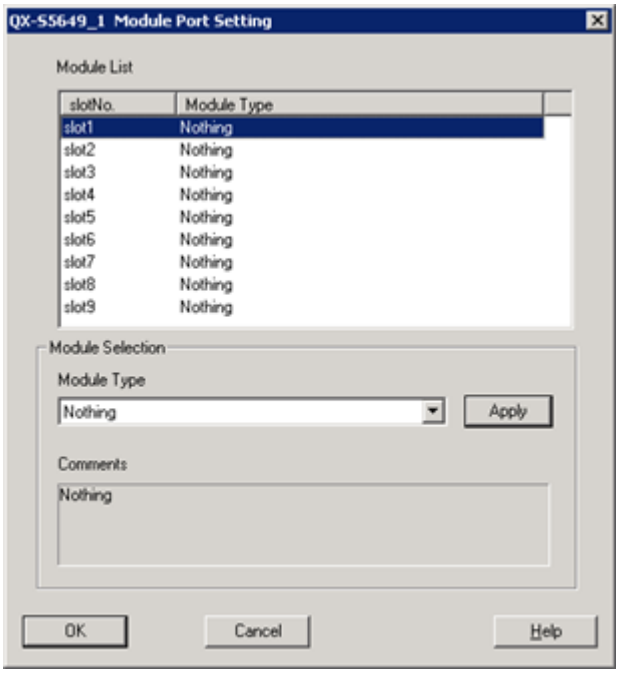
1. Display the device front panel.

   Right-click the device icon and select **Device Front Panel** menu.

   For details, refer to "5.9.1 Opening a device front panel (page 476)".

2. Open the Module Port Setting dialog box.

   In the panel window, select **Edit**>**Module Port Settings** menu.



- **slotNo.** / **Module Type**

  Display information on current slots and the types of modules applied.

- **Module Type**

  Used for the currently selected slot can be chosen from this list.

- **Apply** button

  Reflects the chosen module type. Clicking the button updates the module list.

- **Comments**

  Provides descriptions and other information concerning the selected module type.

3. Perform the following steps for each slot.

a. Select **slotNo.** in **Module List**.

b. Select an appropriate module type out of the list of **Module Type** of the **Module Selection**, click **Apply** button.

List of supported models in the module port setting

Supported models	Module name
Catalyst6506	SupervisorEngine module
	8PortGBIC switching module
	16PortGBIC switching module
	48 port10/100TX switching module
Catalyst6509-E	SupervisorEngine module720-3B
	48 port10/100/1000BASE-TX
	switching module

4.18.2.2 Editing a background of the panel window

You can change the panel background image of the general-purpose panel window.

You must first change to the "configuration mode (page 27)".

1. Display the device front panel.

   Right-click the device icon and select **Device Front Panel** menu.

   For details, refer to "5.9.1 Opening a device front panel (page 476)".

2. In the panel window, select **Edit**>**Change Bitmap** menu.

3. Select the bitmap file name that you want to use as a background image.

   The bitmap file must be in the BMP format.

Caution

a. The size of the port icon cannot be changed. Create the bitmap background image based on the port icon size.

b. When creating a panel window type from the general-purpose panel window, do not specify a file including single-byte space in the file name. Checking will fail at the creation of the panel window type.

4.18.2.3 Editing port displays

The customize ports function can be used to hide some ports and change port attributes. This is useful when not wishing to display all default port information with general-purpose device front panels.

You must first change to the "configuration mode (page 27)".

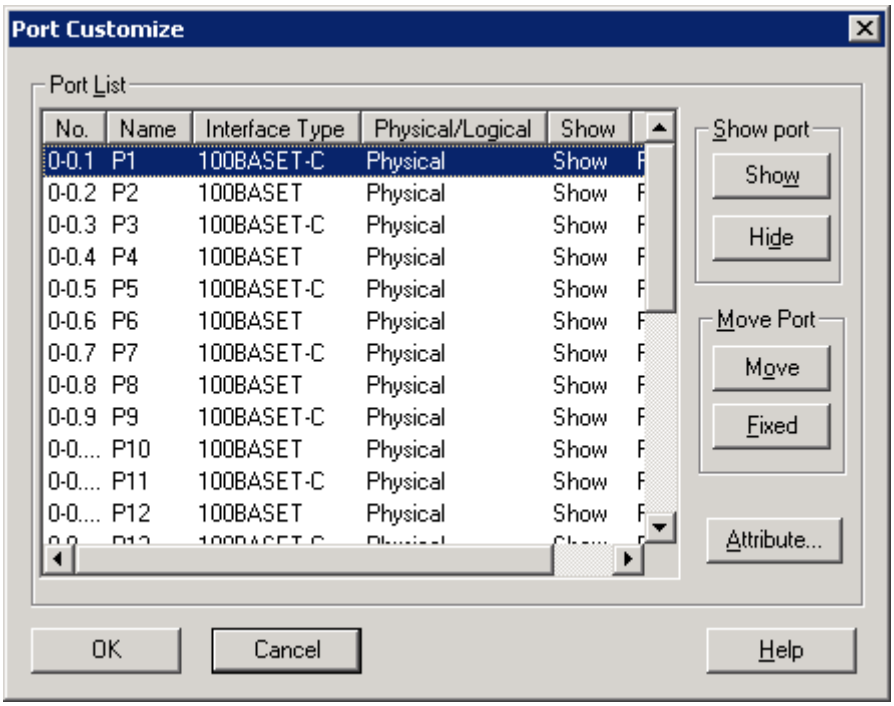
1. Display the device front panel.

   Right-click the device icon and select **Device Front Panel** menu.

   For details, refer to "5.9.1 Opening a device front panel (page 476)".

2. Open the "4.18.2.3.1 Port Customize dialog box (page 383)".

   In the panel window, select **Edit**>**Port Customize** menu.



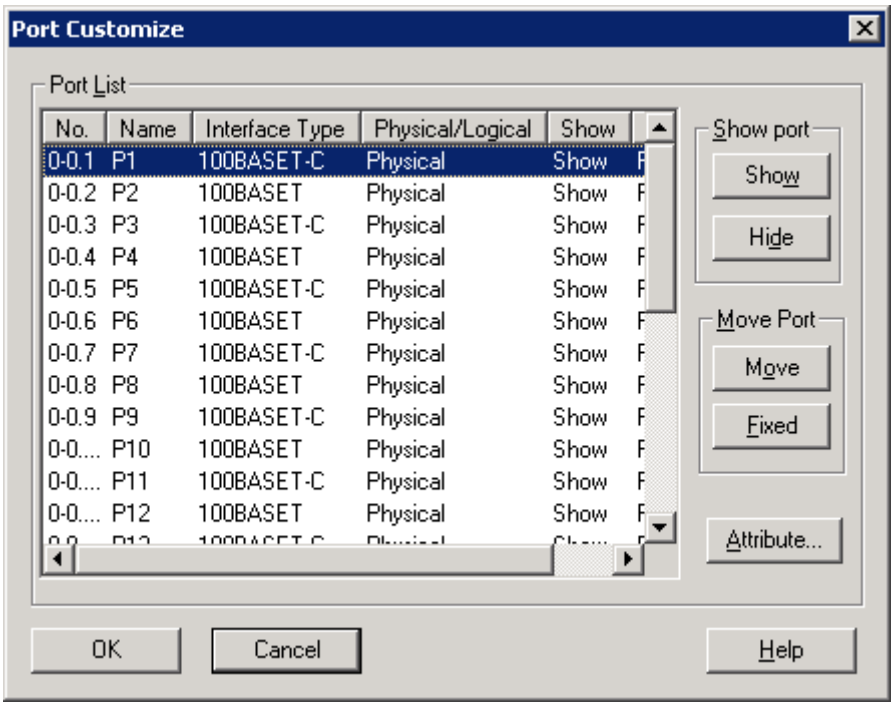
3. To show or hide a port, select a port from the **Port List** and click **Show**/**Hide** button in the **Show port**.
4. To move or fix a port position, select a port from the **Port List** and click **Move**/**Fixed** button in the **Move Port**.

   Only the port that **Move** button is clicked can be moved on the panel window.
5. To change a port name and port type (icon), select a port from the **Port List** and click the **Attributes** button, and then edit the appropriate settings.

   For information on the various procedures, click the **Help** button in the Customize Ports dialog box and browse the displayed Help files.
6. Click **OK** button to save the customized settings.

   Save Position menu does not need to be executed.

Port Customize dialog box



- **No.**

  Displays the port number.

- **Name**

  Displays the port name.

- **Interface Type**

  Displays the port type currently selected for the port.

- **Physical/Logical**

  Displays whether a port is physical or logical. "Physical" indicates a physical port and "Logical" indicates a logical port. The default setting for the general-purpose device front panel is all physical.

- **Show**

  Displays whether a port is displayed in the device front panel. "Show" indicates the port is displayed and "Hide" indicates it is not. The default is set to "Show" status for physical ports and "Hide" status for logical ports.

- **Move**

  Displays whether a port can be moved or not in the edit mode of the panel window. "Move" indicates the port can be moved, "Fixed" indicates the port is fixed (cannot be moved).

- **Show**/**Hide** button in **Show port**

  Show or hide the selected port in the panel window.

- **Move**/**Fixed** button in **Move Port**

  Move or fix the selected port in the panel window. The movable ports can be moved after the port customization has been completed.

- **Attributes** button

  Displays and enables editing of attribute information (port name, port type) for the selected port.

4.18.2.4 Editing port positions

For the general-purpose panel window or the model implementing the extension module that is not supported by the module port setting, you can change the port positions to adjust them to the actual front panel.

Since some ports are not currently displayed, you should confirm the port information to be changed in the "port customization" function in advance.

If port position cannot be change, in the Port Customize dialog box, click **Move** button in **Move Port**. For details, refer to "4.18.2.3 Editing port displays (page 382)".

You must first change to the "configuration mode (page 27)".

1. Display the device front panel.

   Right-click the device icon and select **Device Front Panel** menu.

   For details, refer to "5.9.1 Opening a device front panel (page 476)".

2. Click-hold a port and drag-and-drop it using a mouse to change a port position.

   Tip

   - If you want to align ports vertically, select the port to be the baseline and select **Edit**>**Vertical Arrange** menu. This realigns ports nearby the selected row.
   - If you want to return to the default port positions, select **Edit**>**Defaults** menu.

3. Select **Edit**>**Save Position** menu.

   After customizing the port positions, select **Save Position** to save.

4.18.2.5 Editing management and statistics menus

For the general-purpose panel window, you can add new menus under the management and statics menu.

You must first change to the "configuration mode (page 27)".

1. Display the device front panel.

   Right-click the device icon and select **Device Front Panel** menu.

   For details, refer to "5.9.1 Opening a device front panel (page 476)".

2. Open the "4.18.2.5.1 Customizer window (page 386)".

   In the panel window, select **Edit**>**Customizer** menu.

3. Select a MIB that you want to display from the MIB tree on the left side of the Customizer window.

   Tip

   a. After selecting the MIB, select **Customize**>**MIB Browse**>**Get** to confirm whether the selected MIB information can be obtained from the node.

   b. If you want to add MIBs to the MIB tree on the left side of the customizer, store the MIB definition file (*.MIB) to the location below. The file extension must be "MIB". Only ASCII or standard OS multi-byte character code are acceptable in MIB files.

      <On the monitoring terminal, %installfolder%>\Svc\sg\NvPRO\NodeManager\MIB

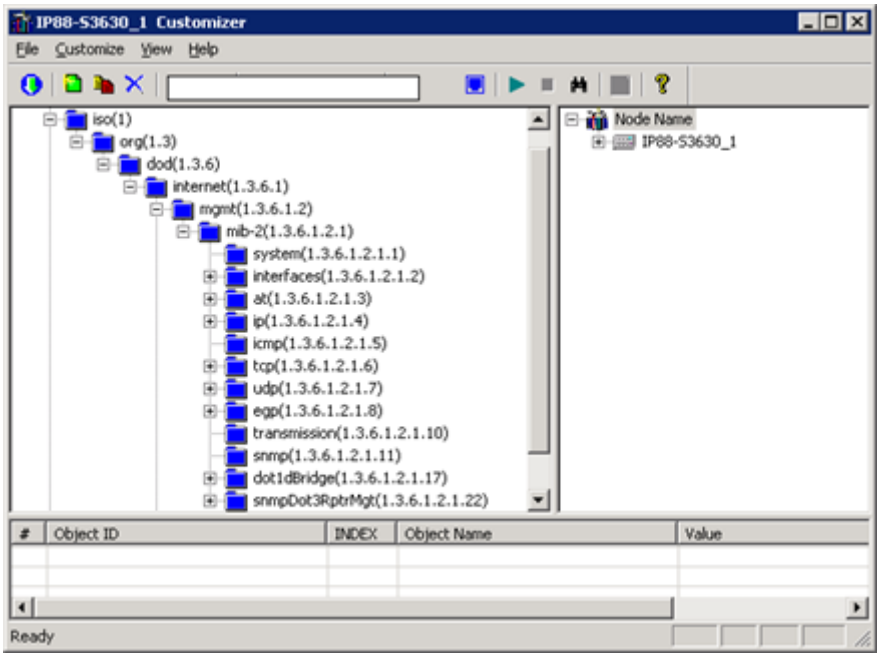
4. Select a node displayed in the **Node Name** on the right side of the Customizer window, and select either **Management** or **Statistics**.
5. Select **Customize**>**Menu**>**Create** menu.
6. Configure the menu settings in the Menu Edit dialog box.

   In the Menu Edit dialog box, only ASCII or standard OS multi-byte character code are acceptable in the **Menu Name** and **Item Name**.

   For details, click **Help** button and refer to the help file displayed in the Menu Edit dialog box.
7. In the Menu Edit dialog box, click **OK** button.

Customizer window

To open the Customizer window, select **Edit**>**Customizer** menu in the panel window.



Contents to be displayed

- MIB Tree (Left pane)

  Displays the MIB tree currently targeted for customization. MIB information not registered in this tree cannot be customized as a menu.
- Node Name (Right pane)

  Displays the name of the target node and current customization activity targeting the node.
- MIB List (Bottom pane)

  The MIB information selected from the MIB tree list displays results obtained from the target node.

Menu

- **File**
  - **Restructure**

Updates the MIB tree to the most recent status. In this case new MIBs to add can be specified.

- **Exit Application**

  Closes the customizer feature.

- **Customize**
  - **Menu**
    - **Create**

      Creates a new menu within the management menu or statistics menu hierarchy. Underneath **Node Name**, select **Management** or **Statistics**, then select this menu.

      In **Menu Name** and **Item Name**, only ASCII or standard OS multi-byte character code are acceptable.

    - **Property**

      Displays registered information for newly added menus and enables editing.

    - **Delete**

      Deletes registered information for newly added menus.

  - **Customize>Port**

    Displays node port information and enables editing.

  - **MIB Browse**
    - **Get**

      MIB information specified in the MIB tree is obtained from the target node (device) and then displayed in the MIB list.

    - **Stop**

      Stops displaying obtained results in the MIB list (data gathering also stops).

  - **Find MIB**

    Searches for and displays MIBs matching the search criteria in the MIB tree.

  - **Output MIB List**

    Outputs information currently displayed in the MIB list to a file (CSV or text format).

  - **MIB Path Settings**

    Registers to proper location the isolated MIB subtree (no parent node in the tree) elements displayed in the unknown section of the MIB tree.

- **View**
  - **Tool Bar**

    Displays the tool bar.

  - **Status Bar**

    Displays the status bar.

  - **MIB Tree**
    - **Standard MIB**

Performs jump to standard MIB position in MIB tree.

* **Vender MIB**

  Performs jump to enterprise MIB position in MIB tree.

* **Property**

  Displays MIB information currently selected in the MIB tree.

- **Help**
  - **Help Topics**

    Displays Help.

4.18.2.6 Editing MIBs for port status decision

In a general-purpose device front panel, the port type and port status color are decided from the standard MIB information: ifType and ifOperStatus. You can change these MIBs.

You must first change to the "configuration mode (page 27)".

1. Display the device front panel.

   Right-click the device icon and select **Device Front Panel** menu.

   For details, refer to "5.9.1 Opening a device front panel (page 476)".

2. Open the "4.18.2.5.1 Customizer window (page 386)".

   In the panel window, select **Edit**>**Customizer** menu.

3. Change MIBs in the Port MIB Customize dialog box.

   Right-click the node dispalyed in the **Node Name** on the Customizer window, and select **Port MIB Customize** menu.

   For operation, click **Help** button in the Port MIB Customize dialog box, and refer to the Help file.

4.18.2.7 Editing a polling interval

Polling is performed at regular intervals on nodes to check port and LED states while the device front panel is displayed. This interval can be changed.

Caution

A time lag may be caused by other data gathering operations.

You must first change to the "configuration mode (page 27)".

1. Display the device front panel.

   Right-click the device icon and select **Device Front Panel** menu.

   For details, refer to "5.9.1 Opening a device front panel (page 476)".

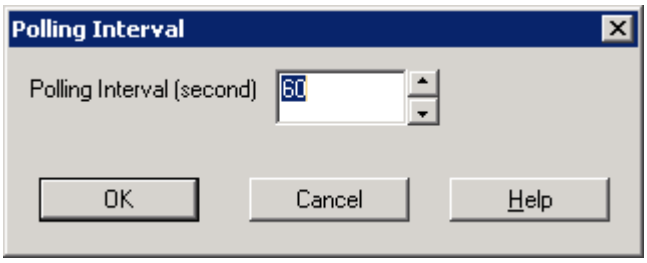
2. Open the Polling Interval dialog box.

   In the panel window, select **Option**>**Polling Interval** menu.

3. Set the interval of polling.

   The default value is 60 seconds. If you want to change this, the interval can be set in the 0 to 1,000,000 (sec) range.

If the value is set to "0", polling is not performed.



4.18.2.8 Clearing panel window customizations

Clears the customizations and return the panel window to its original state.

You must first change to the "configuration mode (page 27)".

1. Display the device front panel.

   Right-click the device icon and select **Device Front Panel** menu.

   For details, refer to "5.9.1 Opening a device front panel (page 476)".

2. In the panel window, select the **File**>**Restructure**.

   Customized contents will be cleared, and the default panel image will be saved automatically.

   Caution

   Restructuring cannot be canceled. The panel image is cleared immediately after the execution menu, and cannot be restored.

3. If the node is configured as a stack, clear the customized data for each device panel window.

   If the device front panel is supported in a stack configuration and the panel was edited, display all device front panels and select the **Restructure** menu for each panel.

   To change a displayed panel, select **File**>**Change Device** menu.

4.18.3 Using a customized device front panel for multiple icons

Customized panel window image can be saved as new panel window type.

Newly saved panel window types are treated in the same way as other model-specific panel window type, and can be applied other nodes which are the same model. Perform the following procedure to save as new panel window type and use this panel type in multiple node icons.

You cannot create new panel window type from the model-specific device front panels which support the stack configuration. Create from the general-purpose device front panel instead.

1. Edit the panel window contents so that it matches what you want to save as new panel window type. Refer to "4.18.2 Customizing a device front panel (page 380)".

2. Save the edited panel window as a new panel window type.

   After editing the device front panel, select **File**>**Device Front Panel**>**Save As**. Save the current panel window image as a new panel window type.

   - Specify the name of new panel window type up to 28 characters including the prefix ("exp_"). Valid characters include alphanumeric characters, hyphen (-), and underscore (_).

If the length of the name is over 28 characters, the panel windows may not be displayed.

- The list of panel window types that were already saved can be confirmed in the file below. The name of saved panel window type starts with "exp_".

  <On the monitoring terminal, %installfolder%>\Svc\sg\NvPRO\NodeManager\export\PanelList*<panel window type name>*.IMP

3. Set the saved panel window type to the panel window type of the node icon to which you want to apply it.

   Open the Properties dialog box of the node and specify the name of the saved panel window type ("exp_XXX") into the **Device Front Panel** property.

   The **Device Front Panel** property is not automatically changed in the node icon that was used to edit and save the new panel window type. Change manually if needed.

4. Open the device front panel and confirm that it opens in the saved panel window type.

5. If there are multiple monitoring terminals for the manager, you must enable the created panel window type in all other monitoring terminals.

   Perform the procedure explained in "4.18.4 Using a customized device front panel in other monitoring terminals (page 390)" for all other monitoring terminals.

Tip

To remove the saved definitions of panel window types, delete the files listed in the following text file.

<On the monitoring terminal, %installfolder%>\Svc\sg\NvPRO\NodeManager\export\PanelList*<panel window type name>*.IMP

4.18.4 Using a customized device front panel in other monitoring terminals

Newly created panel window types (see "4.18.3 Using a customized device front panel for multiple icons (page 389)") can be used in other monitoring terminals or in other Network Manager systems.

Perform the following procedure to copy the definition files of the saved panel window types into other monitoring terminals.

1. Perform "4.18.3 Using a customized device front panel for multiple icons (page 389)".

   When saving a new panel window type from **File**>**Device Front Panel**>**Save As** menu, the definition files for other monitoring terminals are automatically created in the following folder.

   <On the monitoring terminal, %installfolder%>\Svc\sg\NvPRO\NodeManager\export*<panel window type name>*\

Caution

Do not edit, rename, or delete the files and folders in *<panel window type name>* folder. If files or folder structure has been changed, the device front panel window may not be displayed correctly.

2. Copy the entire folder that contains the definition files of the new panel window type into another monitoring terminal.

   There are folders named "bin" and "sg" in *<panel window type name>* folder. Copy these folders into the following folder:

   <On the monitoring terminal, %installfolder%>\Svc\

Caution

If there is the panel window type that has a same name in a monitoring terminal, do not copy the definition files. It may not operate properly.

Tip

a. Depending on the device front panel on which new panel window type is based, "bin" folder may not exist in the <*panel window type name*> folder.

b. To remove the copied definitions of panel window types, delete the files listed in the following text file.

`<On the monitoring terminal, %installfolder%>\Svc\sg\NvPRO\NodeManager\export\PanelList\<panel window type name>.IMP`

3. Specify the name of the copied panel window type into the **Device Front Panel** property of the node icons.
4. Open the device front panel and confirm to be displayed with the copied panel window type image.

4.19 Setting for Running Device Commands

You can send pre-prepared command lines to the network devices and run commands according to a schedule.

Caution

The login settings must be performed in advance for a monitored device on which a device command will be executed.

For details regarding login settings, refer to "4.3 Registering Login Information (page 189)".

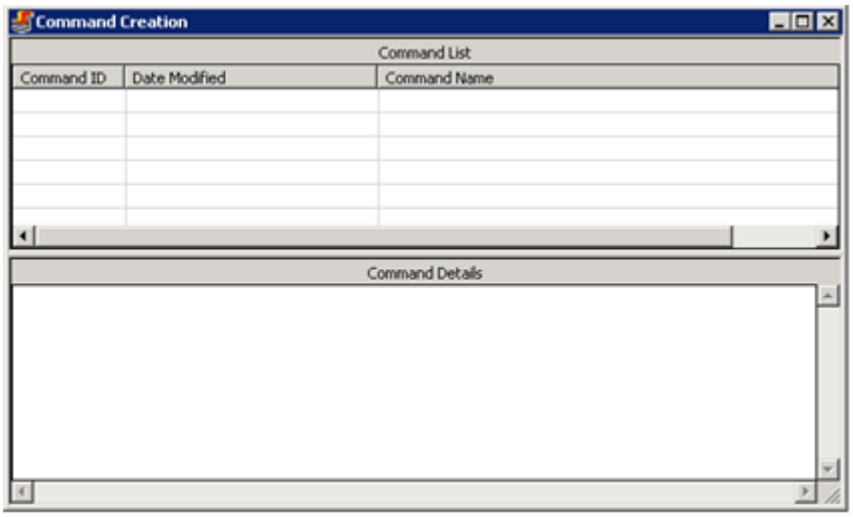
4.19.1 Defining commands

Device commands are defined in the Command Creation window.

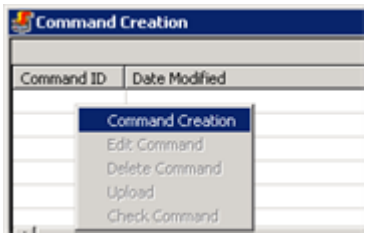
You must first change to the "configuration mode (page 27)".

1. Open the Command Creation window.

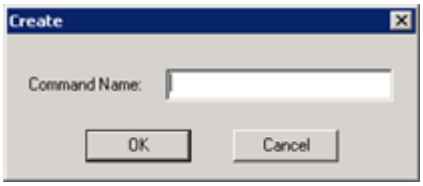
   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Configuration Management**>**Command Creation**.



2. In the Command List pane, right-click and select **Command Creation** menu.



3. Type the command name as you want it to be displayed in the window.



4. The text editor will open. To complete the command setup, enter a description of the command you want to run and save it.

   Basically, the entered command is sent to a device and run one line at a time. In th case of the blank line, only linefeed code is sent to a device. It is also possible to use the simple scripts explained in "4.19.1.1 Simple scripts (page 393)".

   After execution of each command, if Network Manager does not receive any other character for one second [1)] after receiving the prompt character (prompts, such as "#" or "> ", vary depending on the device type), Network Manager assumes that the command has been finalized, and then executes the next command. If Network Manager receives any other character within one second after receiving the prompt character, Network Manager waits for receiving the prompt characters again. The maximum wait time for a prompt is 5 minutes. If a prompt is not received within five minutes, the process is terminated and the command will fail to run.

   1) It is possible to change this time. It should be changed if a prompt is incorrectly identified due to the device or network status. Refer to the simple script *PTIME.

⚠ Caution

a. A check is not performed for the command file syntax. The creator is responsible for performing this check.

b. The following commands cannot be specified in commands executed using the command schedule function.

Commands that cannot be specified using the command schedule function	Command examples
Commands that change the device prompt.	Prompt
Commands that enable the display of system log messages or debug messages for telnet sessions.	terminal monitor

c. If password information is updated using a command, the login settings must be reset with the updated information.

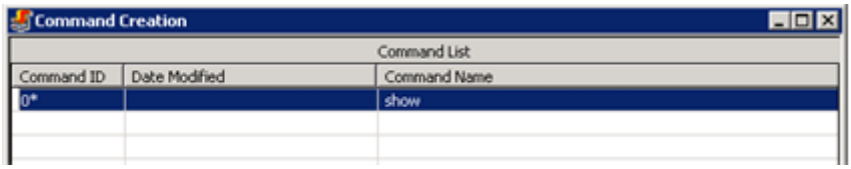
d. The maximum supported command file is 2MB. A command file exceeding 2MB is not available.

5. In the Command List pane, right-click the command that you want to upload and select **Upload** menu.

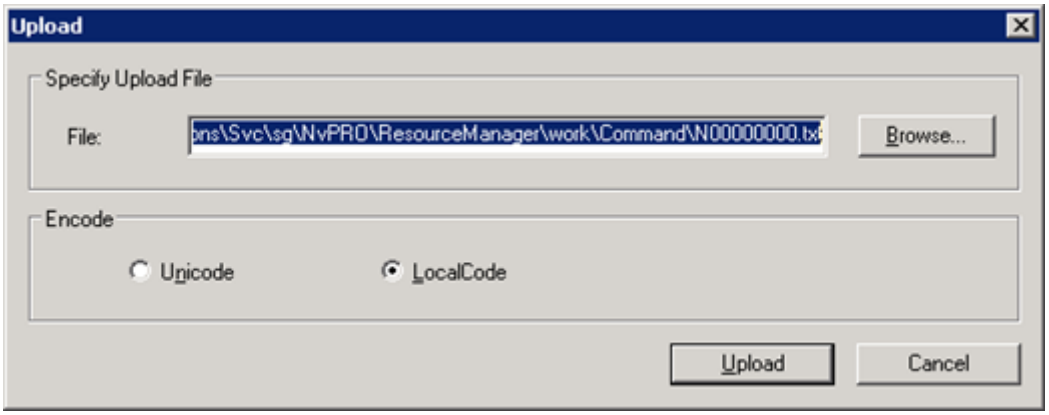
   The command line that you have created is recorded on the monitoring terminal. For this reason, it is necessary to upload it to the manager.

Tip

Commands that have not been uploaded have a "*" displayed in the **Command ID** column.



6. In the Upload dialog box, verify the information and click **Upload** button.



To edit or delete a registered command, select **Edit Command** menu or **Delete Command** menu. After editing a command, you must upload it again.

4.19.1.1 Simple scripts

Simple scripts can be used to assess the results of commands that have been run and to run conditional commands. This simple scripts can be assessed in the **Check Command** menu of the Command Creation window.

The following are the script formats.

Format	Summary	Function
*CHECK	Format check	If this script is specified in the first line, the command for the device is not run and a format check is performed for the entire command. The appropriateness of commands being sent to devices and inconsistencies in script flow (infinite loops, etc.) are not checked.
//	Comment line	This line is treated as a comment and nothing is processed
*PTIME 1-5	Command completion wait time	You can specify a time between 1 - 5 seconds for the time between when the command is run and when the command is considered complete. The default value is 1 second. After receiving the a character string that ends with a prompt character from the device, if Network Manager has not received any character within the duration time specified in `*PTME`, it considers that the command has finished. Use this script for changing the wait time when a response from a device takes a long time. If `*WAIT` or `*WAITRB` script is executed after a device command, the time specified in `*PTIME` is ignored, and the wait time specified in `*WAIT` or `*WAITRB` script is adopted.
*SLEEP 1-600	Sleep	A time is specified between 1 - 600 seconds at which point processes are suspended.
*END [0-9]	Command execution completion	Stops a command that is being executed. A specified value between 0 - 9 indicates the completion status. If the value is omitted, it will be considered as 0.
*:Label	Label	Sets a label. The maximum number of characters in a label is 20. The label must be in alphanumeric characters and may include an "_" (underscore). An error will result if a label is specified more than once.
*GOTO label	Jump	Jumps to a specified label. An error will result if the specified label is not defined.
*WAIT[(1-600)] [:label] [wait string] *WAITRB[(1-600)] [:label] [wait string]	Wait	Waits for a prompt or the string specified in the wait string. When executing a device command which returns not a prompt but confirmations such as `"y/n"`, use these scripts to wait for confirmations. The wait time can be set to a time between 1 - 600 seconds in units of seconds. The default value is 60 seconds. The wait time specified by `*PTIME` is not used. If the wait time has passed but a prompt or the wait string has not been received, the system jumps to the specified label or the process ends in an error. The wait string can be a maximum of 50 characters and must be specified in a valid format. If the wait string has not been specified, the system waits for a prompt. If the connection to a device is lost during the wait time, the `*WAITRB` script attempts to reconnect and continues to wait for a prompt or wait string. This assumes that that a device restart or similar command has been run.
*MATCH:label [search string]	String search	Searches for the specified search string in response to the character string received after running a command. If the search string is found, the system jumps to the specified label. The search string can be a maximum of 50 characters and must be specified in a valid format. The search target string is updated every time a command is run. Until the next command is run, the search target string is not updated, and searching can be repeated.

Format	Summary	Function
*FTPI_START "subfolder name"	Starting FTP server	Starts the internal FTP server of Network Manager. The root directory of the internal FTP server is as follows. *<On the manager, %sharedfolder%>*\Manager\sg\NvPRO\RMAPI\dat\ftp In FTP transfer processing, use the directory under the root directory specified by "subfolder name". If the directory specified by "subfolder name" does not exist, create a new one.
*FTPI_STOP	Stopping FTP server	Stops the internal FTP server of Network Manager.
*PROMPT "prompt character"	Specifying prompt character	Identifies the character string specified by "prompt character" as a prompt character.

4.19.1.2 Precautions in creating commands

This section describes notes in creating commands to be run.

- To run a command that requires the confirmation by the user (`copy`, etc.)

  While a command such as `copy` is running, a confirmation such as `"y/n"` may return instead of the prompt. If a command is stopped with a confirmation such as `"y/n"`, the maximum wait time of the prompt (five minutes) will elapse and then the command will fail.

  To run a command to be suspended before a prompt is returned, use a simple script `*WAIT`, etc. and control the system waiting for a confirmation string such as `"y/n"`.

  Example of the command description: (commands vary depending models.)

```
copy running-config running-config.backup
*WAIT y/n
y
```

- To run a command on a device that has a paging function (`more`, etc.)

  When the paging function is valid, if multi-line strings are output by a command such as `show` command, the output may be interrupted by the paging function. In such a case, since the system cannot detect completion of the command, the next command cannot be run. By inserting a command to disable the paging function into the beginning of the commands list, the paging function can be inhibited in the commands afterwards.

  Example of the command description: (command varies depending models.)

```
terminal length 0
device-command
```

  For the model that the paging function cannot be disabled, use the simple script such as `*WAIT` for waiting for the character string to be output by the paging function, and send the character string that cancel the suspension.

- To run a command on a device that is not supported by the Resource Manager function

  For the device model that is not supported by the Resource Manager function, the confirmation of user's mode transition is not supported. It is recommended that the prompt confirmation using the simple script is inserted into the beginning of the commands list. Concretely, the current

mode of the logged in user can be confirmed by analyzing the character string received after sending linefeed and confirming if the intended prompt character can be received .

Example of the command description:

```
(Linefeed)
*WAIT # $
device-command
```

When running a command on a device that is not supported by the Resource Manager function, the system automatically detects a prompt received from the device immediately after login. Since the system considers completion of each command from appearance of the prompt character, if a prompt is changed by a command, the system will fail to detect completion of the command and not work correctly. When using such commands, use the simple script `*WAIT` to wait for a prompt explicitly.

- To set the timeout for running the device command

  To set the timeout for the device command, use the simple script `*WAIT` immediately after the device command in order to wait for completion of the command until the timeout occurs.

  Use the simple script `*MATCH` in the next line of `*WAIT` to analyze the output of a command execution. In the following example, if the device command is finished successfully and a prompt or a string indicating the normal end is output, the system will jump to "NEXT_LABEL". If not, it will jump to "ERR_LABEL".

  Example of the command description:

```
device-command
*WAIT(Timeout value):ERR_LABEL
*MATCH:NEXT_LABEL Device output string at the normal end
*GOTO ERR_LABEL
*:NEXT_LABEL
```

- To run a commands list that takes a long time to complete

  The device command running function measures the elapsed time since a first command has been started after login. After each command completion, the system confirms the elapsed time from start. If the elapsed time is longer than eight minutes, the system considers it as a timeout error and terminates.

  Additionally, when 10 minutes have elapsed since a request for running a command was made, the system consider it as a timeout error. When a command that takes a long time is included in the commands list, or a vast amount of commands is included, be sure not to exceed eight minutes in total. If eight minutes may elapse, the command file should be divided.

- To run a commands list that transfer files using internal FTP server of Network Manager

  In the login processing to the internal FTP server of Network Manager, use the following substitution strings.

Substitute Strings	Description
%_FtpIp%	Substituted for IP address of the internal FTP server (Network Manager).
%_FtpUsername%	Substituted for the account name of the internal FTP server.
%_FtpPassword%	Substituted for the account password of the internal FTP server.

  In the login processing to the internal FTP server of Network Manager, the response character string to wait change. And after the login processing, the prompt character to wait change. In

order to properly handle the change of the character string to wait, define the command list as follows.

Example of the command description:

```
*FTPI_START Subfolder_Name
ftp %_FtpIp%
*WAIT .*:.*
*PROMPT "ftp> "
%_FtpUsername%
*WAIT .*Password:.*
%_FtpPassword%
binary
put File_Name /Subfolder_Name/File_Name
bye
*PROMPT "Original_Prompt_Character"
*FTPI_STOP
```

4.19.1.3 Example of creating a command

As an example of creating a command, this section describes the example when setting VLAN to the specific interface. The processing sequences are outlined below.

1. `"terminal length 0"` disables the paging function.
2. After transition into the global configuration mode, create a VLAN. If a character string including `"rejected"` is received during the VLAN creation, the system jumps to ":ERR_END" label and finishes in an error.
3. Transit from the global configuration mode to the interface mode. If a character sting including `"Invalid"` is received during the transition, the system jumps to ":ERR_END" label and finished in an error.
4. After allocating the VLAN to the interface, write the configuration in memory. At this time, the system waits for a character string including `"confirm"`. After receiving the `"confirm"`, it sends `"y"` and finishes successfully.

Example of the command description:

```
terminal length 0
configure terminal
vlan 100
*MATCH:ERR_END rejected.*
exit
interface fastethernet 0/5
*MATCH:ERR_END Invalid.*
switchport mode access
*MATCH:ERR_END Invalid.*
switchport access vlan 100
*MATCH:ERR_END Invalid.*
end
write memory
*WAIT \[confirm\]
*MATCH:RECV_CONFIRM \[confirm\]
*END 0
*:RECV_CONFIRM
y
*END 0
```

```
*:ERR_END
*END 9
```

For each command, errors are checked by using the simple script, and the exit code will be changed according to the error status.

4.19.2 Scheduling command execution

Commands registered using the **Command Creation** menu can be run according to a schedule by going to the **Command Scheduling** menu.

If you want to run a registered command at once, refer to "5.10.1 Executing a registered device command (page 482)".

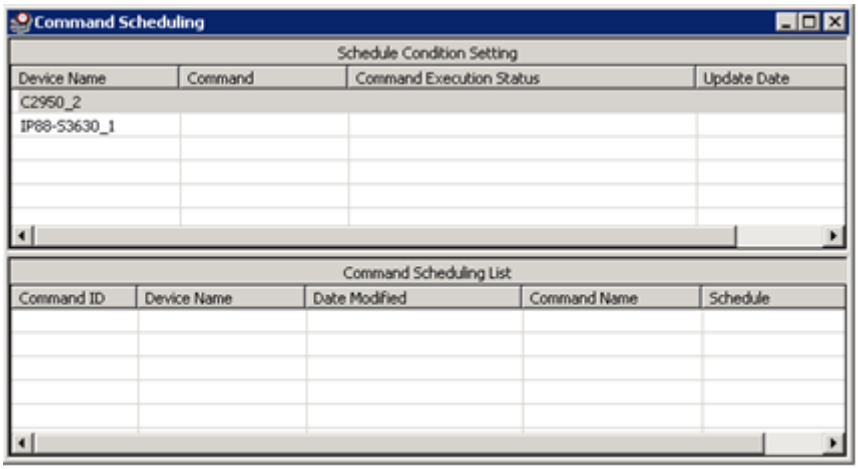
Set the monitoring mode of the device to which the schedule is set to ON. Scheduled command executions will not be performed if the monitoring mode is set to OFF.

Conduct "4.19.1 Defining commands (page 391)" in advance.

You must first change to the "configuration mode (page 27)".

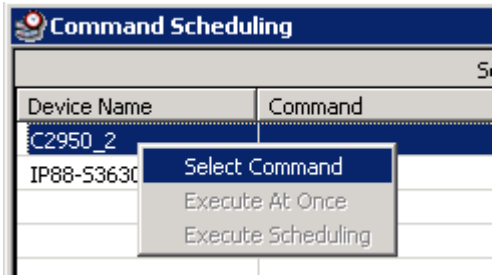
1. Open the **Command Scheduling** window.

   Right-click the **NetworkView** icon, **NetworkManagement** icon, or map icon. Select **Configuration Management**>**Command Scheduling**.



2. Select the command that you want to run on a node.

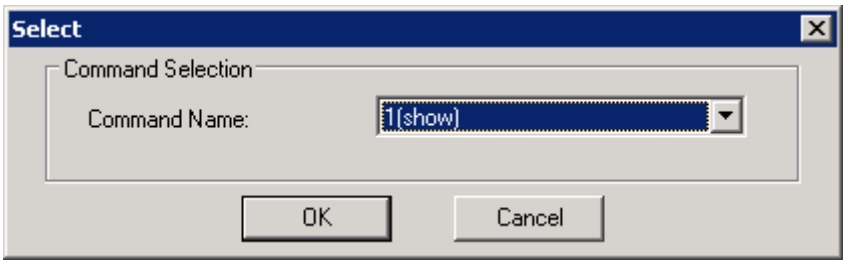
   In the Schedule Condition Setting pane, right-click and select **Select Command** menu.



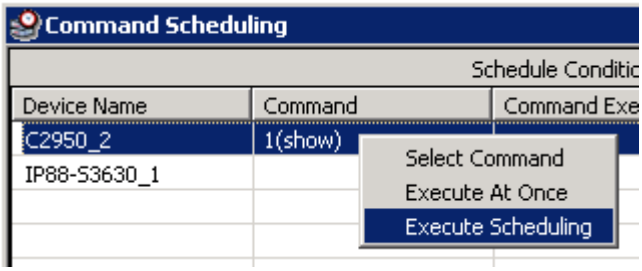
Tip

You can select multiple devices and apply the settings to all selected devices at once.

3. The Select dialog box will be displayed. Select the created command on the "4.19.1 Defining commands (page 391)".



4. In the Schedule Condition Setting pane, right-click and select **Execute Scheduling** menu.



5. Configure the scheduling setting in the Schedule Setting window.

   For details, refer to "4.22.2 Setting a time schedule (page 435)".

If schedule setting is configured, commands are run in accordance with the setting. The status of running commands are displayed in the **Command Execution Status** column of the Schedule Condition Setting pane.

To confirm the detailed running result, refer to "5.10.3 Checking command execution results (page 484)".

Caution

The scheduling list to be displayed in the Command Scheduling List pane is not deleted after the command is run and continues to be displayed.

To delete a completed command from the list, select the command row, right-click and select **Delete Schedule** menu.

4.20 Setting for Managing Device Configuration (Resource Manager)

Network Manager provides the device configuration management: collect, deploy the configuration files for network devices, and monitor the configuration changes.

An RM License (Resource Manager advanced functions license) is required to manage configurations.

Caution

1. For details regarding the supported devices in Resource Manager function, refer to "8.1.2 Supported Devices in Resource Manager function (page 671)".
2. To manage device configurations, register login information for the target devices beforehand.

   For details regarding login information setting, refer to "4.3 Registering Login Information (page 189)".

4.20.1 Registering an FTP or TFTP server

When the Resource Manager function is used to manage device configurations, the ftp or tftp server function is used to deploy the configuration files.

In Network Manager, the following three configurations are available when using the ftp or tftp server function.

- Using the internal ftp or tftp server provided by Network Manager

  Normally, use the internal ftp or tftp server provided by Network Manager. It is set automatically.

  Tip

  The managed device is the ftp or tftp server. Even for a model for which Network Manager needs to operate as an ftp or tftp client, it is treated the same way as the internal ftp or tftp server. Therefore, no special settings are required.

  For details on the status of the file transfer type for each model, refer to "8.1.2 Supported Devices in Resource Manager function (page 671)".

- Using an external ftp or tftp server provided by another application coexisting with Network Manager

  If other application coexisting with Network Manager manager function is running an ftp or tftp server, the internal ftp or tftp server function of Network Manager cannot be used due to a resource conflict.

  In such a case, you can avoid a resource conflict by configuring the settings to use an external ftp or tftp server provided by another application coexisting with Network Manager.

  For details, refer to "4.20.1.1 Using an external FTP or TFTP server (page 401)".

- Using an external ftp or tftp server run by another host

  If another application coexisting with Network Manager manager function is running an ftp or tftp server, or if an ftp or tftp server cannot be started on a server on which Network Manager manager function is installed for system operational reasons, you can configure the settings to use an external ftp or tftp server run by another host.

  For details, refer to "4.20.1.1 Using an external FTP or TFTP server (page 401)".

Tip

- If a specific managed device cannot conform to the ftp or tftp server settings of the entire system shown above, you can configure the ftp or tftp server settings specific to that device.

  For details, refer to "4.3.5 Setting external server information (page 195)".

- In Network Manager, the source IP address in the communication used to connect to the managed device is treated as the IP address of the ftp or tftp server. In the following special configurations, if the source IP address in the communication used to connect Network Manager to the managed device is different from the IP address of the ftp or tftp server as viewed from the managed device (ftp or tftp client), you can address this issue by configuring the **IP for Device** settings.

  Example of a configuration requiring the **IP for Device** settings:

  - When the managed device is being communicated with via NAT.
  - When using an outside tftp server and the outside tftp server IP address is different to the IP address when communicating from the Network Manager server and the IP address when communicating from a managed device (when the outside tftp server belongs to multiple IP subnets).

- When the Network Manager server has multiple NICs, and the NIC used to connect to a managed device and the NIC used by a managed device to connect to the Network Manager server are different.
- When the port server setting is configured in the login setting of the device, and when external tftp server is not used in transferring a file (A server in Network Manager is used).

For details on the **IP for Device** settings, refer to "4.20.1.2 Configuring the IP for Device (page 403)".

4.20.1.1 Using an external FTP or TFTP server

Configure the settings to enable the use of an external ftp or tftp server when the internal ftp or tftp server function provided by Network Manager cannot be used.

Caution

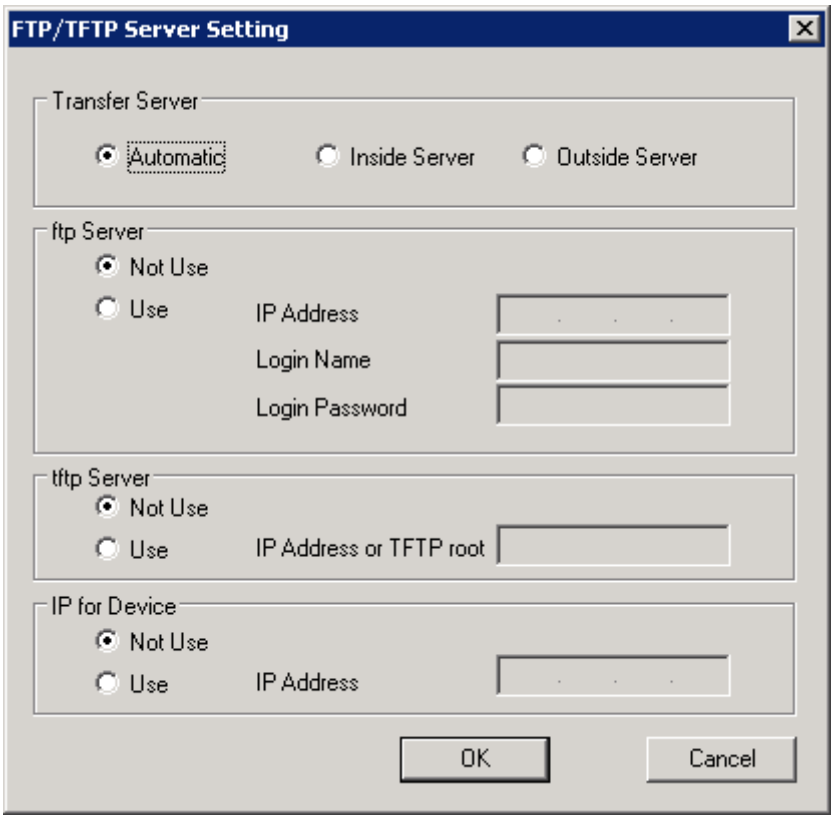
Before using an external tftp server, confirm that the external tftp server supports writes from external devices to the root path of the tftp server.

When writes from external devices are not supported, the Resource Manager function does not operate correctly even if the following steps are used to configure the settings.

You must first change to the "configuration mode (page 27)".

1. To open the FTP/TFTP Server Setting dialog box.

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Configuration Management**>**FTP/TFTP Server Setting**.



2. In **Transfer Server**, select **Automatic** or **Outside Server**.

Tip

When **Automatic** is selected, if the external ftp or tftp server is found to be stopped (unavailable) during operation, the specified external ftp or tftp server settings are ignored, and the operation continues using the Network Manager internal ftp or tftp server.

3. Select **Use** of **ftp Server** or **tftp Server**.
4. Specify connection information in **ftp server** or **tftp server**.
   - If **User** is selected in **ftp Server**, enter information in **IP Address**, **Login Name**, and **Login Password**.
     - **IP Address**

       The setting range is between 1.0.0.0 and 223.255.255.255.

       To use an external ftp server provided by another application coexisting with Network Manager, enter the IP address of the self host.

       To use an external ftp server run by another host, enter the IP address of that host.
     - **Login Name**

       A maximum of 127 characters can be entered.

       To log in to the ftp server, users are required to have the following authorities.

       * Reference authority for the login directory and all files under that directory
       * Creation authority for directories and files under the login directory
       * Deletion authority for directories and files under the login directory
     - **Login Password**

       A maximum of 127 characters can be entered.
   - If **User** is selected in **tftp server**, enter information in **IP Address or TFTP root**.
     - **IP Address or TFTP root**

       A maximum of 255 characters can be entered.

       To use an external tftp server provided by another application coexisting with Network Manager, enter the IP address of the self host or the root path name of the tftp server.

       To use an external tftp server run by another host, enter the IP address of that host.

       #### Tip

       * If the IP address is entered, you must place a file, in accordance with the following naming rules, in the root path of the tftp server.

         File name: `nvpro_`*`IP-address-of-target-device`*

         The IP address of the target device must consist of 12 decimal digits.

         Example:

         When the IP address of the target device is 192.168.0.1

         File name: `nvpro_192168000001`

       To use the software management function for the IP8800/700 series or ES8800/1700 series, you must also place the following file.

       `File name: nvprod_`*`IP-address-of-target-device\file-name-of-deployed-software`*

       The IP address of the target device must be comprised of 12 decimal digits.

Example :

If the IP address of the device to which you are distributing software is 192.168.0.1 and the file name of the distributed software is `hr710170.gz`:

File name : `nvprod_192168000001\hr710170.gz`

* If the root path of the tftp server is entered, you do not need to place a file in the root path of the tftp server.

5. Click the **OK** button to apply the settings.

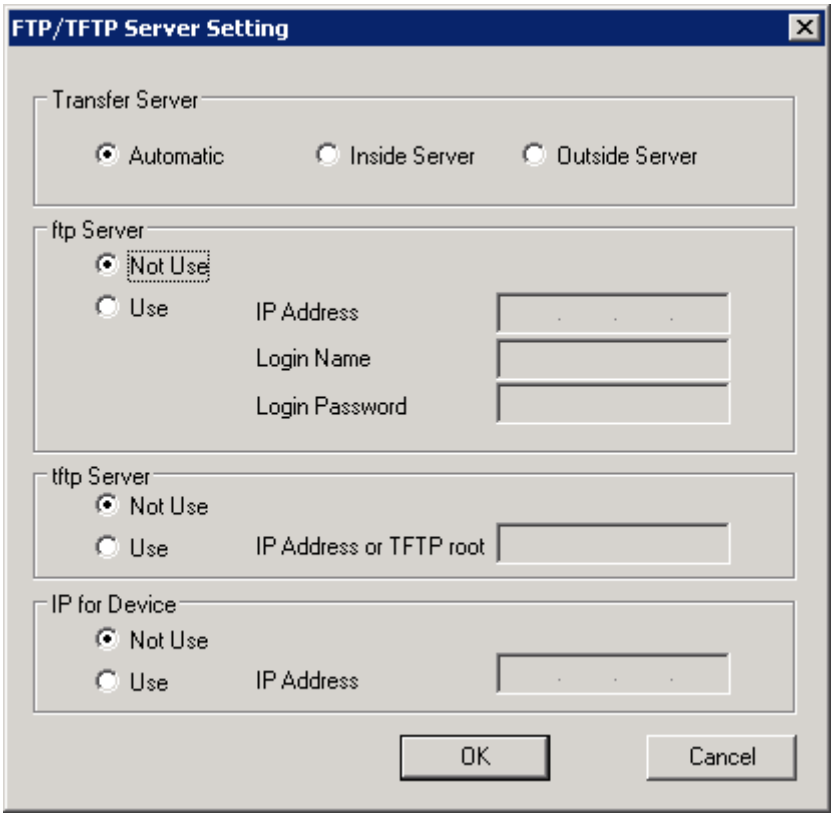
4.20.1.2 Configuring the IP for Device

Configure the IP for Device to run the device in an environment where the source IP address of communication used to connect Network Manager to the managed device is different from the IP address of the FTP or tftp server as viewed from the managed device (FTP or tftp client).

You must first change to "configuration mode (page 27)".

1. Open the FTP/TFTP Server Setting dialog box.

   Right-click the **Network View** or **NetworkManagement** icon, and then select **Configuration Management**>**FTP/TFTP Server Setting** menu.



2. Select **Use** in **IP for Device**.
3. Enter the IP address of the ftp or tftp server connected from the managed device (ftp or tftp client).

   The setting range of **IP Address** is between 1.0.0.0 and 223.255.255.255.
4. Click the **OK** button to apply the settings.

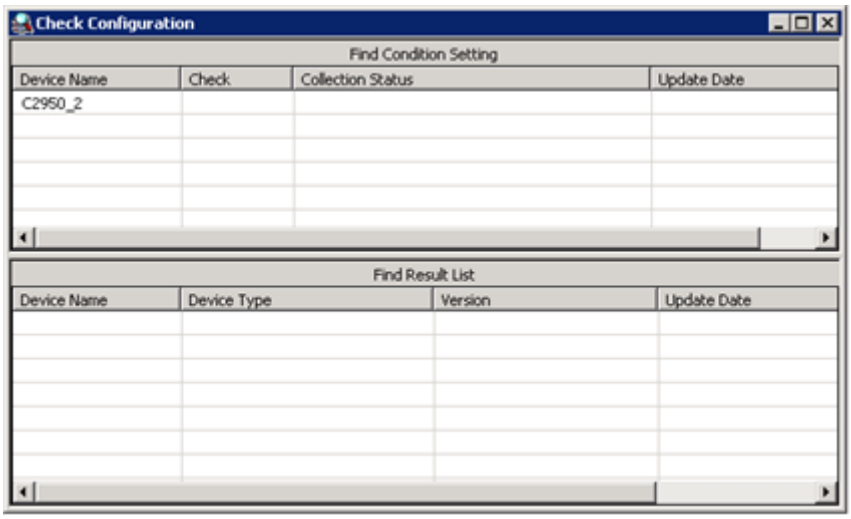
4.20.2 Monitoring configuration changes

You can monitor changes to current configuration information (running-config) for monitored devices. When any change is detected, an alert can be issued to inform it.

The management of change of configuration is conducted in the "4.20.2.1 Check Configuration window (page 404)".

4.20.2.1 Check Configuration window

To open the Check Configuration window, right-click the **NetworkView** icon or **NetworkManagement** icon or the map icon or device icon, and then select **Device Config Management**>**Check Configuration**.



Caution

If the following operations are performed while this window is opened. The device list in this window is not updated immediately. To reflect changes, open this window again.

- Add and delete a device icon.
- Change a device name.
- Move an icon to another map.

4.20.2.2 Starting config change management

Set an interval to periodically monitor the difference of configurations.

Set the monitoring mode of the device to which schedule is set to ON. Scheduled change management will not be performed for devices if the monitoring mode is set to OFF.

You must first change to the "configuration mode (page 27)".

1. Open the "4.20.2.1 Check Configuration window (page 404)".

   Right-click the **NetworkView** icon, **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Check Configuration**.

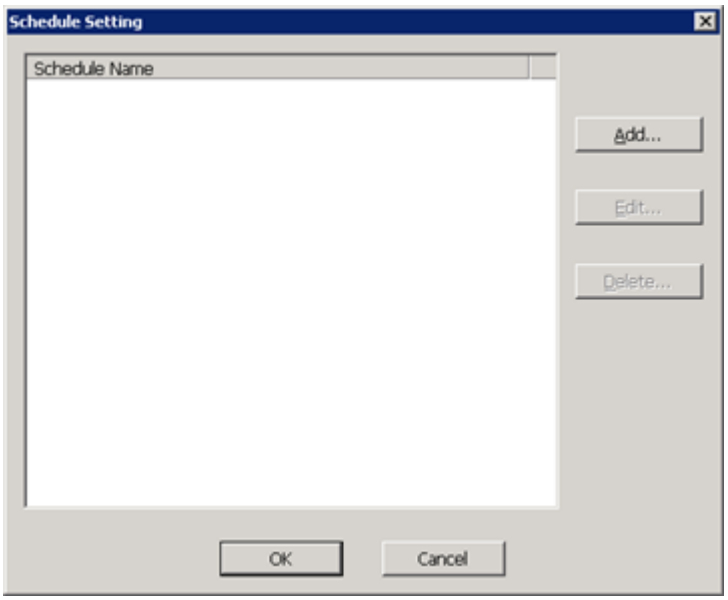
2. Open the Schedule Setting dialog box.

   In the Check Configuration window, right-click the node and select **Start Checking** menu.

Tip

You can select multiple devices and apply the settings to all selected devices at once.

3. Specify the interval for monitoring configuration variances.

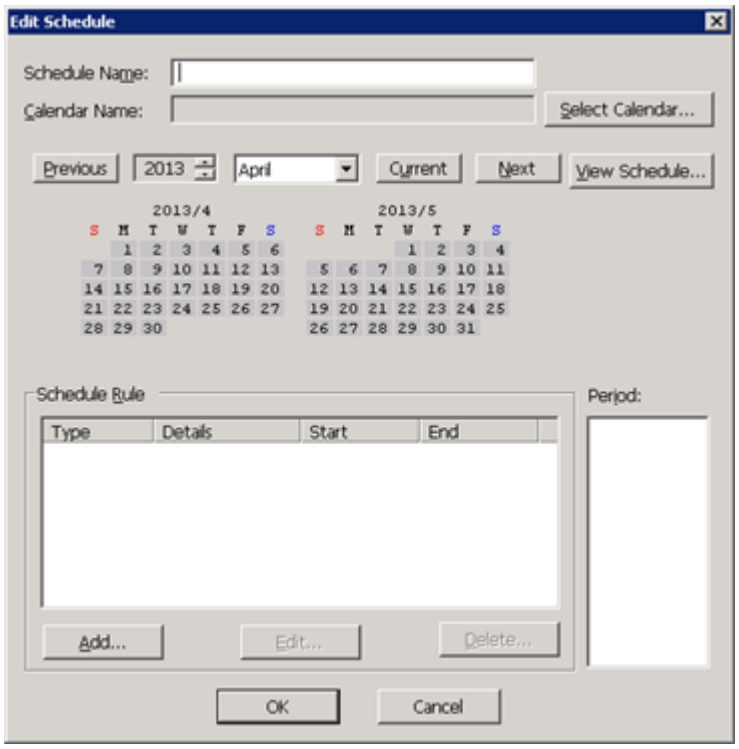


- When using the existing schedule

  Click the schedule in the **Schedule Name** column and click **OK** button.

- When creating a new schedule

  Click **Add** button, configure the necessary setting int the Edit Schedule dialog box, and then click **OK** button.



For details, refer to "4.22.2.1.3 Creating a new time schedule (page 436)".

Caution

When a repetition schedule is set, if the schedule intervals are too short by minutes or tens of minutes, the next checking operation may start before the previous checking operation has finished. In this case, even if **Stop Checking** menu is specified, operations may not end immediately. Schedule intervals must be sufficiently long.

4. Click **OK** button.

Upon setting of schedule, "Start" is displayed in the **Check** column in the "4.20.2.1 Check Configuration window (page 404)", the monitoring starts.

If difference of running-config is detected while change management is being performed, an alert indicating that "running-config was changed" is issued.

Caution

If the amount is over the limit of the history because change of configuration is detected in the "Check Configuration", the old histories are automatically deleted.

4.20.2.3 Stopping config change management

Stop the periodical monitoring of the configuration difference (change management)

You must first change to the "configuration mode (page 27)".

1. Open the "4.20.2.1 Check Configuration window (page 404)".

   Right-click the **NetworkView** icon, **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Check Configuration**.

2. In the Check Configuration window, right-click the node and select **Stop Checking** menu.

Tip

You can select multiple devices and apply the settings to all selected devices at once.

Caution

If there are 100 or more devices specified for change management operations in one schedule, the process may not finish immediately. In this case, change management operations may be performed on devices whose schedule is going to stopped.

4.20.2.4 Batch registration of change management schedule information

Change management schedules can be batch-registered with Network Manager by importing change management schedule information from an external file.

This function is designed for use in cases where there are many devices that will register change management schedules, etc. This function can reduce GUI operations related to change management schedules.

Also, currently registered change management schedule information can be exported to external files.

Tip

When batch-registering change management schedule information, a file in which the calendar/schedule information to be used is defined (hereafter, FW schedule import/export file) is necessary.

If exporting change management schedule information, the FW schedule import/export file will be output to the same folder as the schedule information configuration file with the following file name: "SchImport_*YYYYMMDDhhmmss*.txt".

When importing change management schedule information, use this file without editing contents.

Preparing the schedule information configuration file

It is necessary to prepare in advance files that contain descriptions of change management schedule information (schedule information configuration files) and FW schedule import/export files in order to batch-register change management schedule information. These can be comma-delimited CSV files using ASCII code (*.csv) or tab-delimited Unicode text files (*.txt).

Use the FW schedule import/export file that was created by exporting the change management schedule information (do not change file content).

Newly created files are stored in a directory in the monitoring terminal.

Description rules

The conventions used in schedule information configuration files are given below.

- When compiling in ASCII code, use comma-delimited CSV files (*.csv). When compiling in Unicode, use tab-delimited text files (*.txt).
- Lines beginning with the "#" symbol are treated as comment lines.

  Example:

```
#schedule name,FW schedule file,function name,device name,option 1,opti
on 2
```

- Specify the item name in line 1.
- One line represents one device.
- Device name and function name are required. Also, if the same device name is specified more than once, the last item in which it is specified is valid.

Details of each column

Detailed descriptions of the table columns and their required/optional status are provided below.

No.	Item name	Description of setting	Omit
1	Schedule name	Specify a schedule name defined in either an FW schedule import/export file or in the system as the schedule information to be linked with a device. If specifying an FW schedule import/export file, a schedule name defined in that file must be used. If a schedule with the same name is already defined in the system, the schedule defined in the system will be used. If not specifying an FW schedule import/export file, the name of a schedule that is already defined in the system and in use as a configuration management schedule must be used. If no schedule name is specified, preexisting schedule information will be deleted when importing.	

No.	Item name	Description of setting	Omit
2	FW schedule import/export file	Specify the FW schedule import/export file name by its absolute path or by its relative path from the schedule information setting file. If omitted, the "schedule name" in column 1 will use a schedule already defined on the system and being used as a configuration management file schedule. Examples of FW schedule import/export file names: `Sch_exprt.csv` (existing in the same folder as the schedule information setting file) `..\Sch_exprt.csv` (existing in the folder above the schedule information setting file's folder) `C:\Program Files (x86)\NEC\UMF\Operations\SVC\tmp\Sch_exprt.csv` (absolute path specification)	
3	Function name	Specify the import/export target's function name. This is a mandatory item. "`Check Configuration`" is fixed.	
4	Device name	Specify a registered device name. The import target devices must all be configuration management targeted devices (devices with an RM license assigned and for which login settings have been made). If devices not targeted for configuration management are specified, the import process for those devices will be skipped.	
5	Option 1	Blank	o
6	Option 2	Blank	o

Sample Files

Sample schedule information setting files are stored at the location below:

<On the monitoring terminal, %installfolder%>`\Svc\sg\NvPRO\NvPROCsvIOConfig\Sample\`

The content of sample files is described below.

- Sample_RMScheduleImport.csv

  A sample file linking the same schedule (schedule name "Regular Monitor") with all devices.

- Sample_FWSchImport.txt

  This is the FW schedule import/export file used in "Sample_RMScheduleImport.csv". A schedule executed at one-hour intervals at the 0 minute of every hour (schedule name "Regular Monitor") is set.

Importing schedule information setting files

You must first change to the "configuration mode (page 27)".

1. Prepare a schedule information configuration file.

   For details, refer to "4.20.2.4.1 Preparing the schedule information configuration file (page 407)".

Caution

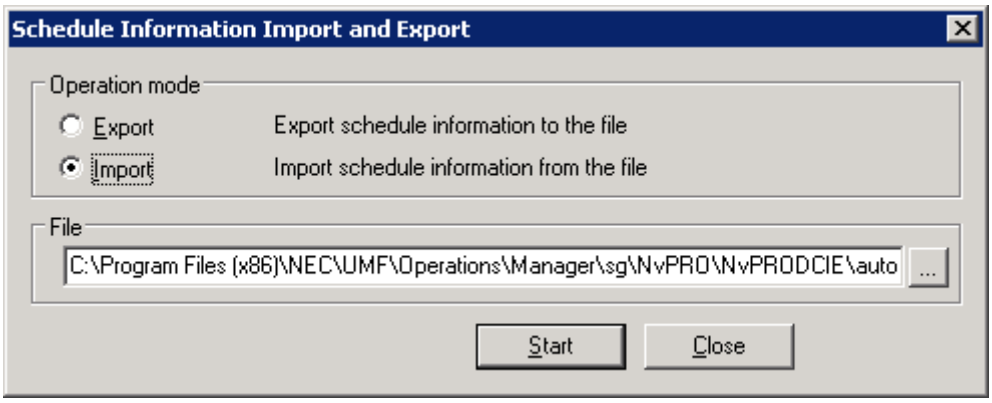
a. Use the exported change management schedule information file as the FW schedule import/export file. Do not change the content of this file.

b. If a calendar/schedule defined in the system has the same name as a calendar/schedule defined in the FW schedule import/export file, the information defined in the system is valid. (Does not replace the information defined in the FW schedule import/export file).

   If you want to import calendar/schedule information with the same name but different content, first change the name of the calendar/schedule defined in the system in the Schedule Setting window, and then import change management schedule information.

2. Open the Schedule Information Import and Export dialog box.

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Device Config Management**>**Schedule Information Import and Export**.



3. Select **Import** in the **Operation mode**.
4. Specify the import file name with the absolute path in the **File** column.
5. Click **Start** button.

Tip

When a dialog box appears to confirm overwriting or deletion, hold down SHIFT and press **Cancel** button to process all remaining rows without confirmation. (This dialog box will not appear again.)

Caution

a. Import operations place extra load on the CPU of the manager machine, resulting in possible delays in response to the monitoring terminal. Therefore, connections from other monitoring terminals during import operations are not recommended.

b. During import operations, all scheduled operations of **Device Config Management**>**Check Configuration**, **Configuration Management**>**Command Scheduling** and **Reboot Scheduling** in Software Upgrade window will be skipped.

c. Import in the order of the lines in the schedule information configuration file. If a line specifies an FW schedule import/export file, import calendar/schedule information first and then set the schedule for that device.

   Furthermore, if the same FW schedule import file is specified in multiple lines, only the calendar/schedule information in the first line will be imported.

6. In the completion dialog box, click **Operation Log** button and confirm the import results.

   For details, refer to "4.20.2.4.4 Operation log file (page 410)".

Also, if there are rows that cannot be registered due to entry error, etc., these row are saved in another file as an "error record file". For details, refer to "4.20.2.4.5 Error record file (page 411)".

7. Open the "4.20.2.1 Check Configuration window (page 404)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Device Config Management**>**Check Configuration**.

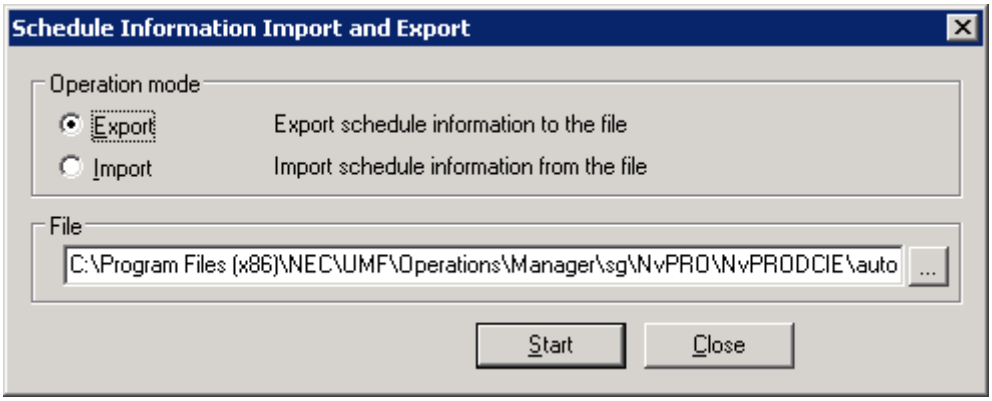
   Schedule operations related to a device for which the import operation was successful are enabled (monitoring begins) after the import process finishes. You can confirm the status of the schedule in the **Check** column of the "4.20.2.1 Check Configuration window (page 404)".

Exporting schedule information settings

You must first change to the "configuration mode (page 27)".

1. Open the Schedule Information Import and Export dialog box.

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Device Config Management**>**Schedule Information Import and Export**.



2. Select **Export** in the **Operation mode**.
3. Specify an export file with the absolute path in the **File** column.

   Export may fail if specifying a file/folder name including "nul" (either upper or lower case) to save schedule information configuration file.

   Specify a path name that does not contain "nul" (either uppercase or lowercase).
4. Click **Start** button.
5. In the completion dialog box, click **Operation Log** button and confirm the export results.

   For details, refer to "4.20.2.4.4 Operation log file (page 410)".

1. When exporting, only device information for devices executing a change management schedule (monitoring on) is exported.
2. The FW schedule import/export file will be created under the same folder as the schedule information configuration file. The FW schedule import/export file is necessary during import. Be sure to save it.

Operation log file

The following information is output to the operation log file.

- Import

  The result of checking the import file and import operation

- Export

  The results of the export operation

The operation log backup file uses the name "*%incrementalnumber%*_ImportExportLog.txt". *%incrementalnumber%* starts at 000 and 1 is added each time. The maximum number is 099.

The operation log of activity, prior to the most recent operation, is saved as a backup.

In cases where the number of backup files has already reached 100, when operation commences, the message "`Delete the backup operation log file`" is displayed and the operation is not performed. Delete all unnecessary backup files and retry the operation.

- The log is stored in the following:

  <On the monitoring terminal, %installfolder%>`\Svc\log\NvPROCsvIOConfig\_ImportExportLog.txt`

- The backup logs are stored in the following:

  <On the monitoring terminal, %installfolder%>`\Svc\log\NvPROCsvIOConfig\ImportExportLog`

Error record file

Use the error record file to import only those records that could not be registered or deleted.

Correct the error record file according to the operation log before performing import.

Location of the error record file

Directory

Same directory as the import file

File Name

"TMP_" + *import_file_name.extension*

4.20.3 Changing the limit for the number of config histories

In the device config management of the Resource Manager function, the running-config management, startup-config management, change management, respectively manages their histories of the difference information.

Respective histories are independently managed in principle. However, the history of the running-config management is added when a change of configuration is detected in the change management.

The upper limit of the storing number of these history information can be changed, respectively.

4.20.3.1 Changing the number of running-config histories

The default number of running-configs saved for each node is 10 generations. This number can be changed.

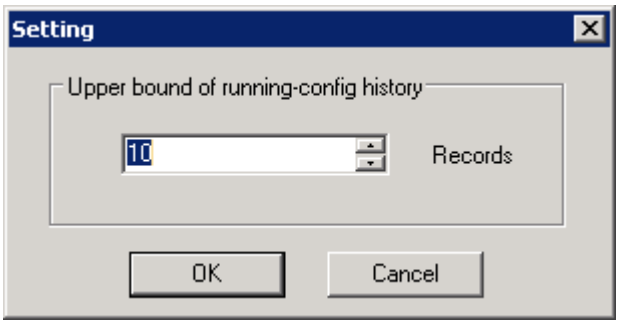
You must first change to the "configuration mode (page 27)".

1. Open the Running-config Management window.

Right-click the **NetworkView** icon, **NetworkManagement** icon, the map icon, or the device icon. Select **Device Config Management**>**Running-config Management**.

2. Right-click the target device in the **running-config Operation** list and select **Upper Bound of History** menu.
3. In the Setting dialog box, set the upper limit of the histories.

   You can specify a number between 5 and 65,535.



4. Click **OK** button.

4.20.3.2 Changing the number of startup-config histories

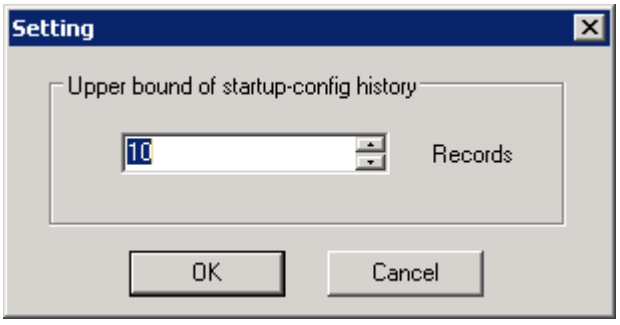
The default number of startup-configs saved for each node is 10 generations.

You must first change to the "configuration mode (page 27)".

1. Open the Startup-config Management window.

   Right-click the **NetworkView** icon, **NetworkManagement** icon, the map icon, or the device icon. Select **Device Config Management**>**Startup-config Management**.
2. Right-click the target device in the **startup-config Operation** list and select **Upper Bound of History** menu.
3. In the Setting dialog box, set the upper limit of the histories.

   You can specify a number between 5 and 65,535.



4. Click **OK** button.

4.20.3.3 Changing the number of change management histories

The default number of difference information saved for each node is 10 generations. This number can be changed.

You must first change to the "configuration mode (page 27)".

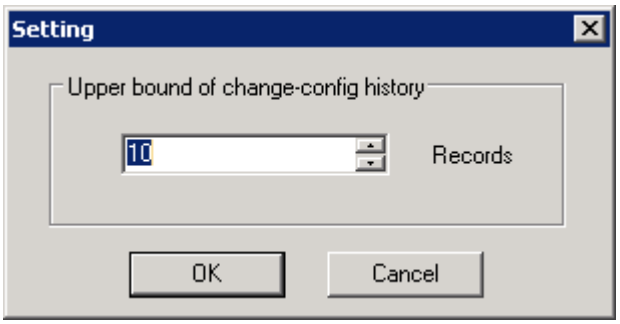
1. Open the Check Configuration window.

   Right-click the **NetworkView** icon, **NetworkManagement** icon, the map icon, or the device icon. Select **Device Config Management**>**Check Configuration**.

2. Right-click the target device in the **Find Condition Setting** list and select **Upper Bound of History** menu.

3. In the Setting dialog box, set the upper limit of the histories.

   You can specify a number between 5 and 65,535.



4. Click **OK** button.

4.20.4 Exporting the latest configuration

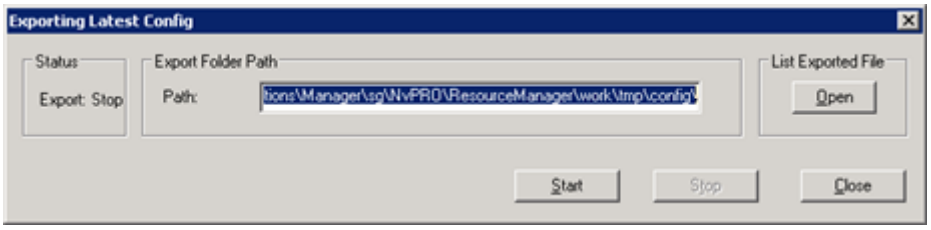
In Network Manager, updated running-config and startup-config files can be stored on the manager.

The automatic export function targets collected configurations when the **Start** button is clicked. Updated device configurations are not exported if a collection operations (a collect configuration command has been run or configurations have been collected using the Change Monitor function) are not performed for that device.

File names for files exported using the automatic export function are *DeviceName*_startup.txt or *DeviceName*_running.txt.

1. Open the Exporting Latest Config dialog box.

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Device Config Management**>**Export Latest Config**.



Caution

The export may fail if specifying a path name including "nul" (either upper or lower case) to save. Specify a path name that does not contain "nul" (either uppercase or lowercase).

2. Click **Start** button.

   The latest configuration file will be always exported on the manager.

3. To stop exporting, click **Stop** button.

4.20.5 Setting for sending an alert

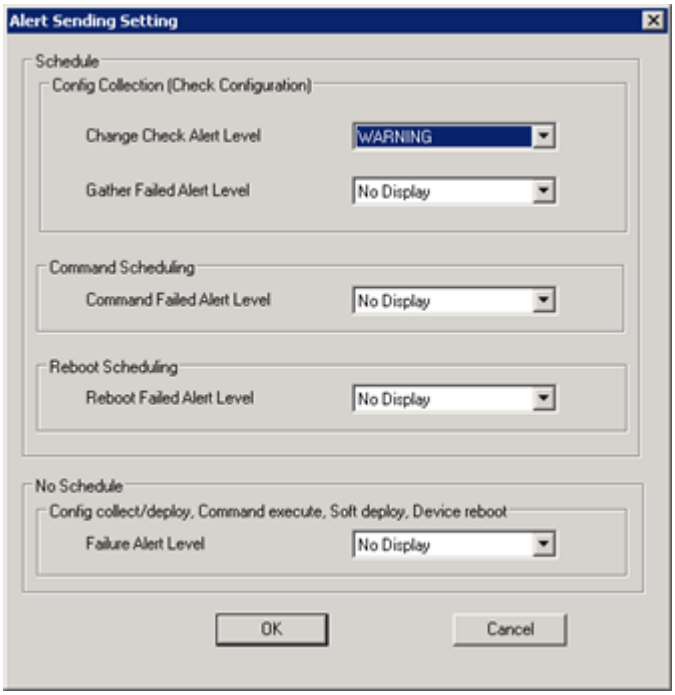
Error events in each type of the processing such as the scheduled execution of the device command or configuration management, etc. are notified as alerts.

1. Open the Alert Sending Setting dialog box.

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Device Config Management**>**Alert Sending Setting**.

2. Set an alert severity level.

   Since **No Display** is set by default except the setting of the configuration change management. Change the level if necessary.



The following describes each of the setting items.

- **Config Collection (Check Configuration)**
  - **Change Check Alert Level**

    Sets the severity level of alerts when change of running-config is detected.
  - **Gather Failed Alert Level**

    Sets the severity level of alerts when a failure occurs during running-config collection using the change management function.
- **Command Scheduling**

  Sets the severity level of alerts if a failure occurs when running a command using command scheduling.
- **Reboot Scheduling**

  Sets the severity level of alerts if a failure occurs during the planned restarting of a device using software deployment.
- **Config collect/deploy, Command execute, Soft deploy, Device reboot / Failure Alert Level**

Sets the severity level of alerts when a failure occurs in each of the processes in the GUI command.

The following is an explanation of alert severities.

No Display :

An alert is not displayed.

FATAL :

The severity level of the alert is displayed as FATAL.

MAJOR :

The severity level of the alert is displayed as MAJOR (in the extended mode) or FATAL (in the compatible mode).

MINOR :

The severity level of the alert is displayed as MINOR (in the extended mode) or FATAL (in the compatible mode).

WARNING :

The severity level of the alert is displayed as WARNING.

NORMAL :

The severity level of the alert is displayed as NORMAL.

3. Click **OK** button.

4.21 Linking with NEC SigmaSystemCenter (Network Provisioning)

Change the VLAN settings for switches and the load balancing settings for the load balancer by using the Network Provisioning function to link to the server provisioning operations (SystemProvisioning function) provided with NEC SigmaSystemCenter (hereafter referred as SigmaSystemCenter).

4.21.1 Preparing for linking

To link with SigmaSystemCenter, setup is needed on both the Network Manager side and the SigmaSystemCenter side. This section describes how to configure the settings on the Network Manager side. For information on setting up the SigmaSystemCenter side, refer to the SigmaSystemCenter documentation.

The following are the advance configuration settings.

1. Register the switches and load balancing devices.

   Register information for the switches and load balancing devices to control with the Network Provisioning function in Network Manager. For information about registering devices, refer to "4.2 Creating Network Configuration Map (page 127)".

   If the devices are registered manually, update device information for target devices in order to register the information used in the Network Provisioning function controls. For more information regarding updating device information, refer to "4.2.7 Updating device information via a network (page 179)".

Caution

If using Route Domain function in the BIG-IP series device, Network Manager cannot set the load balancer setting for this device.

2. Configure the CLI mode setting (for blade server built-in switches control).

   To control NEC's blade server (SIGMABLADE) built-in switches, set the CLI mode of switch to ISCLI.

3. Set up the login information.

   Before linking to SigmaSystemCenter, set up the login information for logging in to the switches and load balancing devices to control using the Network Provisioning function. For information about login settings, refer to "4.3.2 Registering device login information (page 191)".

   To control NEC QX-S switches, either one of the following settings should be configured in the login setting.

   - Configure the login setting of user level 3.
   - If the user level is 2, set the super password to raise the user level to 3 in super column of the login setting.

4. Create an option definition file (for load balancer control).

   To use settings commands customized for load balancer device types, create an option definition file in advance. For details, refer to "4.21.4 Load balancer option settings function (page 417)".

5. Create a UFD settings definition file (for blade server internal switch control).

   To use the Uplink Failure Detection (UFD) function in NEC blade server (SIGMABLADE) internal switches, first create a UFD settings definition file. For details, refer to "4.21.5 Uplink Failure Detection (UFD) setup function (page 422)".

4.21.2 Coexisting with related applications

When installing the following SigmaSystemCenter-related applications and Network Manager on the same server, configure the following settings to prevent network port number conflicts.

1. MasterScope DeploymentManager

   When MasterScope DeploymentManager is installed on the same server, conflicts occur with the network port number for tftp transfers (69/UDP).

   For instructions on how to avoid this conflict, refer to "Notes on Using MasterScope Network Manager" in "MasterScope DeploymentManager Reference Guide".

2. ESMPRO/ServerManager

   When NEC ESMPRO Manager is installed on the same server, conflicts occur with the network port number for receiving SNMP traps (162/UDP).

   To avoid this conflict, change the settings on both the NEC ESMPRO Manager and Network Manager sides so that the Windows SNMP Trap Service is used instead.

   To see how to change Network Manager settings, refer to "11.4.1 Using the Windows SNMP Trap service (page 776)" .

   To see how to change NEC ESMPRO Manager settings, refer to the NEC ESMPRO Manager documentation.

4.21.3 Precautions during operation

Precautions on configuring VLAN settings

1. QX-S5200G series, QX-S5900 series

   If VLAN settings are configured for a trunk port, VLAN number "1" is also added due to the specification of the device. For details, refer to the QX-S5200G series and QX-S5900 series manuals.

4.21.4 Load balancer option settings function

By creating an option definition file, settings commands specific to each kind of load balancer device can be executed from Network Provisioning's load balancer settings function.

4.21.4.1 Option definition file overview

An option definition file is a text-format file prepared by individual load balancer devices. If not conducting option settings for each type of device, it is not necessary to prepare option definition files.

Following is an overview of an option definition file.

File name	Device name.txt Example: The option definition file of a load balancer device (LB1) is: LB1.txt
Stored directory	*<On the manager, %sharedfolder%>*\Manager\sg\NvPRO\NvPRODCCmd\option\
Character code	Little-Endian UTF-16(UTF-16LE) with BOM. Linefeed code: CRLF. When editing in Notepad, specify "Unicode" in the **Encoding** of Save As dialog box and then save.

4.21.4.2 Option definition file format

This section describes the format of option definition files.

General rules

Format

```
<Resource character string>
*Command character string
```

Rules

- All content from a number sign (#) to the end of a line will be treated as a comment.
- Enter a character string representing the resource between less-than and greater-than marks (<>).

  Example:

  ```
  <server port 80>
  ```

- Specify the character string for the command to be executed after an asterisk (*).

  Example:

```
*source-nat
```

- Do not enter a space or TAB at the beginning of a line.
- It is possible to describe several resources within one option definition file.
- It is possible to specify numerous command character strings under one resource.
- It is possible to specify numerous message character strings under one command.

⚠ Caution

Regarding specific command character strings and message character strings, refer to the load balancer device manual.

Resources for ServerIron

Types of resources that can be specified in an option definition file for ServerIron and supplemental explanation regarding those resources are included below.

1. Real server

Resource character string	`<server real real server IP address localserver>` Or, `<server real real server IP address>` Example: `<server real 1.1.1.1 localserver>`
Command execution timing	When the applicable real server (IP) is applied to a device for the first time from Network Manager, executed on the real server level of the command line interface. Real server is registered as local server when `localserver` is specified.
Supplemental explanation	`localserver` is specified when it is registered in the server real. (When it is omitted, it is registered in the server remote.)

2. Real server port

Resource character string	`<server real port real server IP address:port number>` Example: `<server real port 1.1.1.1:80>`
Command execution timing	hen applicable real server port is applied to a device for the first time from Network Manager, executed on the real server level of the command line interface. Example: `<server real port 192.168.1.1:80>` `*keepalive`
Supplemental explanation	Specify the command (option) following "`port n`" (*n* is the real server port number).

3. Virtual server

Resource character string	`<server virtual virtual server IP address>` Example: `<server virtual 2.2.2.2>`
Command execution timing	When applicable virtual server (IP) is applied to a device for the first time from Network Manager, executed on the virtual server level of the command line interface.

4. Virtual server port

Resource character string	`<server virtual port virtual IP address:port number>` Example: `<server virtual port 2.2.2.2:80>`
Command execution timing	When applicable virtual server port is applied to a device for the first time from Network Manager, executed on the virtual server level of the command line interface. Example: If setting the lb-pri-servers option at port number 80 `<server virtual port 192.168.1.1:80>` `*lb-pri-servers`
Supplemental explanation	Specify the command (option) following "`port n`" (*n* is the real server port number).

Resources for BIG-IP, BIG-IP v9

Types of resources that can be specified in an option definition file for BIG-IP and supplemental explanation regarding those resources are included below.

1. Pool

Resource character string	`<pool pool virtual server IP address:port number>` Example: `<pool 3.3.3.3:80>`
Command execution timing	Executed when applicable virtual server port is applied to a device for the first time from Network Manager. Example: `*bigpipe pool POOLNAME {snat enable}` If the above is specified, `bigpipe pool NVP_PL_3.3.3.3_tcp_80 {snat enable}` will be executed. `*bigpipe profile PROFILENAME { timeout 300}` If the above is specified,

	`bigpipe profile NVP_PROFILE_3.3.3.3_tcp_80 {timeout 300}` will be executed.
Command supplemental explanation:	When executing a pool command, specify the character sting "POOLNAME" in the pool name position. When the command is executed, Network Manager will substitute the actual pool name for this. In the case of BIG-IPv9, it is also possible to specify the option command of profile command used at the virtual server. Specify the character string "PROFILENAME" in the profile name position. When the command is executed, Network Manager will substitute the actual profile name for this.

2. Pool member (real server)

Resource character string	<pool_member *virtual server IP address*:*port number real server IP address*:*port number*> Example: <pool_member 3.3.3.3:80 4.4.4.4:80>
Command execution timing	Executed when the applicable real server port is applied to a device for the first time from Network Manager. Example: `*bigpipe pool POOLNAME { member 3.3.3.3:80 priority 20}` If the above is specified, `bigpipe pool NVP_PL_3.3.3.3_tcp_80 { member 3.3.3.3:80 priority 20}` is executed.
Command supplemental explanation:	When executing a pool command, specify the character sting "POOLNAME" in the pool name position. When the command is executed, Network Manager will substitute the actual pool name for this.

3. Virtual server port

Resource character string	<virtual *virtual server IP address*:*port number*> Example: <virtual 3.3.3.3:80>
Command execution timing	Executed when applicable virtual server port is applied to a device for the first time from Network Manager. Example: `*bigpipe virtual VIRTUALNAME {limit 10}` If the above is specified, `bigpipe virtual NVP_VS_3.3.3.3_tcp_80 {limit 10}` is executed.
Command supplemental explanation:	When executing a virtual command in BIG-IPv9, specify the character string "VIRTUALNAME" in the virtual name position. When the command is executed, Network Manager will substitute the actual virtual name for this.

Resources for A10 Networks AX series, Thunder ADC series

Types of resources that can be specified in an option definition file for A10Networks AX series ,Thunder ADC seriesand supplemental explanation regarding those resources are included below.

1. Real server

Resource character string	`<real-server real server IP address>` Example: `<real-server 11.0.0.1>`
Command execution timing	When the applicable real server (IP) is applied to a device for the first time from Network Manager, executed on the real server level of the command line interface.

2. Real server port

Resource character string	`<real-server-port real server IP address:port number>` Example: `<real-server-port 11.0.0.1:80>`
Command execution timing	When applicable real server port is applied to a device for the first time from Network Manager, executed on the real server level of the command line interface. Supplemental explanation : Example: `<real-server-port 11.0.0.1:80> *conn-limit 10`
Supplemental explanation	Specify the command (option) following "`port n protocol`" (*n* is the real server port number, *protocol* is the protocol of the real server port).

3. Virtual server

Resource character string	`<virtual-server virtual server IP address>` Example: `<virtual-server 10.0.0.1>`
Command execution timing	When applicable virtual server (IP) is applied to a device for the first time from Network Manager, executed on the virtual server lovel of the command line interface.

4. Virtual server port

Resource character string	`<virtual-server-port virtual server IP address:port number>` Example: `<virtual-server-port 10.0.0.1:80>`

Command execution timing	When applicable virtual server port is applied to a device for the first time from Network Manager, executed on the virtual server level of the command line interface. Example: If setting the conn-limit 10 option at port number 80 `<virtual-server-port 10.0.0.1:80>` `*conn-limit 10`
Supplemental explanation	Specify the command (option) following "`port n protocol`" (*n* is the real server port number, *protocol* is the protocol of the real server port).

5. Virtual server port (with protocol specification)

   By defining it, you can specify a protocol other than tcp and udp in the virtual server port

Resource character string	`<virtual-server-port-protocol` *virtual server IP address*`:`*port number*`:`*protocol*`>` Example: `<virtual-server-port-protocol 10.0.0.1:80:http>`
Command execution timing	When applicable virtual server port is applied to a device for the first time from Network Manager, executed on the virtual server level of the command line interface. Example: If defining virtual server port number 80 as http protocol. `<virtual-server-port-protocol 10.0.0.1:80:http>` If defining virtual server port number 80 as http protocol and setting conn-limit 10 option. `<virtual-server-port-protocol 10.0.0.1:80:http>` `*conn-limit 10`
Supplemental explanation	Specify the command (option) following "`port` *n* `protocol`" (*n* is the real server port number, *protocol* is the protocol of the real server port).

If you want to use the service group name in the option command, specify the character string "`POOLNAME`" in the service group name position. When the command is executed, Network Manager will substitute the actual service group name.

If you want to use the real server name in the option command, specify the character string "`REALNAME`" in the real server name position. When the command is executed, Network Manager will substitute the actual real server name.

4.21.5 Uplink Failure Detection (UFD) setup function

Use the UFD Setup function to dynamically change and synchronize the UFD settings of built-in switches in NEC's blade servers with VLAN control through Network Provisioning.

UFD downlink settings (ltd) are applied/removed simultaneously with the application/removal of VLANs to/from the downlink ports (Ports Nos. 1-16) of blade server built-in switches.

4.21.5.1 Overview of UFD setup function commands

1. Commands when applying VLANs

If all of the following conditions are satisfied,

- The FDP numbers of the VLANs for the target devices are defined in the UFD definition file.
- The numbers of the ports that VLAN is being applied to are 1 through 16.

then run the following commands after executing commands the commands for applying the VLAN.

```
ufd fdp <FDP number>
ltd <Port number>
```

2. Commands for removing VLANs

   If all of the following conditions are satisfied,

   - The FDP numbers of the VLANs for the target devices are defined in the UFD definition files,
   - The numbers of the ports that VLAN is being applied to are 1 through 16.

   then run the following commands after executing commands the commands for applying the VLAN.

```
ufd fdp <FDP number>
no ltd <Port number>
```

4.21.5.2 UFD setup definition file format

UFD setup definition files are text files provided in the built-in switch units of blade servers.

You do not need to have UFD setup definition files if you do not use the UFD Setup function.

Overview of UFD setup definition files

File Name	Device name.txt Example: Option definition file for built-in switches (SW1) in blade servers: SW1.txt
Stored Directory	<On the manager, %sharedfolder%>\Manager\sg\NvPRO\NvPRODCCmd\user\ufd\
Encoding	Little-Endian UTF-16 (UTF-16LE) with BOM. Linefeed code: CRLF. When editing in Notepad, specify "Unicode" in the **Encoding** of Save As dialog box and then save.

Format

```
VLAN number,FDP number
```

- VLAN number

  The number of the VLAN controlled through a Network Provisioning link

- FDP number

  The Failure Detection Pair (FDP) number that corresponds with the VLAN Number

Rule

The portion from "#" to the end of the line is considered as a comment.

⚠ Caution

Different VLAN numbers cannot be assigned the same FDP number.

4.21.5.3 Configuring UFD setup function

The procedure for configuring the UFD Setup function is shown below.

1. Create a UFD setup definition file with the file name *device_name*.csv.

   Example: SW1.txt

```
#VLAN number,FDP number
10,1
20,2
30,3
40,4
```

2. Store the UFD setup definition file in: *<On the manager, %sharedfolder%>*\Manager\sg\NvPRO\NvPRODCCmd\user\ufd\.
3. Manually configure UFD settings for the uplink port of the blade server built-in switch.

4.21.5.4 Changing the VLAN number/FDP number combination

If changes are made to the VLAN number/FDP number combination, modify the UFD definition file after removing all the VLANs configured through Network Provisioning.

Services do not need to be restarted. The VLAN number-FDP number changes will be reflected next time a VLAN is applied.

4.21.6 Checking configuration status of Network Provisioning

To check the configuration status of Network Provisioning without using the SigmaSystemCenter GUI, run the NvPRODCImportExportCmd command to output the configuration status of Network Provisioning in a tab-separated Unicode text file (TSV file).

For details regarding NvPRODCImportExportCmd, refer to "9.10.4 VLAN/Load Balancer setting information export command (NvPRODCImportExportCmd) (page 730)".

4.21.6.1 TSV file format output by NvPRODCImportExportCmd (VLAN)

The format of TSV files containing VLAN configuration information, as output by NvPRODCImportExportCmd, is shown below.

No.	Item Name	Description	Example
1	VLAN name	VLAN name	VLAN10
2	VLAN ID	VLANID	10
3	Switch name controlled by Network Manager	Device name to be configured for VLAN	SW1
4	Port name of switch to add VLAN	Port name of switch where VLAN is set up	Ethernet0/1

No.	Item Name	Description	Example
5	VLAN type	0: untagged VLAN 1: tagged VLAN	0
6	Applied status	Configuration status on the device 0: not applied 1: applied	1

4.21.6.2 TSV file format output by NvPRODCImportExportCmd (LB)

The format of the TSV files containing load balancer configuration information, as output by `NvPRODCImportExportCmd`, is shown below.

No.	Item Name	Description	Example
1	Load Balancer name	Device name to be configured for LB.	LB1
2	Redundancy type	Not currently used. (2 must be set)	2
3	LB group name	LB group name entered via SSC GUI (virtual server name)	VS1
4	Virtual server name [1)]	Virtual server name configured in the device. **Tip** Enabled only when the device type is ServerIron or AX.	NVP_VS_10.0.0.1
5	Virtual IP Address	Virtual IP address of the LB group. (IP address of virtual server)	10.0.0.1
6	Virtual Server Port	Virtual server port number of the LB group (Port number of virtual server)	80
7	Session keep method	Session keep method for the virtual server 0:NoSetting 1:Cookie 2:Ssl 3:Sticky	3
8	Profile name [1)]	BIG-IPv9 or later profile name, or AX template name, set up in the device. **Tip** Enabled only when the device type is BIG-IP9 or AX.	NVP_PROFILE_ 10.0.0.1_tcp_80
9	Cookie name	The cookie name used if the session management method is based on using cookies.	testCookieName1
10	Load Balancing Method	Load balancing method used by the virtual server. 0:RoundRobin 1:LeastConnection 2:Weight 3:ResponseTime	0

No.	Item Name	Description	Example
11	Host name	The host name of real server entered via SSC GUI. (Real Server Name)	RS1
12	Real Server Name [1)]	The name of the real server to be set for the device **Tip** Enabled only when the device type is ServerIron or AX.	NVP_RS_11.0.0.1
13	Real Server IP Address	IP address of the real host (IP address of the real server)	11.0.0.1
14	Real Server Port	The port number of the host (port number of the real server)	80
15	Pool Name [1)]	BIG-IP pool name AX service group name **Tip** Enabled only when the device type is BIG-IP or AX.	NVP_PL_10.0.0.1_tcp_80
16	Real Server Weight	The weight value when load balancing is based on using weights	300
17	Protocol	Virtual server protocol "TCP" "UDP"	TCP
18	Virtual Server Name [1)]	BIG-IPv9 virtual server name **Tip** Enabled only when the device type is BIG-IPv9 or later.	NVP_VS_10.0.0.1_tcp_80
19	Applied Status	Device configuration status 0: not applied 1: applied	0

1) A name that is automatically assigned within Network Manager and the resource name that is used in device settings.

4.22 Scheduling

4.22.1 Setting a calendar

By setting the calendar and linking it to a schedule, schedule rules can be applied to the operation dates set in the calendar. The following functions are available in the calendar.

- "4.22.1.2 Customizing a calendar (page 428)"

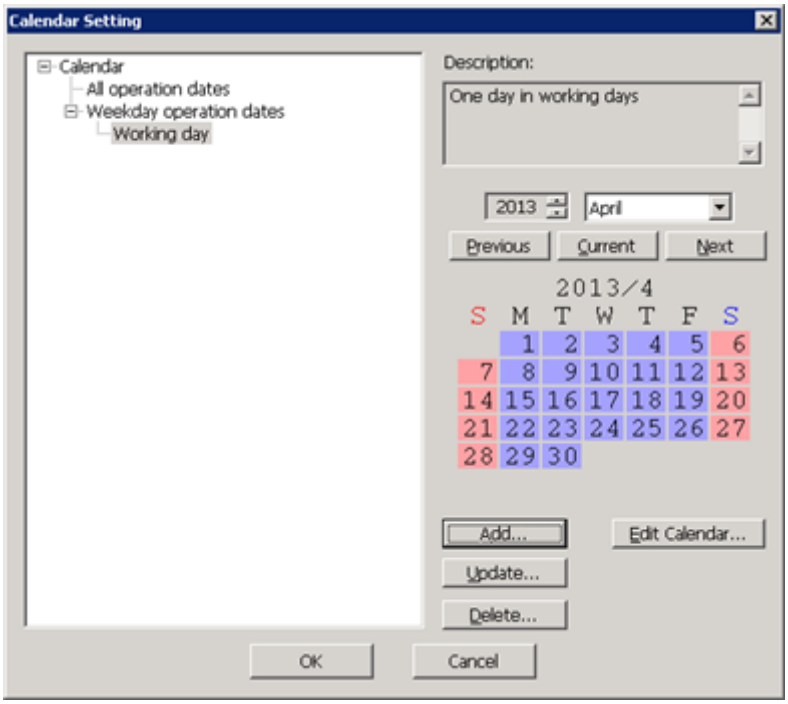
  Adds, changes or deletes a calendar.

- "4.22.1.3 Customizing calendar rules (page 433)"

Adds, changes or deletes calendar rules.

4.22.1.1 Calendar Setting dialog box

To open the Calendar Setting dialog box, in the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)", click **Select Calendar** button.



- **Calendar** tree

  Displays created calendars in a tree hierarchy. **All operation dates** and **Weekday operation dates** calendars that were created by default cannot be updated or deleted.

- **Description**

  Click **Add** button, displays the specified set in the Name Setting dialog box. For details regarding the Name Setting dialog box, refer to "4.22.1.2.2 Creating a new calendar (page 429)".

- **Year** box

  Specify the year of the calendar that you want to display. You can specify any year from 2000 to 2036.

- **Month** combo box

  Select the month of the calendar that you want to display.

- **Previous** button

  Displays the calendar for the previous month.

- **Current** button

  Displays the calendar for the current month.

- **Next** button

  Displays the calendar for next month.

- **Add** button

Adds a calendar below the calendar selected in the calendar tree. Open the Name Setting dialog box.

For details regarding the Name Setting dialog box, refer to "4.22.1.2.2 Creating a new calendar (page 429)".

To add a calendar, you must have calendar setting authority. For details on the calendar setting authority, refer to "4.1.3.4 Detailed authority settings of the calendar (page 123)".

- **Update** button

  Updates the calendar name and description for the calendar selected in the calendar tree. Open the Name Setting dialog box.

  For details regarding the Name Setting dialog box, refer to "4.22.1.2.2 Creating a new calendar (page 429)".

  To update a calendar, you must have setting authority for that calendar. For details on the calendar setting authority, refer to "4.1.3.4 Detailed authority settings of the calendar (page 123)".

- **Delete** button

  Deletes the calendar selected in the calendar tree.

  If the selected calendar has subordinate calendars, the subordinate calendars are also deleted.

  To delete a calendar, you must have setting authority for that calendar and subordinate calendars. For details on the calendar setting authority, refer to "4.1.3.4 Detailed authority settings of the calendar (page 123)".

- **Edit Calendar** button

  Allows changes to be made to the calendar selected in the calendar tree. Open the "4.22.1.2.5.1 Edit Calendar dialog box (page 431)".

  If you do not have setting authority for the target calendar, open "4.22.1.2.5.1 Edit Calendar dialog box (page 431)" in reference mode. For details on the calendar setting authority, refer to "4.1.3.4 Detailed authority settings of the calendar (page 123)".

The calendar tree is arranged according to a hierarchy with lower level calendars having higher priority. For example, assume that you have the following calendar tree.

- [Weekday operation dates]
  - [Do not include Wednesdays in operation dates]
    - [Every second Wednesday of the month is an operation date]

  If you select [Do not include Wednesdays in operation dates], Sunday, Wednesday and Saturday of each week will be excluded from the operation dates.

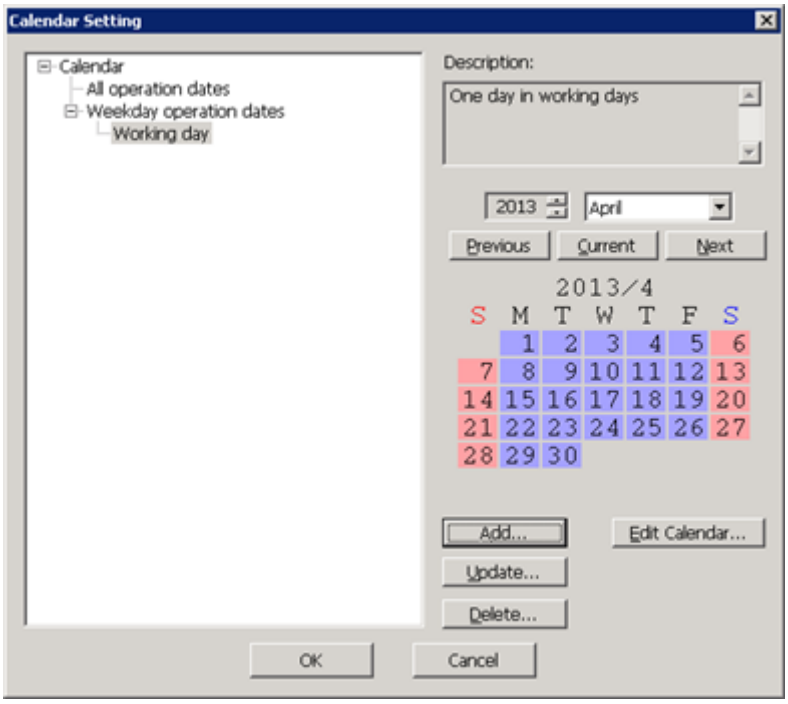
  If you select [Every second Wednesday of the month is an operation date], this option is located below to [Do not include Wednesdays in operation dates], so Sunday and Saturday of every week and all Wednesdays aside from the second Wednesday of every month are excluded from the operation dates.

4.22.1.2 Customizing a calendar

Selecting a created calendar

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".

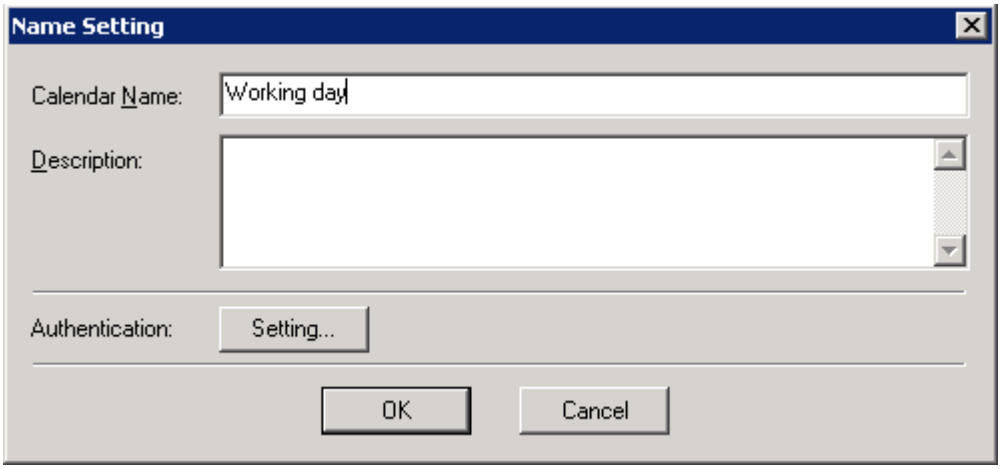
2. Click **Select Calendar** button.
3. In the "4.22.1.1 Calendar Setting dialog box (page 427)", select a calendar name in the calendar tree.



4. Click **OK** button.

Creating a new calendar

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Click **Select Calendar** button.
3. In the "4.22.1.1 Calendar Setting dialog box (page 427)", click **Add** button.
4. Set items in the Name Setting dialog box.



- **Calendar Name**

  Type a name for the calendar (required). A maximum of 64 characters can be entered.

Any spaces before or after the specified calendar name will be deleted. Spaces within the name are permitted.

If the specified calendar name contains only spaces it will result in an error.

- **Description**

  Type a description of the calendar. A maximum of 128 characters can be entered.

- **Authentication**

  Specify the calendar authority settings. For details, refer to "4.1.3.4 Detailed authority settings of the calendar (page 123)".

5. Click **OK** button.

Changing a calendar name

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Click **Select Calendar** button.
3. In the "4.22.1.1 Calendar Setting dialog box (page 427)", select the calendar name and click **Update** button.
4. In the Name Setting dialog box, change the settings.
5. Click **OK** button.

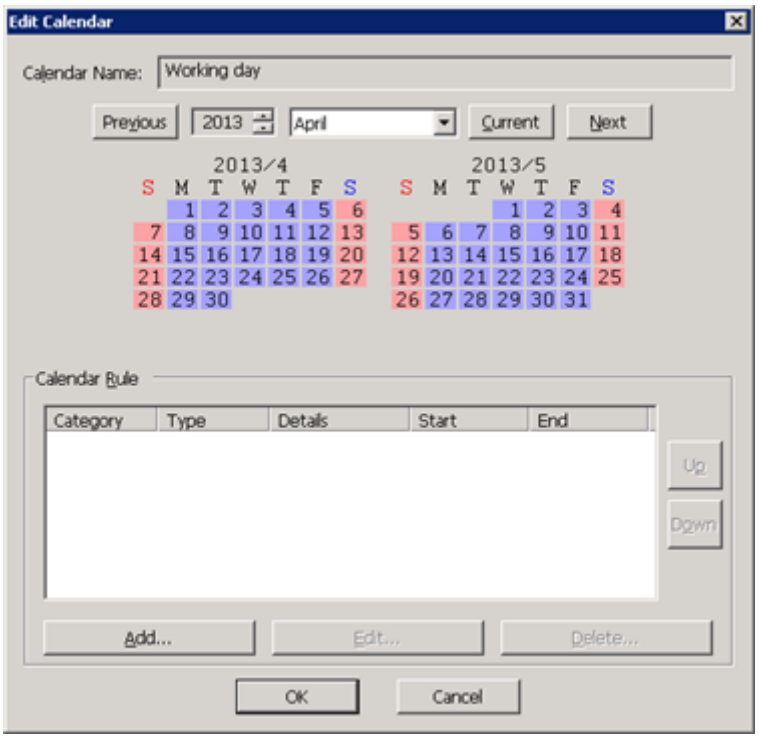
Deleting a calendar

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Click **Select Calendar** button.
3. In the "4.22.1.1 Calendar Setting dialog box (page 427)", select the calendar name and click **Delete** button.
4. In the deletion confirmation dialog box, click **OK** button.

Editing a calendar

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Click **Select Calendar** button.
3. In the "4.22.1.1 Calendar Setting dialog box (page 427)", select the calender name and click **Edit Calendar** button.

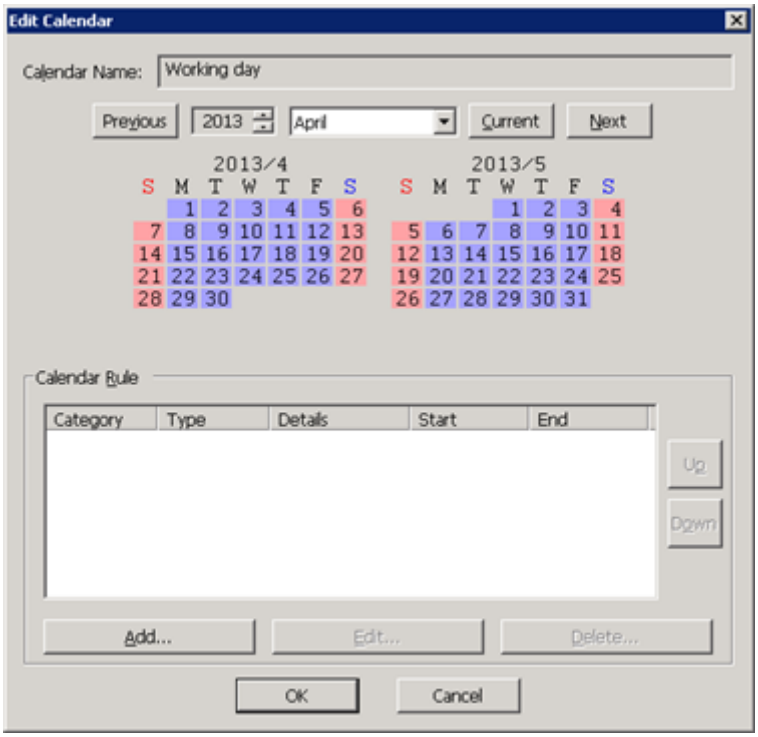
   To perform this operation, you must have setting authority for the target calendar. For details on the calendar setting authority, refer to "4.1.3.4 Detailed authority settings of the calendar (page 123)".
4. In the "4.22.1.2.5.1 Edit Calendar dialog box (page 431)", set the necessary information.



5. Click **OK** button.

Edit Calendar dialog box

To open the Edit Calendar dialog box, click **Select Calendar** button in the "4.22.1.1 Calendar Setting dialog box (page 427)".



- **Calendar Name**

  Displays the name of the selected calendar.

- **Previous** button

  Displays the calendar for the previous month.

- **Year** box

  Specify the year of the calendar that you want to display. You can specify any year from 2000 to 2036.

- **Month** combo box

  Select the month of the calendar that you want to display.

- **Previous** button

  Displays the calendar for the previous month.

- **Current** button

  Displays the calendar for the current month.

- **Next** button

  Displays the calendar for next month.

- **Calendar**

  The calendar status for each day is indicated by its background color. The colors have the following meanings.

  Unspecified day : Gray

  Operation day : Blue

  Non-operation day : Red

  An operation day according to a calendar rule added in the "4.22.1.3.1 Calendar Rule Settings dialog box (page 433)" : Dark blue

  A non-operation day according to a calendar rule added in the "4.22.1.3.1 Calendar Rule Settings dialog box (page 433)" : Dark red

- **Calendar Rule**

  Displays a list of calendar rules. The calendar rules higher in the list have more priority than the lower ones.

- **Add** button

  Open the "4.22.1.3.1 Calendar Rule Settings dialog box (page 433)" so that you can add **Calendar Rule**.

- **Update** button

  Open the "4.22.1.3.1 Calendar Rule Settings dialog box (page 433)" so that you can make changes to **Calendar Rule**.

- **Delete** button

  Deletes **Calendar Rule**.

- **Up** button

  Moves a calendar rule up, making it higher in priority.

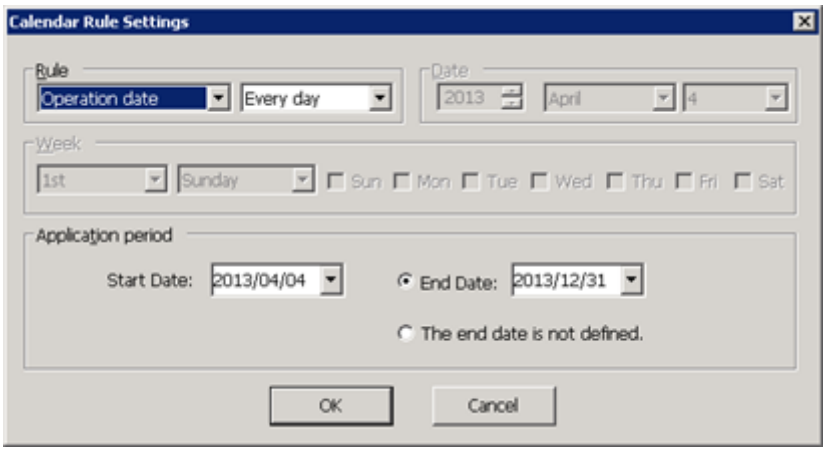
- **Down** button

  Moves a calendar rule down, making it lower in priority.

4.22.1.3 Customizing calendar rules

Calendar Rule Settings dialog box

To open the Calendar Rule Settings dialog box, in the "4.22.1.2.5.1 Edit Calendar dialog box (page 431)", select **Add** button or Calender Rule, and click **Update** button.



- **Rule** group

  Select "Unspecified day", "Operation date", or "Non-operation date".

  Select the type of the calendar rule. For enable/disable of each item depending on the type of the calender rule, refer to the table below.

  In the current version, "Unspecified day" is treated the same as "Non-operation day".

- **Date** group

  Specify a year, month and day. For enable/disable of each item, refer to the table below.

- **Week** group

  Select from a particular day that falls within a certain week of the month or the same day (s) every week. Refer to the list below to sea how to enable or disable each control.

- **Application period** group

  Specify the period to which you want to apply the calendar rule. If you do not specify an end date, the end date will be set to 12/31/2036. For enable/disable of each item, refer to the table below.

Enable/Disable of each entry items

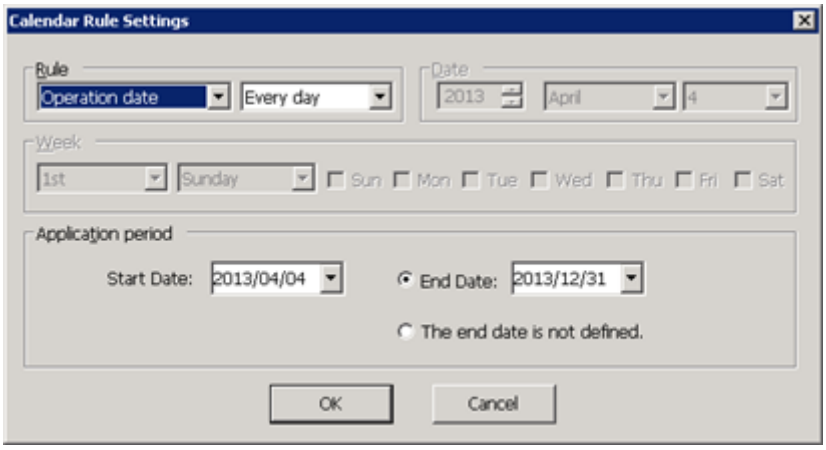
Depending on the calendar rule type selected, the following items can be entered.

Input item	Year	Month	Date	The n (th) week	Day	Day check box	Application period
Every day	x	x	x	x	x	x	o
Weekly	x	x	x	x	x	o	o
Monthly (date)	x	x	o	x	x	x	o
Monthly (day)	x	x	x	o	o	x	o
Yearly (date)	x	o	o	x	x	x	o
Yearly (day)	x	o	x	o	o	x	o

Input item	Year	Month	Date	The n (th) week	Day	Day check box	Application period
Specific date	o	o	o	x	x	x	x

Creating a calendar rule

1. Open the "4.22.2.1.1 Schedule Setting dialog box (page 435)".
2. To open "4.22.2.1.3.1 Edit Schedule dialog box (page 436)", select **Add** button, or select **Schedule Name** and click **Edit** button.
3. Click **Select Calendar** button.
4. In the "4.22.1.1 Calendar Setting dialog box (page 427)", click **Edit Calendar** button.
5. In the "4.22.1.2.5.1 Edit Calendar dialog box (page 431)", click **Add** button.
6. In the "4.22.1.3.1 Calendar Rule Settings dialog box (page 433)", set the information.



7. Click **OK** button.

Deleting a calendar rule

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Click **Select Calendar** button
3. In the "4.22.1.1 Calendar Setting dialog box (page 427)", click **Edit Calendar** button.
4. In the "4.22.1.2.5.1 Edit Calendar dialog box (page 431)", select **Calendar Rule** and click **Delete** button.
5. In the deletion confirmation dialog box, click **OK** button.

Changing a calendar rule

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Click **Select Calendar** button.
3. In the "4.22.1.1 Calendar Setting dialog box (page 427)", click **Edit Calendar** button.
4. In the "4.22.1.2.5.1 Edit Calendar dialog box (page 431)", select a **Calendar Rule** and click **Update** button.
5. Change the setting in the "4.22.1.3.1 Calendar Rule Settings dialog box (page 433)".

6. Click **OK** button.

4.22.2 Setting a time schedule

By setting a time schedule, you are able to perform processes at scheduled dates and times.

The following functions are available in the time schedule.

- "4.22.2.1 Customizing a time schedule (page 435)"

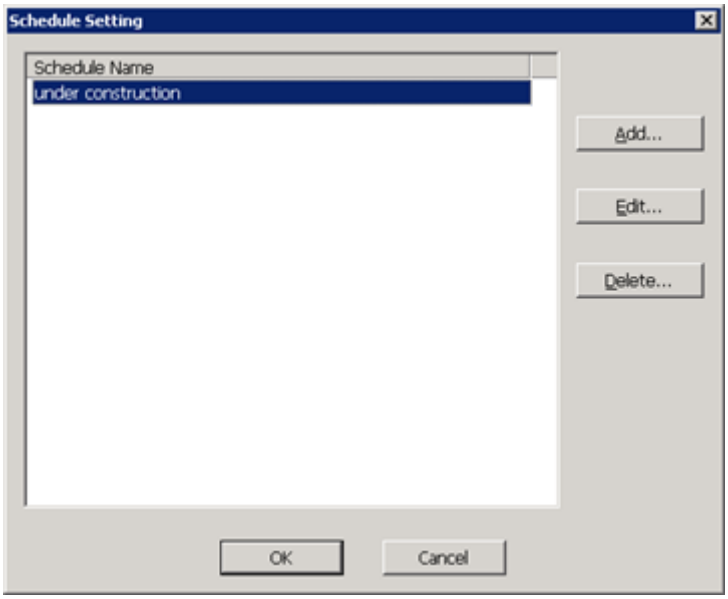
  Adds, update or delete settings for time schedules.

- "4.22.2.2 Customizing time schedule rules (page 439)"

  Adds, updates or deletes time schedule rules.

4.22.2.1 Customizing a time schedule

Schedule Setting dialog box



- **Schedule Name**

  Displays created schedules in a list.

  If you have previously selected a schedule, it will still be selected.

- **Add** button

  Adds a schedule.

  Opens the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".

- **Edit** button

  Updates the schedule that has been selected in the list.

  Opens the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".

- **Delete** button

  Deletes the schedule that has been selected in the list.

  Schedules that are currently in use cannot be deleted.

Selecting a created time schedule

1. Open the "4.22.2.1.1 Schedule Setting dialog box (page 435)".
2. Select a **Schedule Name**.
3. Click **OK** button.

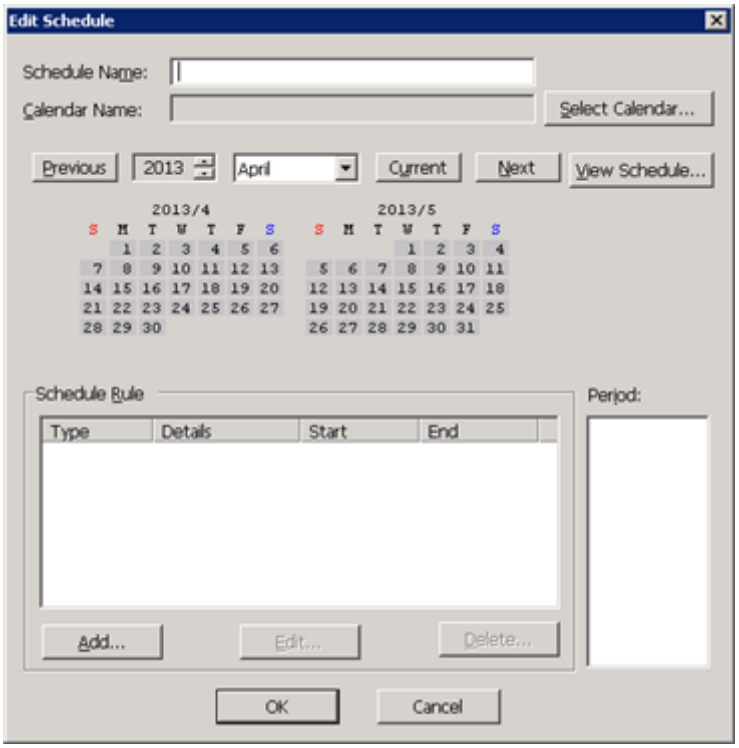
Creating a new time schedule

1. Open the "4.22.2.1.1 Schedule Setting dialog box (page 435)".
2. Click **Add** button.
3. In the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)", set the information.
4. Click **OK** button.

Apply the schedule rule to the "Operation day" set in the schedule rule.

Edit Schedule dialog box

To open the Edit Schedule dialog box, in the "4.22.2.1.1 Schedule Setting dialog box (page 435)", click **Add** button, or select **Scheduel Name** and click **Edit** button.



- **Schedule Name**

  Type a name for the schedule (required). A maximum of 64 characters can be entered.

  Any spaces before or after the specified schedule name will be deleted. Spaces within the name are permitted.

  If the specified schedule name contains only spaces it will result in an error.

- **Calender Name**

Select a calendar (required). Click **Select Calendar** button to open the "4.22.1.1 Calendar Setting dialog box (page 427)".

The name of the selected calendar is displayed in the "4.22.1.1 Calendar Setting dialog box (page 427)".

- **Previous** button

  Displays the calendar for the previous month.

- **Year** box

  Specify a year. Years from 2000 to 2036 are supported.

- **Month** combo box

  Specify a month.

- **Current** button

  Displays the calendar for the current month.

- **Next** button

  Displays the calendar for next month.

- **Select Calendar** button

  Opens the "4.22.1.1 Calendar Setting dialog box (page 427)".

- **View Schedule** button

  Opens the Schedules dialog box.

- **Calendar Display**

  The background colors of the scheduled dates for the schedule selected according to the **Schedule Rule**.

  Based on the rules for the calendar selected in **Select Calendar**, operation dates are displayed in green, non-operation dates in red and unspecified dates in gray.

  If a calendar has not been selected, the dates will be displayed in gray.

- **Schedule Rule**

  Displays a list of schedule rules. There is no priority given to the individual schedule rules.

- **Add** button

  Adds a schedule rule. Opens the "4.22.2.2.1 Schedule Rules Settings dialog box (page 439)".

- **Update** button

  Updates a schedule rule. Opens the "4.22.2.2.1 Schedule Rules Settings dialog box (page 439)".

- **Delete** button

  Deletes a schedule rule.

- **Period** list

  Displays the schedule times set for the selected schedule rule.

  In **Schedule Rule**, if the **Type** is set to **Repetition**, up to ten schedule times will be displayed from the current time on the current day.

  For the term schedule setting, today's start time - end time is displayed considering title as the Term (T).

Changing a time schedule

1. Open the "4.22.2.1.1 Schedule Setting dialog box (page 435)".
2. Select a **Schedule Name** and click **Edit** button.
3. In the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)", set the information.
4. Click **OK** button.

Deleting a time schedule

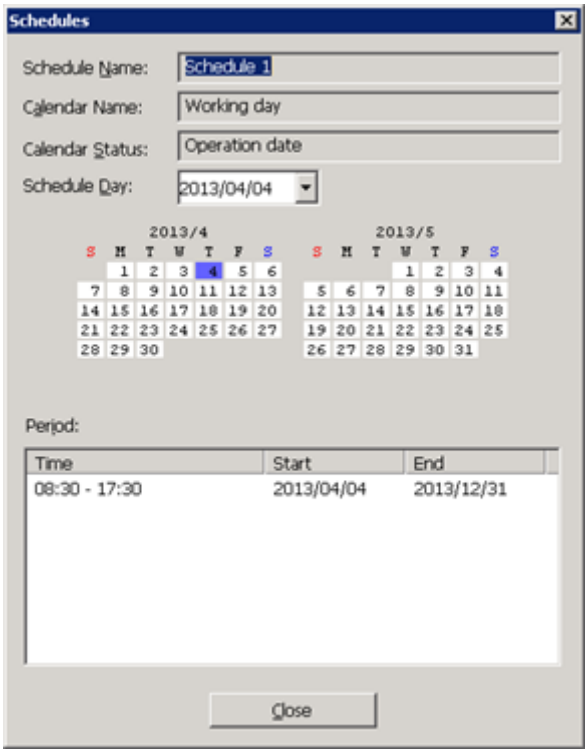
1. Open the "4.22.2.1.1 Schedule Setting dialog box (page 435)".
2. Select a **Schedule Name** and click **Delete** button.
3. In the deletion confirmation dialog box, click **OK** button.

   If the schedule is in use, it cannot be deleted. First, delete the schedule settings in the settings of the function that is using the schedule, and then delete the schedule.

Viewing a time schedule

Displays a list of schedule times for the specified date.

Schedules dialog box



- **Schedule Name**

  Displays the schedule name.

- **Calendar Name**

  Displays the name of the calendar that is being used by the schedule.

- **Calendar Status**

Displays the calendar status for the dates specified for the schedule.

Shows whether they are operation dates, non-operation dates or unspecified dates.

- **Schedule Day**

  Specify the date that you want displayed in the schedule times list.

  It is possible to specify the date using the box, or by opening the calendar window below by pressing F4.

- **Time**

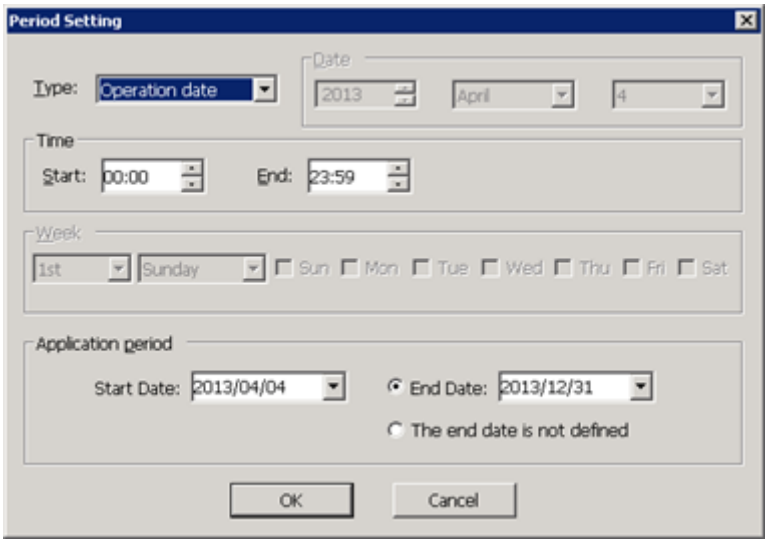
  Displays a list of the schedule times for the date selected in **Schedule Day**. The times are displayed in ascending order.

  In the case of schedules for which the type was set to "Repetition" in the "4.22.2.2.1 Schedule Rules Settings dialog box (page 439)", the times are displayed in the "Start Time - Stop Time - Interval" format.

4.22.2.2 Customizing time schedule rules

Schedule Rules Settings dialog box

To open the Schedule Rules Settings dialog box, in the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)", click **Add** button, or select the schedule rule and click **Edit** button.



- **Type**

  Select the schedule type.

- **Date**

  Specify the date that you want to run the schedule.

  You can select a date within the range of 1/1/2000 to 12/31/2036.

- **Time**

  Specify the time that you want to run the schedule.

  The start time is treated as 0 seconds and the end time as 59 seconds.

- **Week**

  Specify the day that you want to run the schedule.

- **Application period**

  Set the application period for the schedule.

  You can select a date within the range of 1/1/2000 to 12/31/2036.

  If you select **The end date is not defined**, the end date will be set to 12/31/2036.

Depending on the rule type selected, the following items can be entered.

Input item	Year	Month	Date	The n (th) week	Day	Day check box	Start	End	Interval	Period
Operation date	x	x	x	x	x	x	o	x	x	o
Repetition	x	x	x	x	x	x	o	o	o	o
Weekly	x	x	x	x	x	o	o	x	x	o
Monthly (date)	x	x	o	x	x	x	o	x	x	o
Monthly (day)	x	x	x	o	o	x	o	x	x	o
Yearly (date)	x	o	o	x	x	x	o	x	x	o
Yearly (day)	x	o	x	o	o	x	o	x	x	o
Specified day	o	o	o	x	x	x	o	x	x	x

Creating a time schedule rule

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Click **Add** button.
3. In the "4.22.2.2.1 Schedule Rules Settings dialog box (page 439)", set the information.
4. Click **OK** button.

Changing a time schedule rule

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Select a **Schedule Rule** and click **Edit** button.
3. In the "4.22.2.2.1 Schedule Rules Settings dialog box (page 439)", update the information
4. Click **OK** button.

Deleting a time schedule rule

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Select a **Schedule Rule** and click **Delete** button.
3. In the deletion confirmation dialog box, click **OK** button.

4.22.3 Setting a duration schedule

By setting a duration schedule, you are able to perform and stop processes within a planned period.

The following functions are available in the duration schedule.

- "4.22.3.1 Customizing a duration schedule (page 441)"

  Adds, updates or deletes duration schedules. You can also view the settings information.
- "4.22.3.2 Customizing duration schedule rules (page 442)"

  Adds, updates or deletes duration schedule rules.

4.22.3.1 Customizing a duration schedule

Selecting a created duration schedule

This is the same as the procedure for selecting a created time schedule. For details, refer to "4.22.2.1.2 Selecting a created time schedule (page 436)".

Creating a new duration schedule

This is the same as the procedure for creating a new time schedule. For details, refer to "4.22.2.1.3 Creating a new time schedule (page 436)".

Changing a duration schedule

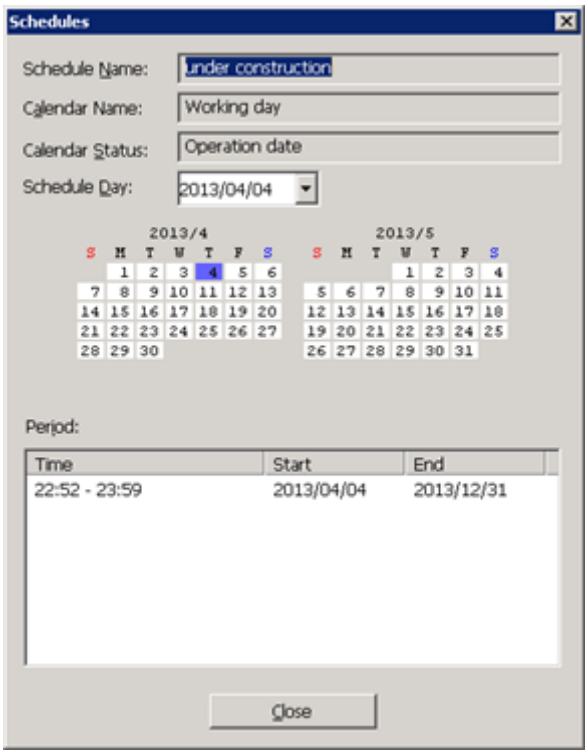
This is the same as the procedure for changing a time schedule. For details, refer to "4.22.2.1.4 Changing a time schedule (page 438)".

Deleting a duration schedule

This is the same as the procedure for deleting a time schedule. For details, refer to "4.22.2.1.5 Deleting a time schedule (page 438)".

Viewing a duration schedule

This is the same as the procedure for viewing a time schedule. For details, refer to "4.22.2.1.6 Viewing a time schedule (page 438)".

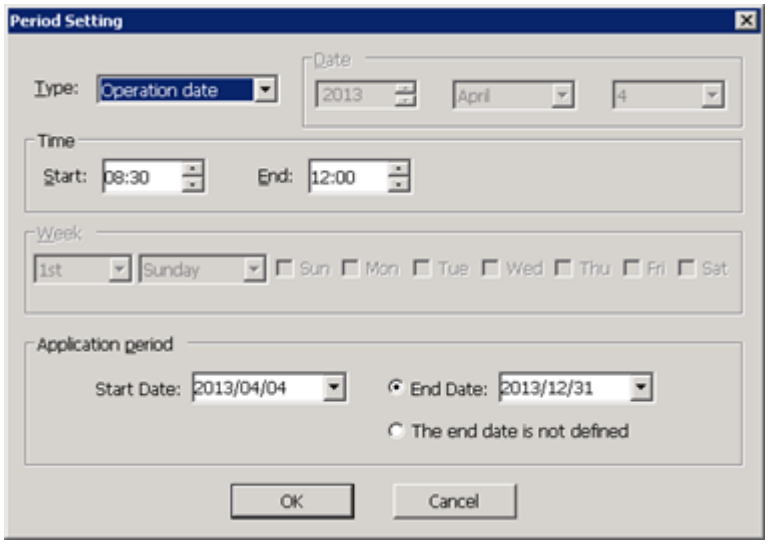


In a duration schedule, the time column is displayed in the [Start Time - End Time] format.

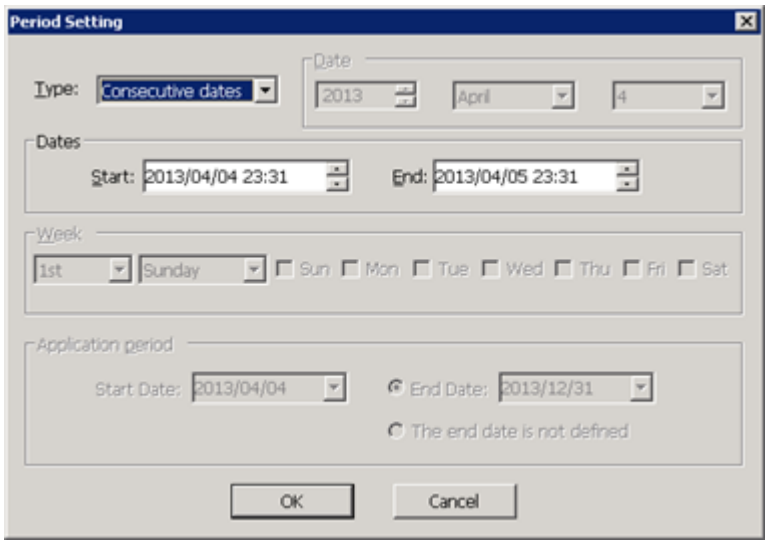
4.22.3.2 Customizing duration schedule rules

Creating a duration schedule rule

1. Open the "4.22.2.1.3.1 Edit Schedule dialog box (page 436)".
2. Click **Add** button.
3. In the Period Setting dialog box, update the information.
   - If the type is anything other than **Consecutive dates**:



   - If the type is **Consecutive dates**:



Explanation of each control is the same as in the "4.22.2.2.1 Schedule Rules Settings dialog box (page 439)".

In the Period Setting dialog box, there is no **Interval** option in the **Dates** group.

Depending on the rule type selected, the following items can be entered.

Input item	Year	Month	Date	The n (th) week	Day	Day check box	Start	End	Period
Operation date	x	x	x	x	x	x	o	o	o
Weekly	x	x	x	x	x	o	o	o	o
Monthly (date)	x	x	o	x	x	x	o	o	o
Monthly (day)	x	x	x	o	o	x	o	o	o
Yearly (date)	x	o	o	x	x	x	o	o	o
Yearly (day)	x	o	x	o	o	x	o	o	o
Specific date	o	o	o	x	x	x	o	o	x
Consecutive dates	x	x	x	x	x	x	o	o	x

4. Click **OK** button.

Changing a duration schedule rule

This is the same as the procedure for changing time schedule rules. For details, refer to "4.22.2.2.3 Changing a time schedule rule (page 440)".

Deleting a duration schedule rule

This is the same as the procedure for deleting time schedule rules. For details, refer to "4.22.2.2.4 Deleting a time schedule rule (page 440)".

4.23 Settings for Managing Audit Logs

Network Manager includes a function that allows you to record a log of operations details and a history of results for operations performed in the monitoring window or manager, or processes performed automatically (audit log).

Audit logs can be reported by Patlite, e-mail, or action notifications when generated.

4.23.1 Defining report settings for audit logs

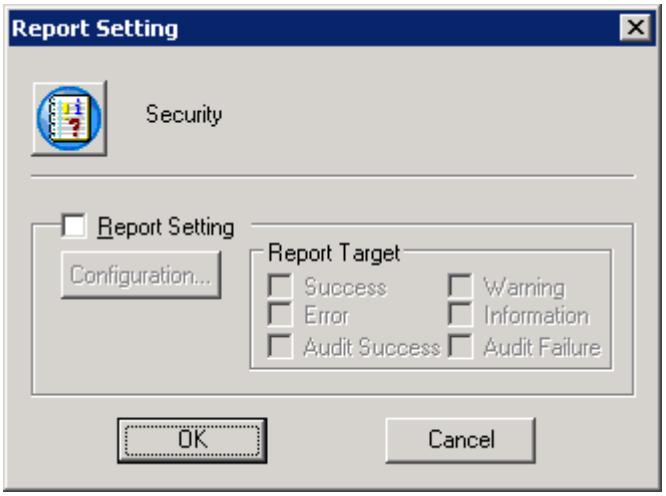
This operation is only available to users belonging to a group with "Audit trail update authority".

You must first change to the "configuration mode (page 27)".

1. Open the Report Setting window.

   To display the Report Setting window, use either of the following two methods.

   - In the tree view, select the audit log category for which you want to set up reports. Right-click and select **Report Setting** menu.
   - In the audit log Map View, select the audit log category for which you want to set up reports. Right-click and select **Report Setting** menu.



2. Check the **Report Setting**.

   If the check box is checked, new audit logs are reported by the Patlite, e-mail, or actioon report. The default setting is no reporting.

3. Click **Configuration** button, to set the reporting details from the Report Setting dialog box.

   For the report setting, refer to "4.14.3 Defining report settings (page 318)".

4. Specify the **Report Target**.

   Only audit logs with the selected severity are reported. The default setting is no check. One or more report targets must be selected.

5. Click **OK** button.

4.23.2 Customizing the audit log display

The position and size of each column in Audit Log window can be changed.

The column settings in the Audit Log window are associated with the ones of the **Audit Log Online View** at the bottom of the main window. By changing the column settings of the **Audit Log Online View**, the ones of the Audit Log window are changed accordingly.

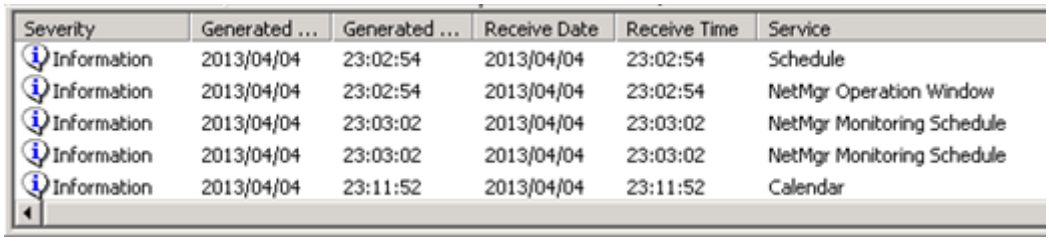
Tip

Changes to the Audit Log window are applied the next time the Audit Log window is displayed.

This operation is only available to users belonging to a group with "Audit trail reference authority".

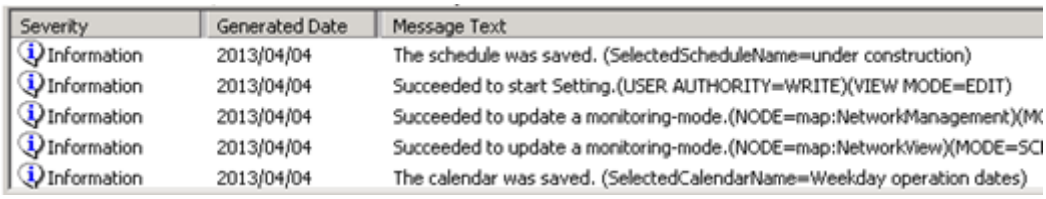
You must first change to the "configuration mode (page 27)".

- To move a column, click-hold it and drag-and-drop it.



Severity	Generated ...	Generated ...	Receive Date	Receive Time	Service
Information	2013/04/04	23:02:54	2013/04/04	23:02:54	Schedule
Information	2013/04/04	23:02:54	2013/04/04	23:02:54	NetMgr Operation Window
Information	2013/04/04	23:03:02	2013/04/04	23:03:02	NetMgr Monitoring Schedule
Information	2013/04/04	23:03:02	2013/04/04	23:03:02	NetMgr Monitoring Schedule
Information	2013/04/04	23:11:52	2013/04/04	23:11:52	Calendar

- To adjust a column width, click-hold the column border and drag it.



Severity	Generated Date	Message Text
Information	2013/04/04	The schedule was saved. (SelectedScheduleName=under construction)
Information	2013/04/04	Succeeded to start Setting.(USER AUTHORITY=WRITE)(VIEW MODE=EDIT)
Information	2013/04/04	Succeeded to update a monitoring-mode.(NODE=map:NetworkManagement)(M
Information	2013/04/04	Succeeded to update a monitoring-mode.(NODE=map:NetworkView)(MODE=SCI
Information	2013/04/04	The calendar was saved. (SelectedCalendarName=Weekday operation dates)

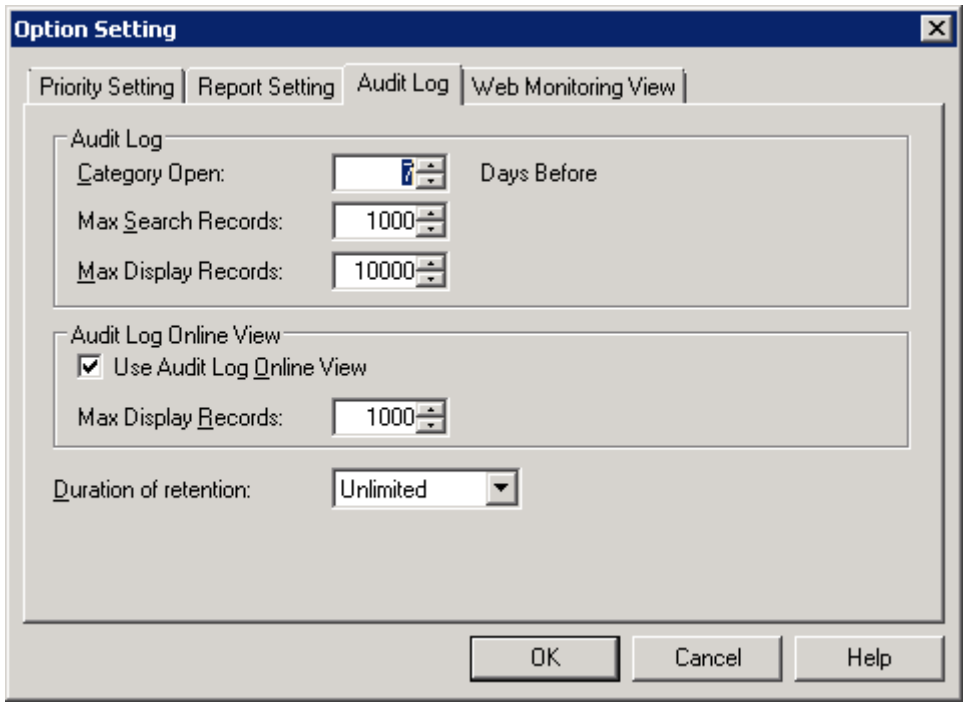
4.23.3 Setting audit log management options

You must first change to the "configuration mode (page 27)".

This operation is only available to users belonging to a group with "Audit trail update authority".

1. Open the Option Setting dialog box.

   In the main menu, select **Setting**>**Option**.



   - **Audit Log**

- **Category Open**

  Specify how many days prior you want to show when opening a category. You can specify any number of days between 0 and 31.

  When opening a category, the category will include records for the specified number of days previous to the current date. The default value is 7 days.

- **Max Search Records**

  Specify the maximum number of records that will be displayed in the Audit Log window when performing a search when a category is open.

  You can specify any number between 1,000 and 20,000. The default value is 1,000 records.

- **Max Display Records**

  Specify the maximum number of records that will be displayed in the Audit Log window.

  You can specify any number between 1,000 and 20,000. The default value is 10,000 records.

• **Audit Log Online View**

- **Use Audit Log Online View**

  Specify whether or not to use the audit log online view.

  To use it, select **Use Audit Log Online View**.

  The default is checked.

- **Max Display Records**

  If **Use Audit Log Online View** is selected, you must select the maximum number of records to display in the audit log online view.

  You can specify any number between 1,000 and 20,000. The default value is 1,000 records.

• **Duration of retention**

  Specify how long the system should keep audit logs.

  Select "Unlimited", "1 Week", "2 Weeks", "1 Month", "2 Months", "3 Months", "6 Months", "9 Months" or "1 Year".

  Audit logs that are older than the specified duration are automatically deleted. The default value is "Unlimited".

2. Click **OK** button.

Chapter 5. Function Reference (Operations)

Contents

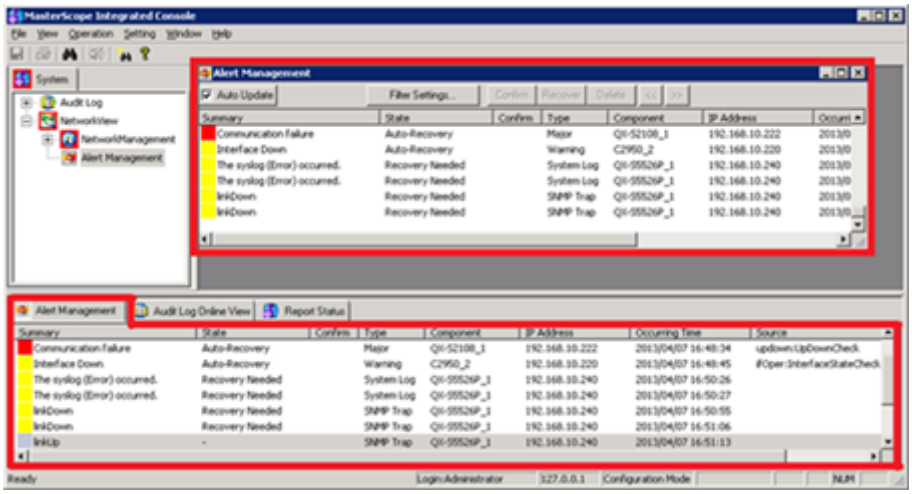
5.1 Checking Alert Information 448
5.2 Checking Results of Device Commands Executed When Alerts Occurred 461
5.3 Checking Syslog Information from External File 462
5.4 Managing Alert Report Status 463
5.5 Executing Monitoring Commands 468
5.6 Launching Device-Specific Management Tools 470
5.7 Displaying Routing Information Map between Two Nodes 471
5.8 Verifying Interface Properties 475
5.9 Displaying Device Front Panels 475
5.10 Executing Device Commands 482
5.11 Checking Collected Performance Data (MIB) 485
5.12 Checking Analysis of Traffic Flow (sFlow) 500
5.13 Starting or Stopping Monitoring by the Monitoring Mode 505
5.14 Managing Device Configuration (Resource Manager) 512
5.15 Managing Device Software (Resource Manager) 531
5.16 Managing Audit Logs 551
5.17 Searching for a Node 556
5.18 Changing Window Appearance 557
5.19 Printing the Map View 557

5.1 Checking Alert Information

Network Manager displays SNMP traps and system logs received from servers, clients, and network devices. It also displays fault and recovery information detected by the state monitoring function as alerts. The icons for devices with failure-type alerts change to the failure color in the Map View window. For details, refer to "2.1.2 Map View (page 17)".

Newly detected alerts are automatically added to the list.

Network Manager provides two types of windows for displaying alerts.



- Alert Management window (Current alert list)

  According to the default setting, the current alert list displays alerts for currently occurring faults in real time. The list can also be set up to display all alerts or to filter display according to specific conditions. To display the Alert Management window, double-clicking **Alert Management** icon in the tree view. For details, refer to "5.1.4 Managing alerts (page 456)".

- **Alert Management** tab (New alert list)

  All alerts detected after the monitoring windows have been launched are displayed in real time under the **Alert Management** tab located in the lower pane. These are displayed in a pane separate from the Network View, allowing the alerts to be displayed and checked, even while users are working on other tasks. For details of the **Alert Management** tab, refer to the "5.1.3 Referencing the new alert list (page 449)".

5.1.1 Auto recovery and manual recovery type alerts

Alerts indicating a fault (failure) are divided into the following two categories according to the type of recovery method used.

- Auto recovery type alerts

  Alerts indicating failures accompanying status changes that Network Manager actively detects using the state monitoring function.

  "Accompanying status changes" refers to situations, typically resulting from device failure or network high-load conditions, where the failure state continues until recovery. Network Manager is capable of automatically detecting recovery with this type of failure.

- Manual recovery alerts

Alerts for failures not accompanying a status change that Network Manager actively detects using the state monitoring function and to alerts based on failure notification (examples: SNMP traps and system logs) received from devices that Network Manager detects passively.

"Not accompanying a status change" refers to detection of such random events as the occurrence of illegal packets for which there is no automatic recovery. As there is no guarantee that devices will always issue failure recovery notices (SNMP trap or syslog, etc.) due to different device specifications and network conditions, Network Manager does not automatically detect failure recovery for these types of failures. Canceling the failure status for this type of failure requires going to the GUI (current alert list) and manually marking the alert status as recovered.

Network Manager can be set to automatically cancel the failure status after a certain time interval. For setting of the Network Manager, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

⚠ Caution

All of auto recovery type alerts are automatically recovered when Network Manager services are restarted or fail-over is occurred in the cluster configuration.

5.1.2 Turning off sound during an alarm

If setting sounds for alert severities, in the alert severity level settings, sound will be played when alerts occur. For details regarding the severity settings, refer to "4.9.2.3 Changing severity level settings (page 239)".

Use one of the following procedures to turn off the sound when an alarm is ringing.

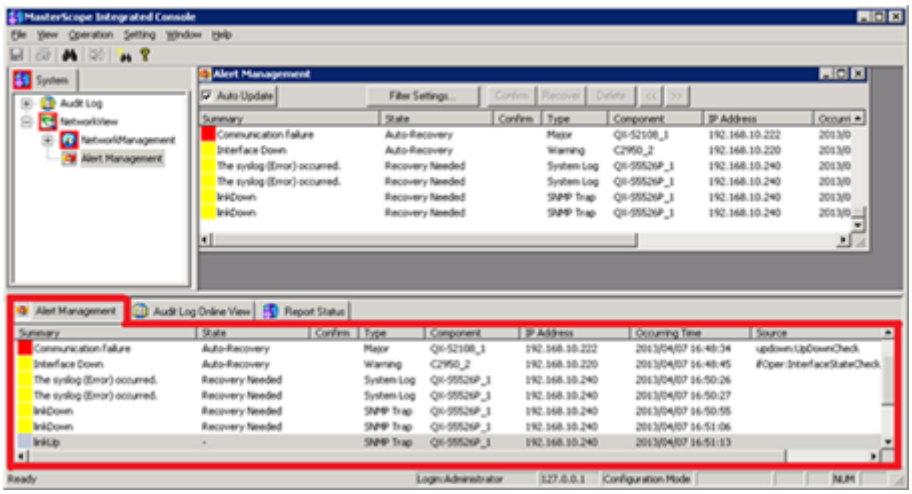
- In the main menu, select **Operation**>**Stop Sound**.
- Click the  icon on the toolbar.

⚠ Caution

In the **Sound** field of the "4.9.2.3.1 Severity Setting dialog box (page 239)", when **WAVE** is selected, an alarm cannot be stopped until one playback of the WAVE file is finished.

5.1.3 Referencing the new alert list

The new alert list is displayed under the **Alert Management** tab located in the lower pane of the monitoring terminal window. The new alert list displays in real time all alerts detected after the state monitoring window has been launched.



Items displayed in the new alert list

- **Summary** column

  Shows an alert summary and color-coded bitmap that indicates level of importance (severity). For details regarding alert colors, refer to "4.9.2 About alert severity and priority (page 237)".

- **State** column

  Shows the recovery status of the alert.

  - Recovery Needed

    Indicates a manual recovery-type alert for which recovery has not yet been performed.

  - Auto Recovery

    Indicates an auto recovery-type alert for which recovery has not yet been performed.

  - Recovered

    Indicates recovery has been performed for the alert.

  - -

    Indicates that further recovery is not required for this alert.

- **Confirm** column

  This mark ✓ is applied to alerts which have been marked in the Alert Management window.

- **Type**

  Indicates the type of alert.

- **Component**

  Lists the component name where the alert occurred.

- **IP Address**

  Displays the device IP address where the alert occurred.

- **Occurring Time**

  Displays the time and date the alert occurred.

- **Source**

  Lists the source of the alert. It is left blank if an SNMP trap has been received.

Alert list right-click menu

- **Alert Detail**

  Detailed information about the selected alert is displayed in the Alert Detail dialog box. For details, refer to "5.1.3.1 Alert Detail dialog box (page 451)".

  To display the Alert Detail dialog box, double-click on the alert line.

- **Jump to Map**

  Clicking this moves the focus to icons contained in Network Management window (Map View). The Node List dialog box is displayed when there are multiple jump destination nodes. For details, refer to "5.1.3.2 Node List dialog box (page 455)".

- **Search trap definition**

  Searches for the trap definition used for the notification of the alert. The search results are displayed in the Matching Definition Search window. For details on the Search Matching Definitions window, refer to "4.11.4.1 Search Matching Definitions window (page 276)".

  You can select this menu item when the **Alert Type** of the selected alert is SNMP Trap.

- **Add trap definition**

  To add a new trap definition for the alert, the Add Trap Definition dialog box is displayed with values set for the "Vendor Identifier", "Specific Trap Code", "Generic Trap Code", and "Node" for the alert.

  For details on the Add Trap Definition dialog box, refer to "4.11.5.1 Add/Edit/Properties of Trap Definition dialog box (page 282)".

  You can select this menu item when the **Alert Type** of the selected alert is **SNMP Trap** and the mode is "configuration mode (page 27)".

Tip

- The **Alert Management** tab displays up to 1,000 alerts. This value can be changed. For details, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".
- For an SNMP trap sent by Network Manager (for which the Enterprise value starts with "21."), you cannot select the **Search trap definition** menu item or **Add trap definition** menu item.
- If the contents of the trap definition displayed by selecting the **Search trap definition** menu item differ greatly from the contents of the actual alert notification, the possible causes include the following.
  - The contents of the trap definition have been changed since the alert notification was issued.
  - The alert contents have been converted with "alert notification control (page 302)".

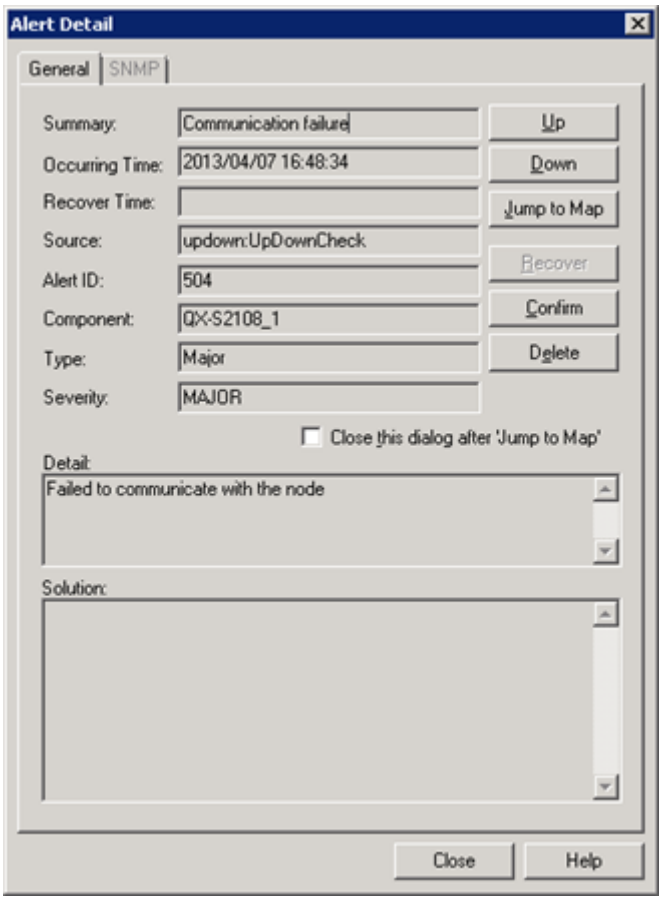
  If you have set alert notification control, and then change the contents of the trap definition, alert notification control cannot be performed appropriately. If you change the contents of the trap definition, therefore, also change the alert notification control settings accordingly.

5.1.3.1 Alert Detail dialog box

Displays detailed information about alerts.

To display the Alert Detail dialog box, double-click on the line containing the desired alert in either the **Alert Management** tab (new alert list) or the Alert Management window (current alert list). Or right-click on the alert line and select **Alert Detail** menu.

For details of the **Alert Management**tab, refer to "5.1.3 Referencing the new alert list (page 449)". For details of the Alert Management window, refer to "5.1.4 Managing alerts (page 456)".



General tab

- **Summary**

  Displays a summary message concerning the alert.

- **Occurring Time**

  Displays the time and date the alert occurred.

- **Recover Time**

  Displays the date and time that the alert was recovered. This box is blank if the alert has not been recovered.

- **Source**

  This field lists the source of the alert.

- **Alert ID**

  This displays the ID (alert ID) used by the system to uniquely identify the alert.

- **Component**

  Lists the component name where the alert occurred.

- **Type**

  Displays the alert type.

- **Severity**

  Indicates the level of severity ("NORMAL", "UNKNOWN", "WARNING", "MINOR", "MAJOR", "FATAL") of the alert.

- **Close this dialog after 'Jump to Map'**

  When selected :

  The Alert Detail dialog box is closed after jumping to the related node.

  When not selected :

  The Alert Detail dialog box is not closed after jumping to the related node.

- **Detail**

  Displays a detailed message concerning the alert. Displays added-value list (VarBindList) information in the case of an SNMP trap.

- **Solution**

  Displays alert response measures.

SNMP tab

- **SNMP Version**

  Displays the SNMP version for the trap.

- **SNMP Community**

  Displays the SNMP community name of the trap. This is not displayed if the SNMP version is "3".

- **Enterprise ID**

  Displays the trap vendor ID using complete numerical string type AMIB. For details, refer to "7.3.4 Standard AMIB Name Specification Format (page 646)".

- **Specific Trap Code**

  Shows the specific trap code used for the trap.

  A hyphen (-) is used in the specific trap code when the standard trap code is between 0 and 5.

- **Generic Trap Code**

  The standard trap code of the trap is displayed using the following format.

cold start	0 (coldStart)
warm start	1 (warmStart)
interface down	2 (linkDown)
interface up	3 (linkUp)
authentication error	4 (authenticationFailure)
EGP neighbor down	5 (egpNeighborLoss)
vendor definition	6 (enterpriseSpecific)

- **Agent Address**

  Displays the IP address set by the agent that sent the trap. The IP address is displayed only when the trap is SNMPv1.

  Normally the IP address of the trap send source is set. However, a different value might be set, depending on the agent for the monitored device.

- **Time Stamp (second)**

  Displays the time stamp of the trap in seconds.

- **Close this dialog box after 'Jump to Map'**

  When selected :

  The Alert Detail dialog box is closed after jumping to the related node. This setting is stored in memory for each of the monitored terminals.

  When not selected :

  The Alert Detail dialog box is not closed after jumping to the related node.

Tip

For the SNMPv2c/v3 traps, identification information is converted into the same **Enterprise ID**, **Generic Trap Code**, and **Specific Trap Code** formats as for SNMPv1, before being displayed. For details, refer to "7.6 SNMP Trap Identification Method (page 664)".

Buttons

- **Close** button

  Closes the dialog box.

- **Up** button

  Displays the contents of the above list (alert).

- **Down** button

  Displays the contents of the below list (alert).

- **Recover** button

  Recovers the current displayed alert.

- **Confirm** button

  Confirms or deletes the confirmation for the current displayed alert.

- **Delete** button

  If the alert to be deleted is a manual recovery-type alert, the failure status will change to "Recovered".

- **Jump to Map** button

  Moves the focus to icons contained in Network Management window (Map View).

- **Help** button

  Displays Help.

- **Add trap definition** button

  To add a new trap definition for the alert, the Add Trap Definition dialog box is displayed with values set for the "Vendor Identifier", "Specific Trap Code", "Generic Trap Code", and "Node" for the alert.

  For details on the Add Trap Definition dialog box, refer to "4.11.5.1 Add/Edit/Properties of Trap Definition dialog box (page 282)".

  You can click this button when the **Alert Type** of the selected alert is **SNMP Trap** and the mode is "configuration mode (page 27)".

- **Search trap definition** button

Searches for the trap definition used for the notification of the alert. The search results are displayed in the Search Matching Definitions window. For details on the Search Matching Definitions window, refer to "4.11.4.1 Search Matching Definitions window (page 276)".

You can click this button when the **Alert Type** of the selected alert is **SNMP Trap**.

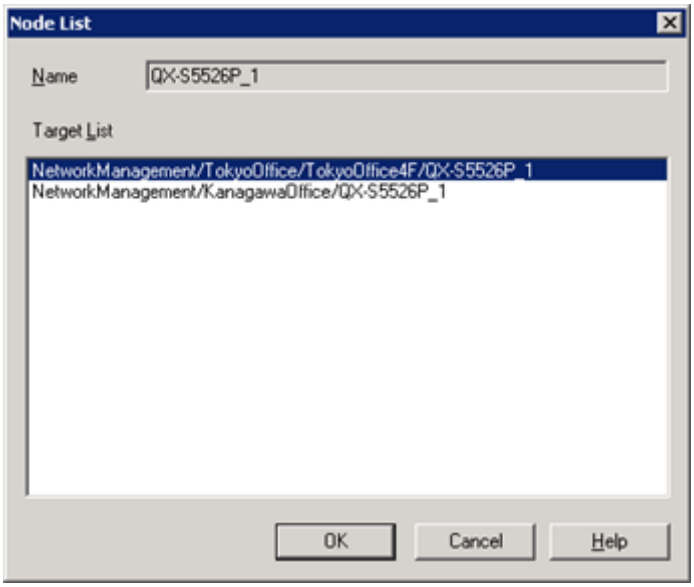
Tip

- For an SNMP trap sent by Network Manager (in which the Enterprise value starts with "21."), you cannot click the **Search trap definition** button or the **Add trap definition** button.
- If the contents of the trap definition displayed by clicking the **Search trap definition** button differ greatly from the contents of the actual alert notification, the possible causes include the following.
  - The contents of the trap definition have been changed since the alert notification was issued.
  - The alert contents have been converted with "alert notification control (page 302)".

  If you have set alert notification control, and then change the contents of the trap definition, alert notification control cannot be performed appropriately. If you change the contents of the trap definition, therefore, also change the alert notification control settings accordingly.

5.1.3.2 Node List dialog box

This dialog box is displayed if there are multiple target nodes when **Jump to Map** button is clicked from an alert's right-click menu or the Alert Detail dialog box.



- **Name**

  Displays the destination node name.

- **Target List**

  Displays a list of nodes matching the destination node name.

- **OK** button

  Displays the node selected from the target list and closes the dialog box.

- **Cancel** button

  Closes the dialog box without jumping to the related node.

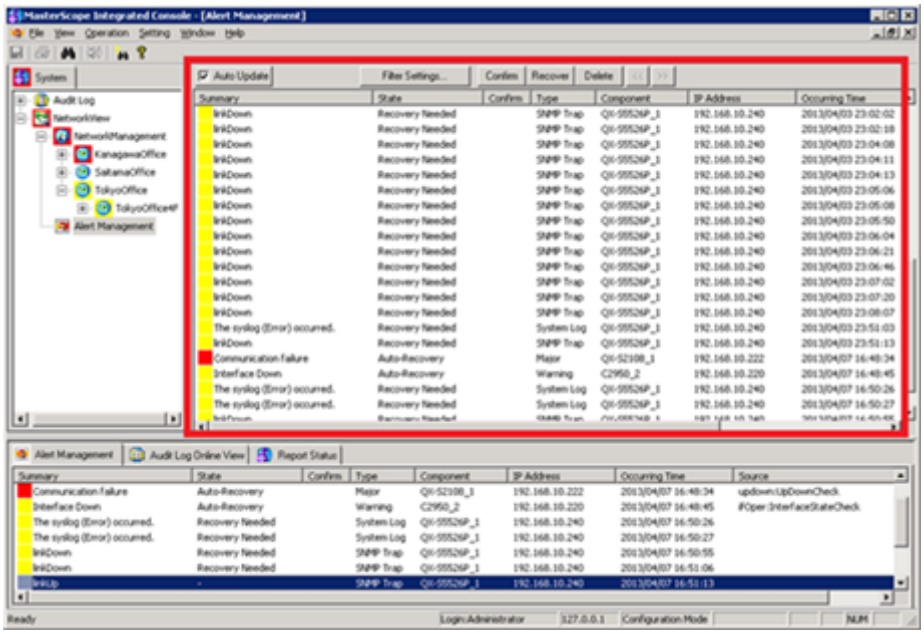
- **Help** button

  Displays Help.

5.1.4 Managing alerts

The alert list (current alert list) is displayed in the Alert Management window. The Alert Management window is the main window used for monitoring and managing alerts in Network Manager.

To open the Alert Management window, in the tree view, double-click the **Alert Management** icon.



By default the Alert Management window filters alerts and displays only unrecovered failure alerts. The Alert Management window is also used to display filtered lists of alerts and perform various alert operations (examples: failure recovery and alert deletion).

Right-click the device icon in the Map View or tree view, and select **Show Unrecovered Alert** menu or **Show All Alert** menu. Then an alert list that was filtered by the **Component** name of the specified device. If you specify a large quantity of icons and display the alerts, it may take a long time to retrieve the results for the filtering conditions and form the current alert list.

Tool bar

- **Auto Update** checkbox

  Specify to automatically add and display new alerts when they occur.

  When ON, new alerts are automatically added to the displayed information.

  When OFF, the automatic addition of new alerts is stopped. Alerts continue to be recorded in the database.

- **Filter Settings** button

  Shows or hides the **Filter Settings** dialog bar. For details, refer to "5.1.4.1 Filter Settings dialog bar (page 459)".

- **Confirm** button

  Adds a ✓ mark in the **Confirm** column for the selected alerts. Users are free to create definitions for the check mark to suit individual operating styles. The ✓ marks are also reflected in the **Alert Management** tab (new alerts list). For details, refer to

"5.1.3 Referencing the new alert list (page 449)". They are also displayed in the Alert Management window (current alert list) and the **Alert Management** tab (new alert list) of all monitoring terminal windows.

- **Recover** button

  Changes the failure status of selected alerts to "Recovered". The system default setting (unrecovered alert display ON) specifies that alerts with status changed to "Recovered" cease to be displayed in the Alert Management window (current alert list).

  Enabled only when a manual recovery-type alert is selected. For a manual recovery-type alert, refer to "5.1.1 Auto recovery and manual recovery type alerts (page 448)".

- **Delete** button

  Deletes the selected alert. If the alert to be deleted is a manual recovery-type alert, the failure status will change to "Recovered".

  Alert deletion is also reflected in the **Alert Management** tab (new alert list). They are also reflected in the Alert Management window (current alert list) and the **Alert Management** tab (new alert list) of all monitoring terminal windows.

- **<<** and **>>** button

  Displays either the previous page or the next page. The Alert Management window displays 1,000 alerts per page.

Items displayed in the alert list

- **Summary** column

  An alert summary and color-coded bitmap that indicates level of severity. For details, refer to "4.9.2 About alert severity and priority (page 237)".

- **State** column

  Shows the recovery status of the alert.

  - Recovery Needed

    Indicates a manual recovery-type alert for which recovery has not yet been performed. Network Manager is not set up to detect its recovery status. The **Recovery** button must be used to attain "Recovery" status for this alert.

  - Auto Recovery

    Indicates an auto recovery-type alert for which recovery has not yet been performed. With this type of alert, the Network Manager state monitoring function automatically issues a recovery alert during recovery, and status is changed to "Recovered".

  - Recovered

    This status indicates recovery has been performed for the alert.

  - -

    Indicates that further recovery is not required for this alert.

- **Confirm** column

  The ✓ mark is attached when the alert is marked using the **Confirm** button,.

- **Type**

  Indicates the type of alert.

- **Component**

  Lists the device name where the alert occurred.

- **IP Address**

  Displays the IP address where the alert occurred.

- **Occurring Time**

  Displays the time and date the alert occurred.

- **Source**

  Lists the source of the alert. It is left blank if an SNMP trap has been received.

Tip

To sort by the content of each column, click the title row of that column in the alert list.

The sort function is only valid if **Auto Update** checkbox is not selected in the toolbar.

If **Auto Update** checkbox is selected while the sort operation is being performed, the sort status is canceled.

Alert list right-click menu

- **Select All**

  Selects all items in the list.

- **Check**

  The equivalent of the **Check** button.

- **Recover**

  The equivalent of the **Recover** button.

- **Delete**

  The equivalent of the **Delete** button.

- **Alert Detail**

  Detailed information about the selected alert is displayed in the Alert Detail dialog box. The Alert Detail dialog box can also be displayed by double-clicking on the alert line. For details, refer to "5.1.3.1 Alert Detail dialog box (page 451)".

- **Jump to Map**

  Moves the focus to icons contained in Network Management window (Map View). The Node List dialog box is displayed when there are multiple jump destination nodes. For details, refer to "5.1.3.2 Node List dialog box (page 455)".

- **Search trap definition**

  Searches for the trap definition used for the notification of the alert. The search results are displayed in the Search Matching Definitions window. For details on the Search Matching Definitions window, refer to "4.11.4.1 Search Matching Definitions window (page 276)".

  You can select this menu item when the **Alert Type** of the selected alert is **SNMP Trap**.

- **Add trap definition**

  To add a new trap definition for the alert, the Add Trap Definition dialog box is displayed with values set for the "Vendor Identifier", "Specific Trap Code", "Generic Trap Code", and "Node" for the alert.

For details on the Add Trap Definition dialog box, refer to "4.11.5.1 Add/Edit/Properties of Trap Definition dialog box (page 282)".

You can select this menu item when the **Alert Type** of the selected alert is **SNMP Trap** and the mode is "configuration mode (page 27)".

Caution

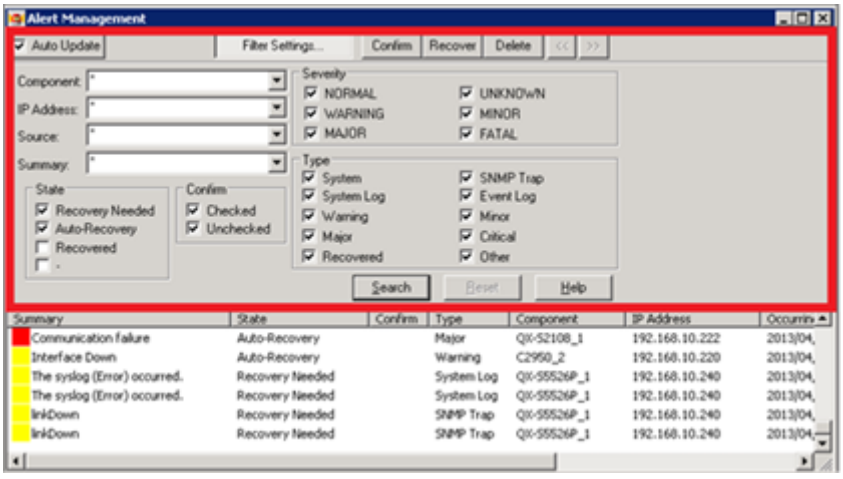
1. The alert filter displayed in the Alert Management window is a display filter. The storage capacity provided for alerts in the database stays the same regardless of alert filtering conditions.
2. Any SNMP traps and system log files newly received from the following devices will be discarded. Alerts will not be accumulated in the database or displayed.
   - Devices not registered with Network Manager
   - Devices with monitoring mode turned OFF
3. The maximum database alert storage capacity is 100,000. This value can be changed. For details, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".
4. To perform an operation such as confirming and recovering alerts while consecutive alerts are being issued, first remove the check from the **Auto Update** checkbox. If Auto Update is set to ON, it may not be possible to select an alert appropriately, so that the operation may be performed upon the occurrence of other than the intended alert.
5. For an SNMP trap sent by Network Manager (for which the Enterprise value starts with "21."), you cannot select the **Search trap definition** menu item or **Add trap definition** menu item.
6. If the contents of the trap definition displayed by selecting the **Search trap definition** menu item differ greatly from the contents of the actual alert notification, the possible causes include the following.
   - The contents of the trap definition have been changed since the alert notification was issued.
   - The alert contents have been converted with "alert notification control (page 302)".

   If you have set alert notification control, and then change the contents of the trap definition, alert notification control cannot be performed appropriately. If you change the contents of the trap definition, therefore, also change the alert notification control settings accordingly.

5.1.4.1 Filter Settings dialog bar

Specify alert filter settings.

To display the **Filter Settings** dialog bar, click the **Filter Settings** button in the Alert Management window. For details of the Alert Management window, refer to "5.1.4 Managing alerts (page 456)".



- **Component**

  This field displays the names of devices targeted for filtering. The asterisk (*) and the question mark (?) can be specified as wildcards. For details, refer to "5.1.4.2 Specifying wildcards (page 460)".

- **IP Address**

  Specifies the IP address targeted for filtering. The asterisk (*) and the question mark (?) can be specified as wildcards. For details, refer to "5.1.4.2 Specifying wildcards (page 460)". These can be specified using up to 45 characters.

- **Source**

  Specify the sources of alerts targeted for filtering. The asterisk (*) and the question mark (?) can be specified as wildcards. For details, refer to "5.1.4.2 Specifying wildcards (page 460)". These can be specified using up to 63 characters.

- **Summary**

  Specifies summary messages targeted for filtering. The asterisk (*) and the question mark (?) can be specified as wildcards. For details, refer to "5.1.4.2 Specifying wildcards (page 460)". These can be specified using up to 128 characters.

- **State**

  Specify filter target states (**Recovery Needed**, **Auto Recovery**, **Recovered**, **-**). The presence of checks in multiple status boxes is interpreted as a logical sum.

- **Confirm**

  Specify the confirmation status (**Checked**, **Unchecked**) for filtering target. When checks are present for more than one confirmation status, it is interpreted as a logical sum.

- **Severity**

  Specify the level of severity (**NORMAL**, **UNKNOWN** ,**WARNING**, **MINOR**, **MAJOR**,**FATAL**) of the filtering target. The presence of checks for multiple levels of severity is simply interpreted as a logical sum.

- **Type**

  Specifies the types of alerts (**System** , **SNMP Trap**, **System Log**, **Event Log**, **Warning**, **Minor**, **Major**, **Critical**, **Recovered**, **Other**) for the filtering target. Checks for multiple alert types that are interpreted as a logical sum.

- **Search** button

  Searches for alerts based on those search conditions.

- **Reset** button

  Returns to the conditions for the last search.

- **Help** button

  Displays Help.

5.1.4.2 Specifying wildcards

This section describes the wildcards used in the Filter Settings dialog bar.

- The asterisk (*) matches any character string of zero or more characters.

The following example matches with all names that start with "nvpc", such as "nvpc32" and "nvpcx".

Example: nvpc*

- The question mark (?) matches with a given single character.

  The following example matches with all five-character names that start with "nvpc", such as "nvpc3" and "nvpcx".

  Example: nvpc?

- Multi-byte characters can be matched.

5.2 Checking Results of Device Commands Executed When Alerts Occurred

When SNMP traps occur, Network Manager can automatically perform a telnet or ssh login to the devices that issued the alerts and execute specified commands. For details, refer to "4.15 Settings for Executing Device Commands When Alerts Occur (page 333)".

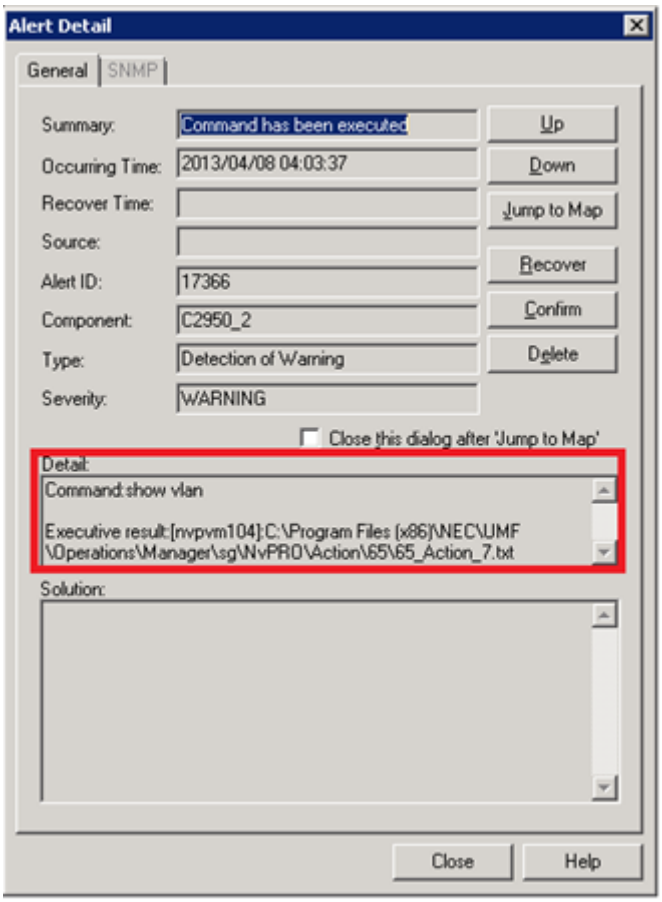
When commands are executed, any strings output on the device side as a result of the command are saved as a file in the Network Manager manager and the information is reported as an alert.

The alert of command execution result is displayed as the following:

- Summary: Command has been executed
- Detail:

  Command:<*command line*>

  Executive result:<*[hostname]: path to execution result file*>



5.3 Checking Syslog Information from External File

Network Manager stores received syslogs to an external file, not just to the alert database. This section describes the storage location and file format for stored syslogs.

Tip

Network Manager only receives syslogs with a severity level of WARNING or higher. As a result, the syslogs stored in the external files are only those syslogs with a level of WARNING or higher.

File path

Received syslogs are stored under the following file paths:

- Current file

  <On the manager, %sharedfolder%>\Manager\sg\NvPRO\syslog\syslog_1.txt

- Backup file

  <On the manager, %sharedfolder%>\Manager\sg\NvPRO\syslog\syslog_*N*.txt

  * *N* is a number from 2 to 10, with 10 representing the oldest information.

File encoding

The following character encoding is used for files storing received syslogs:

Windows:

UTF-16LE

Linux:

UTF-8

File format

The following record format is used for files storing received syslogs:

```
Received time, Component name, All information in the syslog message
```

Received time :

The time is added on the Network Manager side in the format YYYY/MM/DD HH:MM:SS.

Component name:

The name used to identify the device registered in Network Manager.

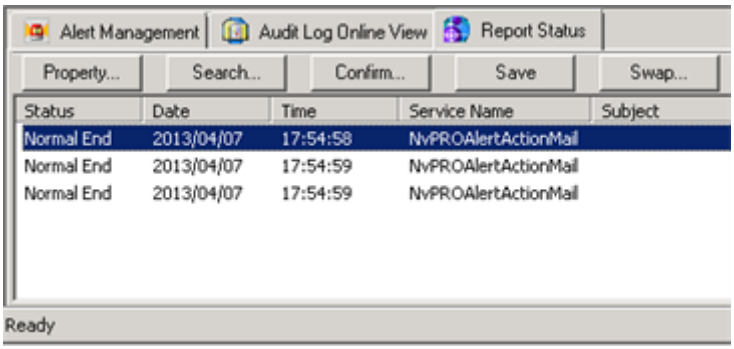
All information in the syslog message:

The PRI, HEADER, and MSG described in RFC3146.

5.4 Managing Alert Report Status

5.4.1 Referencing report status (list)

All report status that occur after the monitoring terminal has been started are displayed in the **Report Status** tab located in the bottom half of the window. The **Report Status** tab includes a toolbar at the top and the list of report status below it.



⚠ Caution

When the monitoring terminal is closed, all report status will be confirmed, removed from display, and not displayed next time the monitoring terminal is opened. The confirmed report conditions can be referenced again by using the search function.

Tool Bar

- **Property** button

To display the properties of the currently selected notification condition using the Report Detail dialog box. For details, refer to "5.4.2 Referencing report conditions (information) (page 465)".

- **Search** button

  To display the Search window used for searching report conditions. For details, refer to "5.4.3 Searching report status (page 467)".

- **Confirm** button

  To remove the currently selected reporting condition from the list. For details, refer to "5.4.4 Confirming report status (and removing from list) (page 467)".

- **Save** button

  To save details of all the notification conditions to the CSV file. In the Save As dialog box, specify the saved location, file name and character encoding, then click **OK** button.

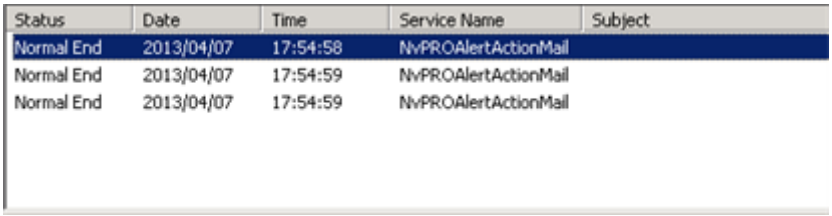
- **Swap** button

  To completely delete report histories according to the date specified. This button is displayed only in "configuration mode (page 27)". For details, refer to "5.4.5 Deleting report histories (page 467)".

- **Initialize** button

  To delete the report history. This button is displayed only in "configuration mode (page 27)". For details, refer to "5.4.5 Deleting report histories (page 467)".

Report list



Details about report are displayed at the bottom of the report status.

- **Status**

  Displays the status of the current report ("Normal End", "Abnormal End", or "Waiting"). In cases where there are multiple notification definitions from Patlite, e-mail and action command, the status with the highest priority is displayed. Status priority levels are described below.

  "Waiting" > "Abnormal End" > "Normal End"

  ### Tip

  In the following cases, the report status is Abnormal End.

  - Patlite report

    When a serial connection type is used, Abnormal End results if it is not possible to communicate with the machine to which Patlite is connected.

    When a LAN connection type is used, Abnormal End results if the execution of the rsh command (for Windows, another command equivalent to rsh) fails. Normal End results even if it is not possible to be connected to Patlite.

  - E-mail report

    Abnormal End results if it is not possible to communicate with the mail server or if the mail server returns an error during communication.

- Action report

  Abnormal End will never result. The command execution results have no influence on the report status.

- **Report Date**

  Displays the date on which the report was issued.

- **Report Time**

  Displays the time at which the report was issued.

- **Service Name**

  Displays the name of the monitoring function that issued the report.

- **Subject**

  Displays a summary of the report.

Caution

The report histories are saved in the manager and kept for the duration specified in the Option Setting dialog box. If the duration of retention is set to "Unlimited", delete report histories regularly to prevent the out of disk space. For details of the optional setting, refer to, "4.14.5 Setting report options (page 331)". For details of the delete report setting, refer to "5.4.5 Deleting report histories (page 467)".

- Report histories are saved to the following path.

  <On the manager, %installfolder%>\Manager\sg\Report\log

- Calculating report history size:

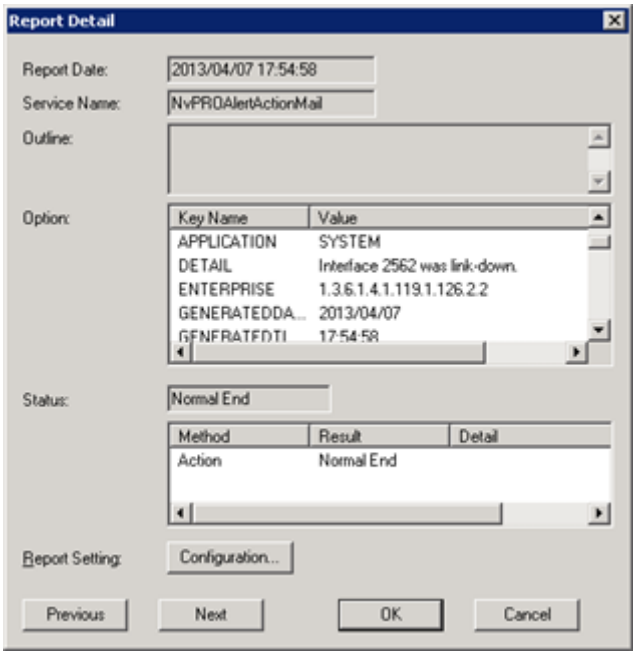
  One report history (Patlite, e-mail, action command) occupies approximately 1,500 to 3,000 bytes (depending on text describing the report cause). This value varies according to system operating conditions.

5.4.2 Referencing report conditions (information)

Display detailed information on the events triggering reports. The following procedures are used to display details.

- Select a report in the **Report Status** tab and click the **Property** button.
- In the **Report Status** tab, double-click a report.

Report Detail dialog box



- **Report Date**

  Displays the time and date the report occurred.

- **Service Name**

  Displays the name of the monitoring function that issued the report.

- **Outline**

  Displays a summary of the report.

- **Option**

  Displays the details of events triggering reports. The contents of "4.14.3.4 List of substitute strings (page 329)" is displayed.

- **Status**

  Displays the status of the current report ("Normal End", "Abnormal End", or "Waiting"). In cases where there are multiple notification definitions from Patlite, e-mail and action command, the status with the highest priority is displayed. Status priority levels are described below.

  "Waiting" > "Abnormal End" > "Normal End"

  - Method

    Displays the defined reporting method.

  - Result

    Displays the execution results for the reports. Results displayed include "Normal End", "Abnormal End", and "Executing".

- **Report Setting**

  - **Configuration** button

    To display theReport Setting dialog box. Future report definitions can be confirmed and redefined as necessary. This item is only available in "configuration mode (page 27)".

- **Previous** button

To display the next report above the currently selected report in the **Report Status** tab list.

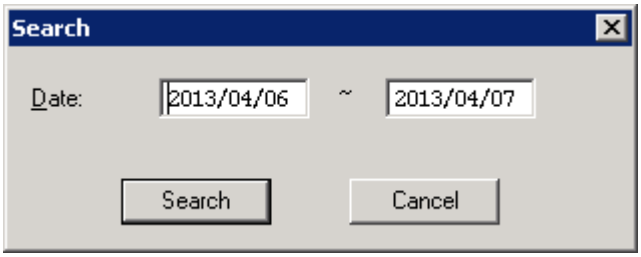
- **Next** button

  To display one report below the one currently selected in the **Report Status** tab list.

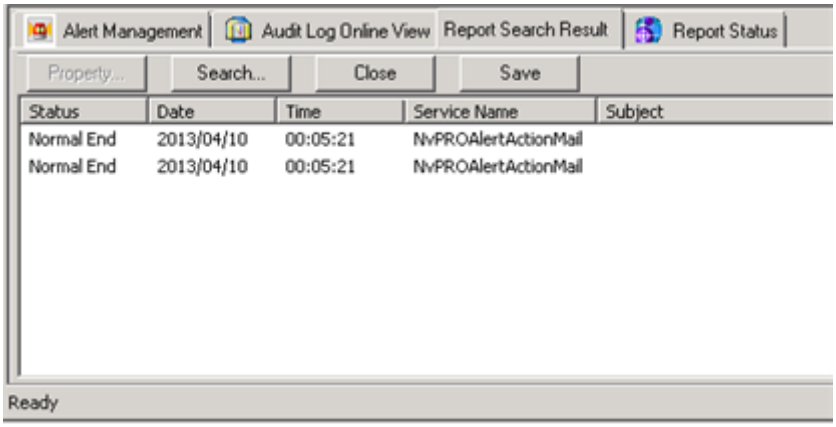
5.4.3 Searching report status

Searching for report status and refining your focus is an easy way to understand report status.

1. In the **Report Status** tab, click **Search** button.
2. Enter the timeframe that you want to search, and click **Search** button.



Search results are displayed as the **Report Search Result** tab in the lower part of the window.



5.4.4 Confirming report status (and removing from list)

In order to organize reports, the reports that have already been confirmed can be hidden.

Confirmation can only performed on unconfirmed reports. The confirmed report status can be referenced by using the search function.

To delete the report status completely, refer to "5.4.5 Deleting report histories (page 467)".

1. Select the report status in the **Report Status** tab.
2. Click **Confirm** button.

5.4.5 Deleting report histories

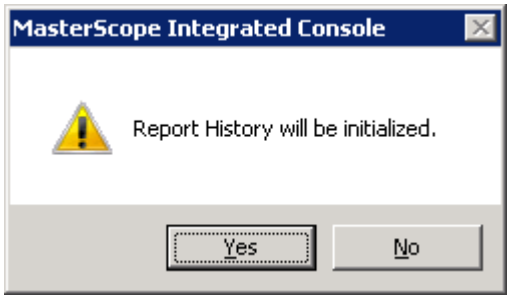
Report histories are deleted in the monitoring terminal, or by entering a command line.

For the method by entering a command line, refer to "9.2 Commands for Alert Report History (ReportCmd) (page 689)".

Note that deleted report histories cannot be restored.

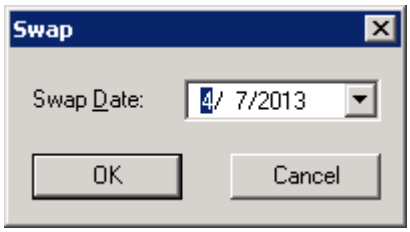
You must first change to the "configuration mode (page 27)".

- Deleting all report histories
  1. In the **Report Status** tab, click **Initialize** button.
  2. When the deletion confirmation dialog box appears, click **Yes** button.



- Deleting report histories according to a specified date

  All report histories up to the specified date are deleted.
  1. In the **Report Status** tab, click **Swap** button.
  2. When the Swap window is displayed, enter the desired date.
  3. Click **OK** button.



5.5 Executing Monitoring Commands

5.5.1 Executing a ping command

This operation is only available to users belonging to a group that has operation authority. The manager machine can use the ping command with registered devices to check TCP/IP connectivity.

This operation is only available to users belonging to a group that has operation authority.

1. Execute in one of the following ways.
   - To execute the IPv4 ping command, right-click on the target device's icon, select **Fault Management**>**Ping (IPv4)**.
   - To execute the IPv6 ping (ping6) command, right-click on the target device's icon, select **Fault Management**>**Ping (IPv6)**.

Results are displayed in the Output Display Window window.

5.5.2 Executing a traceroute command

The manager machine executes the traceroute command for registered devices in order to check route information for target devices.

This operation is only available to users belonging to a group that has operation authority.

⚠ Caution

If intending to use this function, make sure the tracert (traceroute) command is enabled for the root user in the manager machine.

1. Execute in one of the following ways.
   - To execute the IPv4 tracert (traceroute) command, right-click on the target device's icon, select **Fault Management**>**Trace Route(IPv4)**.
   - To execute the IPv6 tracert (traceroute, traceroute6) command, right-click on the target device's icon, select **Fault Management**>**Trace Route (IPv6)**.

Results are displayed in the Output Display Window window.

5.5.3 Logging in to devices from the monitoring terminal

You can login to a registered device via telnet or SSH protocol remotely, and operate it.

In login information settings, you can select the SSH setting to encrypt communication between the manager and the monitoring terminal for security purpose.

This is only enabled when the telnet client is installed in the monitoring terminal and the target device supports a **Telnet** or **SSH** server.

Tip

It is possible to change the telnet client, used for remote login, to a client other than the standard Windows telnet command. Correct operations are not guaranteed when using telnet clients that are not standard in Windows. When changing this setting, check carefully that operations remain correct.

Change the telnet client in the following configuration files:

Use the "IMAGE=" field in the configuration file to define the launch path for the client software that you want to use.

- Configuration file for the normal monitoring terminal

  `<On the monitoring terminal, %installfolder%>\Svc\sg\NvPRO\RMAPI\NvPROrlogin.ini`

- Configuration file for the web monitoring window function

  `<On the manager, %installfolder%>\Manager\Svc\Common\sg\NvPRO\RMAPI\NvPROrlogin.ini`

In the icon property of the target device, you need to enter the **IP Address** in the **Basic** tab and set the **Telnet Server** to ON in the **Function** tab.

This operation is only available to users belonging to a group that has operation authority.

1. Right-click on the target device's icon, select **Fault Management**>**Remote Login**.

   The command prompt window appears.

   "*Device name*(*device IP address*)@Mgr:*Manager name*" is displayed in the title bar of the remote login window.

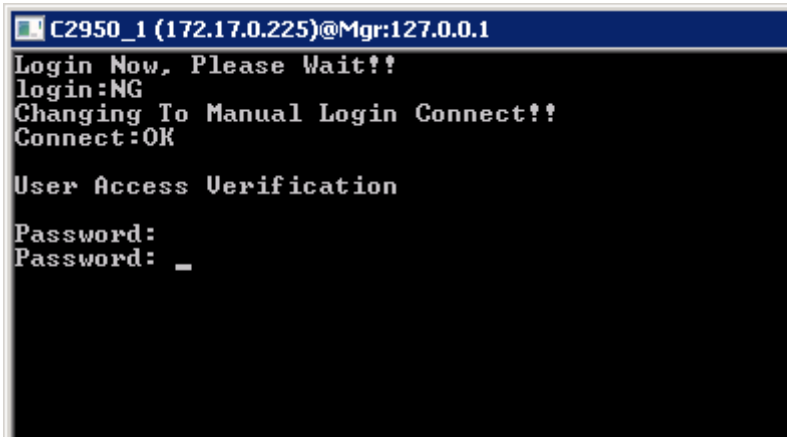
2. If login settings have been made for the target device, the command prompt will be displayed when the login process completes.

   You can start the operation without manual login.

   For the login setting, refer to "4.3 Registering Login Information (page 189)".

3. In all other cases, the window appears when the command prompt displays, so operation must proceed from login.

   Start with the login operation.



Caution

1. If the monitoring terminal is shut down while the remote login window is open, the remote login window will close at the same time.
2. The connection closes if there is no activity for five minutes.
3. Multiple remote login windows can be simultaneously opened for the same device. Depending on individual node specifications, there are restrictions on the number of simultaneous connections and on the number of connections permitted after login completes.

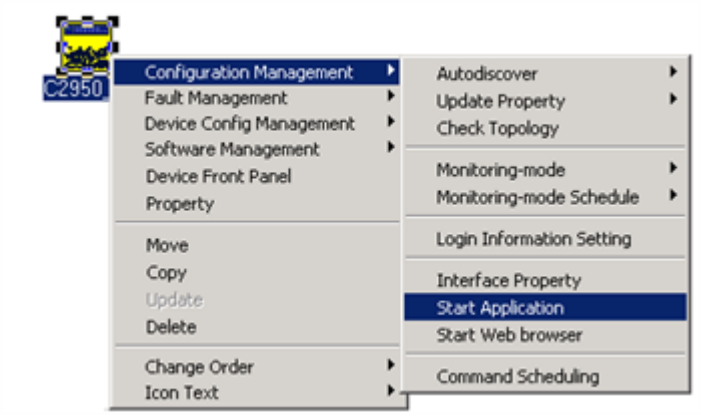
5.6 Launching Device-Specific Management Tools

Launch tools from an icon right-click menu by pre-registering the application path and URL in the icon properties. For instructions about settings, refer to "4.5 Registering Device-Specific Tools (page 204)".

5.6.1 Launching applications from icons

To launch an application, the application must be installed in the location specified in the application path on the monitoring terminal that this command is executed from.

1. Right-click the icon, select **Configuration Management**>**Start Application**.



Caution

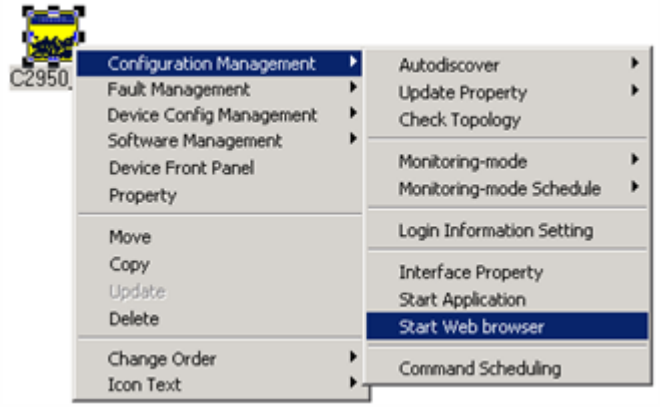
a. Applications launched using this function will not close even if you exit the monitoring terminal.

b. If the user who is operating Network Manager (The logged in user of OS) does not have execution permissions for the specified application, the application will not be executed.

c. Application operations and errors that occur after the application is launched are not supported in this function.

5.6.2 Launching web browsers from icons

1. Right-click the icon, select **Configuration Management**>**Start Web browser**.



5.7 Displaying Routing Information Map between Two Nodes

5.7.1 Displaying a point-to-point map

The PointToPoint Map window provides graphical illustration of the L3 route linking two specified network devices (including PC terminals), according to routing information that was collected on ahead. For details about collecting routing information, refer to "4.7 Registering Routing Information for the Map between Two Nodes (page 231)".

Caution

1. When resources (nodes and ports) are not present on the network, such as when nodes and connection lines are manually set up, it will not be possible to draw accurately.
2. The point-to-point map does not reference source device route information. The L3 route searches will be successful even if there are errors in the route information (example: default gateway settings) of source devices.

Topology information must first be registered to ensure accurate drawing of the physical topology between the L3 devices in the point-to-point map. For registration of topology information, refer to "4.2.3 Registering topology information (page 147)".

Route L3 relay nodes (L3 devices) and their topology information must be registered with Network Manager.

The L3 route information referenced by the point-to-point map consists of route information that has already been collected. It may be difficult to find the correct route L3 when using old route information or when such information has not been collected. For collection of route information, refer to "4.7 Registering Routing Information for the Map between Two Nodes (page 231)".

1. Open the PointToPoint Map window.

   Right-click the **NetworkView** icon or the **NetworkManagement** icon or a device icon, select **Fault Management**>**Show Route of 2 Devices**.

2. Specify the start and end points of L3 route to be searched.

   - **Source IP Address**

     Specifies the IP address (example: 192.168.0.1) of the device which serves as the L3 route search starting point.

     May also be specified as FQDN (example: server1.xxx.com, up to 256 bytes).

   - **Source Node**

     Specifies the name of the device registered with Network Manager which serves as the L3 route search starting point.

     In this case, the route search is performed using the **IP Address** property of the specified device icon.

   - **Dest IP Address**

     Specifies the IP address (example: 192.168.0.1) of the device that serves as the L3 route search ending point.

     May also be specified as FQDN (example: server1.xxx.com, up to 256 bytes).

   - **Dest Node**

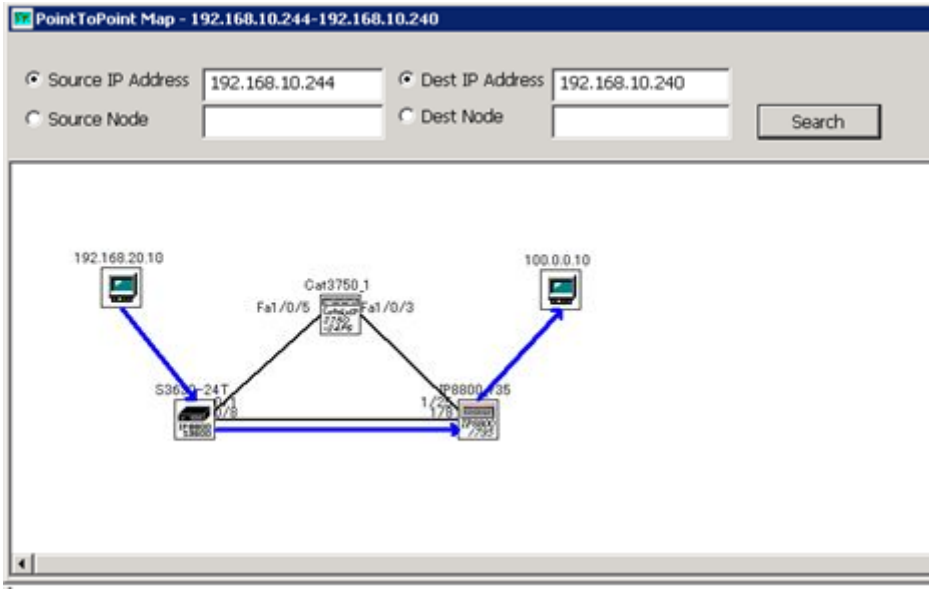
     Specifies the name of the device registered with Network Manager, which serves as the L3 route search ending point.

     In this case, the route search is performed using the **IP Address** property of the specified device icon.

   - **Search** button

     Generates the point-to-point map.

3. Click **Search** button.



The L3 Route is represented by the blue arrow.

All routes are displayed when multiple candidate L3 routes exist. Line sections for which an L3 route cannot be detected are displayed using broken lines.

Map right-click menu:

- **Jump Map**

  Moves the focus to icons contained in network management (Map View). The Node List dialog box is displayed when there are multiple jump destination nodes. For the Node List dialog box, refer to "5.1.3.2 Node List dialog box (page 455)".

⚠ Caution

1. In cases where a node registered with physical topology management during point-to-point map drawing cannot be connected via SNMP transmission, it may take several minutes to draw the map.
2. The topology and the display colors (fault level) that appear on the map represent system states during the drawing process. Network Manager does not support automatic redrawing of the map when status changes occur.

   Click the **Search** button to update the map to the latest status.

For details regarding other display contents of the map, refer to "5.7.2 Description of map display (page 473)".

5.7.2 Description of map display

Design of node icons

The device icons displayed on the point-to-point map are identical in design to icons displayed in Map View.

Icons unique to point-to-point mapping are used for the following nodes.

- 

  Represents a device with unknown properties.

  Refers to a device with unknown physical topology information; a typical example being a non-intelligent hub.

- 

  Represents either a source or destination node on a point-to-point map.

  Icons for nodes registered with Network Manager have the same design as icons used in Map View.

- 

  Represents an L3 device not yet registered with Network Manager.

  Icons for nodes registered with Network Manager have the same design as icons used in Map View.

Device icon display colors

The color coding used for displaying point-to-point map icons indicate device fault levels.

The default color is as follows.

 Red -- > FATAL

 Yellow -- > WARNING, MINOR, MAJOR

 White -- > NORMAL

 Grey -- > Monitoring-mode OFF, UNKNOWN

To change display colors of each alert level, refer to "4.9.2 About alert severity and priority (page 237)".

Connection-line display attributes

The color coding used for displaying point-to-point map connection lines indicates connection line fault levels.

Red -- > FATAL

Yellow -- > WARNING, MINOR, MAJOR

Black -- > NORMAL

To change display colors of each alert level, refer to "4.9.2 About alert severity and priority (page 237)".

The color black, which represents a normal state, cannot be changed.

The thick connection lines represent LAG.

Thick -- > LAG

Thin -- > non-LAG

5.8 Verifying Interface Properties

Verify the following device interface information in the Interface Properties dialog box.

- Interface names corresponding to ifIndex values
- All IPv4/IPv6 addresses assigned to devices and the MAC addresses for each interface
- Default monitored ports if target interface information has been omitted (an asterisk (*) has been specified) in the Status Monitoring and Data Collection functions

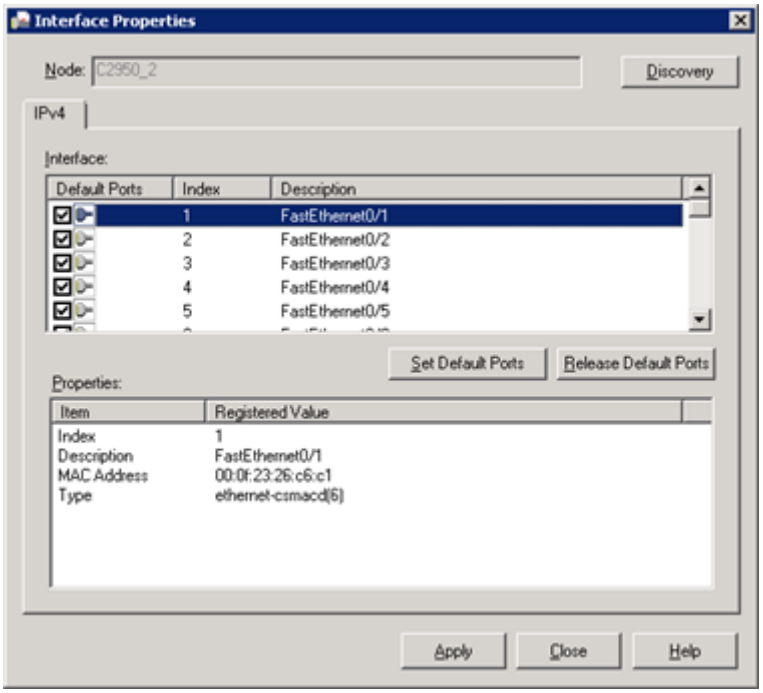
⚠ Caution

The Interface Properties dialog box can only display for devices that support SNMP.

To open the Interface Properties dialog box, first register the interface information or change the settings so that SNMP communication is established with the target device. For information about interface registration, refer to "4.2.8 Registering interface information (page 180)".

1. Open the "4.2.8.1.1 Interface Properties dialog box (page 181)".

   Right-click the device icon and select **Configuration Management**>**Interface Property**.



2. In the "4.2.8.1.1 Interface Properties dialog box (page 181)", select the interface that you want to confirm.

   The detailed information is displayed in the **Properties** pane.

5.9 Displaying Device Front Panels

Displaying a window (panel window) patterned after a front panel makes it possible to provide the functions described below.

- Displaying an image of a device front panel and each port status.
- Changing the device attributes by SNMP Set, and set network interfaces to up or down from the image of the device front panel.

- Displaying of current configuration and statistical information for the device.

5.9.1 Opening a device front panel

You must assign an NM license to the node in order to be able to display the front panel.

The **Device Front Panel** menu does not activate for nodes not allocated a license and nodes without a set IPv4 address or IPv6 address.

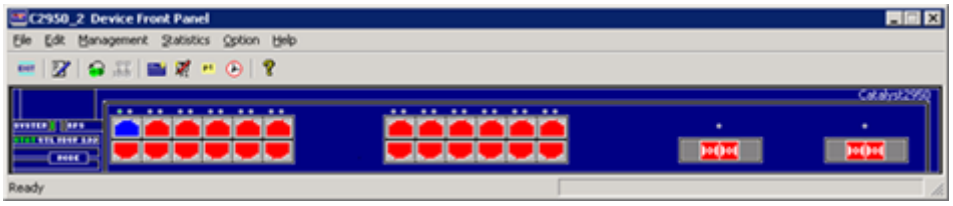
The "configuration mode (page 27)" is not necessary for opening a device front panel, but is necessary for configuration on a device front panel.

This operation is only available to users belonging to a group that has operation authority.

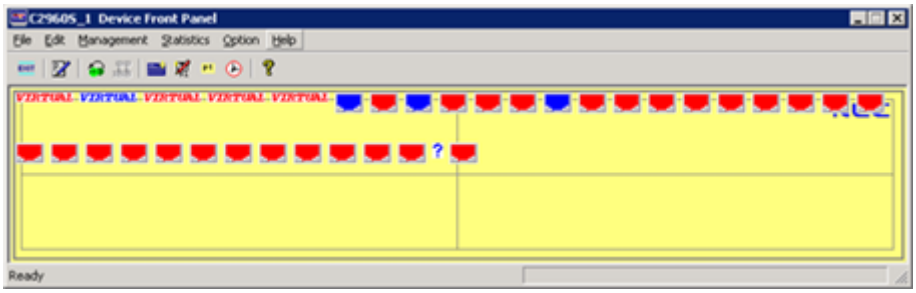
1. Right-click on the device node and select **Device Front Panel** menu.

The front panel that is displayed will either be a device front panel designed for supported models or a general-purpose device front panel.

Example of a supported device front panel:



Example of a general-purpose device front panel:



The display content varies widely according to model and main body configuration.

⚠ Caution

1. If unable to connect to a target node, an error dialog box appears and the device front panel is not displayed.
2. If the connection to a target node fails, a warning dialog box appears and the inside of the panel window becomes black. Normal display returns when the connection is reestablished.

3. In cases where the device front panel type specified is not the type for the actual model, a warning dialog box may be displayed and the device front panel may not be displayed. An example would be when a "Catalyst2950G-48" device front panel is specified for use with a "Catalyst3550-24" node.

5.9.2 Device front panel menu

- **File**
  - **Device Front Panel>Save As**

    Saves the current device front panel image as new panel window type. For details, refer to "4.18.3 Using a customized device front panel for multiple icons (page 389)" and "4.18.4 Using a customized device front panel in other monitoring terminals (page 390)".
  - **Change Device**

    In instances where multiple nodes are stacked together, the Change Device dialog box can be used to select a different node in the stack and display its panel image.

    For the list of models supported in displaying the device front panel in a stack configuration, refer to "4.18 Settings for Displaying Device Front Panel (page 378)".
  - **Restructure**

    Returns the panel window to its status when first set up.

    Any changes to port position and port type information will be reset. This menu might not be able to be selected according to the device model. For details, refer to "4.18.2.1 Setting module ports (page 380)".
  -  **Exit Application**

    Closes the device front panel.
- **Edit**
  -  **Save Position**

    Saves modified port position and port type information.

    Failure to save changes made to port position or port type in the panel window will result in the previous settings appearing the next time it is opened.
  -  **Defaults**

    Returns the device front panel port icon positions to their layout at the time that the window was first opened. Changes to port name and port type will remain.
  -  **Vertical Arrange**

    Port vertical alignment involves moving other icons (not including labels) currently positioned between selected port icons on the upper and lower lines to the line above the selected icons.
  -  **Port Customize**

    Customize port displays on the device front panel. For details, refer to "4.18.2.3 Editing port displays (page 382)".
  - **Customizer**

    Allows the addition of various management and statistics windows to the general-purpose device front panel. For details, refer to "4.18.2.5 Editing management and statistics menus (page 385)".
  - **Module Port Settings**

Users can employ the Module Port Settings dialog box to configure and determine which expansion modules should go into which node slots, thereby enabling module port positions to be configured correctly. For details, refer to "4.18.2.1 Setting module ports (page 380)".

- **Change Bitmap**

  Changes the background design (corresponding to image of front of node) of the device front panel.

  Having a background bitmap (BMP format) makes it possible to create an easy-to-understand front panel visual image with general-purpose panel windows. For details, refer to "4.18.2.2 Editing a background of the panel window (page 382)".

- **Management**

  Allows configuration information for the various nodes to be viewed easily. Menus displayed vary according to the node.

- **Statistics**

  Allows statistical information for the various nodes to be viewed easily. Information can be displayed in the snapshot, line graph, bar graph, and list formats. Menus displayed vary according to the node.

- **Option**

  - **Redraw**

    Displays the current node status.

    Setting the polling intervals too long means that actual interface and LED states (colors) will differ from those displayed on the device front panel for comparatively long periods. Selecting the **Display Most Recent** menu updates the device front panel to the current state.

  - **Display Port Name**

    Displays port names in the device front panel.

  - **Polling Interval**

    Sets the intervals at which the node ports and LED states are checked.

    The default value is 60 (sec). The interval can be set in the 0 to 1,000,000 (sec) range. Polling is not performed when interval is set to "0".

- **Help**

  - **Help Topics**

    Displays Help information related to the device front panel.

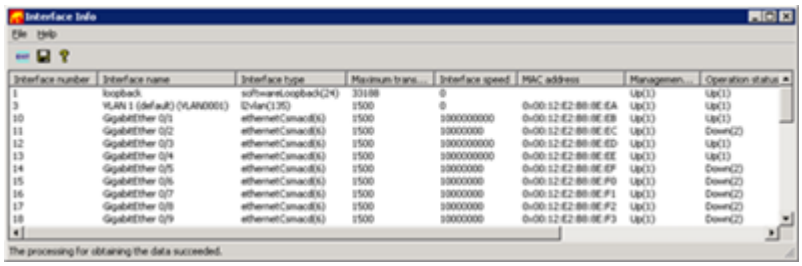
5.9.3 Displaying configuration information

Displays configuration information according to a device model using management menus. The information displayed varies according to the menu selected.

Caution

Configuration information cannot be displayed if unable to communicate with node.

- Table Information Display window



- **File**
  - * **Save As**

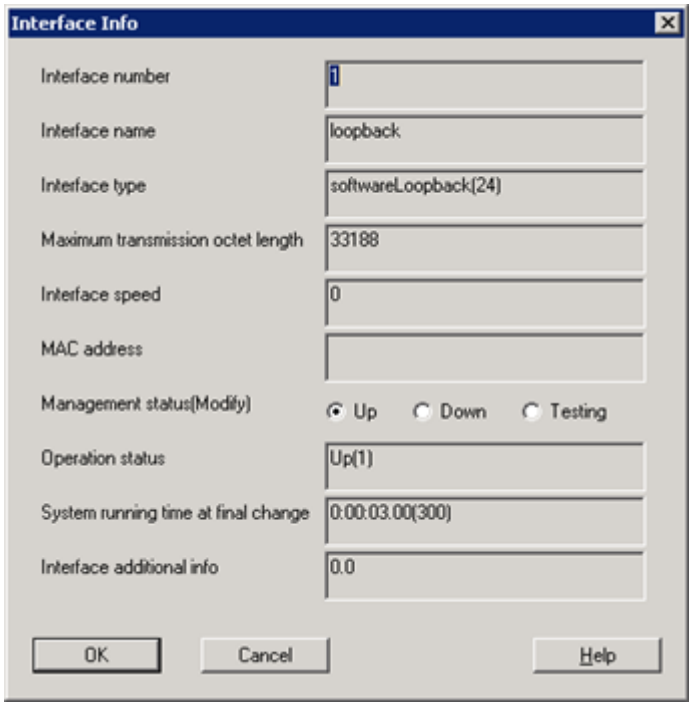
    Saves displayed information to file (CSV format), using OS multi-byte character encoding.

  - * **Exit Application**

    Closes the current window.
- **Help**
  - * **Help Topics**

    Displays Help.

- Information dialog

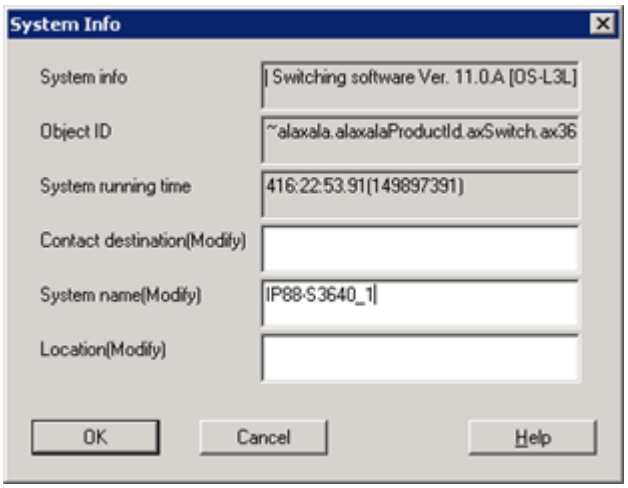


5.9.4 Changing configuration information

Device type-specific configuration information is in the menus under the management menu. It is possible to change some of the registered information on the device side.

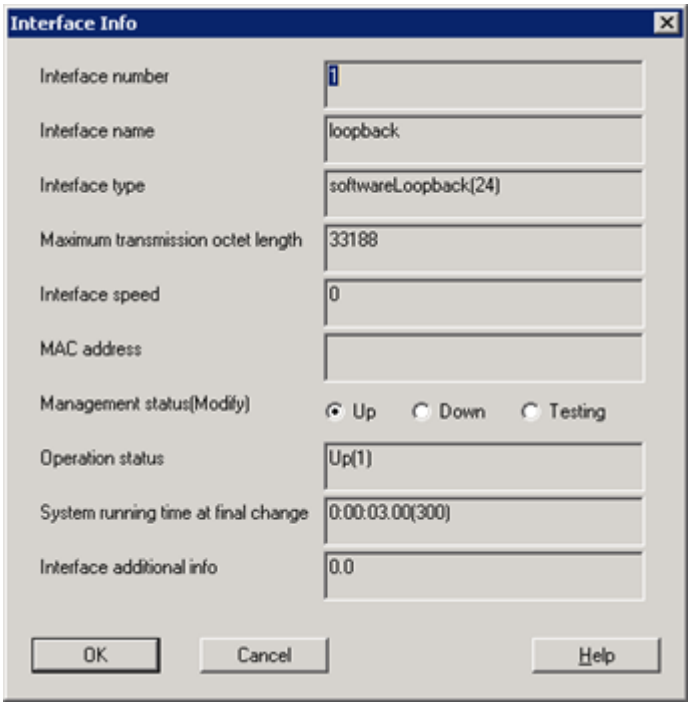
Example:

1. In the panel window menu, select the **Management**>**System Info** to open the System Info dialog box. In this dialog box, it is possible to change the following items.



- Contact destination (.iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysContact(4))
- System name (.iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysName(5))
- Location (.iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysLocation(6))

2. In the panel window menu, select the **Management**>**Interface Info** to open the Interface Info dialog box. In this dialog box, it is possible to open or close the network interfaces.



To close (shut down) a network interface, from the **Management status (Modify)** option button, select **Down** and click the **OK** button.

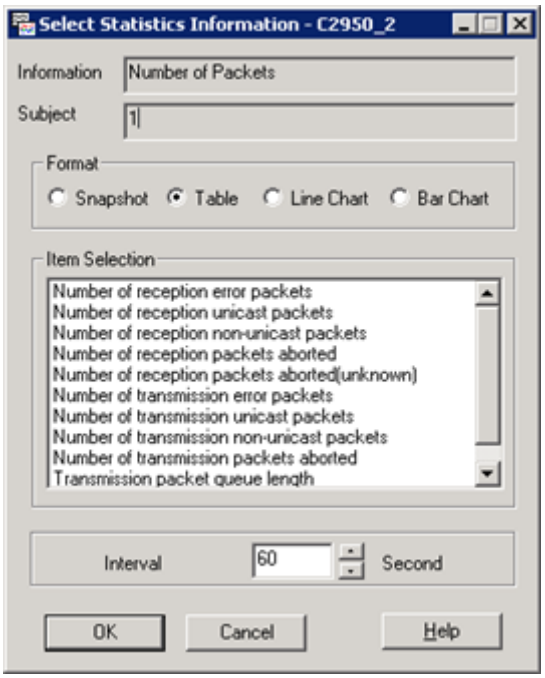
Caution

1. It may not be possible to display menus or information or change settings, depending on the specifications on the device side.
2. SNMP Set is used to change settings. Configure settings on the device side to accept SNMP Set. Also, register an community name appropriate in the **SNMP Community Name (set)** property for the target node in advance. For more information regarding property information registration, refer to "4.2.9.1 Changing icon properties manually (page 184)".

5.9.5 Displaying statistical information

Various types of statistical information are obtained directly from nodes and displayed in multiple formats (snapshot, tables, line graphs, and bar graphs). The information available for display varies depending on individual node models.

After choosing from the menu, use the displayed dialog box to narrow down the items targeted for display. The Select Statistics Information dialog box for selecting statistics information enables selection of multiple items. Click the **OK** button to display information based on the applied conditions.



- **Information**

  Displays the menu name for statistical information to be acquired.

- **Subject**

  Displays the value specified in the Select Statistics Information dialog box. This item is not displayed if there when there is no selected target.

- **Format**

  Collects statistical data at intervals specified by the **Interval** setting and displays information on statistical volume (difference with previous interval) between intervals in the selected format.

  Tip

  The statistical information from managed devices is saved in a historically cumulative format in the managed devices. It is recommended the information normally be displayed in the form a table, a line graph, or a bar graph.

- **Item Selection**

  Select the item that you want to display. The SHIFT or CTRL key can be used to select multiple items.

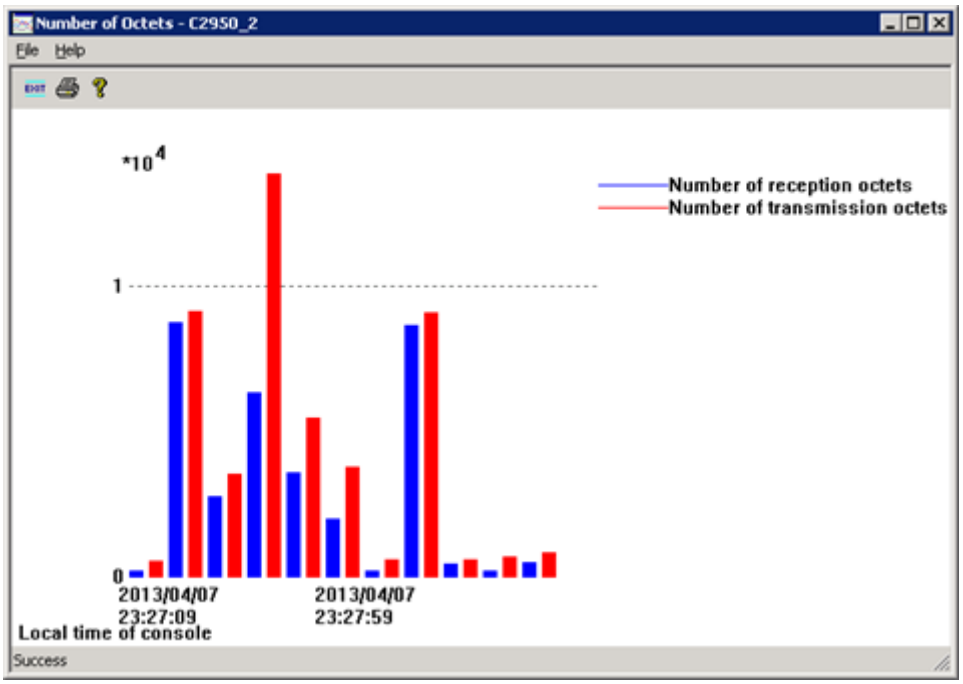
- **Interval**

If anything other than **Snapshot** is selected in the **Format**, set the intervals for acquiring information in units of seconds. Intervals should be a minimum of 10 seconds (up to 1,000,000 seconds).

Caution

1. Statistical information cannot be displayed if unable to communicate with a node.
2. As data is constantly retained in memory during data collection, long collection operations can place a burden on memory resources. It is recommended that data collection functions be used when collecting data for long periods at a time.
3. In some device models, statistical information cannot be acquired.

When selecting **Line Chart** or **Bar Chart**, the information displays at a specified interval in the graph view window.



5.10 Executing Device Commands

Connect to a device using telnet or ssh and perform a scheduled execution of pre-registered command definitions. Also execute registered command definitions immediately using window operations.

For information on registering command definitions and other priming tasks, refer to "4.19 Setting for Running Device Commands (page 391)".

In addition to execute pre-registered device commands, it is also possible to execute the device commands defined in the external text file on the manager.

Caution

The login settings must be performed in advance for a monitored device on which a device command will be executed. For details regarding login settings, refer to "4.3 Registering Login Information (page 189)".

5.10.1 Executing a registered device command

To execute a command registered in the **Command Creation** menu immediately, right-click the device in the Schedule Condition Setting pane, and select the **Execute At Once** menu.

A command to be executed should be prepared in advance. For details, refer to "4.19.1 Defining commands (page 391)".

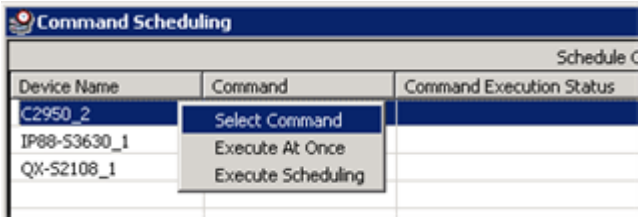
This operation is only available to users belonging to a group that has operation authority.

1. Open the Command Scheduling window.

   Right-click the **NetworkView** icon or the **NetworkManagement** icon or a map icon or device icon and select **Configuration Management**>**Command Scheduling**.

2. The selected command is sent to the device and executed.

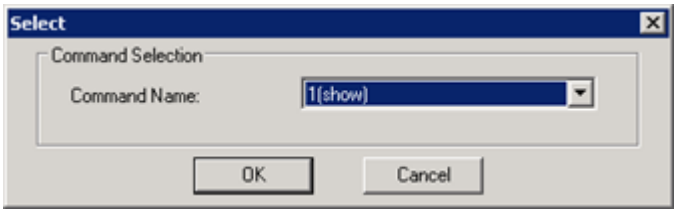
   In the Schedule Condition Setting pane, right-click the device of which command is executed, select the **Select Command** menu.



Tip

You can select multiple devices and execute all the commands at once.

3. In the Select dialog box, select a command created in the **Command Creation** menu.



4. In the Schedule Condition Setting pane, right-click the device on which the command is executed, and select the **Execute At Once** menu.

   The selected command is sent to the device, and status of the command execution is displayed in the **Command Execution Status**.

5. You can see if the command execution is complete by checking under Command Scheduling List pane.

   If the execution is complete, right-click the relevant command ID row in the Command Scheduling List pane, and select **Display Result** menu to get the output message output on the device side. For details, refer to "5.10.3 Checking command execution results (page 484)".

Caution

The command scheduling list displayed in the Command Scheduling List pane is not deleted after the command is run and continues to be displayed. To delete a completed command from the list, select the command row, right-click, and select **Delete Schedule** menu. If a command schedule has been deleted using the **Delete Schedule** command, the results file is also deleted. Where necessary, perform the deletion after backing up.

5.10.2 Executing a command immediately on the manager

On the manager, you can execute commands defined in an external file immediately. Differently from the execution of commands by operating the display, an advance registration of command definition is not required.

For details of command on the manager, refer to "9.14 Command for Executing Device Commands (nvpdevcmdexe) (page 741)".

1. Create a command file describing the device command row to be executed.

   A command file can be described in the same format as the command rows described in "4.19.1 Defining commands (page 391)"

   In addition to the device command, the simple script can be used in the command file.

2. Execute a `nvpdevcmdexe` command.

```
> nvpdevcmdexe -node switch01
     -cmdfile command-file.txt -log command.log
```

3. Open the log file of the command execution result generated after the execution, confirm that the expected command was executed.

   In the above example, open a command.log file to confirm it.

5.10.3 Checking command execution results

5.10.3.1 Viewing command execution results

You can confirm the messages output from the devices when commands were executed in "5.10.1 Executing a registered device command (page 482)" or "4.19.2 Scheduling command execution (page 398)".

⚠ Caution

- The maximum size of the supported command result file is 2MB.
- The command execution results are managed immediately in execution units on the **Execute At Once** menu for each command schedule. Up to 500 execution results are retained for each. If the number of execution results exceeds 500, they will be automatically deleted, starting from the oldest.

1. Open the Command Scheduling window.

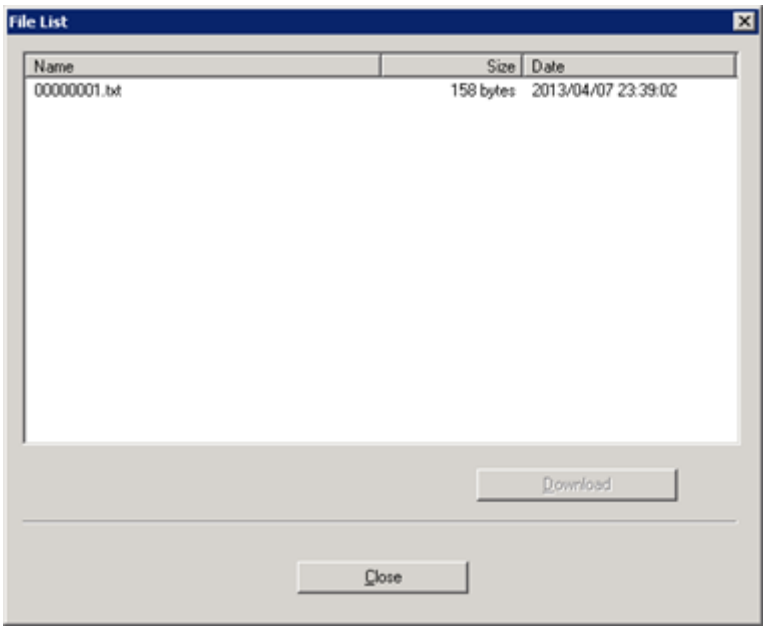
   Right-click the **NetworkView** icon, the **Network Management** icon, the map icon, or device icon. Select **Configuration Management**>**Command Scheduling**.

2. Select a target device in the **Command Execution Status** column in the Schedule Condition Setting pane, and confirm that the command has already been executed.

3. When the command is finished running, right-click the relevant command ID row in the Command Scheduling List pane, and select the **Display Result** menu.

   The File List window displays that allows for download execution results files residing on Manager.

4. Select the file to download, and then click **Download** button.



A window for selecting the download destination displays.

5. Specify the file name and click **Save** button.

   The command execution result is saved in the monitoring terminal.

   The downloaded file contains the message output from the device when the command was executed.

5.10.3.2 Exporting the list of command execution results

To manage the command execution history and other information in the results files, export the information to an external CSV file.

The created CSV file is comprised of the following columns.

- Command ID
- Execution time
- Execution results
- Command name
- Execution results file path

Use the information in this CSV file to maintain and manage the results files stored on Manager.

⚠ Caution

The maximum size of the supported list file is 2MB.

1. Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Configuration Management**>**Command Execution Result**.
2. In the Save As dialog box, specify the output file name and click **Save** button.

   The list of command execution result is saved in the monitoring terminal.

5.11 Checking Collected Performance Data (MIB)

based on the collected data in the data collection function, you can display a status at the day in a graph, and create and display a daily, weekly, monthly, or annual report. By setting a threshold, the value is checked every time data is obtained. If the value exceeds the threshold, an alert indicating the threshold excess will be issued.

5.11.1 Displaying a graph

Data gathered by the data collection function can be displayed in a graph. A graph can be displayed for each data collection entry.

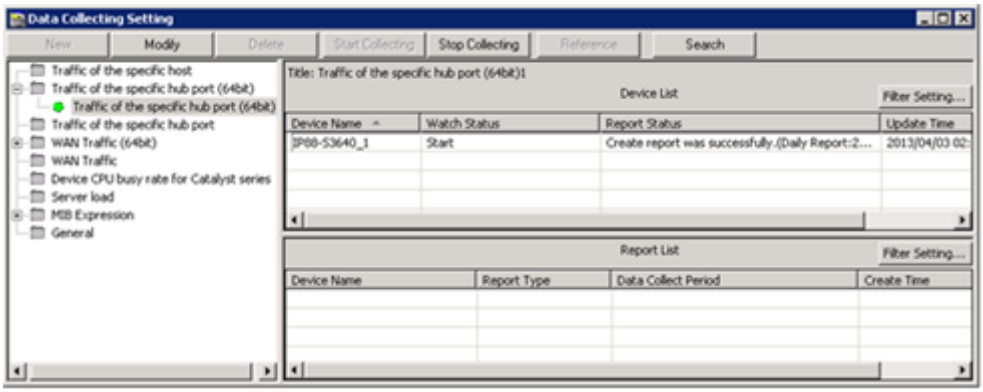
However, the data of multiple days (for example, from 2012/7/30 to 2012/7/31) cannot be displayed in the same graph.

Data collecting setting should be configured in advance. For details, refer to "4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices (page 334)".

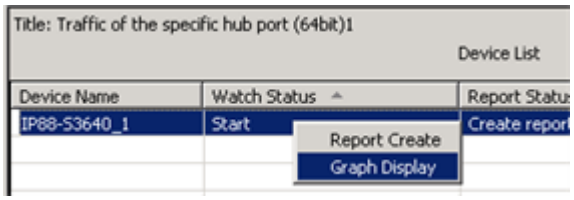
1. Open the "4.16.1 Data Collecting Setting window (page 334)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.

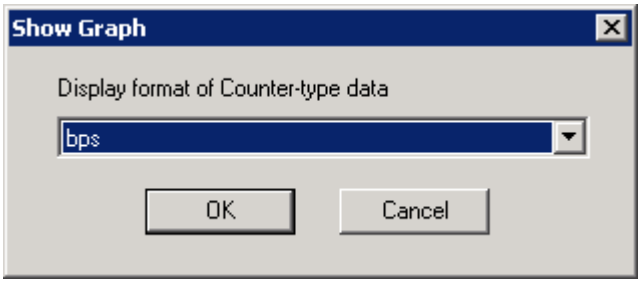
2. In the data collection entry tree, select the entry that you want to display.



3. Right-click the target device in the Device List pane and select **Graph Display** menu.



4. When the Show Graph dialog box is displayed, select a display format.



Select the counter-type data display format for displaying the graph.

- Select from bps, Kbps, Mbps

- When using the following rules.
  - * Traffic of the specific host
  - * Traffic of the specific hub port (64bit)
  - * Traffic of the specific hub port
  - * WAN Traffic (64bit)
  - * WAN Traffic
- When using the "General" rule with "bps" unit.
- When using the "MIB Expression" with a MIB expression whose units of CSV output data are all "bps".

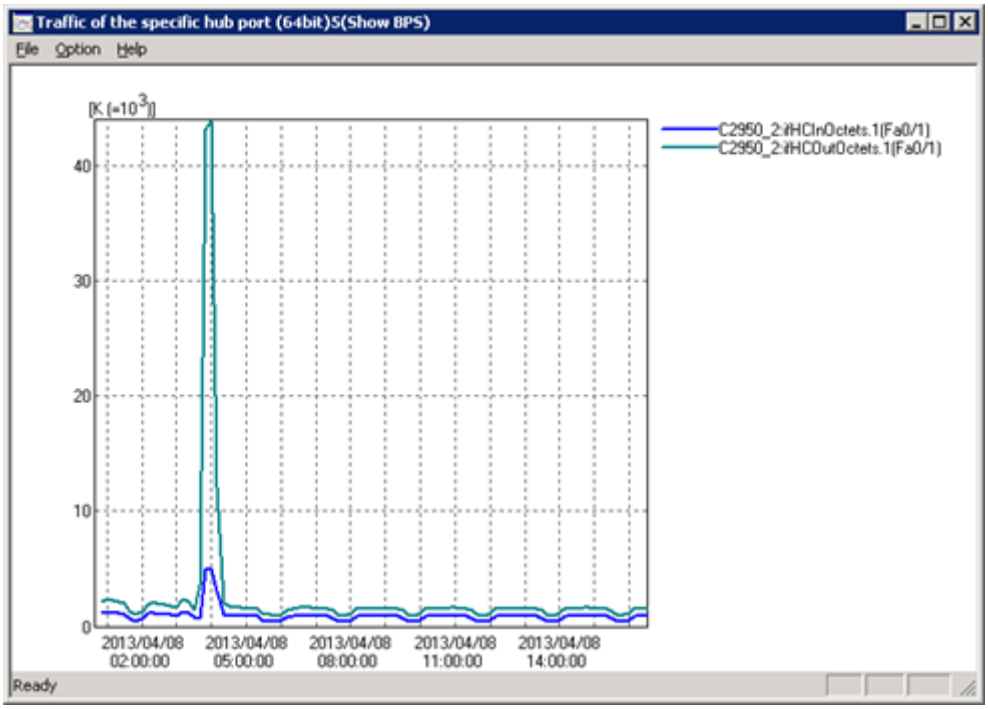
• Select from pps, Kpps, Mpps

- When using the "General" rule with "pps" unit.
- When using the "MIB Expression" with a MIB expression whose units of CSV output data are all "pps".

Caution

This dialog box is not displayed if the collected data is not the counter-type data, such as "Server load" or "Device CPU busy rate for Catalyst series".

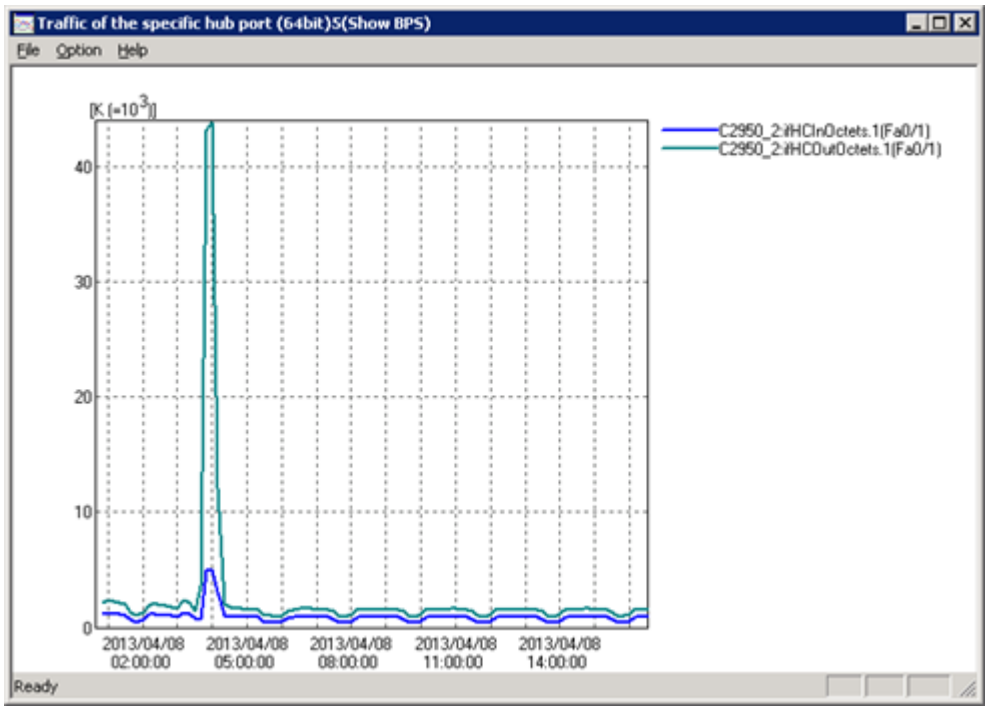
5. A graph is displayed in a graph view window.



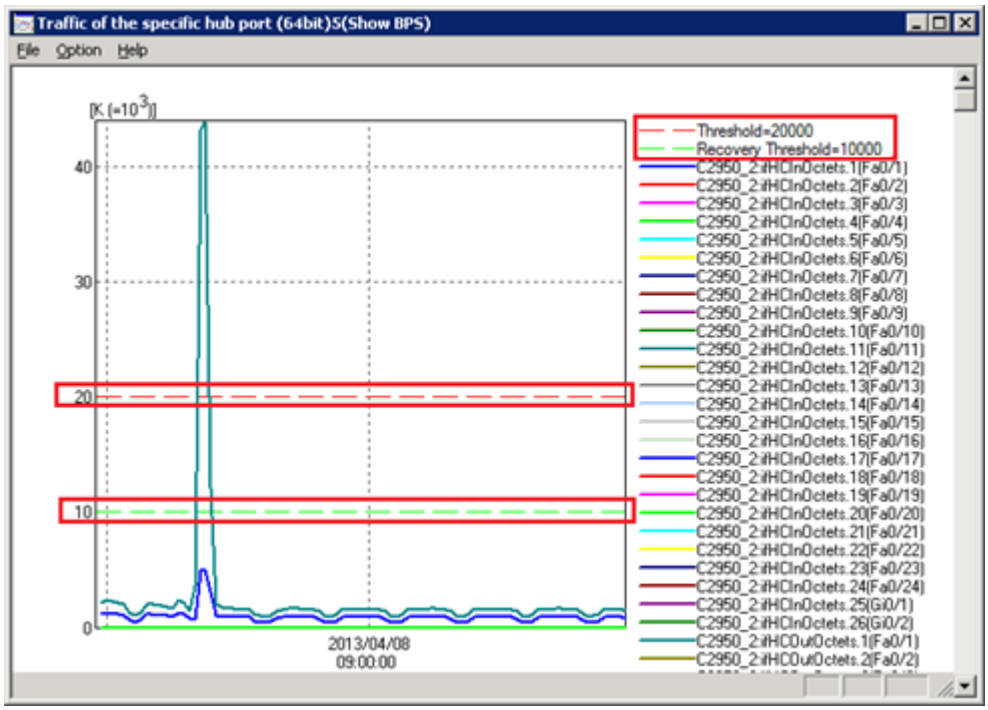
5.11.1.1 Graph view window

Display graphs based on collected data. When a threshold and a recovery value are specified, the threshold (red dotted line) and the recovery value (green dotted line) are displayed in the graph, and the specified value are displayed in the graph legends.

• When a threshold is not specified



- When a threshold is specified



- **File**
  - **Print**

    Displays the Print dialog box.
  - **Print Setup**

    Displays the Print Setup dialog box
  - **Exit**

    Closes the graph window.

- **Option**
  - **Set X axis**

    Displays the Set X axis dialog box. For details, refer to "5.11.1.2 Set X axis dialog box (page 489)".
  - **Set Y axis**

    Displays the Set Y axis dialog box. For details, refer to "5.11.1.3 Set Y axis dialog box (page 490)".
  - **Select Item**

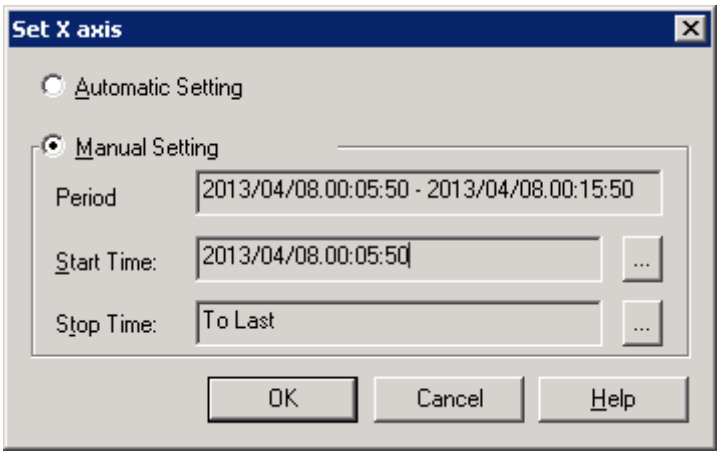
    Displays the Select Item dialog box. For details, refer to "5.11.1.4 Select Item dialog box (page 490)".
  - **Show Legends**

    Switches between displaying and hiding legends (screen top right).
- **Help**
  - **Help Contents**

    Displays Help information for the graph window.

5.11.1.2 Set X axis dialog box

Set the display range for the graph.



- **Automatic Setting**

  Displays a graph using currently available data.
- **Manual Setting**
  - **Period**

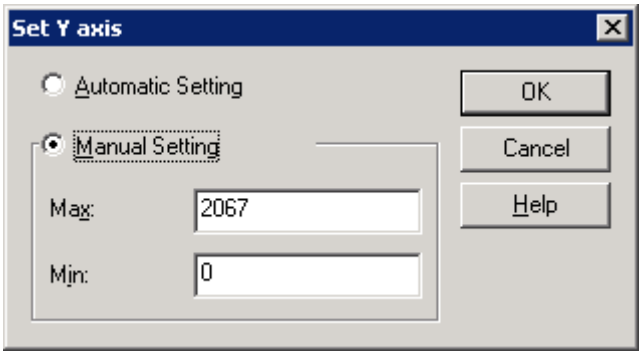
    The period for which a graph may be displayed is shown.
  - **Start Time**

    Sets the start time for the first data to be displayed on the graph. If "From First" is specified, display begins with the earliest data available. If no data exists for the specified time, the data closest after the specified time is displayed.
  - **Stop Time**

Sets the stop time for the last data to be displayed on the graph. If "To Last" is specified, display ends with the most recent data available. If no data exists for the specified time, the next closest data within the specified time is displayed.

5.11.1.3 Set Y axis dialog box

This dialog box is used to set the range of the Y axis (display range) for the graph.



- **Automatic Setting**

  Calculates the maximum value for the collected data and sets the Y axis.

- **Manual Setting**
  - **Max**

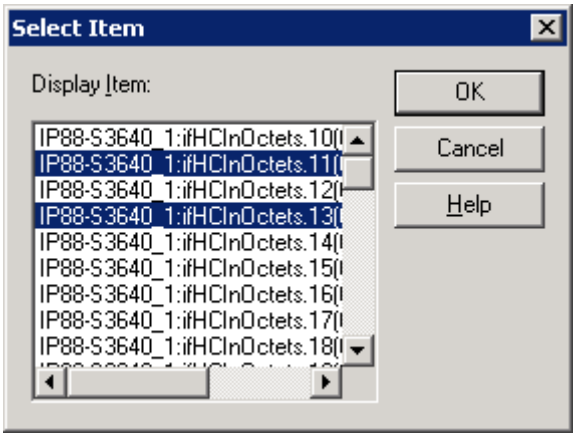
    Sets the maximum value to be displayed on the graph.
  - **Min**

    Sets the minimum value to be displayed on the graph.

5.11.1.4 Select Item dialog box

Select the display items (MIB objects) for the collected data.

Multiple items can be selected by using either SHIFT or CTRL.



5.11.2 Creating and displaying a report

Network Manager can be configured to generate and display daily, weekly, monthly or annual reports based on accumulated statistical information. Generating reports in this way enables analysis of long-term trends in statistical information. Reports are created based on performance data collected by the data collection function.

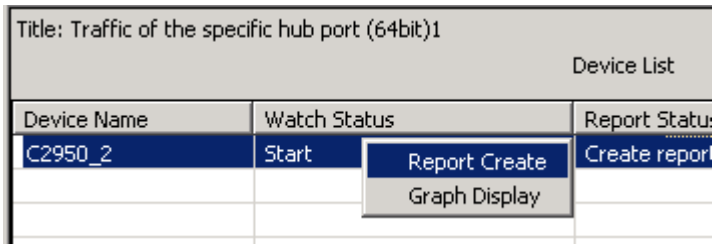
1. Open the "4.16.1 Data Collecting Setting window (page 334)".

   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.

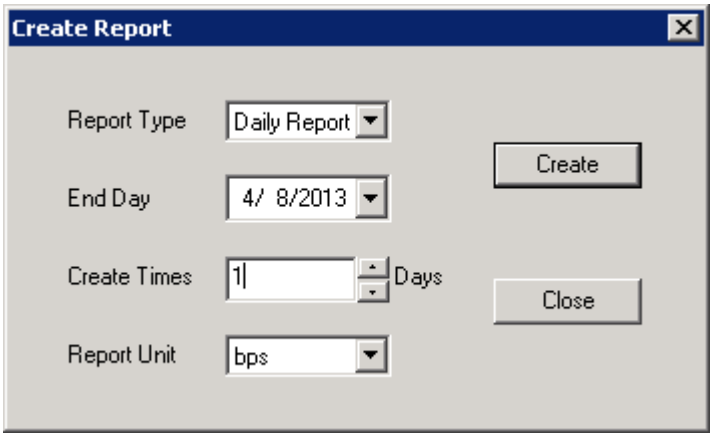
2. In the data collection entry tree, select the entry that you want to display.

   The Device List pane or Report List pane is displayed.

3. Right-click the target node in the Report List pane and select **Report Create** menu.



4. In the Create Report dialog box, select **Report Type**, etc. and select **Create** button.



- **Report Type**

  Specifies the report type. The options are daily report, weekly report, monthly report, annual report.

- **End Day**

  Specifies the last day of the report period.

- **Create Times**

  You can specify the number of daily or weekly reports to create.

- **Report Unit**

  You can specify "Kbps" or "Mbps" for collection data entries that are in units of "bps", or "Kpps" or "Mpps" for entries in units of "pps".

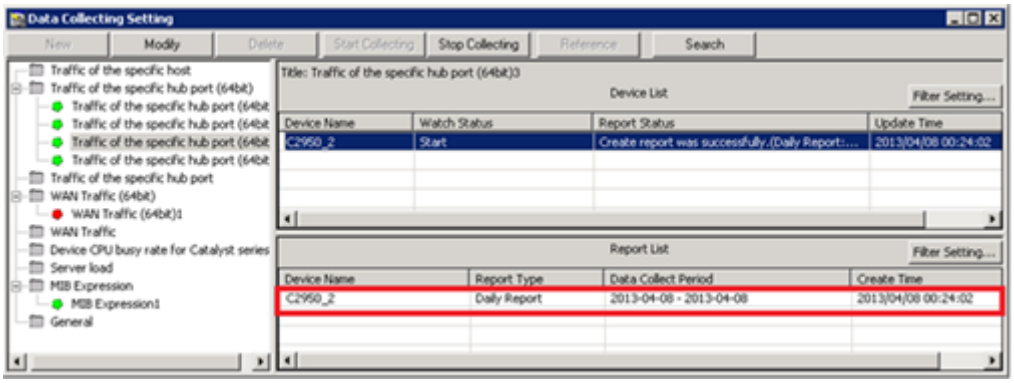
- **Create** button

  Creates the report. Created reports are displayed in order in the Report List pane.

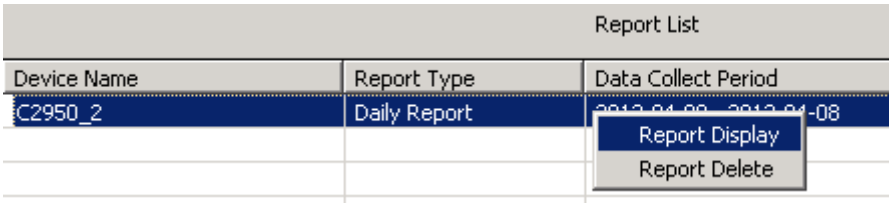
- **Close** button

Closes the dialog box.

Reports are created and displayed in the Report List pane.



5. Select the target report in the Report List pane, right-click the report and select **Report Display** menu.

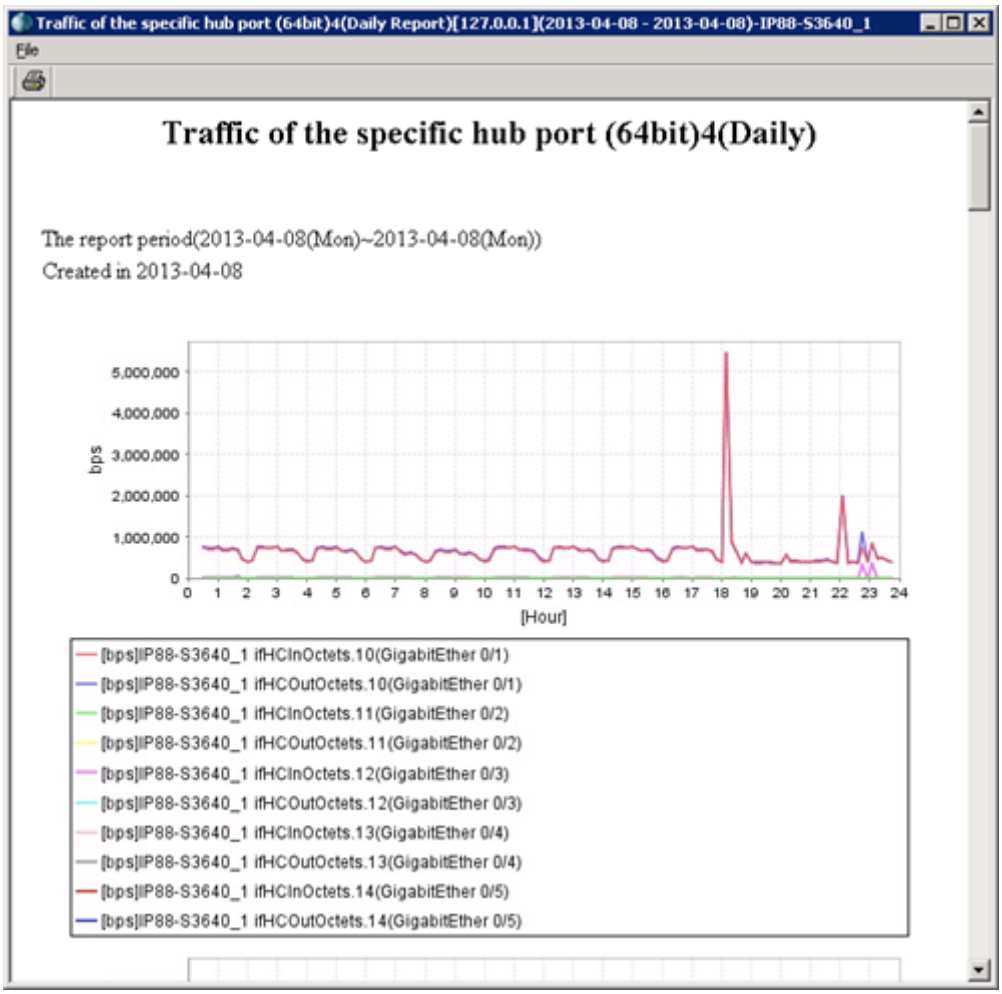


Caution

When recreating a report, if an operation to display a report is performed before the report creation has finished, a dialog indicating "Failed to display a report" may be displayed and the report may not be displayed.

In this case, confirm that a report creation has finished from the **Report Status** column in the Device List pane or from the **Update Time** column in the Report List pane, and then operate report display again.

The report specified is displayed in the View Report window.



For details regarding the View Report window, refer to "5.11.2.1 View Report window (page 493)".

For information regarding the various report formats, refer to "7.2 Data Collection Rules (page 622)".

⚠ Caution

If collected value is 64 bit integer type and the value exceeds $1.0*10^{14}$, y-axis of a report may not be displayed correctly.

In this case, in the **Report Unit** of the Create Report dialog box, re-create the report with a larger report unit.

5.11.2.1 View Report window

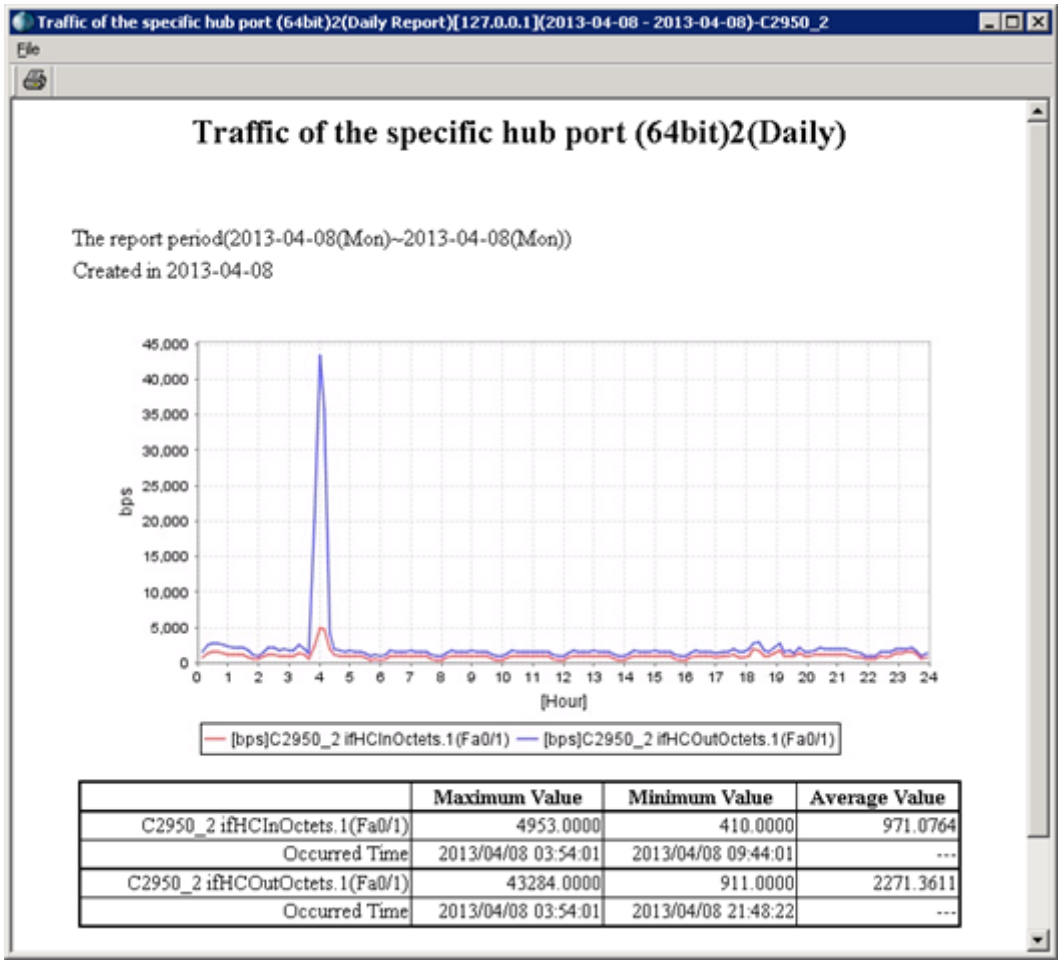
Displays reports for specified data collection entries. If a threshold and recovery value are specified, the threshold (red dotted line) and the recovery value (green dotted line) are displayed in the graph, and the numerical values are displayed under the graph.

Plot values in the graph, despite of collecting intervals, are shown below, depending on report types.

- Daily Report: Peak value for five minutes
- Weekly Report: Peak value for thirty minutes
- Monthly Report: Peak value for two hours
- Yearly Report: Peak value for one day

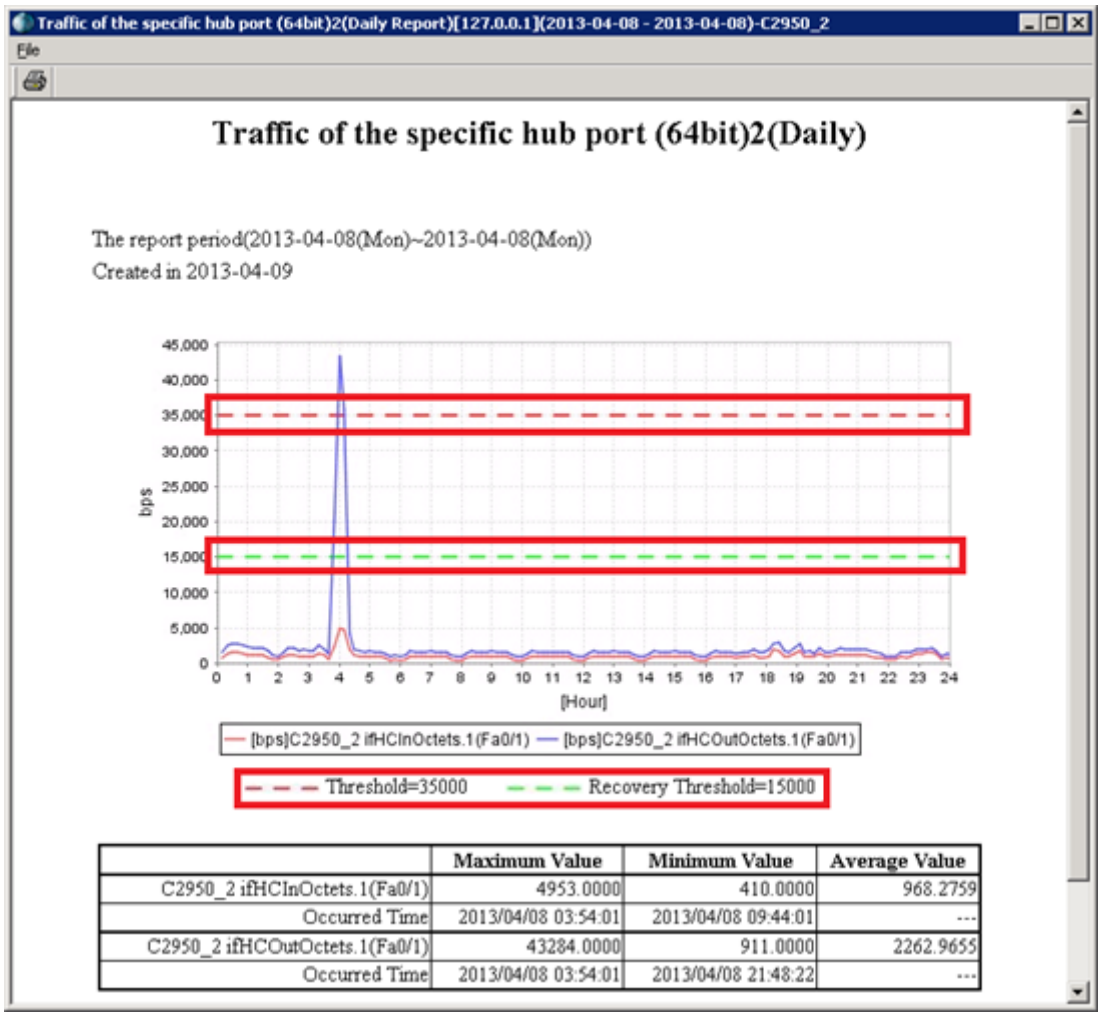
For details of a report for each collection rule, refer to "7.2 Data Collection Rules (page 622)".

- When a threshold is not specified



	Maximum Value	Minimum Value	Average Value
C2950_2 ifHCInOctets.1(Fa0/1)	4953.0000	410.0000	971.0764
Occurred Time	2013/04/08 03:54:01	2013/04/08 09:44:01	---
C2950_2 ifHCOutOctets.1(Fa0/1)	43284.0000	911.0000	2271.3611
Occurred Time	2013/04/08 03:54:01	2013/04/08 21:48:22	---

- When a threshold is specified



	Maximum Value	Minimum Value	Average Value
C2950_2 ifHCInOctets.1(Fa0/1)	4953.0000	410.0000	968.2759
Occurred Time	2013/04/08 03:54:01	2013/04/08 09:44:01	---
C2950_2 ifHCOutOctets.1(Fa0/1)	43284.0000	911.0000	2262.9655
Occurred Time	2013/04/08 03:54:01	2013/04/08 21:48:22	---

Caution

1. The View Report window is capable of simultaneously displaying four windows.
2. Due to such factors as the port number and ifIndex value for a node not being properly aligned, the lines displayed in report graphs may not always display in the order they were specified.

5.11.2.2 Deleting a report

1. Open the "4.16.1 Data Collecting Setting window (page 334)".

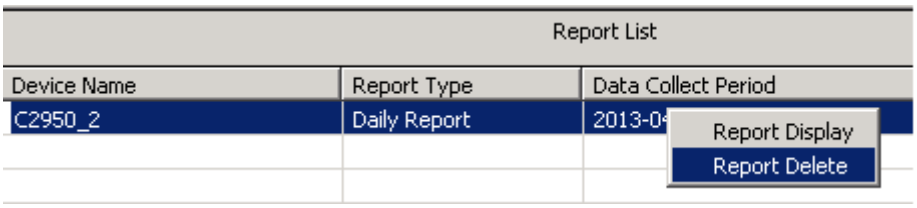
   Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.

2. In the data collection entry tree, select the entry name.

   The Device List pane and Report List pane is displayed.

3. Select the target node in the Device List pane.

4. In the Report List pane, right-click the report that you want to delete and select **Report Delete** menu.



5. In the deletion confirmation dialog box, click **OK** button.

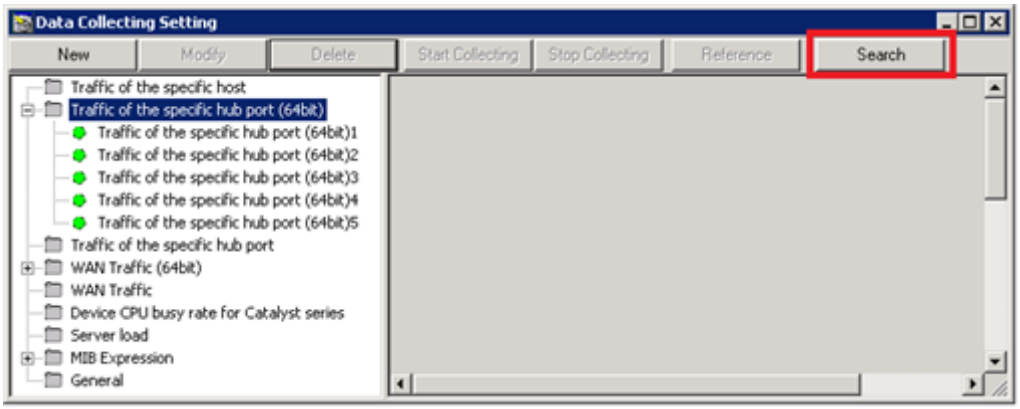
5.11.3 Searching for collection entries

If a large number of collection entries are registered, it can be difficult to find the entries to display in a graph or report in the tree that shows the collection entries list. Use the Data Collect Entry Search window to search for collection entries. Follow the steps below to search for collection entries.

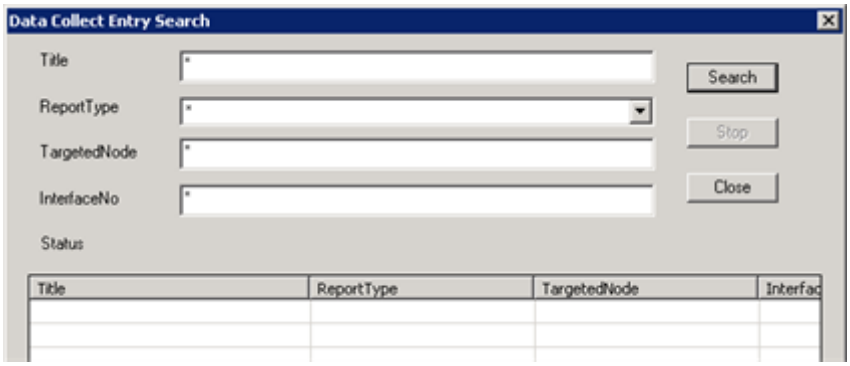
1. Open the "4.16.1 Data Collecting Setting window (page 334)".

   Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.

2. In theData Collecting Setting window, click **Search** button.



3. Set the search conditions in the Data Collect Entry Search window.



As a search condition, the following items can be specified. A wildcard "*" can be used in each of the settings.

- **Title**

  Set the title of the collection entry.

- **ReportType**

  Select a report type from the list, such as the "Traffic of the specific host".

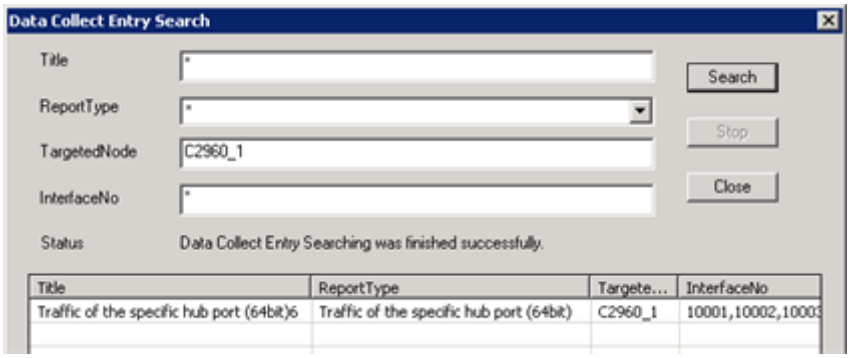
- **TargetedNode**

  Specify the name of the node to target.

- **InterfaceNo**

  Specify the interface number.

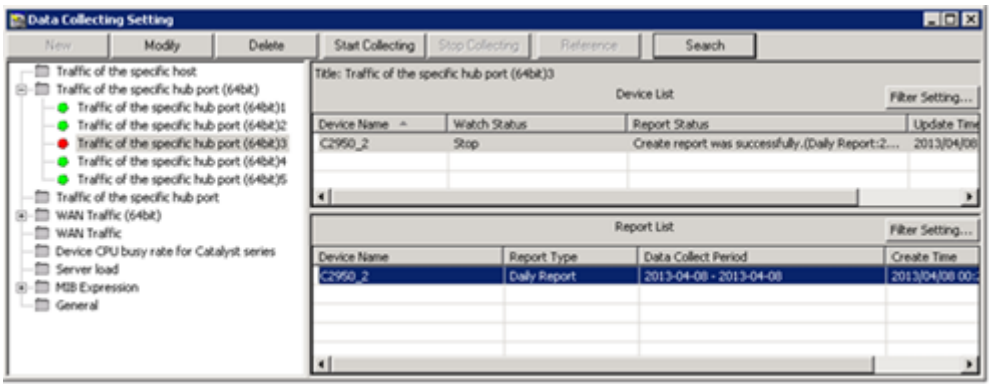
4. Click the **Search** button.



To display the search results in the list.

5. Double-click an item in the list of search results.

Jumps to the Data Collecting Setting window corresponding to the item, and selects the corresponding node.



At this time, as the Data Collect Entry Search window is not closed, you can search with another condition quickly.

6. Display graphs and create and display reports in the Data Collecting Setting window.

5.11.4 Setting filters in the Data Collecting Setting window

In the Data Collecting Setting window, there may be a large number of lists that display in the Device List pane and Report List. It may take a long time to find the rows to use to display a graph, create or display a report.

To make the search easier, specify filter settings for the lists.

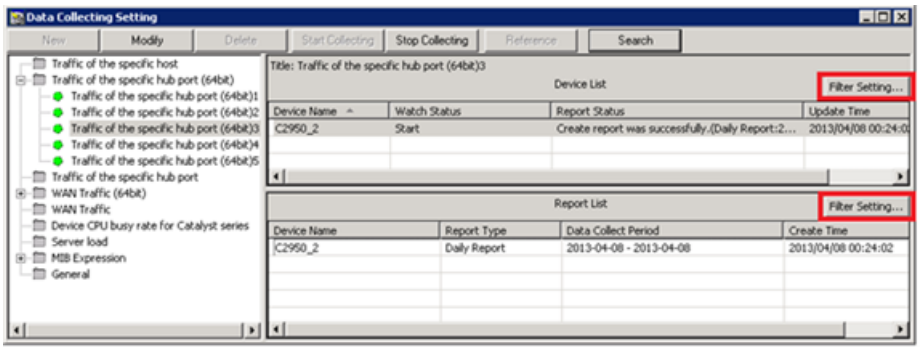
1. Open the "4.16.1 Data Collecting Setting window (page 334)".

   Right-click the **NetworkView** icon or the **NetworkManagement** icon, and select **Performance Management**>**Data Collecting**.

2. In the data collection entry tree, select the entry name.

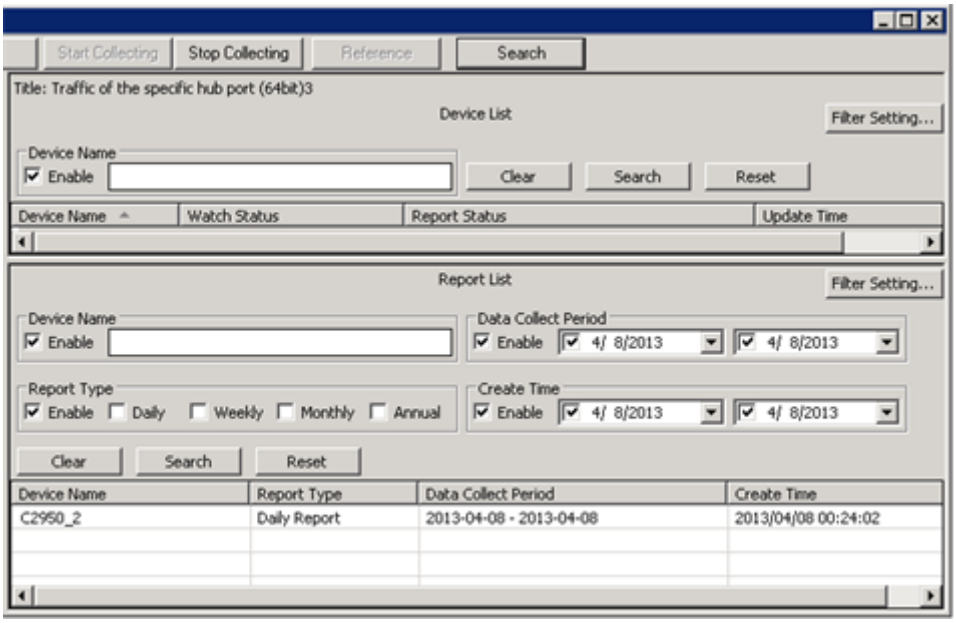
   The Device List pane and Report List pane is displayed.

3. In the Device List pane or the Report List pane, click **Filter Setting** button.



The filter settings are displayed.

4. Select the **Enable** check box for conditions to specify.



5. Click the **Search** button to filter the list using the specified conditions.

5.11.5 Storage folders for performance data (CSV files, report files)

In Network Manager, collected performance data is exported to a CSV file in units of days.

Performance data collected using the settings in the Data Collecting Setting window is stored (in CSV files) in the folder below.

<On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\data\report\logdata*collection_entry_name**node_name**YYYY**MM**DD*.csv

Example: the name of a CSV file created on 07/25/2008 will be 2008\07\25.csv. For performance data (CSV file) formats, refer to "7.2 Data Collection Rules (page 622)".

Report files created from collected performance data are stored in the following folder:

<On the manager, %sharedfolder%>\Manager\sg\NvPRO\report\RPT*<collection_entry_ID>**<node_ID>*

Verify the "collection_entry_ID" and "node_ID" using the methods below.

1. Verify the collection "entry ID".

   Run the following command in *<On the manager, %installfolder%>*\Manager\bin

   ```
   NvPROAmibGetMgr -file logEnt.txt logEnt:* obj.logEnt.logEntTitle
   ```

   The results below are output to logEnt.txt. Look at the first column (collection entry ID) and the third column (collection entry name) and find the collection entry ID corresponding to the collection entry name.

logEnt1	logEntTitle.0	Restore
logEnt2	logEntTitle.0	Traffic of the specific hub port 1
logEnt3	logEntTitle.0	General 1
logEnt4	logEntTitle.0	**Traffic of the specific host 1**

   In this example, the collection entry ID that corresponds to the collection entry name "Traffic of the specific host 1" is "_logEnt4".

2. Verify the "node ID".

   Run the following command in *<On the manager, %installfolder%>*\Manager\bin

   ```
   NvPROAmibGetMgr -file deviceid.txt *:* nvpromib.nvproGen.nvproGenEquipId
   ```

   The results shown below are exported to "deviceid.txt". Look at the first column (node name) and the third column (node ID) and find the node ID that corresponds with the node name.

Catalyst2950	nvproGenEquipId.0	**48**
IP8800-720	nvproGenEquipId.0	54
QX-S3026E	nvproGenEquipId.0	52

   In this example, the "Catalyst2950" device ID is "48".

   In the example above, the storage path for the report file for collection entry name "Traffic of the specific host 1" and node name "Catalyst2950" are the following:

   <On the manager, %sharedfolder%>\Manager\sg\NvPRO\report\RPT_logEnt4\48

The report files are a set of html files and jpg files. They are saved in the folders above, in the following formats:

- html files

  <Type>_<start_date>_<end_date>.htm

  - Type: Y = annual report, M = monthly report, W = weekly report, D = daily report
  - Start and end dates: YYYYMMDD format
  - Example: D_20110513_20110513.htm

- jpg files

  Img/<Type>_<start_date>_<end_date>.jpg

  - Type: Y = annual report, M = monthly report, W = weekly report, D = daily report

- Start and end dates: YYYYMMDD format
- Example: `Img/D_20110513_20110513.jpg`

If you are not using the auto delete settings for performance data (CSV files) and report files, it is recommended to monitor the amount of disk space that is being used and performing regular maintenance, including the manual deletion of old data.

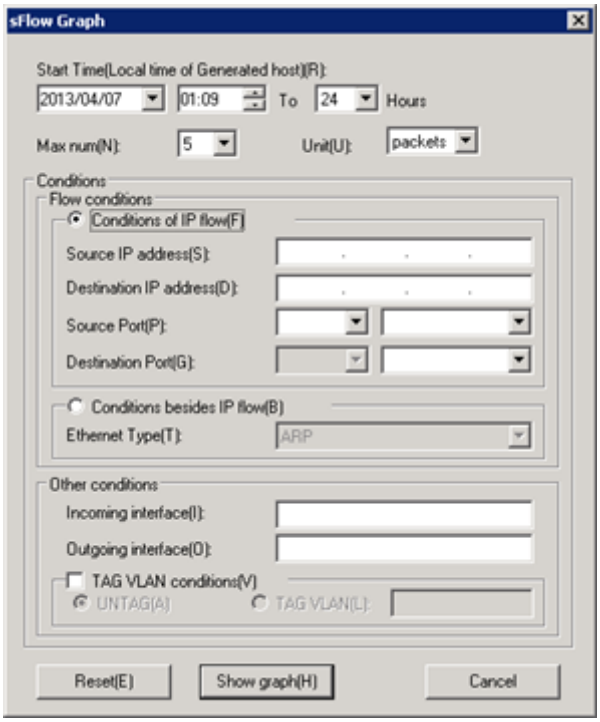
To see how to configure the auto delete settings for performance data (CSV files) and report files, refer to "4.16.7 Maintaining performance data (CSV files, report files) (page 368)".

5.12 Checking Analysis of Traffic Flow (sFlow)

5.12.1 Graph display of traffic-flow information from sFlow

Selecting a device from the "4.17.1.1 sFlow Agent List window (page 374)" and clicking the **Show Graph** button opens a dialog for specifying graph display conditions for traffic flow information collected at selected sFlow agents.

sFlow Graph dialog box



- **Start Time**

  Specify the time range to be displayed. The default setting is for the 24 hours up until the present. Times in the future or in intervals smaller than one hour cannot be specified. The time range is specified by the local time of the monitored terminal. The time range in the sFlow graph title is displayed by the local time of the manager.

- **Max num**

  Select 1, 5, or 10 as the TOP-N for the flow to be displayed. The default value is TOP-5.

- **Unit**

Select packets (the default value) or bytes as the units for flow statistical information to be displayed.

- **Conditions**
  - **Flow conditions**
    - **Conditions of IP flow**

      When refining the IP flow, you must specify four items: the IP address and the port number (if ICMP, zero for convenience) for both the source and the destination.

      All are blank by default, with all IP flow information being the target.

    - **Source IP address** / **Destination IP address**

      Specify the IPv4 address in decimal dot notation.

    - **Source Port** / **Destination Port**

      Left-side field :

      Select the IP upper protocol name from the list (TCP, UDP, ICMP).

      Right-side field :

      If specifying TCP or UDP as the IP upper protocol in the left-side field, make a selection from the list. If specifying ICMP, zero will be used for convenience, and no entry can be made here.

    - **Conditions besides IP flow**

      If a communication situation based on an Ethernet type other than IP is displayed, choose from ARP, IPv6, and others.

  - **Other Conditions**
    - **Incoming interface** / **Outgoing interface**

      Specify an integer from 1 to 2147483647 (2^{31}-1) in single-byte numeric characters as the input/output interface above the sFlow agent that detected traffic flow information.

      Specify an index number (IfIndex) in the input/output interface number.

      Right-click the sFlow agent and select **Configuration Management**>**Interface Property**. Specify the port index value displayed in Interface Properties dialog box as the index number.

    - **TAG VLAN conditions**

      Specify whether or not traffic flow communication has TAG. The default value is UNTAG (no TAG). If selecting TAG VLAN, specify an integer from 1 to 4095 in single-byte numeric characters.

- **Reset** button

  Resets initial values.

- **Show graph** button

  Displays a graph based on specified conditions (AND conditions of all settings).

- **Cancel** button

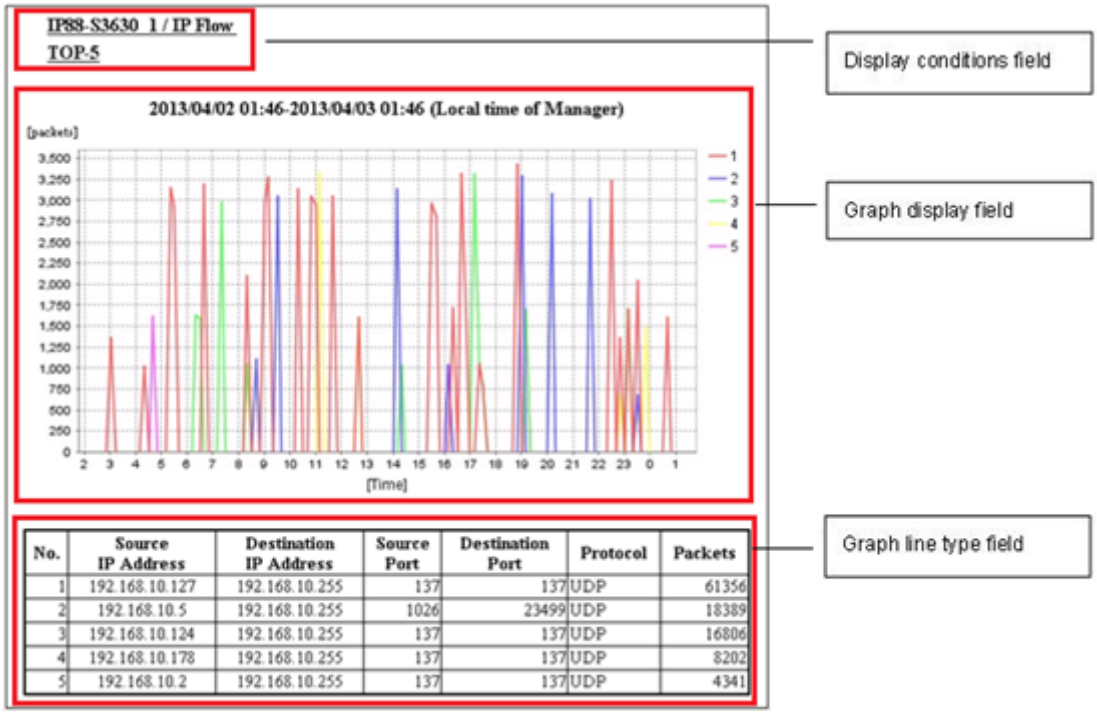
  Ends the sFlow Graph dialog box.

5.12.2 sFlow graph structure

The sFlow graph is structured as shown below.

IP flow graph display

The following is an IP flow graph display sample.



No.	Source IP Address	Destination IP Address	Source Port	Destination Port	Protocol	Packets
1	192.168.10.127	192.168.10.255	137	137	UDP	61356
2	192.168.10.5	192.168.10.255	1026	23499	UDP	18389
3	192.168.10.124	192.168.10.255	137	137	UDP	16806
4	192.168.10.178	192.168.10.255	137	137	UDP	8202
5	192.168.10.2	192.168.10.255	137	137	UDP	4341

- Display conditions field

  Displays the conditions specified in the sFlow Graph dialog box.

- Graph display field

  Displays traffic flow information in a line graph. In the title of the graph, the local time of the manger is displayed.

- Graph line type field

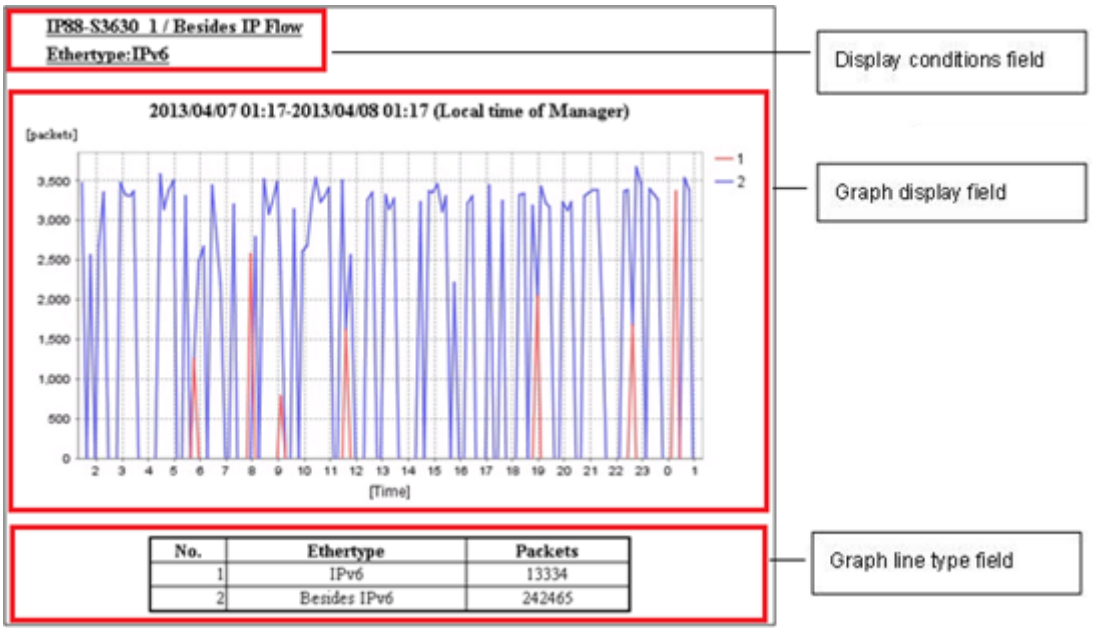
  Displays detailed flow information corresponding to each line graph.

⚠ Caution

The graph's vertical axis value and the number of packets in the graph line-type field are numeric values projected from sampling information. They are not completely accurate values.

Non-IP flow graph display

The following is a non-IP flow graph display sample.



- Display conditions field

  Shows the conditions specified in the sFlow Graph dialog box.

- Graph display field

  Displays a graph with two lines, one for the conditions specified in Ethernet type and one for other data. In the title of the graph, the local time of the manger is displayed.

- Graph line type field

  Displays detailed flow information corresponding to each line graph.

  There is no flow information corresponding to the conditions, 0 is displayed in the packets column.

5.12.3 CSV file storage folder and format

If settings to **Output to CSV File** have been made in the sFlow Data Received Setting dialog box, CSV files will be stored in the following path name. For setting of the receptino data, refer to "4.17.3 Setting duration of flow data retention (page 376)".

<On the manager, %installfolder%>\Manager\sg\NvPRO\SFlowCollector\work\dat*sFlow agent name**YYYY**MM*\FLA_*DD*.csv

For example, a CSV file of Switch1 created on 2008/07/25 would be: Switch1\2008\07\FLA_25.csv

⚠ Caution

1. Even if a device registered in the sFlow agent list is deleted, the folder for that sFlow agent name will not be deleted. If unnecessary, this must be deleted manually.
2. If the device name of a sFlow agent has been changed, the folder corresponding to the previous device name will remain unchanged.

The CSV file used for storing flow data is comprised of the following information.

No.	Content	Meaning	Format	Comments
1	agentname	sFlow agent name	Character string	

No.	Content	Meaning	Format	Comments
2	unix_time	Received time	YYYY/MM/DD hh:mm	
3	frametype	Ether frame format type	Character string	Ethernet II (IEEE) 802.3 SNAP (IEEE) 802.3 RAW (IEEE) 802.2 LLC
4	ethertype	MAC header type information	Hexadecimal numeric value	0 to 0xffff
5	tag	IEEE 802.1Q/P header value	Decimal numeric value	TAG: 0x81000012, etc. UNTAG: 0x00000000
6	iptype	iptype	Decimal numeric value	IPv4: 4 IPv6: 6 0 if non-IP
7	srcip	Source IP address (IPv4 or IPv6)	Character string	
8	dstip	Destination IP address (IPv4 or IPv6)	Character string	
9	nexentryop	NEXTHOP IP address (IPv4 or IPv6)	Character string	
10	in_if	Input interface ifIndex value	Decimal numeric value	
11	out_if	Output interface ifIndex value	Decimal numeric value	
12	packets(total)	Total flow packet number (projected)	Decimal numeric value	
13	bytes(total)	Total flow byte number (projected)	Decimal numeric value	
14	error%	Error rate	Percentage	Maximum 196, minimum 0, -1 if uncomputable
15	packets(received)	Number of flow samples	Decimal numeric value	
16	bytes(received)	Number of flow bytes	Decimal numeric value	
17	start_clock	sysUpTime when flow received	Decimal numeric value	
18	last_clock	sysUpTime when final data received	Decimal numeric value	
19	srcport	Source TCP/IP port number	Decimal numeric value	
20	dstport	Destination TCP/IP port number	Decimal numeric value	
21	proto	IP upper protocol number	Decimal numeric value	ICMP: 1,TCP: 6,UDP: 17, etc.
22	tos	Type of Service value	Decimal numeric value	
23	priority	IP priority (for IPv6)	Decimal numeric value	

No.	Content	Meaning	Format	Comments
24	in_speed	Input interface line speed	Decimal numeric value	
25	out_speed	Output interface line speed	Decimal numeric value	

Caution

1. Data for the same flow occurring within 10 minutes is merged into one record.
2. By analyzing the CSV files, it is possible to analyze previous flow situations. However, Network Manager does not have a function to display graphs from CSV files.

5.13 Starting or Stopping Monitoring by the Monitoring Mode

The monitoring mode is a function for switching on and off the monitoring function for individual devices.

If the monitoring mode is OFF or not set, the following functions will not be performed for the applicable device.

1. State monitoring function
2. Data collection function
3. Configuration change monitoring
4. Device command execution based on the schedule
5. SNMP trap receiving
6. Syslog receiving

The device icons for which the monitoring mode is OFF or not set will be displayed in gray by default. To change the color of icons, refer to "4.9.2 About alert severity and priority (page 237)".

The following three methods can be used to set the monitoring mode.

- Manual setting

  Set the mode by right-clicking on the device icon or map icon. The settings are applied immediately. For details, refer to "5.13.1 Manually setting monitoring mode (page 506)".

- Batch register

  When registering configuration information in a batch, the monitoring mode for each device can also be registered in a batch. For details, refer to "4.6 Batch Registering or Deleting Configuration Information (page 206)".

- Monitoring mode schedule

  Sets a schedule for switching the monitoring mode. For details, refer to "5.13.2 Setting and changing a monitoring mode schedule (page 506)".

Caution

1. When registering a new device through auto discover or manual registration, the device is registered without setting the monitoring mode.

   When performing state monitoring or data collection, the monitoring mode for the device must manually be set to ON.

2. The device can still be operated from Network Manager even if the monitoring mode for the device is set to OFF (or not set).

   For example, operations other than State Monitoring and Data Collection, such as Update Device Property, Collect Routing Information, Execute Device Commands and Display Front Panel are all performed as normal (the same as when the monitoring mode is ON).

3. When the monitoring mode of Nexus 5000 is OFF, Nexus 2000 connected to Nexus 5000 is not monitored even if the monitoring mode of Nexus 2000 is "ON".

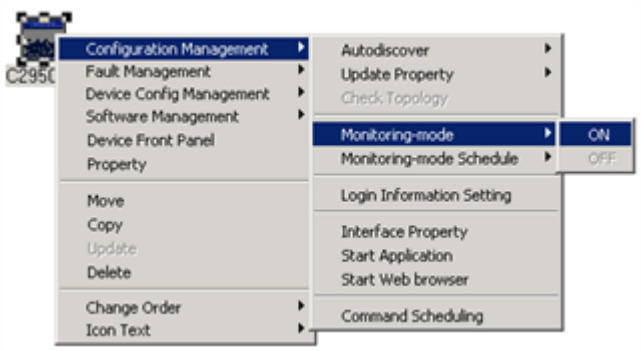
   When the monitoring mode of Nexus 5000 is OFF, Nexus 2000 is not monitored even if the monitoring mode of Nexus 2000 that is under the Nexus 5000 is "ON".

5.13.1 Manually setting monitoring mode

You must first change to the "configuration mode (page 27)".

1. Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Configuration Management**>**Monitoring-mode** and select **ON** or **OFF**.

   If a map icon is specified, the setting will apply to all devices and sub maps under the selected map.



Tip

For the device icon, the monitoring mode can be set to ON/OFF in the **Monitor** tab of the Properties dialog box.

5.13.2 Setting and changing a monitoring mode schedule

In the monitoring mode schedule, set the duration for which the monitoring mode is to remain off (example: during network maintenance).

The monitoring mode can be set individually for map icons including the **NetworkView** icon and **NetworkManagement** icon, and all device icons.

The monitoring mode schedule is applied as follows:

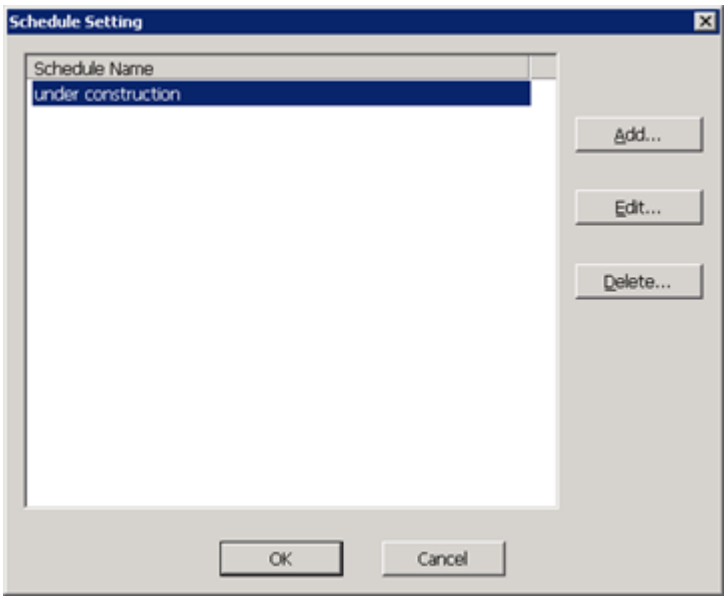
- When the monitoring mode schedule is set for a map icon, the schedule is applied to all devices and submaps under the selected map.
- When a device is moved from a map for which the monitoring mode schedule has been set to another map, the monitoring mode schedule of the new map is applied to the device.
- If a monitoring mode schedule is set for both a map icon and the subordinate device or submap icons, both the schedules for the actual device or submap and the schedule for the parent map are applied.

- If the monitoring mode is not set, operations will take place as if the monitoring mode were set to OFF.

You must first change to the "configuration mode (page 27)".

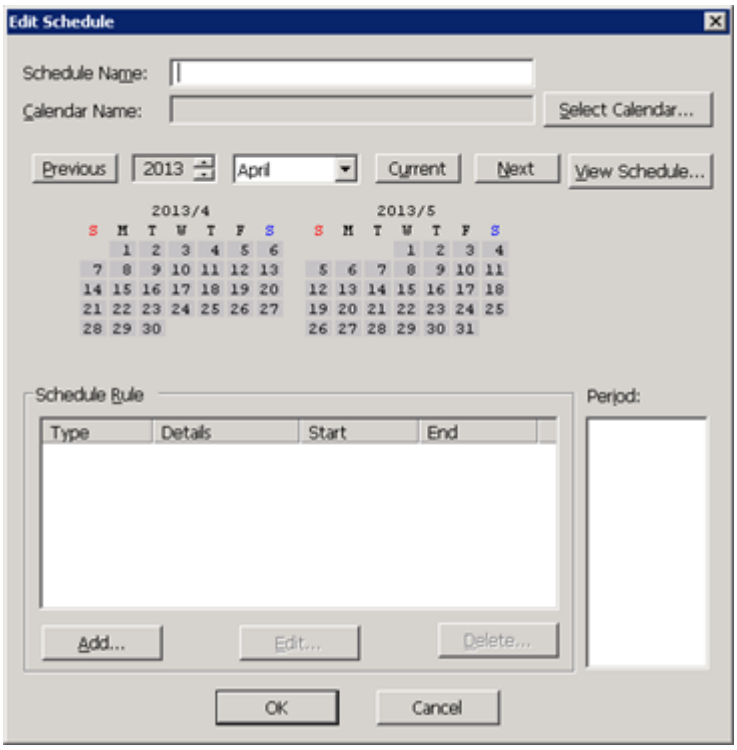
1. Right-click the map icon or device icon, and select **Configuration Management**>**Monitoring-mode Schedule**>**Setting**.

   The "4.22.2.1.1 Schedule Setting dialog box (page 435)" opens.



2. In the "4.22.2.1.1 Schedule Setting dialog box (page 435)", click **Add** button, or select the **Schedule Name** and click **Edit** button.

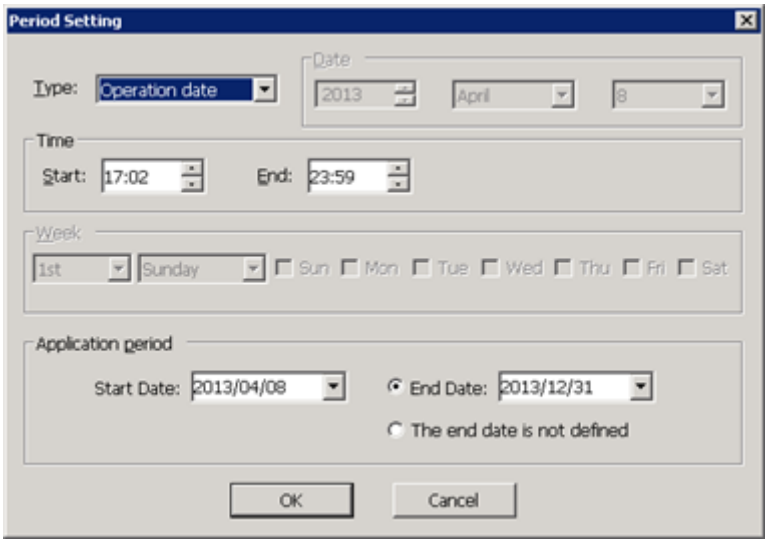
   The "4.22.2.1.3.1 Edit Schedule dialog box (page 436)" opens.



3. In the Edit Schedule dialog box, enter a **Schedule Name**.

4. In the Edit Schedule dialog box, click **Select Calendar** button and select a calendar in the "4.22.1.1 Calendar Setting dialog box (page 427)".

5. In the Edit Schedule window, click **Add** button to set in the Period Setting dialog box.



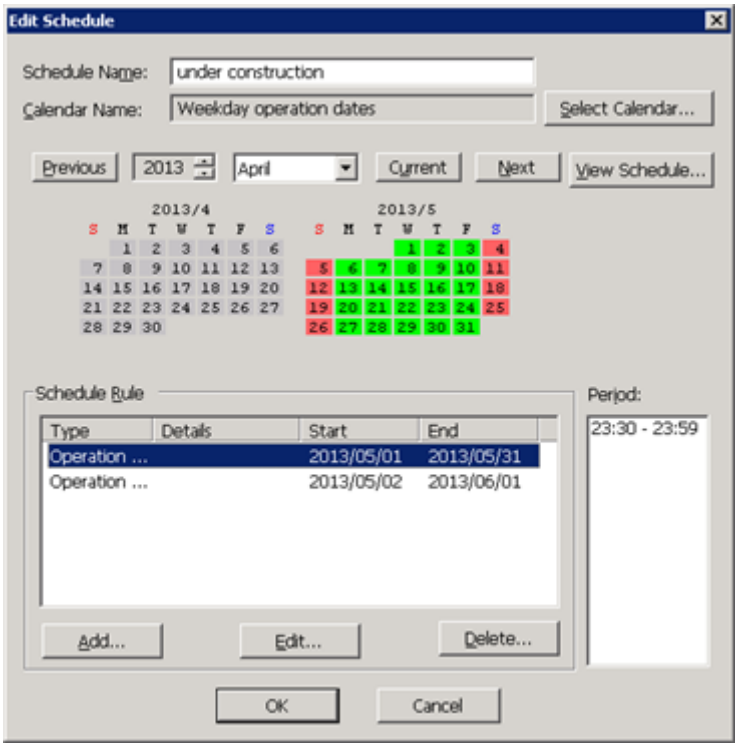
a. Specify the schedule rule (the period in which the monitoring mode is OFF).

Multiple schedule rules can be set in one schedule. For details, refer to "4.22.3.2.1 Creating a duration schedule rule (page 442)".

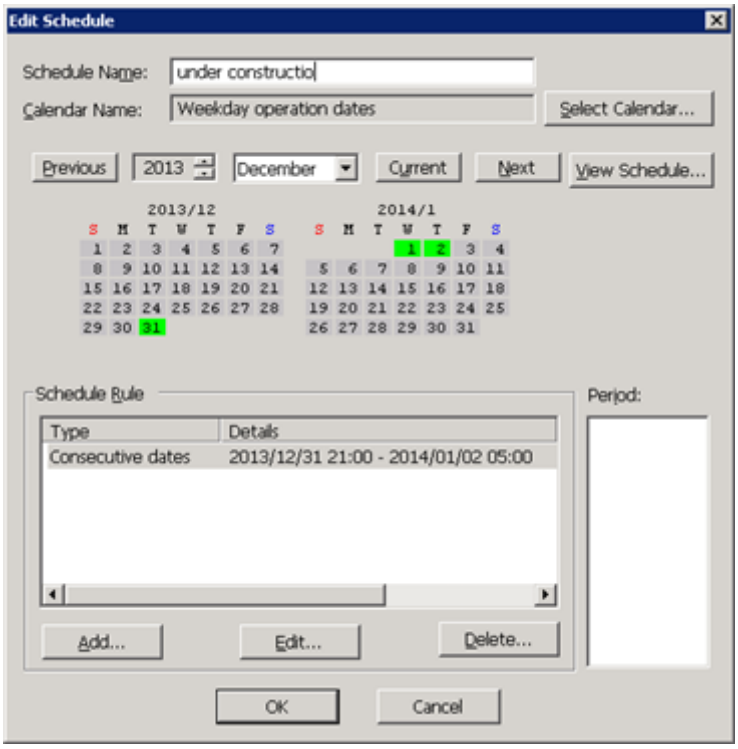
Caution

To set a schedule over a period of days, create a rule that applies until 23:59 on one day and another rule that begins at 0:00 on the following day, or select the "Consecutive dates" in **Type** of the Period Setting dialog box.

- **Example of creating two schedule rules**

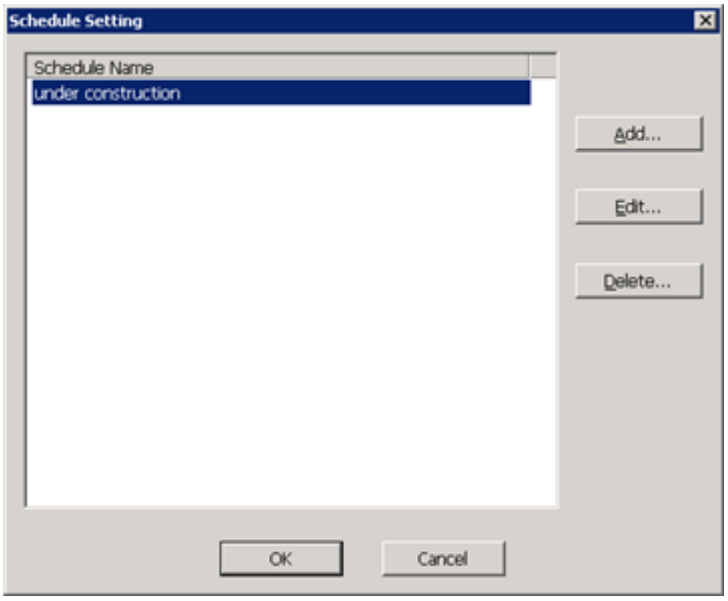


- **Example of specifying "Consecutive dates"**



b. Click **OK** button.

6. In the Edit Schedule dialog box, click **OK** button.
7. In the Schedule Setting dialog box, select the schedule name to be set.



Only the one schedule can be selected.

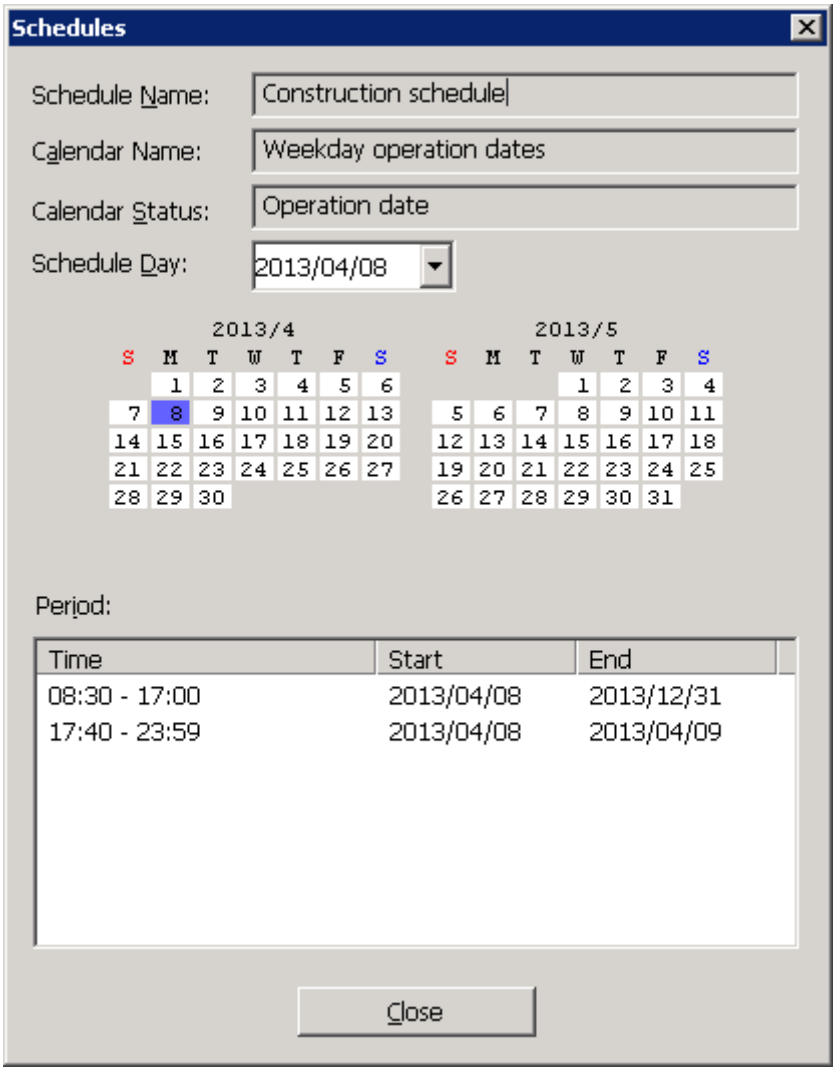
8. In the Schedule Setting dialog box, click **OK** button.

5.13.3 Viewing a monitoring mode schedule

The monitoring mode schedule is viewed.

1. Right-click the map icon or device icon, and select **Configuration Management**>**Monitoring-mode Schedule**>**Property**.

   The Schedules dialog box opens.



2. Confirm a calendar and periods in the the Schedules dialog box.

   For details, refer to "4.22.3.1.5 Viewing a duration schedule (page 441)".

5.13.4 Canceling a monitoring mode schedule

You must first change to the "configuration mode (page 27)".

1. Right-click the map icon or device icon, and select **Configuration Management**>**Monitoring-mode Schedule**>**Cancel**.

   Caution

   Schedule settings information remains in the system even after a monitoring mode schedule is canceled. These schedule settings can be used in other device and map monitoring mode schedules.

   For operation to delete the schedule setting, refer to "5.13.5 Deleting a monitoring mode schedule (page 511)".

5.13.5 Deleting a monitoring mode schedule

Deletion of the monitoring mode schedules is performed together with setting or modifying monitoring mode schedule settings.

You must first change to the "configuration mode (page 27)".

Monitoring mode schedules can be deleted through the Schedule Setting dialog box.

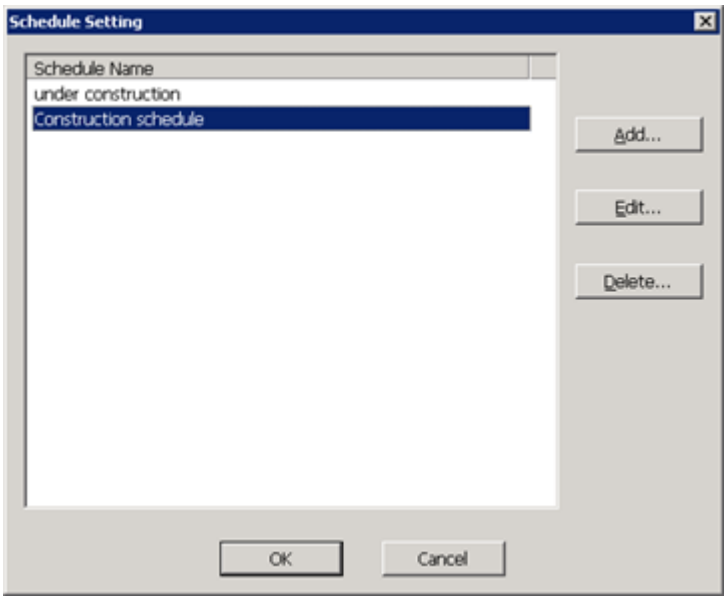
Caution

To delete a monitoring mode schedule, it is necessary to cancel the target schedule from all icons in advance. For details of canceling a schedule, "5.13.4 Canceling a monitoring mode schedule (page 510)".

1. Right-click the map icon or device icon on which you want to configure the monitoring mode schedules, and select **Configuration Management**>**Monitoring-mode Schedule**>**Setting**.

   To display the "4.22.2.1.1 Schedule Setting dialog box (page 435)".

2. In the Schedule Setting dialog box, select the schedule that you want to delete and click **Delete** button.



3. In the deletion confirmation dialog box, click **OK** button.

Tip

- At this stage, the schedule is hidden from the Schedule Setting dialog box but is not deleted. To complete the deletion, click **OK** button on the Schedule Setting dialog box. If **Cancel** button on the Schedule Setting dialog box is clicked, the schedule is not deleted. (deletion is canceled.)
- **OK** button on the Schedule Setting dialog box cannot be clicked unless one displayed schedule is selected. However, if a selectable schedule does not exist, **OK** button can be clicked and a schedule can be deleted without schedule settings.

4. Configure schedule settings.

   For details of operations, refer to the explanation of the Schedule Setting dialog box in "5.13.2 Setting and changing a monitoring mode schedule (page 506)".

5. In the Schedule Setting dialog box, click **OK** button.

5.14 Managing Device Configuration (Resource Manager)

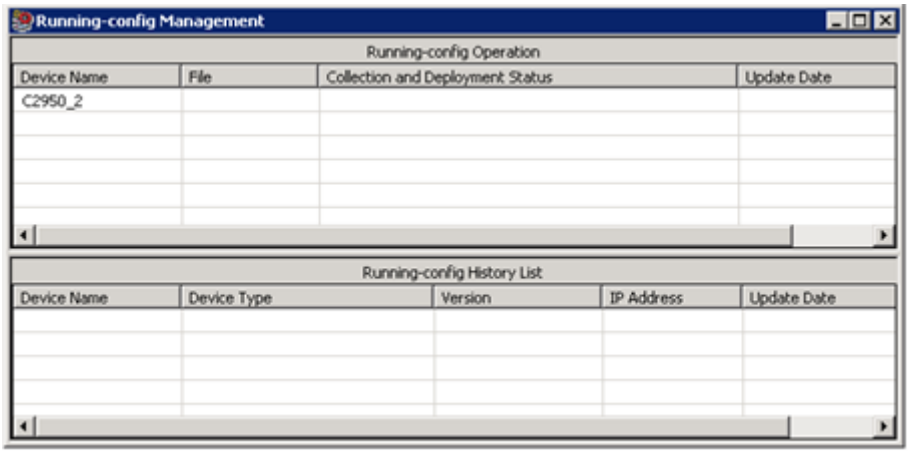
5.14.1 Managing running-config

Manage the current settings information (running-config) for monitored devices. Running-config is managed in the"5.14.1.1 Running-config Management window (page 512)".

5.14.1.1 Running-config Management window

The Running-config Management window is used to manage running-config.

To open the Running-config Management window, right-click the **NetworkView** icon or **NetworkManagement** icon or the map or device icon and select **Device Config Management**>**Running-config Management**.



Running-config Operation pane

- **Device Name**

  Displays the name of the device for which running-config is being managed.

- **File**

  If there are running-configs in the manager that can be distributed, the  icon is displayed. If there are edited running-configs on the monitoring terminal that have not been uploaded to the manager, the  icon is displayed.

- **Collection and Deployment Status**

  Displays the running-config collection and deployment results.

- **Update Date**

  Displays the date and time of the most recent file distribution.

Running-config History List pane

- **Device Name**

  Displays the name of the nodes to which running-config was distributed.

- **Device Type**

  Displays information about the device type, such as the model name.

- **Version**

  Displays the obtained version.

- **IP Address**

  Displays the IP address used for login.

- **Update Date**

  Displays the time that the running-config history was created.

Menu displayed when right-clicking in the Running-config History List pane

- **Collect Config**

  Obtains the running-config from network devices. The collection results are displayed under **Collection and Deployment Status**.

- **Edit Config**

  Edits the file registered for distribution to network devices and saves it on the monitoring terminal. This operation changes the icon to  , indicating that there is a file that should be uploaded.

- **Discard Config**

  Deletes the file registered for distribution to network devices.

- **Deploy Config**
  - **Save to Startup-config**

    Sends registered files to network devices, updates running-config and writes to startup-config.

  - **Not Save to Startup-config**

    Sends registered files to network devices and updates running-config, but does not write to startup-config.

- **Upload**

  Sends files edited on the monitoring terminal to the manager. Files sent using this operation become the target files for sending to network devices.

- **Upper Bound of History**

  Specify an integer between 5 and 65535 for the number of running-config changes saved in the history. The default is 10.

Menu displayed when right-clicking in the Running-config History List pane

- **Display Config**

  Displays the contents of the specified configuration.

- **Display History**

Displays the view and edit window for the specified configuration history. For details, refer to "5.14.1.4 Managing running-config history (page 516)".

- **Apply Config**

  Uses the configuration associated with the history information as the running-config to be distributed to network devices, copies and registers it in the manager.

- **Export**

  Exports the configuration associated with the history information to the monitoring terminal.

- **Show Difference**

  Displays the differences between two separate sets of history information.

- **Delete History**

  Deletes the specified history information.

Caution

If the following operations are performed while this window is opened. The device list in this window is not updated immediately. To reflect changes, open this window again.

- Add and delete a device icon.
- Change a device name.
- Move an icon to another map.

5.14.1.2 Collecting running-config

Collect running-configs from the network devices.

Caution

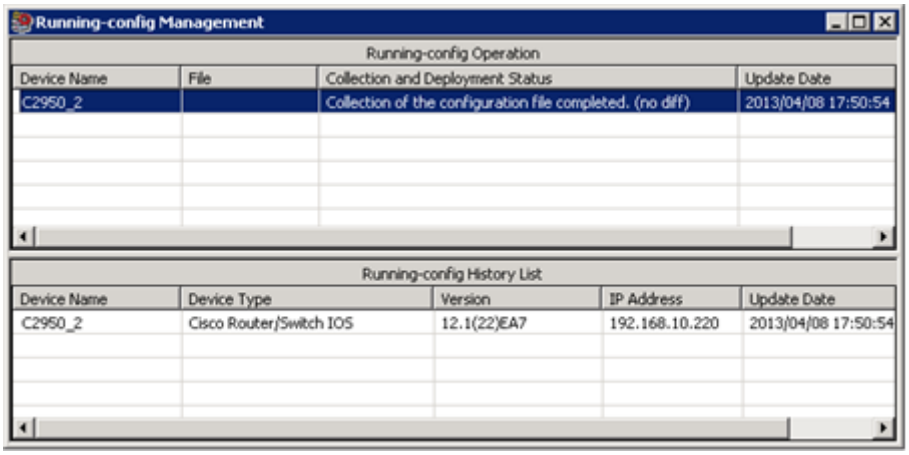
The maximum size of the supported running-config file is 40MB.

1. Open the "5.14.1.1 Running-config Management window (page 512)".

   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Running-config Management**.

2. Right-click the node and select **Collect Config** menu.

   Running-config is retrieved from the network device. The results are displayed in the **Collection and Deployment Status** column. In addition, the history of collected running-configs is added to the Running-config History List pane for that node.



Caution

a. Differences detected during the running-configs collection are not added to the change management differences history. In addition, difference detection alert information is not issued.

b. This operation may fail if the target network device is in the process of installing software or performing commands from the command schedule. If you encounter this type of failure, try performing the operation again.

c. If the size of the running-config exceeds 10MB, this operation may fail. In this case, the maximum memory size to be used in the Resource Manager function needs to be extended. To extend the maximum memory size, change "Xmx" value in the jservice.ini. For details, refer to "8.2.2 Extended Settings for the Resource Manager Function (page 682)".

d. If there are a lot of rows of PF6800 configuration setting, it may take a lot of time to complete collecting the configuration.

e. The Juniper JUNOS has two types of configurations, one for active configuration, one for a candidate for the setting. Network Manager considers an active configuration as a running-confg. There is no file equivalent to startup-config. An active configuration is read in restarting next time.

f. For HP Procurve2510, the default terminal mode is "VT100". If the terminal mode is "VT100", the control characters are displayed while executing commands on the device. If controls characters are included in the output result of executed commands, Network Manager cannot recognize the result of execution correctly. By changing the terminal mode to "raw", control characters can be deleted from the output of device commands. Therefore, if the device is the monitoring target of Network Manager, be sure to configure the following setting.

```
# console terminal none
# write memory
```

5.14.1.3 Viewing running-config differences

Displays differences between configurations.

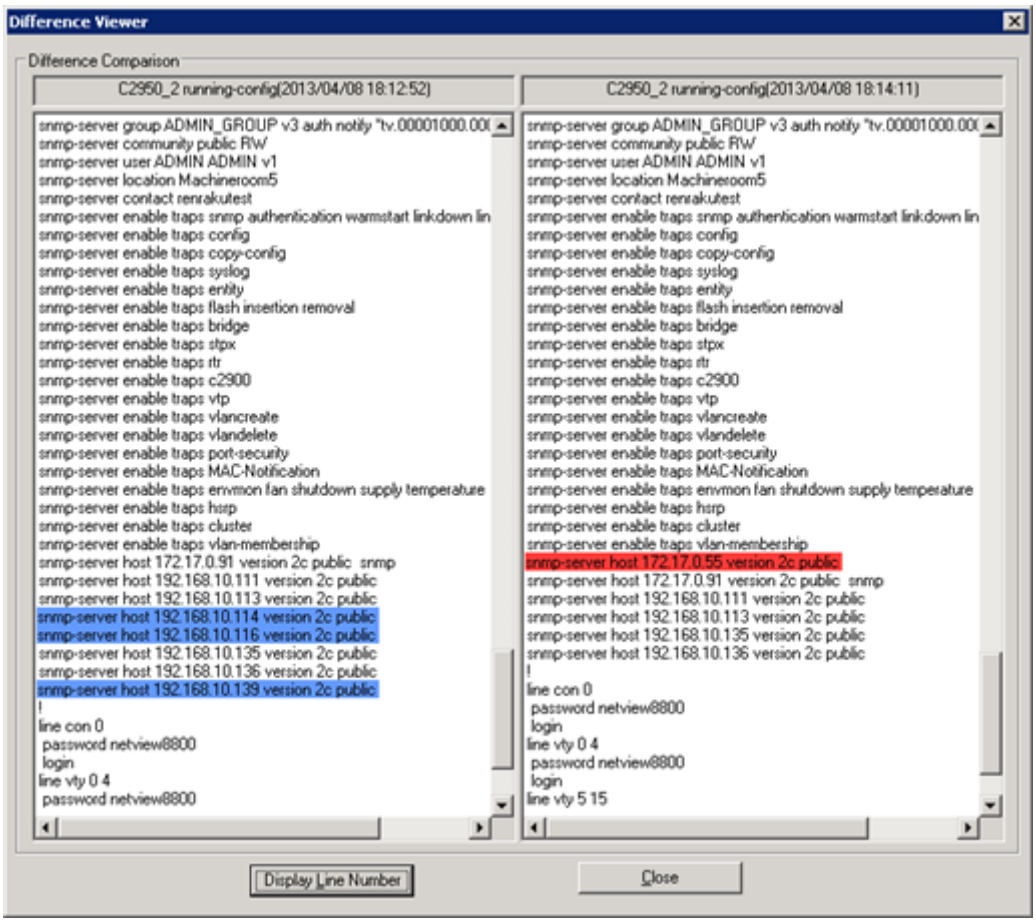
1. Open the "5.14.1.1 Running-config Management window (page 512)".

   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Running-config Management**.

2. In the Running-config History List pane, specify any two running-config histories by clicking them while pressing CTRL key.

3. Right-click and select **Show Difference**.

   The differences between two running-configs are displayed.



The old running-config is displayed to the left and the new running-config is displayed to the right. Rows on the left side only are displayed with a blue background. Rows on the right side only are displayed with a red background.

Rows that have been updated are displayed on the left and right with a red or blue background. It is also possible to view the differences in running-config histories between different devices. In this case, there is no distinction between old and new and the differences appear in the order in which they are displayed in the Running-config History List pane.

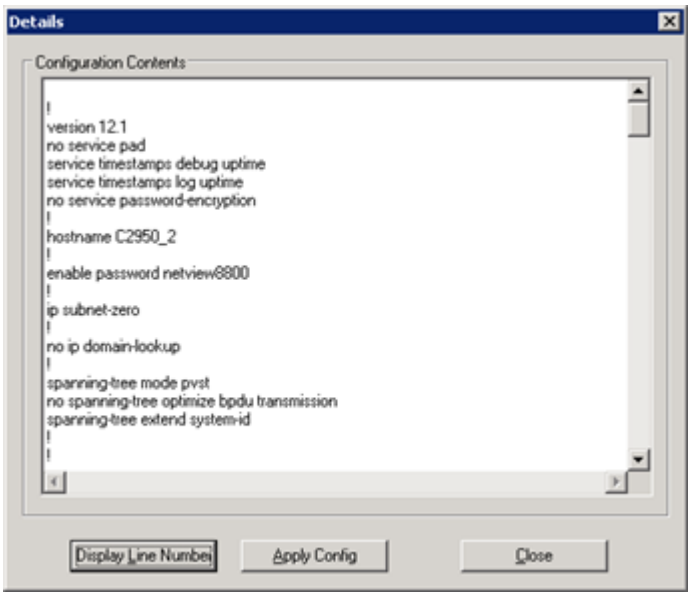
5.14.1.4 Managing running-config history

In addition to displaying collected running-config information, you can add notes as history and attach files as related information.

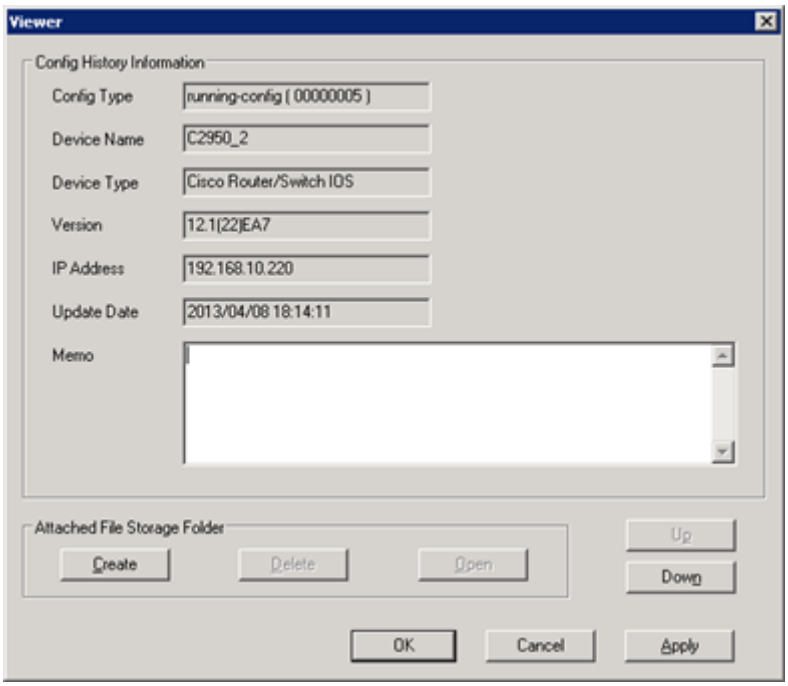
1. Open the "5.14.1.1 Running-config Management window (page 512)".

   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon and select **Device Config Management**>**Running-config Management**.

2. To view runnning-config information, right-click the history that you want to view in the Running-config History List pane and select **Display Config** menu.



3. To view running-config properties, right-click the history in the Running-config History List pane and select **Display History** menu.



Additional information for the running-config can be entered in the **Memo** box as needed.

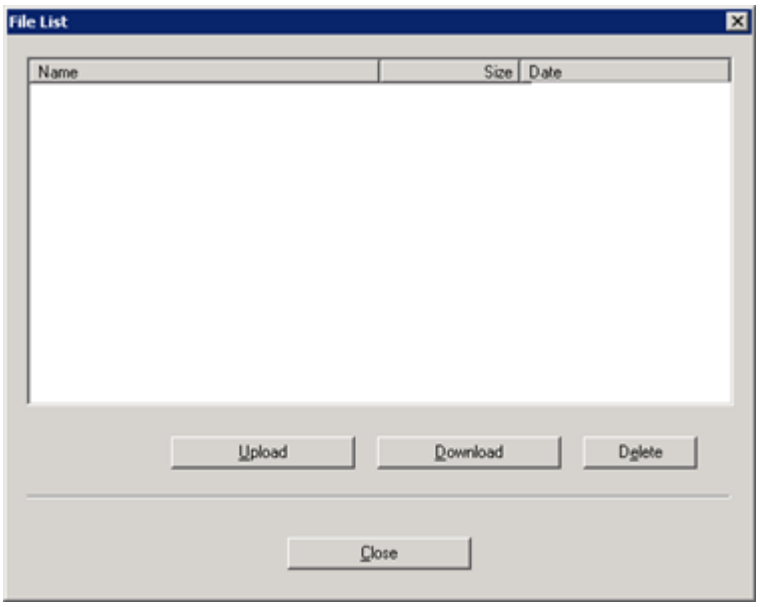
You can also store detailed information by files and associate it with the history.

a. In the **Attached File Storage Folder**, click **Create** button.

   Create a folder that can store the detailed information to correlate to the history.

b. In the **Attached File Storage Folder**, click **Open** button.

c. In the File List dialog box, click **Upload** button to upload the file.



To download attached files, click **Download** button.

4. Download the configuration of the specified history to the monitoring terminal.
   a. Right-click the relevant history in the Running-config History List pane, and select **Export**.
   b. In the Save As dialog box, specify the destination of storing history, click **Save** button.
   c. The running-config is saved to the monitoring terminal.

5.14.1.5 Uploading running-config

Running-config files can be sent to a network device and run on that device.

Deploying running-config means that the specified configuration file is run on the device. The running-config file is not replaced. It is overwritten. Note that deploying running-config to BIG-IP V9 means replacing the whole image of " bigip.conf/bigip_base.conf".

Caution

The maximum size of the supported running-config file is 40MB.

Collect the running-config in advance. For details, refer to "5.14.1.2 Collecting running-config (page 514)".

You must first change to the "configuration mode (page 27)".

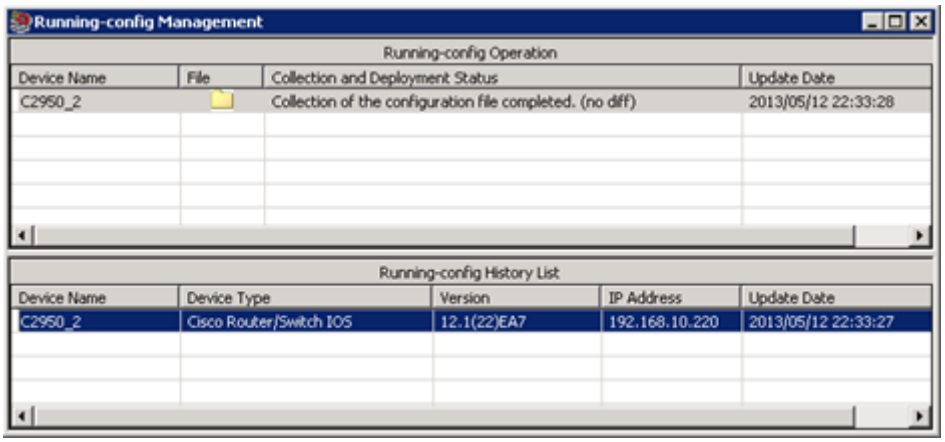
1. Open the "5.14.1.1 Running-config Management window (page 512)".

   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Running-config Management**.

2. In the Running-config Operation pane, select the target device.
3. In the Running-config History List pane, right-click a running-config file that has already been downloaded, and select **Apply Config** menu.

   It becomes a source of the running-config to be sent to the network device.

   The icon is displayed in the **File** column of the Running-config Operation pane to indicate that the file is registered on the manager.



4. In the Running-config Operation pane, right-click the device and select **Edit Config** menu.
5. The editor is opened. Edit the information that you want to upload and save it.

Caution

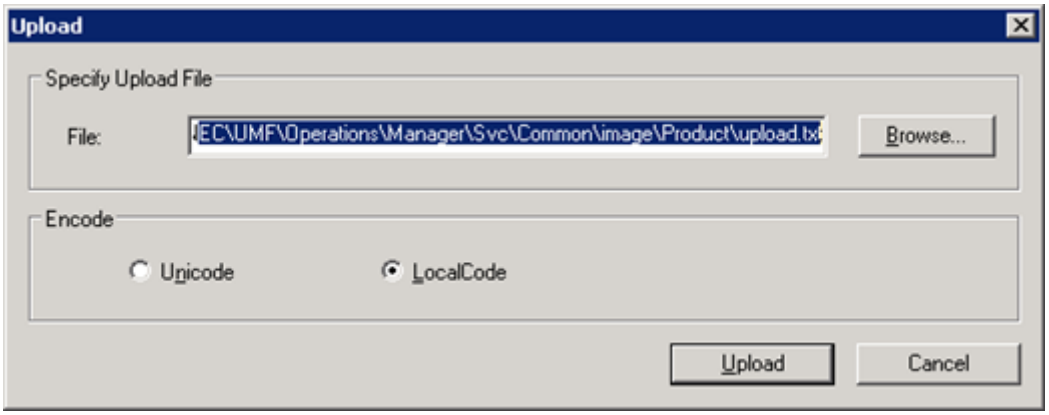
a. For device config management in the IP8800/700 series and the ES8800/1700 series, deployable files must start with "!\n" and end with "end\n".

b. When using the Catalyst operating system, they must begin with "begin\n".

The icon in the **File** column is changed to the icon, indicating that the file has been updated on the monitored terminal.

To discard the changes and delete the file, right-click the appropriate device and select **Discard Config** menu.

6. In the Running-config Operation pane, right-click the device and select **Upload** menu.
7. In the Upload dialog box, specify the file that you want to upload and the encoding type.



8. Click **Upload** button.

Running-config file is sent to the manager.

9. Upload the edited running-config information to the network device.
   - If you want to save the running-config to the startup-config after uploading, right-click the appropriate device and select **Deploy Config**>**Save to Startup-config**.
   - If you do not want to save the running-config to the startup-config after uploading, right-click the appropriate device and select **Deploy Config**>**Not Save to Startup-config**.

The changes are sent to the network device and the command is processed.

Caution

a. Text mode in the Catalyst operating system is not supported. However, if **Save to Startup-config** menu is selected, the write memory command is run without conditions.

b. If password information is updated when the configuration is reflected, the login settings must be reset with the updated information.

c. This operation may fail if the target device is in the process of installing software or performing commands from the command schedule. If you encounter this type of failure, try performing the operation again.

d. When deploying running-config for the following devices, the startup-config is also changed.

- IP8800/S300, S400, R400

e. In Cisco ASA 5500 multiple context mode, running-config for System configuration can be uploaded, but not for Admin contexts and general contexts.

f. When deploying running-config for PF6800, the following processing is performed.

i. Store the configuration file to be deployed in the candidate-configuration.

ii. Execute the commit command to reflect it in the running-configuration.

g. When deploying running-config for Juniper EX4200 (updating the active configuration), the following processing is performed.

i. Store the configuration file to be deployed in the candidate configuration. (The contents that was manually set to the candidate configurations before the processing will be cleared.)

ii. Execute the commit command to reflect in the running-configuration (active configuration).

h. When deploying running-config for BROCADE VDX 6720, consider the following important points.

- If the configuration for the stand-alone mode is deployed while BROCADE VDX 6720 is operating in the VCS mode, the operation mode needs to be changed from VCS mode to the stand-alone mode.
- "vcsid" and "rbridgeid" cannot be restored by deploying the running-config. Configure them manually before deploying the running-config.
- "snmp-server user" command cannot be restored by deploying the running-config. Configure it manually after deploying the running-config. (Since the password part show "*", it is necessary to enter the actual password manually.)

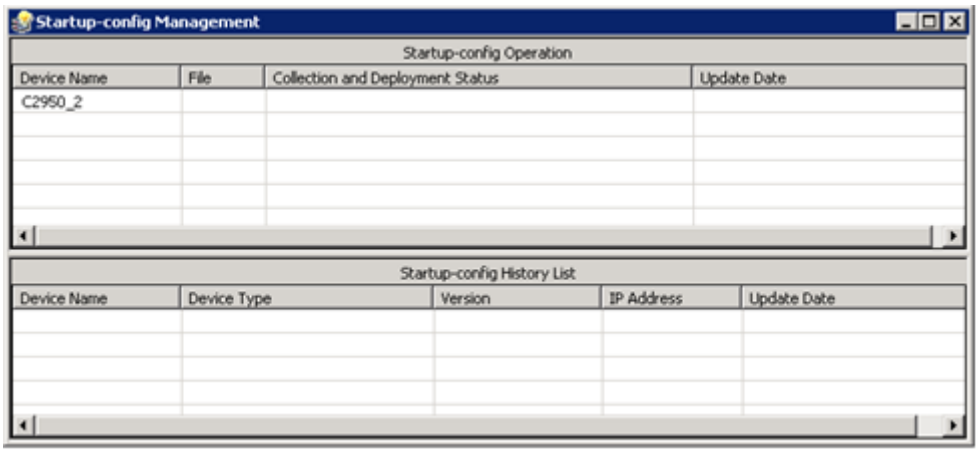
5.14.2 Managing startup-config

Manage the settings information (startup-config) applied to monitored devices the next time that they are started. Startup-config is managed in the "5.14.2.1 Startup-config Management window (page 520)".

5.14.2.1 Startup-config Management window

The Startup-config Management window is used to manage startup-config.

To open the Startup-config Management window, right-click the **NetworkView** icon or **NetworkManagement** icon or the map or device icon and select **Device Config Management**>**Startup-config Management**.



Startup-config Operation pane

- **Device Name**

  Displays the name of the device for which startup-config is being managed.

- **File**

  The icon is displayed if there are startup-configs in the manager that can be distributed. The icon is displayed if there are edited startup-configs on the monitoring terminal that have not been uploaded to the manager. In this case, an upload operation must be performed.

- **Collection and Deployment Status**

  Displays the startup-config collection and deployment results.

- **Update Date**

  Displays the date and time of the most recent file distribution.

Startup-config History List pane

- **Device Name**

  Displays the name of the nodes to which startup-config was distributed.

- **Device Type**

  Displays information about the device type, such as the model name.

- **Version**

  Displays the obtained version.

- **IP Address**

  Displays the IP address used for login.

- **Update Date**

  Displays the time that the startup-config history was created.

Menu displayed when right-clicking in the Startup-config Operation pane

- **Collect Config**

Obtains the startup-config from network devices. The collection results are displayed under **Collection and Deployment Status**.

- **Edit Config**

  Edits the file registered for distribution to network devices and saves it on the monitoring terminal. This operation changes the icon to  , indicating that there is a file that should be uploaded.

- **Discard Config**

  Deletes the file registered for distribution to network devices.

- **Deploy Config**

  - **Reboot Device**

    Sends registered files to network devices, updates startup-config and restarts the device.

  - **Not Reboot Device**

    Sends registered files to network devices and updates startup-config, but does not restart the device.

- **Upload**

  Sends files edited on the monitoring terminal to the manager. Files sent using this operation become the target files for sending to network devices.

- **Upper Bound of History**

  Specify an integer between 5 and 65,535 for the number of startup-config changes saved in the history. The default is 10.

Menu displayed when right-clicking in the Startup-config History List pane

- **Display Config**

  Shows the contents of the specified configuration.

- **Display History**

  Displays the view and edit window for the specified configuration history. For details, refer to "5.14.2.4 Managing startup-config history (page 524)".

- **Apply Config**

  Uses the configuration associated with the history information as the startup-config to be distributed to network devices, copies and registers it in the manager.

- **Export**

  Exports the configuration associated with the history information to the monitoring terminal.

- **Show Difference**

  Displays the differences between two separate sets of history information.

- **Delete History**

  Deletes the specified history information.

Caution

If the following operations are performed while this window is opened. The device list in this window is not updated immediately. To reflect changes, open this window again.

- Add and delete a device icon.
- Change a device name.
- Move an icon to another map.

5.14.2.2 Collecting startup-config

Collect startup-configs from the network devices.

Caution

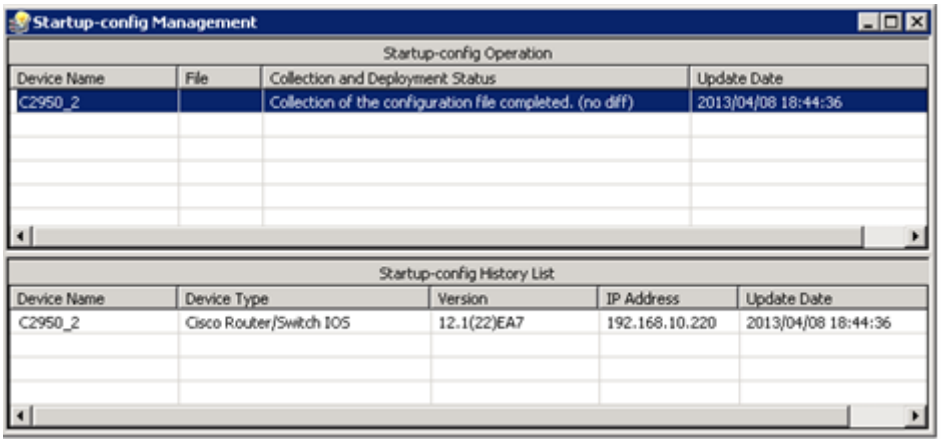
The maximum size of the supported startup-config file is 40MB.

1. Open the "5.14.2.1 Startup-config Management window (page 520)".

   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Startup-config Management**.

2. Right-click the node and select **Collect Config** menu.

   Startup-config is retrieved from the network device. The results are displayed in the **Collection and Deployment Status** column. In addition, the history of collected startup-configs is added to the Startup-config History List pane for that node.



Caution

a. Variances detected during the startup-configs collection are not added to the change management differences history. In addition, difference detection alert information is not issued.

b. This operation may fail if the target network device is in the process of installing software or performing commands from the command schedule. If you encountered this type of failure, try performing the operation again.

c. If the size of the startup-config exceeds 10MB, this operation may fail. In this case, the maximum memory size to be used in the Resource Manager function needs to be extended. To extend the maximum memory size, change "Xmx" value in the jservice.ini. For details, refer to "8.2.2 Extended Settings for the Resource Manager Function (page 682)".

d. If there are a lot of rows of PF6800 configuration setting, it may take a lot of time to complete collecting the configuration.

e. The configuration of FortiGate has only one type, and after setting of the configuration, it is automatically saved when changing the operation mode. Therefore, the Network Manager considers the configuration of FortiGate as a startup-config.

5.14.2.3 Viewing startup-config differences

Displays differences between configurations.

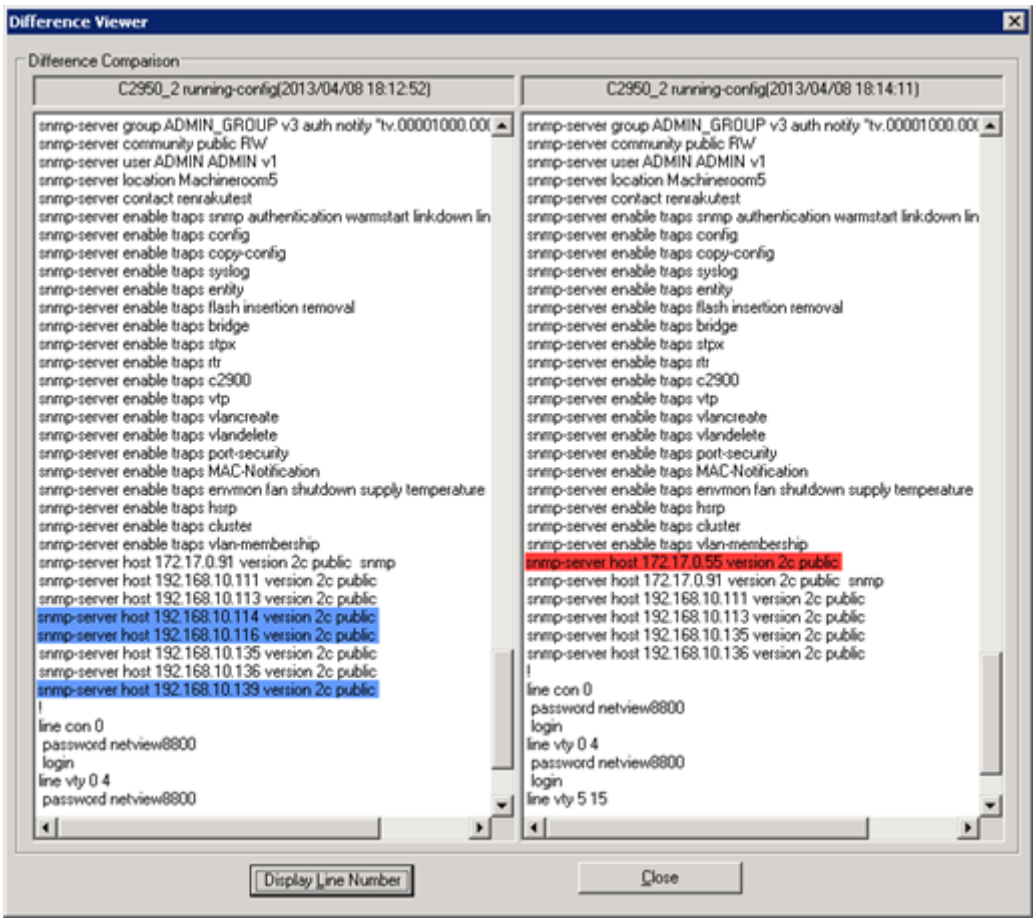
1. Open the "5.14.2.1 Startup-config Management window (page 520)".

   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Startup-config Management**.

2. In the Startup-config History List pane, specify any two startup-config histories by clicking them while pressing CTRL key,

3. Right-click and select **Show Difference** menu.

   The differences between two startup-configs are displayed.



The old startup-config is displayed to the left and the new startup-config is displayed to the right. Rows on the left side only are displayed with a blue background. Rows on the right side only are displayed with a red background.

Rows that have been updated are displayed on the left and right with a red or blue background. It is also possible to view the differences in startup-config histories between different devices. In this case, there is no distinction between old and new and the differences appear in the order in which they are displayed in the Startup-config History List pane.

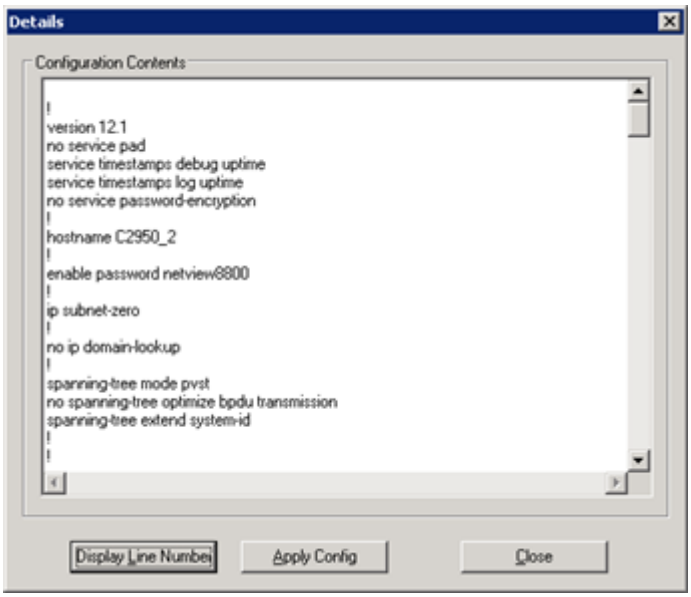
5.14.2.4 Managing startup-config history

In addition to displaying collected startup-config information, you can add notes as history and attach files as related information.

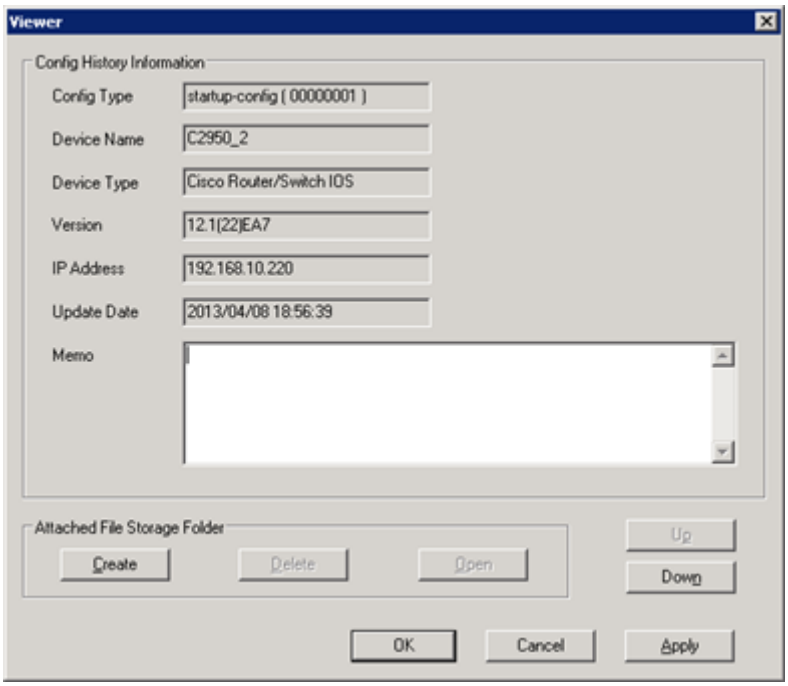
1. Open the "5.14.2.1 Startup-config Management window (page 520)".

   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Startup-config Management**.

2. To view startup-config information, right click the history that you want to view in the Startup-config History List pane and select **Display Config** menu.



3. To view startup-config properties, right-click the history in the Startup-config History List pane and select **Display History** menu.



Additional information for the startup-config can be entered in the **Memo** box as needed.

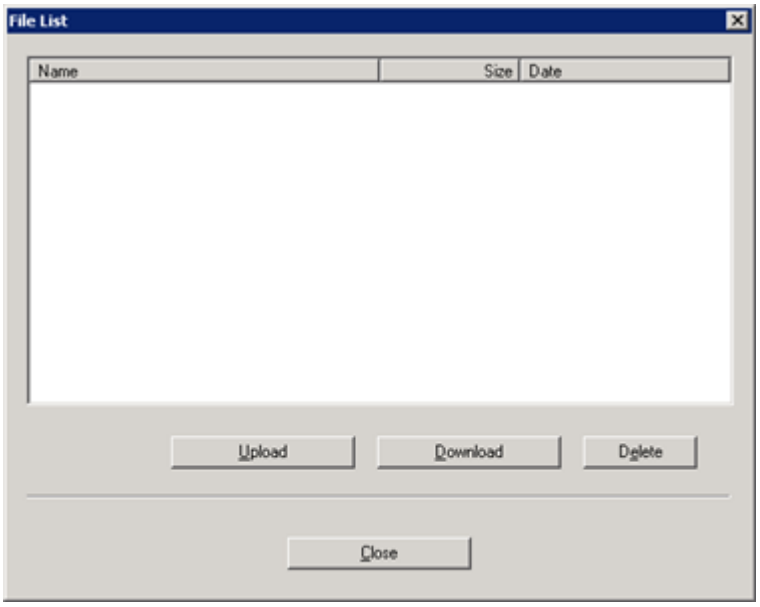
You can also store detailed information by files and associate it with the history.

a. In the **Attached File Storage Folder**, click **Create** button.

   Create a folder that can store the detailed information to correlate to the history.

b. In the **Attached File Storage Folder**, click **Open** button.

c. In the File List window, select **Upload** button to upload the file.



To download attached files, click **Download** button.

4. Download the configuration of the specified history to the monitoring terminal.

   a. Right-click the relevant history in the Startup-config History List pane, and select **Export**.

   b. In the Save As dialog box, specify the destination of storing history, click **Save** button.

   c. The startup-config is saved to the monitoring terminal.

5.14.2.5 Uploading startup-config

Startup-config files can be sent to a network device.

Caution

The maximum size of the supported startup-config file is 40MB.

Collect the startup-config in advance. For details, refer to "5.14.2.2 Collecting startup-config (page 523)".

You must first change to the "configuration mode (page 27)".

1. Open the "5.14.2.1 Startup-config Management window (page 520)".

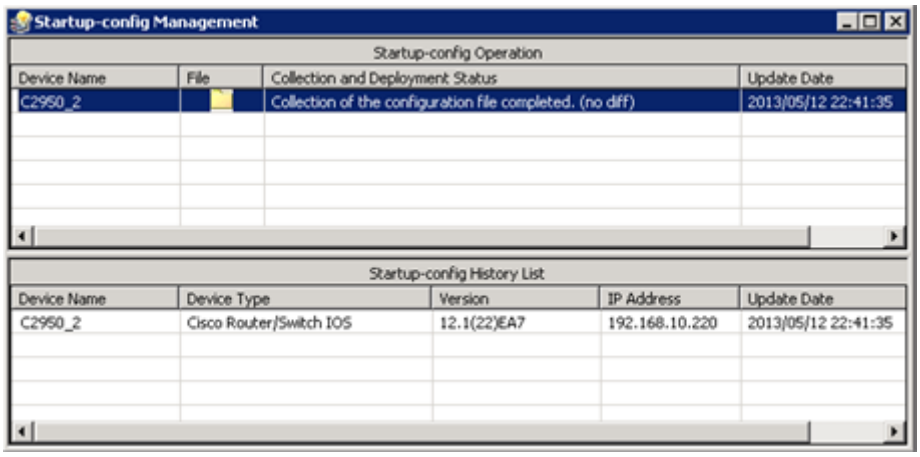
   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Startup-config Management**.

2. In the Startup-config Operation pane, select the target device.

3. In the Startup-config History List pane, right-click startup-config file that has already been downloaded, and select **Apply Config** menu.

   It becomes a source of the startup-config to be sent to the network device.

   The icon is displayed in the **File** column of the Startup-config Operation pane to indicate that the file is registered on the manager.



4. In the Startup-config Operation pane, right-click the device and select **Edit Config** menu.
5. The editor is opened. Edit the information that you want to upload and save it.

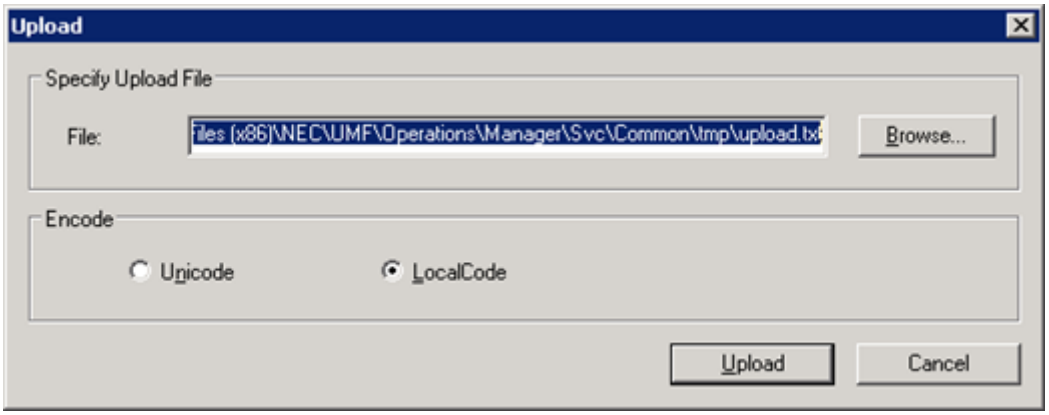
Caution

For the IP8800/700 series and the ES8800/1700 series, deployable files must start with "!\n" and end with "end\n".

The icon in the **File** column is changed to the icon, indicating that the file has been updated on the monitored terminal.

To discard the changes and delete the file, right-click the appropriate device and select **Discard Config** menu.

6. In the Startup-config Operation pane, right-click the device and select **Upload** menu.
7. In the Upload dialog box, specify the file to be uploaded and the encode type.



8. Click **Upload** button.

   Startup-config is sent to the manager.
9. Upload the edited startup-config information to the network device.
   - If you want to reboot the device after uploading,:

     Right-click the appropriate device and select **Deploy Config**>**Reboot Device**.
   - If you do not want to reboot the device after uploading:

     Right-click the appropriate device and select **Deploy Config**>**Not Reboot Device**.

The changes are sent to the network device and are saved ready for implementation when the device is restarted next.

Caution

a. For devices with multistage configuration, if the startup-config is deployed in a batch and the devices restarted, it is possible that the deployment and restart of distant devices will fail when relay devices are restarted.

b. If password information is updated when the configuration is deployed, the device must be restarted and then the login settings must be reset with the updated information.

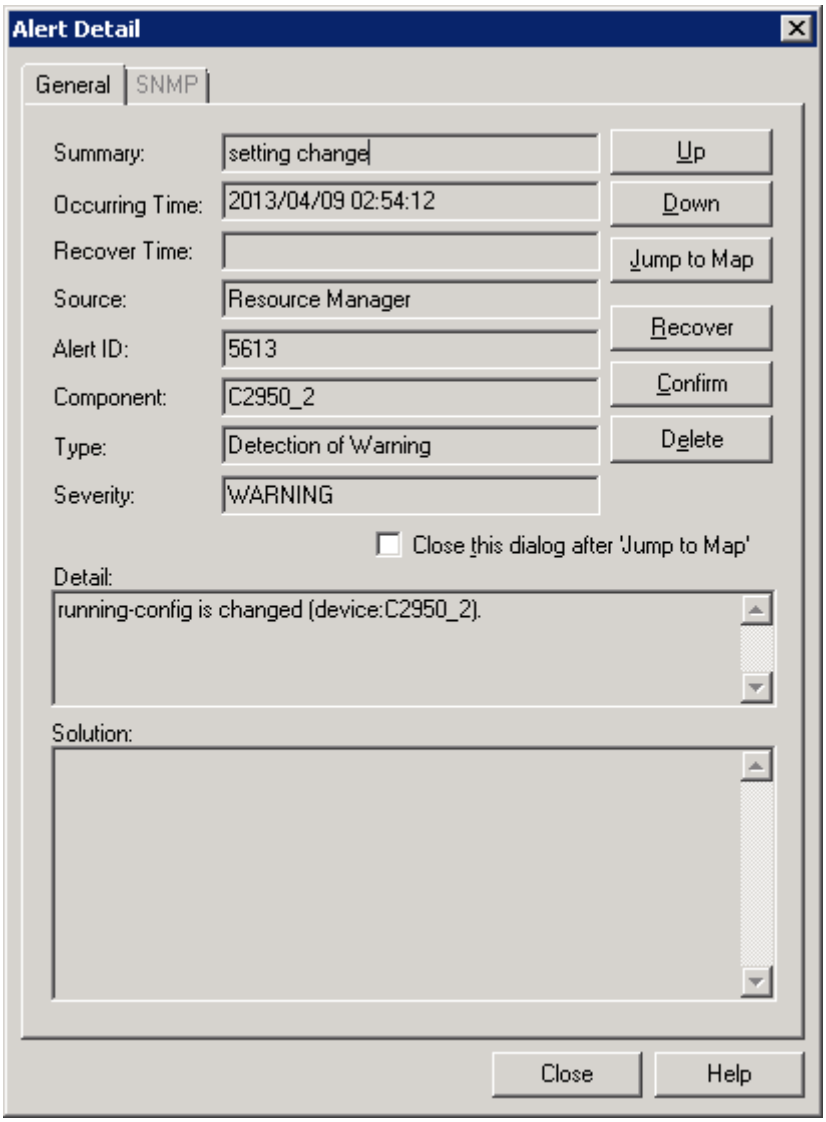
c. This operation may fail if the target device is in the process of installing software or performing commands from the command schedule. If you encounter this type of failure, try performing the operation again.

d. It will not be possible to schedule restarts for some devices (examples: the NEC IX and CX Series). These kinds of devices will be restarted immediately.

e. When the startup-config is deployed to QX-S5500 series devices that are configured as the stack configuration, it is deployed to only the master device. The startup-config on the slave device will be synchronized with the startup-config on the master device when the slave device is restarted. (This is the specification of the device.) When the role is switched between the master and slave device before synchronizing, the startup-configs deployed from Network Manager are not synchronized correctly after the devices are restarted.

5.14.3 Checking config differences in change monitoring

When monitoring config (running-config) changes with the alert display for detected changes enabled, an alert is reported in the Alert Management window and **Alert Management** tab when a config change is detected.

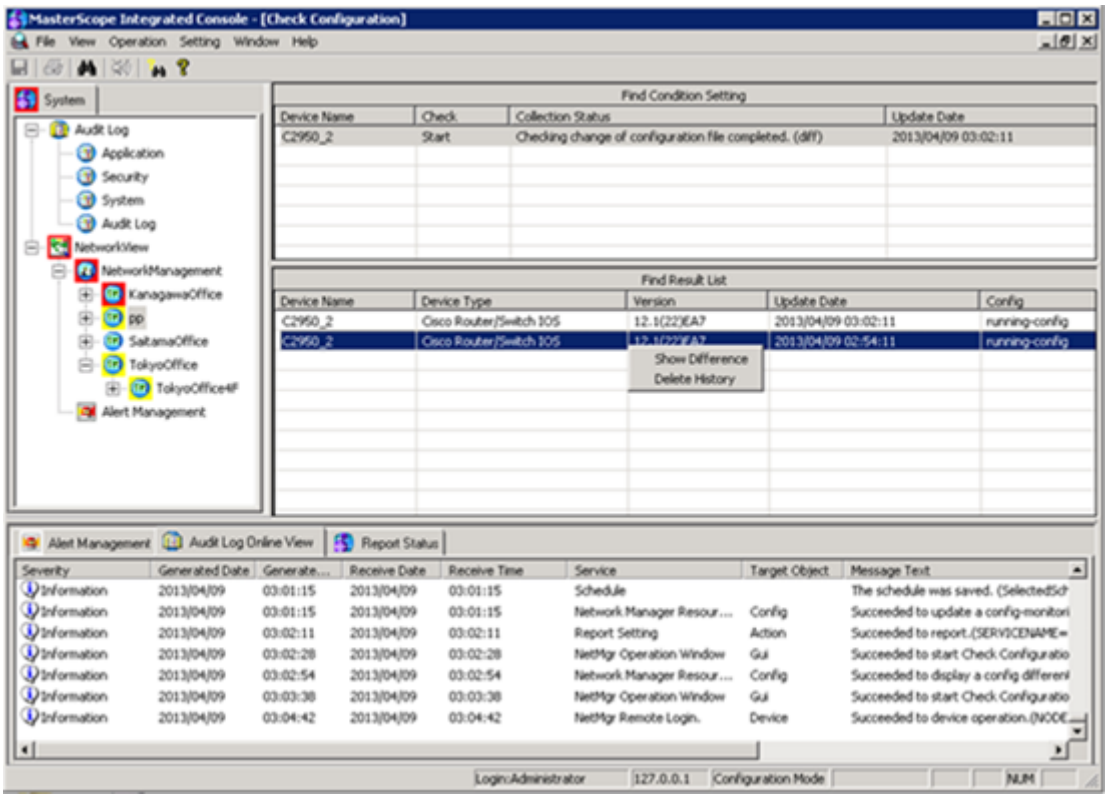


For information about config change monitoring settings, refer to "4.20.2 Monitoring configuration changes (page 404)". For information about alert reporting settings, refer to "4.20.5 Setting for sending an alert (page 414)".

The difference information of the detected running-config is displayed in the **Find Result List** pane of the Check Configuration window.

1. Open the Check Configuration window.

   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Device Config Management**>**Check Configuration**.



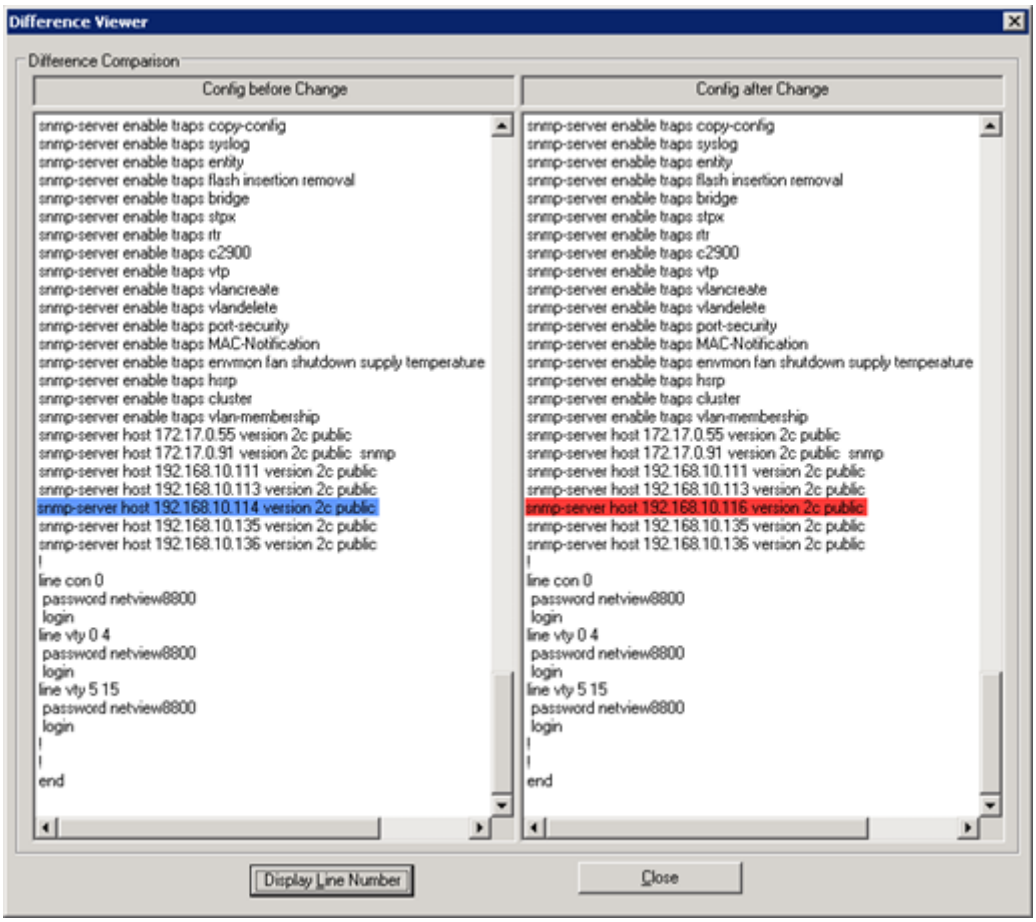
2. Right-click the row of the difference information that you want to view and select **Show Difference** menu.

   Difference information is sorted by dates. (The latest is at the top.)

Tip

To delete the difference information, select **Delete History** menu.

The difference information is displayed.



The old running-config is displayed to the left and the new running-config is displayed to the right. Rows that appear on the left side only are displayed with a blue background. Rows that appear on the right side only are displayed with a red background. Rows that have been updated are displayed on the left and right with a red or blue background.

5.15 Managing Device Software (Resource Manager)

Device software is managed through the File Management window. For details, refer to "5.15.1 Managing software files (page 531)".

Device software is distributed in the Software Upgrade window. For details, refer to "5.15.2.1 Deploying a software file (page 543)".

5.15.1 Managing software files

In Network Manager, you can deploy and install software to network devices. You can also manage software files by device model and version.

To distribute software to the network device, you need to first register (upload) a software file For details, refer to "5.15.1.1 Uploading a software file (page 539)".

A backup file when a registered file or software is distributed can be download later. For details, refer to "5.15.1.2 Downloading a software file (page 541)".

Caution

Using file management, the model and version are determined based on the software file name. For this reason, if the file name is changed to something other than the name provided by the vendor, this function may not operate properly.

The software names recognized by Network Manager are those in the following formats listed below. The software must be registered again if the name is changed.

Device	Software file name format
NEC	
IP8800/ SS1200(AX1200S), S2200(AX2200S) series [1)]	Software is provided with the AX12L20101C-43.bin / AX2230L20204A-48.bin file name. The file name starts with "AX12" or "AX2230" and ends with ".bin". The numbers following "L2"indicate the version. The characters from the hyphen (-) to ".bin" indicate the build number. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
IP8800/S2400(AX2400S), S3600(AX3600S) series [1)]	The format is AX36L31000-128.img.gz or AX24L21000A-240.img.gz. The numbers following "AX36L3" or "AX24L2" to a hyphen (-) indicate the version. The characters from the hyphen (-) to "img.gz" indicate the build number. AX36L31000-128.img.gz is the OS 10.0 Build128 for IP8800/S3630 (AX3630S). In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
IP8800/S2500(AX2500S) series [1)]	Software is provided with AX2530L20300A-136.bin file name. The file name starts with "AX2530L2" and ends with ".bin". The underscore (_)-separated characters following "AX2530L2" indicate the version. The characters from the hyphen (-) to ".bin" indicate the build number. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
IP8800/S6300 (AX6300S), IP8800/ S6700 (AX6700S) series [1)]	Software is provided with AX63S1101D-66.img.gz file names. The file name starts with "AX6" and ends with ".img.gz". The numbers following "AX63S" to "-" indicate the version. The characters from the hyphen (-) to ".img.gz" indicate the build number. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
IP8800/S8300 (AX8300S) series [1)]	Software is provided with AX83S1206-319.img file names. The file name starts with "AX83" and ends with ".img". The numbers following "AX83S" to "-" indicate the version. The characters from the hyphen (-) to ".img" indicate the build number. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
IP8800/S8600 (AX8600S) series [1)]	Software is provided with AX86S1207C-409.img file names. The file name starts with "AX86" and ends with ".img". The numbers following "AX86S" to "-" indicate the version. The characters from the hyphen (-) to ".img" indicate the build number. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
QX-S series	The format is QX-S3026-V214.bin. The three digits following "-V" indicate the version.

Device	Software file name format
	QX-S3026-V214.bin is the QX-Switch3026 Version 2.1.4. The extension is .bin or .app. In Network Manager, information other than the model, version and extension is not recognized, so character strings other than these are not considered.
QX-S5900/PF5459	Software is provided in a file named PF5459-V714.ipe. The three digits following the "-V" in the file name indicate the version. Thus, PF5459-V714.ipe is PF5459 Version 7.1.4. The extension is .ipe. In Network Manager, information other than the model, version, and extension is not recognized, so character strings other than these are not considered.
IX1000, 2000, 3000 Series	The format is ix1000-ds-6.1.13.ldc or ix2000-ds-6.1.13.ldc. The numbers following "ds-" indicate the version. ix1000-ds-6.1.13.ldc is IX1000 Version 6.1.13. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
PF5200 series	Software is provided with the PF52L3PE-V1.0.0.0-5.img file names. The file name starts with "PF52L3PE", and ends with ".img. The characters between "-V" and "-" indicate the version. The characters from "-" to ".img" indicate the build number. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
WA series	Software is provided with the program file name wa1020_4_4_3.bin for WA1020, wa2020_4_4_3.bin for WA2020, wa2021_4_4_3.bin for WA2021. The file name starts with "wa*xxxx*_", and ends with ".bin". The underscore(_)-separated characters following "wa*xxxx*_" indicate the version. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
NEC Express5800/110Ba-e3/120Ba-4	The format is ml-2.2.16-r.mai/des or sl-2.2.16-r.mai/des. The numbers from "ml-" (or "sl-") to "-" indicate the version. ml-2.2.16-r.mai is Version 2.2.16. In Network Manager, information other than the version is not recognized so character strings other than these are not considered. Supplement: The software configuration definition file (*.des file) and main software image (*.mai file) must be registered in file management.
Express5800/ SWM-BNT	The file name is SWM-BNT_100.bin. The characters from "SWM-BNT_" to ".bin" indicate the version. Therefore, SWM-BNT_100.bin is Version 1.0.0. In Network Manager, information other than the model and version is not recognized, so character strings other than these are not considered.
QX-R series	The format is QX-R2809-V123.bin. The three digits following "-V" indicate the version. QX-R2809-V123.bin is the QX-Router2809 Version 1.2.3. The extension is .bin or .app. In Network Manager, information other than the model, version and extension is not recognized, so character strings other than these are not considered.
IP8800/S300 series	Software is provided with ssa093.tgz and ssb093.tgz file names. The numbers following ssa or ssb indicate the version number.

Device	Software file name format
	In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
IP8800/S400 series	Software is provided with ysa093.tgz and ysb093.tgz file names. The numbers following ysa or ysb indicate the version number. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
IP8800/R400 series	Software is provided with yra093.tgz and yrb093.tgz file names. The numbers following yra or yrb indicate the version number. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
IP8800/700 series	The format is hr410230.gz or gr520150.gz. The first two characters show the machine rank. The following three numbers indicate the version. The next three numbers indicate the edition. gr520150.gz is the R5.2 (ed. 15) HI end model. hr: IP8800/700 710A, 720, 730, ES8800 gr: IP8800/700 735, 740, 750
IP8800/620 series	The file name is ip88_600_V160ed27.img. The characters from "_V" to ".img" indicate the version. Therefore, ip88_600_V160ed27.img is IP8800/600 Version 1.60 (ed27). In Network Manager, information other than the model and version is not recognized, so character strings other than these are not considered.
IX5000, 5500 series	For the IX5000 and IX5500 Series, software is provided with the image.dat file name. However, version management, and the management of multiple files with different versions, cannot be performed when all the image.dat files have the same name. For this reason, you must change the file names in accordance with the following naming rules. The four digits following "ix5_" indicate the version. For example, for a version 8.4.02 image.dat, change the name to: "ix5_8402.dat" Similarly, when backing up software on a device, perform the backup using a file name based on the same naming rule. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
CX2610 series	The format is cx2610_Ver040412.dat. The numbers following "Ver" indicate the version. cx2610_Ver040412.dat is the CX2610 Version 04.04.12. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
CX-Hammernet uH24	CX-Hammernet The format is uh24_v1.3_14.bin. The numbers from "_v" to ".bin" indicate the version. uh24_v1.3_14.bin is Version 1.3 (N Build 0014). In Network Manager, information other than the version is not recognized so character strings other than these are not considered.
CX2600/220	There are three types of software distribution possible for the CX2600/220. These are soft distribution, line distribution and UGSW distribution. The software naming rules for each of these are as follows. • If the file name starts with "soft_", a soft distribution is performed. soft_030112.dlm is Version 03.01.12.

Device	Software file name format
	• If the file name starts with "line_" a line distribution is performed. Line distribution has options, so the file name will be: line_option_version.dlm line_gbe_050404.dlm is Version 05.04.04. • If the file name starts with "ugsw_" a UGSW distribution is performed. ugsw_030101.dlm is Version 03.01.01. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
MA155MX/4E	The format is ip88_600_V160ed27.img. The characters from "_V" to ".img" indicate the version. ip88_600_V160ed27.img is the IP8800/600 Version 1.60 (ed27). In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Cisco Systems	
Cisco router, Catalyst series(IOS)	The format is c4500-is-mz.121-20.bin/tar or c2950-i6q412-mz.121-13.EA1.bin/tar. The numbers following the initial "c" indicate the model. The two numbers connected by a hyphen (-) indicate the version. c4500-is-mz.121-20.bin is the Model c4500 IOS 12.1 (20). In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Cisco Catalyst series(Catalyst OS)	The format is cat4000.4-4-1.bin or RTSYNC_cat6000-sup2_6-4-4a.bin. The numbers following "cat" indicate the model. The three numbers connected by a hyphen (-) indicate the version. cat4000.4-4.1.bin is the Model 4000 CatOS 4.4(1). In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Cisco Catalyst series(IOS-XE)	The format is cat3k_caa-universalk9.16.06.03.SPA.bin or cat4500e-universal.SPA.03.06.08.E.152-2.E8.bin/tar. The characters following the initial "cat" indicate the model. The three numbers after the first dot (.) indicate the version. cat3k_caa-universalk9.16.06.03.SPA.bin is the Model Catalyst3850/3650 IOS-XE 16.6(3). In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Cisco Nexus5000 series	Software is provided with the n5000-uk9.4.1.3.N1.1a.bin / n5000-uk9-kickstart.4.1.3.N2.1a.bin file name. The file name starts with "n5000" and ehds with ".bin". The dot(.)-separated characters from "n5000-" to "." indicate the version.
Cisco Nexus7000 series	Software is provided with the n7000-s1-dk9.5.0.3.bin / n7000-s1-kickstart.5.0.3.bin file name. The file name starts with "n7000" and ends with ".bin". The dot (.)-separated characters following "n7000-" indicate the version.
Cisco ASR 920, 1000 series	Software is provided with the asr1000rp1-adventerprisek9.03.02.00.S.151-1.S.bin file name. The digits following "asr" indicate the model. The hyphen (-)-separated numbers indicate the version. For example, asr1000rp1-adventerprisek9.03.02.00.S.151-1.S.bin means the model "asr1000" and the version "15.1(1)".

Device	Software file name format
	In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Cisco ASA 5500 series	Software is provided with the asa822-k8.bin file name. The file name starts with "asa" and ends with ".bin". One digit (if version length is three) or two digits (if version length is four) indicate the major version, a next digit indicates the sub version, and after the next two digits indicate the minor version.
Cisco PIX Firewall series	The format is pix604.bin. The three digits following "pix" indicate the version. pix604.bin is Version 6.0(4). In Network Manager, information other than the version is not recognized, so character strings other than these are not considered.
Cisco Aironet1100, 1200 siries	The format is c1130-k9w7-mx.123-2.tar. The numbers following the initial "c" indicate the model. The two numbers connected by a hyphen (-) indicate the version. c1130-k9w7-mx.123-2.tar is the Aironet1130 Model IOS 12.3 (2). In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Brocade Communications Systems	
Brocade ICX 6000 series	Software is provided with the icx64r07400a.bin icx64s07400a.bin file names. The file name starts with "icx64r" or "icx64s" and ends with ".bin". The version of icx64r07400a.bin is 07.4.00. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Brocade FastIron SX series	Software is provided in files named sxs07400a.bin, sxl07400a.bin, and sxr07400a.bin. The file name starts with "sxs", "sxl", or "sxr" and ends with ".bin". The version of sxs07400a.bin is 07.4.00. In Network Manager, information other than the model and version is not recognized, so character strings other than these are not considered.
Brocade FastIron WS series	Software is provided in files named fws07400a.bin, fwsl07400a.bin, and fwsr07400a.bin. The file name starts with "fws", "fwsl", or "fwsr" and ends with ".bin". The version of fws07400a.bin is 07.4.00. In Network Manager, information other than the model and version is not recognized, so character strings other than these are not considered.
Brocade TurboIron 24X	Software is provided in files named tis07400a.bin and tir07400a.bin. The file name starts with "tis" or "tir" and ends with ".bin". The version of tis07400a.bin is 07.4.00. In Network Manager, information other than the model and version is not recognized, so character strings other than these are not considered.
Brocade FCX series	Software is provided in files named fcxs07400a.bin and fcxr07400a.bin. The file name starts with "fcx" and ends with ".bin". The version of fcxs07400a.bin is 07.4.00. In Network Manager, information other than the model and version is not recognized, so character strings other than these are not considered.

Device	Software file name format
Foundry FastIronEdge series	The format is fexr02000a.bin. The five digits following "fexr" indicate the version. fexr02000a.bin is 02.0.00. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Brocade ServerIron, BigIron series	The format is BIR07105.bin or SLB07015.BIN. The five digits following the three ASCII characters indicate the version. SLB06015.bin is 06.0.15. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
A10 Networks	
AX series	Software is provided with the ax_upg_2_2_5-p1_20.tgz/ ax2k_upg_1_2_7_476.tgz file name. The file name starts with "ax" and ends with ".tgz". The underscore (_)-separated characters following "_upg_" indicate the version.
Thunder ADC series	Software is provided in files named ACOS_FTA_2_7_1-GR1_58.64.tgz and ACOS_non_FTA_2_7_1-GR1_58.64.tgz. The file name starts with "ACOS" and ends with ".tgz". The characters after "_FTA_" of each file name, separated by "_", indicate the version.
Juniper Networks	
EX4200	Software is provided with the jinstall-ex-4200-10.4R10.7-domestic-signed.tgz file names. The file name starts with "jinstall-ex-4200-", and ends with ".tgz". The numbers between "jinstall-ex-4200-" and "- domestic" indicate the version. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Hitachi Metals	
APRESIA series	Software is provided with the aeosR71201.img / aeosR71201-loader.img file name. The file name starts with "aeos" and ends with ".img" or "-loader.img". Two characters "Rx" following "aeos" indicate the major version, next two digits indicate the sub version, and after the next two digits indicate the minor version.
Citrix Systems	
Citrix NetScaler MPX series	Software is provided with the build-9.2-49.8_nc.tgz file names. The file name starts with "build", and ends with ".tgz". The characters between "build-" and "-" indicate the version. The characters from "-" to "_nc" indicate the build number. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
YAMAHA	
RT series	The format is rt200i_Ver040054.bin. The six digits following "_Ver" indicate the version. rt200i_Ver040054.bin is the RT200i Version 04.00.54. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.

Device	Software file name format
HP	
HP Procurve2510	Software is provided with the Y_11_12.swi file names. The file name starts with "Y_", and ends with ".swi". The numbers prior to ".swi" indicate the version. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
HP A3100-8 v2 EI Switch, HP A3100-16 v2 SI Switch, HP A5120-24G SI Switch	For the HP 3100 series, software is provided in files named A3100V2-CMW520-R5202.bin. For the HP 5120 series, software is provided in files named A5120SI-CMW520-F1513P02.bin. The file name starts with "A3100V2" or "A5120SI" and ends with ".bin". The "***" portion of the "-CMW***-" following "Axxx" indicates the version. Therefore, A3100V2-CMW520-R5202.bin is Version 5.20 of the software for HP 3100 series. In Network Manager, information other than the model and version is not recognized, so character strings other than these are not considered.
HP BL10e	The format is eGbE201.bin. The three digits following "eGbE" indicate the version. eGbE201.bin is Version 2.0.1. In Network Manager, information other than the version is not recognized so character strings other than these are not considered.
HP BL20p	The format is pGbE2_b_113.bin. The three digits following "pGbE" indicate the version. eGbE2_b_113.bin is Version 1.1.3. In Network Manager, information other than the version is not recognized so character strings other than these are not considered.
Extreme Networks	
Summit24, 1i	The format is V700b68.xtr or S712b20.xtr. The version is from the second character through to the period (.). V701b50.xtr is 7.0.1b50. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Seiko Instruments	
NS series	The format is ns2484_10_V20.bin. The two digits following "-V" indicate the version. ns2484_10_V20.bin is the ns2484 Version 2.0. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.
Lucent Technologies	
MAX series	The format is IP28X_V6.1.24.bin. The numbers from "_V" to ".bin" indicate the version. IP28X_V6.1.24.bin is the IP28X Version 6.1.24. In Network Manager, information other than the model and version is not recognized so character strings other than these are not considered.

1) Of the device types shown as supported on the monitoring terminal, the UNIVERGE IP8800/S2400, S2500, S3600, S6300, S6700, S8300, S8600 and SS1200 Series NEC products have been combined with

the ALAXALA Networks Corporation AX Series products and appear as "NEC (ALAXALA) - IP8800S (AX)". This is because the functions supported by Network Manager are the same for both.

5.15.1.1 Uploading a software file

To distribute software, first use the **File Management** menu to register the software in the manager. Then, use the **Software Upgrade** menu to distribute the software to network devices. This section describes how to register (upload) a software file to the manger.

Software files of the network device need to be stored on the monitoring terminal in advance. Since the model and the version are decided from the software file name, put the correct file name and store it. For details, refer to "5.15.1 Managing software files (page 531)".

You must first change to the "configuration mode (page 27)".

1. Open the File Management window.

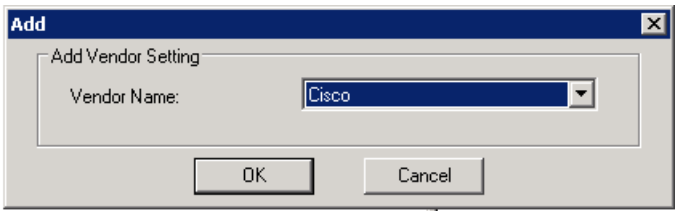
   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Software Management**>**File Management**.

   Only NEC is registered in the default settings.

2. Register the vendor of the network device that you want to manage.

   Right-click the **Software** icon in the tree and then select **Add** menu.

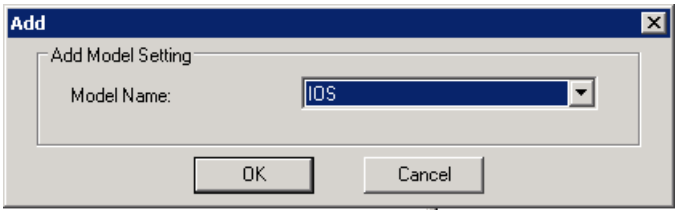
3. In the Add dialog box for the vendor selection, select the vendor that you want to add and click **OK** button.



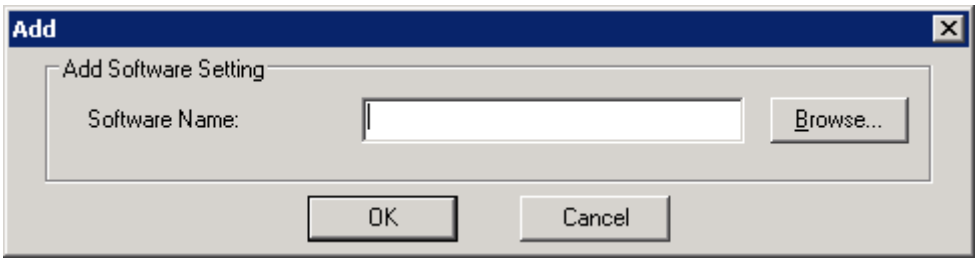
4. Depending on the vendor, you may need to select a model next.

   Right click the vendor name icon and select **Add** menu.

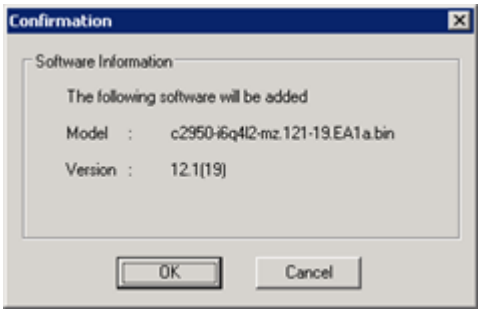
   In the Add dialog box for the model selection, select the model that you want to add and click **OK** button.



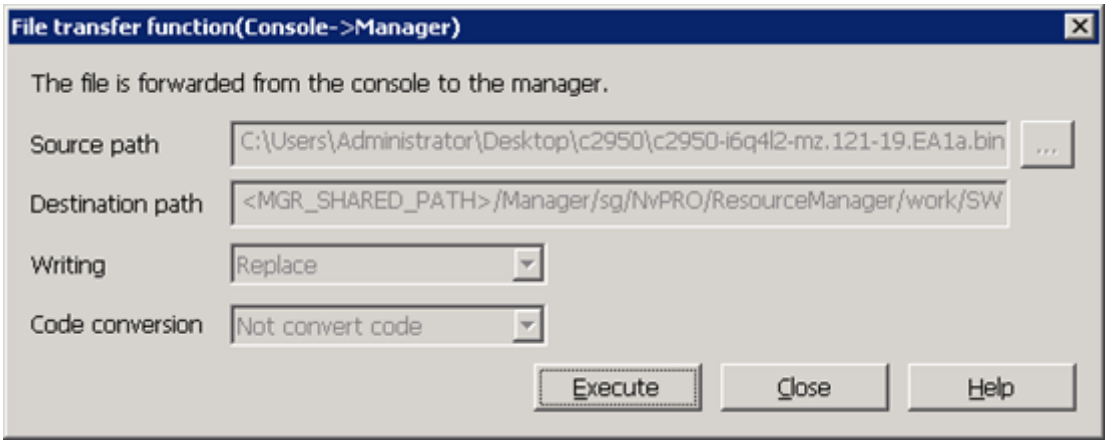
5. Right-click the vendor name or model name and click **Add** menu to display the Add dialog box for software to be deployed.



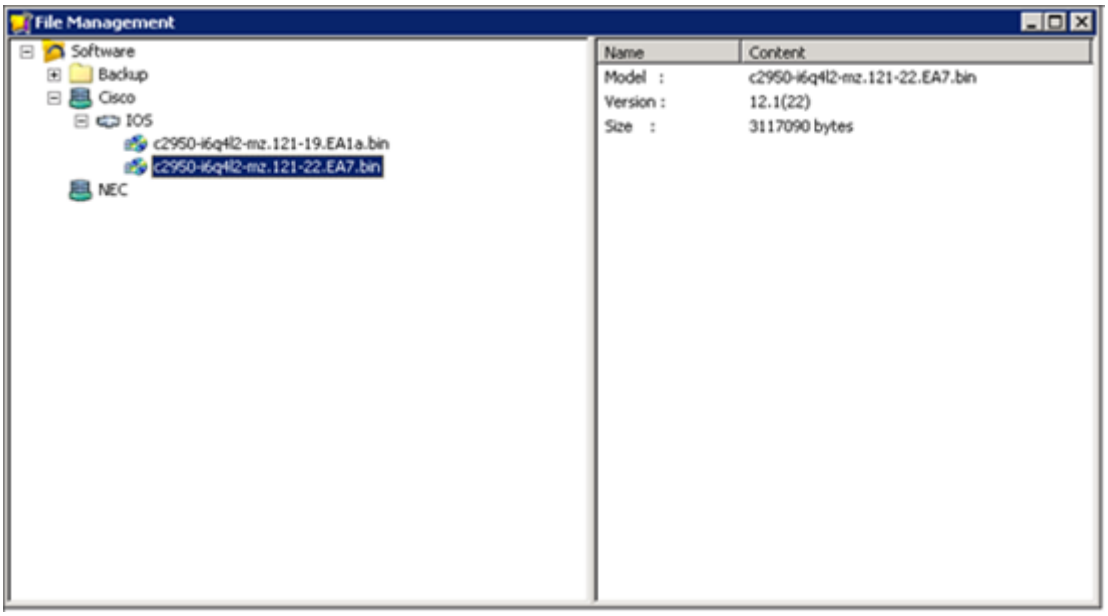
6. Specify the software file that is stored on the monitoring terminal and click **OK** button.
7. The confirmation dialog box is displayed for confirming the software that you want to register. Verify the information and click **OK** button.



8. In the "5.15.1.3 File transfer function dialog box (page 542)", click **Execute** button without making any changes.



The software is transferred from the monitoring terminal to the manager and stored on the manager. The registered file is displayed in the window.



5.15.1.2 Downloading a software file

You can download the software stored on the manger and the backup software in installation to the monitoring terminal.

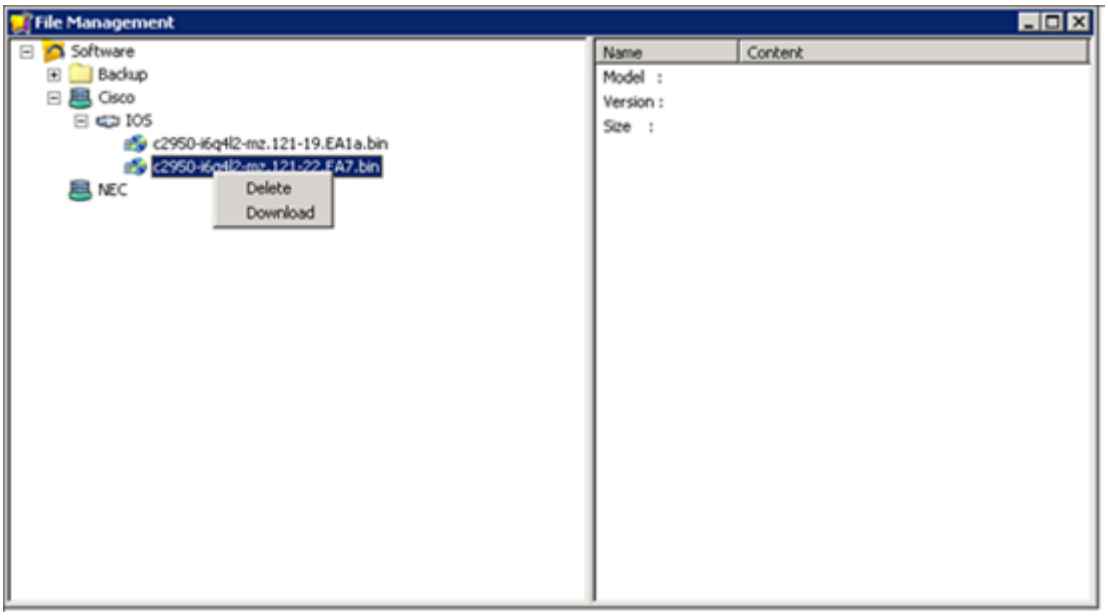
You must first change to the "configuration mode (page 27)".

1. Open the File Management window

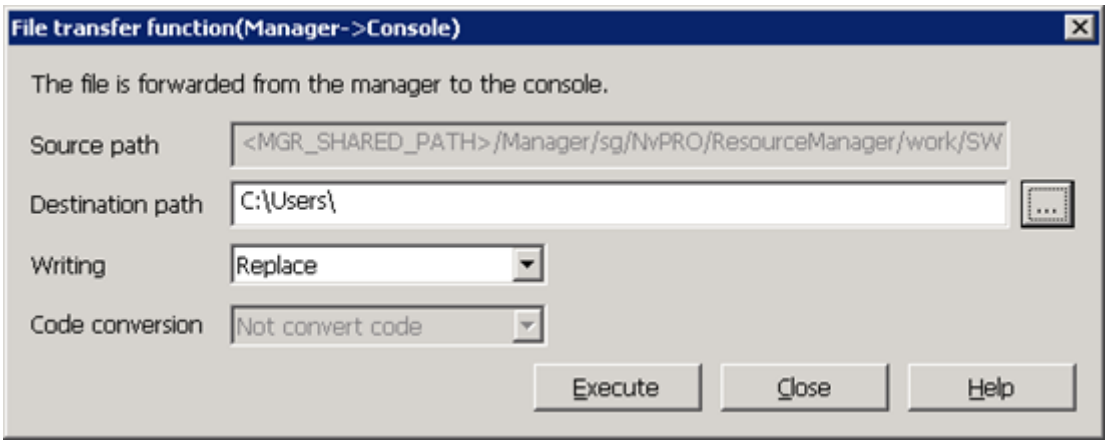
   Right-click the **NetworkView** icon or **NetworkManagement** icon, and select **Software Management**>**File Management**.

2. Right-click the name of the software and select **Download** menu.

   Software backed up at the time of installation is displayed below the **Backup** icon in the tree.



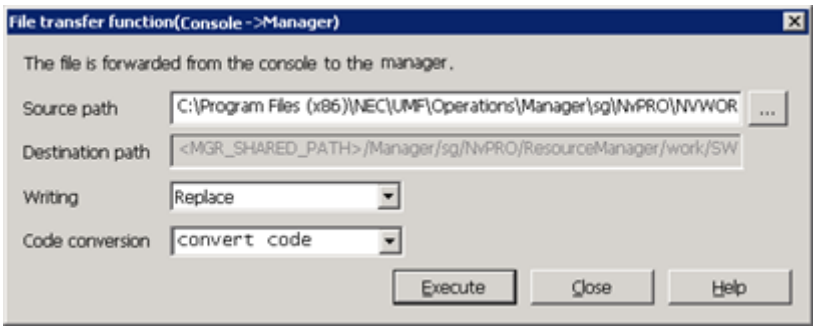
3. In the "5.15.1.3 File transfer function dialog box (page 542)", specify the **Destination Path** and click **Execute** button.



The software is transferred from the manager to the monitoring terminal and stored on the monitoring terminal.

5.15.1.3 File transfer function dialog box

The File transfer function dialog box is accessed through the file management function.



- **Source Path**

  Specify the absolute path of the file that you want to transfer. The path can be a character string containing up to 260 single-byte alphanumeric characters or symbols. If multi-byte characters, or more than 260 characters are specified, the transfer may fail.

- **Destination Path**

  Specify the file name or folder name that you want to use for saving the file that is being transferred. If the last character in the specified character string is "\", it will be treated as a folder name. The path can be a character string containing up to 260 single-byte alphanumeric characters or symbols. If multi-byte characters, or more than 260 characters are specified, the transfer may fail.

- **Writing**

  If a file or folder already exists with the same name as the name specified in the **Destination Path**, the action is different depending on whether a file name or a folder name was specified in the **Source Path**.

  - If a file name was specified in **Source Path**:

    New :

    The file transfer is not performed.

    Replace :

The file is overwritten.

Append :

If a folder name was specified for the transfer destination, the file transfer is not performed.

- If a folder name was specified in **Source Path**:

New :

The file transfer is not performed.

Replace :

The existing folder is deleted and replaced with the transfer source folder.

Append :

The folder is overwritten.

- **Code conversion**

Specify whether or not to convert the code when transferring the file.

Convert code :

If the operating system for the manager is not Windows, the code is converted.

Not convert code :

The code is not converted.

- **Execute** button

Performs the transfer.

- **Close** button

Closes the dialog box.

- **Help** button

Displays Help.

5.15.2 Deploying device software

5.15.2.1 Deploying a software file

Set the monitoring mode of the target device to "ON". For details, refer to "5.13 Starting or Stopping Monitoring by the Monitoring Mode (page 505)".

⚠ Caution

Software can be distributed even if the monitoring mode is set to "OFF". However, the system cannot detect whether the distribution was successful or not, and cannot update the **Software Version** property.

Upload software in advance. For details, refer to "5.15.1.1 Uploading a software file (page 539)".

You must first change to the "configuration mode (page 27)".

1. Open the Software Upgrade window.

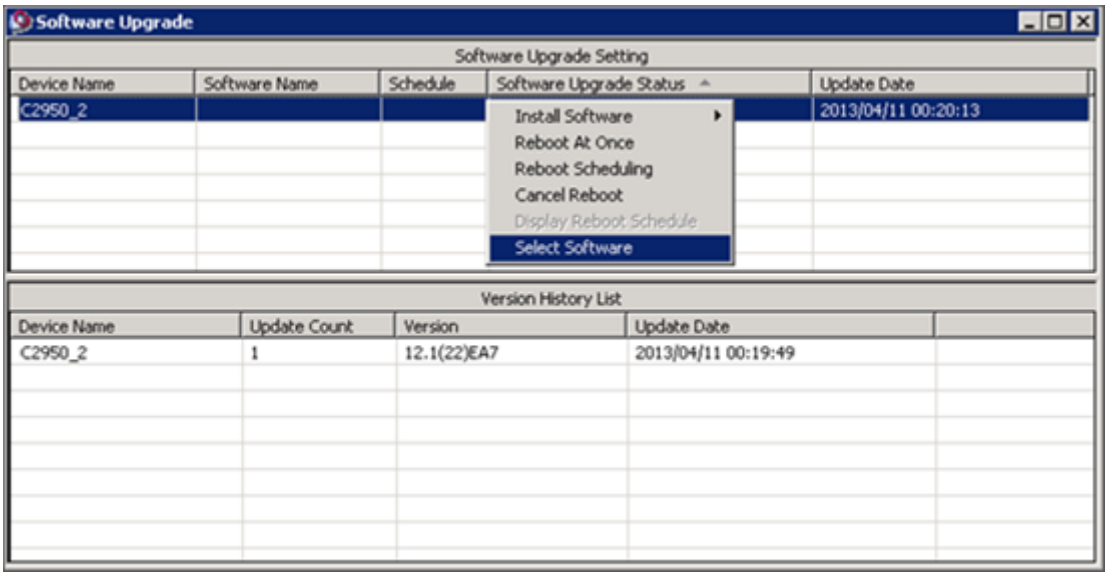
   Right-click the **NetworkView** icon, the **NetworkManagement** icon, the map icon, or device icon. Select **Software Management**>**Software Upgrade**.

Caution

If the following operations are performed while this window is opened. The device list in this window is not updated immediately. To reflect changes, open this window again.

- Add and delete the device icon.
- Change the device name.
- Move an icon to another map.

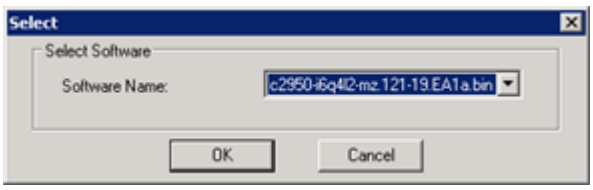
2. Right-click the network devices to which you want to distribute the software and click **Select Software** menu.



Tip

You can select multiple devices and apply the settings to all selected devices at once.

The Select dialog box is displayed with a list of software.



3. In the Select dialog box, select the applicable software and click **OK** button to register the software file that you want to distribute.

   The software to be distributed is registered.

4. After registering the file and distributing it to the network device, restart.

   You can select from the following restart options.

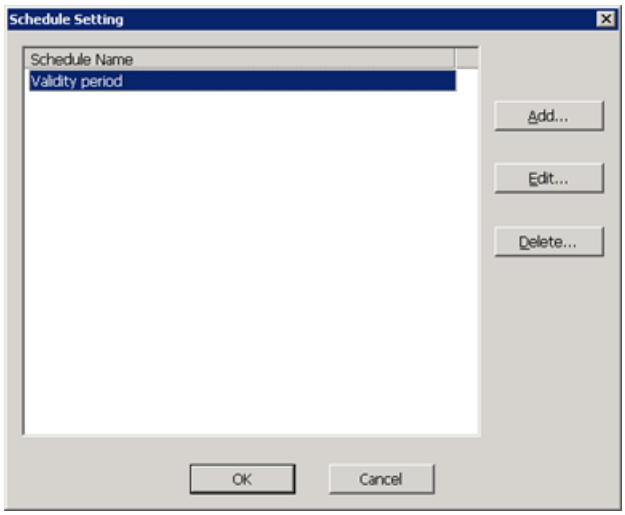
   - **Install Software>Reboot At Once**

     Distributes software and reboots the device immediately.

   - **Install Software>Reboot Scheduling**

     Distributes software immediately, and reboots the device at a specified time.

     The Scedule Setting dialog box is displayed.

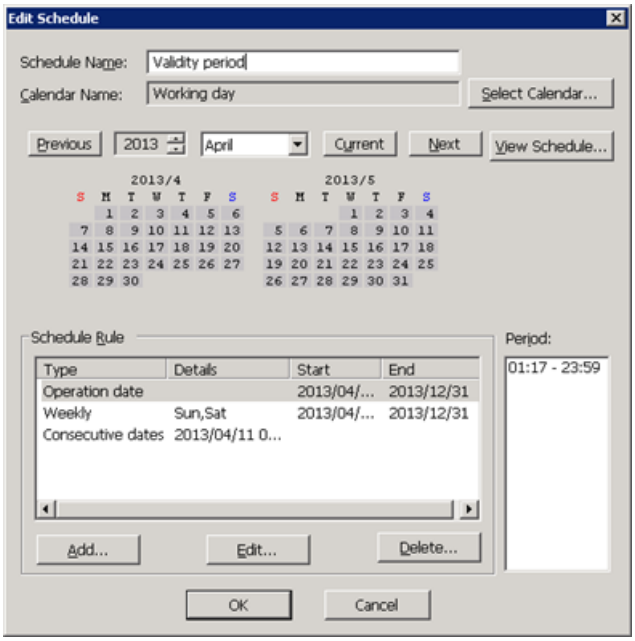


- To use a schedule that has already been set up

  Select the schedule in the **Schedule Name** column and click **OK** button.

- To create a new schedule

  Click **Add** button to open the Edit Schedule dialog box. Enter the necessary settings and click **OK** button.



As soon as the schedule has been set, **Start** is displayed in the **Schedule** column. To set the schedule, refer to "4.22.2 Setting a time schedule (page 435)".

- **Install Software>Not Reboot**

  Distributes software immediately, and does not reboot the device.

- **Reboot At Once**

  Does not distribute software, and reboot the device immediately.

- **Reboot Scheduling**

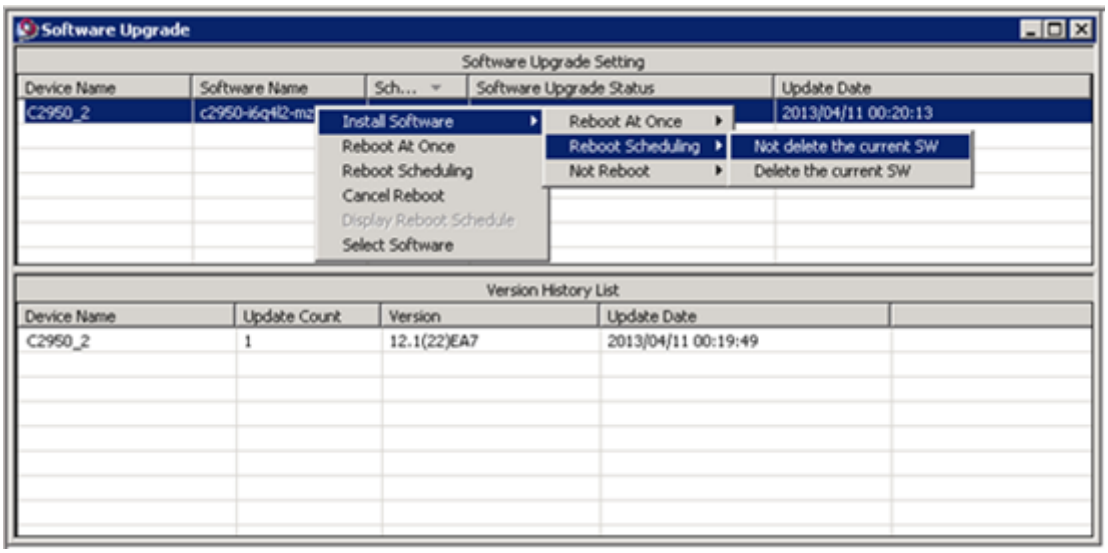
  Does not distribute software, and reboot the device at a specified time.

  The Schedule Setting dialog box is displayed.

- **Cancel Reboot**

  Terminates the scheduled reboot. The restart cannot be canceled during installation or after the reboot command has been executed on the device.

In GUI operation, software is immediately saved on the manger from the network device as a backup file, and the registered file is distributed. The status based on these operations is displayed in the **Software Upgrade Status** column.



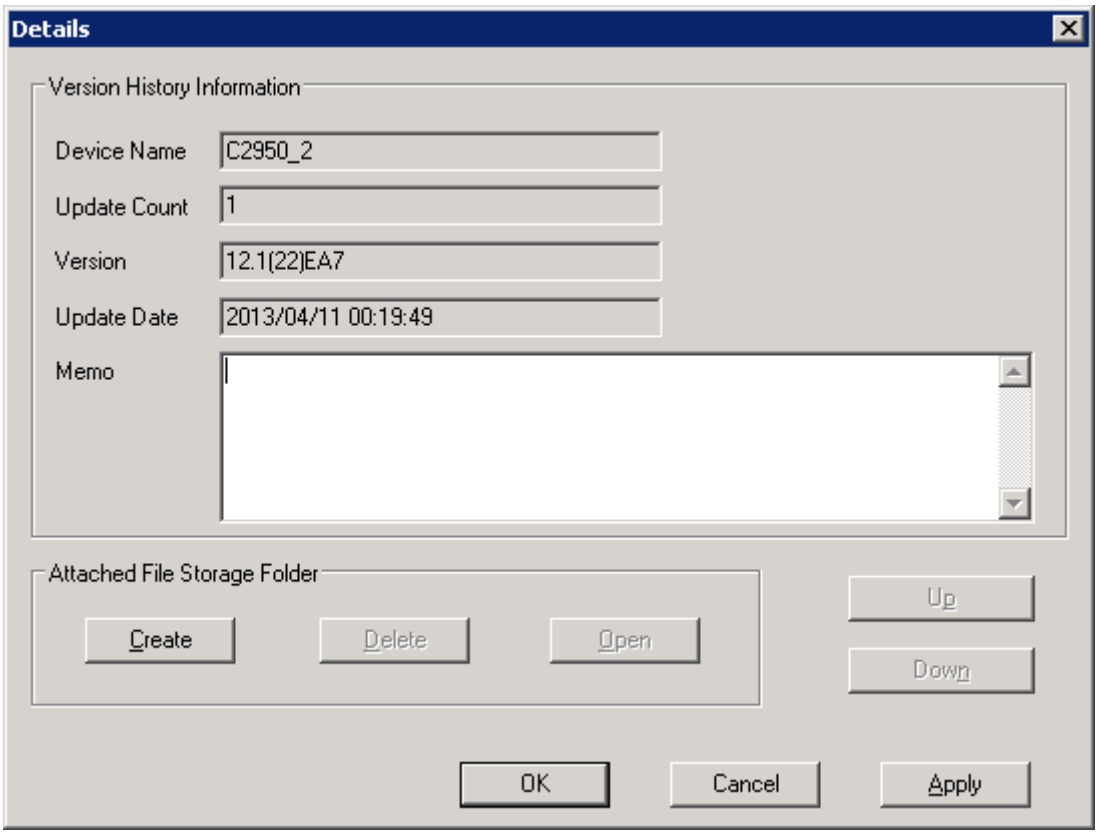
The software installation process may take anywhere from several minutes to several dozen minutes. The current status is displayed under **Software Upgrade Status**. The following information is displayed in the window.

Progress	Software on device is being backed up.
	Backup of software on device is skipped.
	Software with the same name is already backed up.
	Backup of software completed.
	Software is being upgraded.
	Upgrading software completed.
Results	Reboot command of device was executed. Reboot resumes on %Y/%m/%d %H:%M:%S.
	Reboot schedule of device has been added. The reboot command of device will be executed at the appointed time.
	Upgrading software completed. Please reboot device.
	Boot of device was detected.
Failure results	Since the tftp server has not been set, backup of software on device failed.
	Since the ftp server has not been set, backup of software on device failed.
	Since it could not access to device, backup of software on device failed.
	Since it could not login to device, backup of software on device failed.
	Since it was not possible to switch to the enable mode, backup of the software on the device failed.
	Since other processes were accessing the same device, backup of software on device failed.
	Backup of software on device failed.

	Copy to the folder for backup of software failed.
	Creating the work folder for upgrade of software failed.
	Copying software to the work folder failed.
	There is not enough free space in the flash memory of the device. Delete any unnecessary files and execute deployment again.
	Because there is insufficient free space in the flash memory, the specified software cannot be deployed.
	The running software was deleted, but because of there being insufficient free space in flash memory, the specified software could not be deployed.
	After the deletion of the running software, the deployment of the software failed.
	Upgrading software failed.
	Since the tftp server has not been set, upgrading software failed.
	Since the ftp server has not been set, upgrading software failed.
	Since it could not access to device, upgrading software failed.
	Since it could not login to device, upgrading software failed.
	Since it was not possible to switch to the enable mode, the upgrading of the software failed.
	Since other processes were accessing the same device, upgrading software failed.
	Because of the absence of the software for backing up, recovery cannot be performed.
	Recovery after the deletion of the running software failed.
	Since it could not access to device, rebooting device failed.
	Since it could not login to device, rebooting device failed.
	Since it was not possible to switch to the enable mode, rebooting of the device failed.
	Since other processes were accessing the same device, rebooting device failed.
	Rebooting device failed.
	Reboot schedule of device failed.

5. The software distribution history is displayed in the Version History List pane.

   In addition to the software history, the history information also displays the software version information automatically detected by Network Manager. Right-click the row for which you wan to browse the history and select the **Display History** menu to add a note to the software history, register related materials, or link history information.



5.15.2.2 Precautions when deploying software

1. Software deployment is performed using the storage path for software currently being run by the device. However, if the software currently being run cannot be identified, the default path is used. The storage path for software being deployed cannot be expressly specified.
2. The installation may fail if there is insufficient storage space on the device to which you are deploying software. In this case, because automatically determining which files can be deleted is dangerous, the process will not be carried out. Delete unnecessary files and perform the software deployment again.
3. If a software version is changed in the Cisco Catalyst OS by deploying the software, the configuration may not be loaded automatically if there is an inconsistency in the loaded modules. In this case, log in from the console and set up the configuration.
4. SII moves to maintenance mode when deploying software; so a restart is performed. In addition, if you do not select the option to deploy software and restart at the same time, the system stays in maintenance mode after the software is deployed.
5. For Express5800/110Ba-e3 and 120Ba-4, the software configuration definition file (*.des file) and main software image (*.mai file) must be registered as a pair in file management.
6. Some devices (for example, Juniper EX4200) cannot restart with a schedule. Such a device restarts immediately.

Precautions for a stack configuration of the Cisco Catalyst 3750 series

When using a Catalyst 3750 series, it is possible to operate multiple devices under a stack configuration. Normally, when operating under a single-device configuration, it is the same as

operating other devices with the Cisco IOS. However, the following precautions must be considered when operating multiple devices using a stack configuration.

1. When operating multiple devices using a stack configuration, software must be deployed to the master device in the *.tar format. If files have been deployed in the conventional *.bin format, the deployment only applies to the master device; so inconsistencies will occur with slave devices.
2. For a stack configuration, if software is deployed in the *.tar format and the device storage capacity is insufficient, the /html directory is automatically deleted.

   If an error still occurs as the result of insufficient storage capacity, delete unnecessary files in flash memory manually. ResourceManager cannot determine which files are unnecessary; therefore, you must delete unnecessary files directly from the device.

   When software files in the *.tar format are deployed, the /html directory unique to the version of the deployed software is created.
3. If software is deployed after the configuration is changed from a single-device configuration to a stack configuration, backup files may be created in the *.bin format.
4. If there are many slave devices in the stack configuration (a maximum 9-device configuration is possible), it may take time to deploy software from the master device to slave devices, causing a timeout error even during a normal process.

   In this case, set 60 or more to the *"watchTimeout"* (unit: minutes) in the following configuration file and set 3600 or more to the *"WaitTimeout"* (unit: seconds).

   - Configuration file

     %shared folder% of the manager\Manager\sg\NvPRO\RMAPI\nvrmapi.ini

   - Specification format

```
watchTimeout=60
WaitTimeout=3600
```

Precautions for the Cisco Catalyst series with the IOS-XE software

1. When the IOS-XE software version is 3.8 (15.3(1)) or higher and lower than 16, software backup is supported. For other versions, software backup is not performed at software deployment.
2. For the Catalyst 4500 series, the IOS-XE software of version 3.8 (15.3(1)) or higher is supported.

Precautions for the Cisco Nexus 5000 and 7000 series

1. For the Cisco Nexus 5000 and 7000 series, the following two software files must be deployed.
   - NX-OS Kick Start

     Example: n5000-uk9-kickstart.4.0.1a.N1.1.bin
   - NX-OS System software

     Example: n5000-uk9.4.0.1a.N1.1.bin

Register these two software files on the File Management screen and deploy them to a device in order by selecting **Start installation**>**Not restart**. When deployment of these two software files is completed, restart the device.

Precautions for the Cisco ASR 920 and 1000 series

1. The Cisco ASR 920 and 1000 series devices operate by using multiple software products combining the IOS-XE software, IOS-XE ROMMON software, and other package software. They may not operate normally depending on the software combination.

   Network Manager can deploy only the IOS-XE software. Therefore, when deploying the IOS-XE software by using Network Manager, check the versions of software other than IOS-XE deployed on the device in advance to make sure that there will be no problem in device operation after deployment.
2. Note that deployment of IOS-X version 16 or higher is not supported.

Precautions for the IP8800/S300, S400, and R400 series

1. For the IP8800/S300, S400, and R400 series software, back up the existing software by using the *" ftpbackup "* command before deploying the software.

   According to the specifications of the *" ftpbackup "* command, not an IP address but a host name of the transfer destination FTP server is necessary. Therefore, it is necessary to set the host name for the transfer destination FTP server in the device.

   The host name is set using the *" ip hosts "* command. (For details of the command, refer to the device manual.) When using the FTP server within Network Manager, set the host name of the machine on which Network Manager is installed. When using an external FTP server, set the host name of that FTP server.
2. For the IP8800/S300, S400, and R400 series software, software is deployed by transferring its files to the `/PrimaryMC/usr/var/update` directory of the device. Therefore, make sure that login users can access this directory.

Precautions for a stack configuration for the IP8800/S3650, S3660, S3830, and S4630 series

1. For a stack configuration, software is deployed to only the master device.

Precautions for a stack configuration of the NEC QX-S series

1. For a stack configuration, it may take time to deploy software from the master device to slave devices, causing a timeout error even during a normal process.

   In this case, set 60 or more to the *"watchTimeout"* (unit: minutes) in the following configuration file and set 3600 or more to the *"WaitTimeout"* (unit: seconds).

   - Configuration file

     %shared folder% of the manager`\Manager\sg\NvPRO\RMAPI\nvrmapi.ini`

   - Specification format

     ```
     watchTimeout=60
     WaitTimeout=3600
     ```

2. For a stack configuration, if software is deployed to QX-S5500, the software is deployed to only the master device. Enable the software auto upgrade function (irf auto-update) of the device in advance so that the software of slave devices will be synchronized with that of the master device. If the software auto upgrade function is disabled, an inconsistency occurs between the master device and slave devices.

Precautions for the PF5459/QX-S5900, S4100G, S5200G, and S5500G series

1. If you deploy software using the ipe file, the boot image and system image will be expanded in flash memory. For this reason, before deploying software, confirm that the flash memory has sufficient free space as compared with the ipe file to use (approximately twice the size of the file).

   For a stack configuration, confirm the amount of free flash memory in each of the devices constituting the stack.

5.16 Managing Audit Logs

Network Manager includes a function that allows you to record a log of operations details and a history of results for operations performed in the monitoring window or manager, or processes performed automatically (audit log). The audit log manager includes the following functions.

- Logging function

  Audit logs generated for operations performed in the monitoring window or manager, or for processes performed automatically, are consolidated by the manager.

- Display function

  Audit logs logged in the manager are displayed in the monitoring window. For details, refer to "5.16.1 Viewing audit logs (page 551)".

- Notification function

  If audit logs are generated that are of specified importance, Patlite, e-mail, and action notifications are created to warn the operator. For details, refer to "4.23.1 Defining report settings for audit logs (page 444)".

- Audit log file output

  Audit logs for particular categories can be output to a file in CSV format and used in other applications. For details, refer to "5.16.3 Exporting audit logs to a file (page 555)".

- Audit log maintenance function

  Audit logs within particular categories can be deleted. For details, refer to "5.16.4 Deleting audit logs within a category (page 555)".

5.16.1 Viewing audit logs

This operation is only available to users belonging to a group with "Audit trail reference authority". In this function, audit logs are managed according to categories. The four categories are application, security, system, and audit log.

Category	Stored audit log
Application	Audit logs generated by applications. Audit logs generated by Network Manager are included in this category.
Security	Audit logs output by user authentication.
System	Audit logs output by the framework service in the tree view.
Audit log	Audit logs from the audit log function itself.

Audit logs can be viewed according to the categories in the Audit Log window.

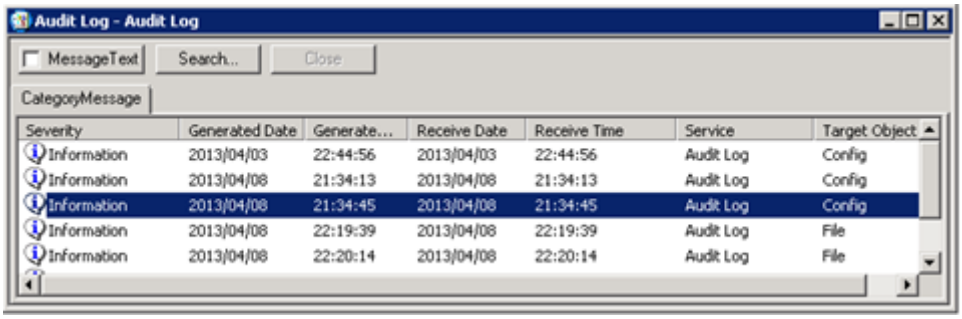
Caution

The **Audio Log Online View** tab displays all audit logs that have been stored in the category since the monitoring view was active. Messages displayed in the **Audio Log Online View** tab are cleared when the monitoring view was closed.

This operation is only available to users belonging to a group that has audit viewing rights.

1. To display the Audit Log window, use one of the following three methods.
   - Double-click the category node in the tree view.
   - Double-click the category node in the Map View.
   - Double-click the icon displayed in the Property View for the category node.

   The Audit Log window is displayed on the right side of the window.



   - Button panel section
     - **Message Text** checkbox

       Shows or hides the pane below the Audit Log window that displays the message text for the selected audit log.
     - **Search** button

       Click **Search** button to find audit logs in a particular category.

       For details, refer to "5.16.2 Searching audit logs (page 554)".
   - Message list section
     - **Severity**

       Displays the importance (severity) level of the audit log.
     - **Generated Date**

       Displays the date that the audit log was generated.
     - **Generated Time**

       Displays the time that the audit log was generated.

- **Receive Date**

  Displays the date that the audit log was received by the audit log function.

- **Receive Time**

  Displays the time that the audit log was received by the audit log function.

- **Service**

  Displays the name of the service that output the audit log.

- **Operation**

  Displays the operation performed by the user.

- **Audit ID**

  Displays the ID of the audit log.

- **User**

  Displays the name of the user who performed the operation.

- **Node**

  Displays the name of the host that output the audit log.

- **Target Node**

  Displays the name of the host targeted for action.

- **Target Object**

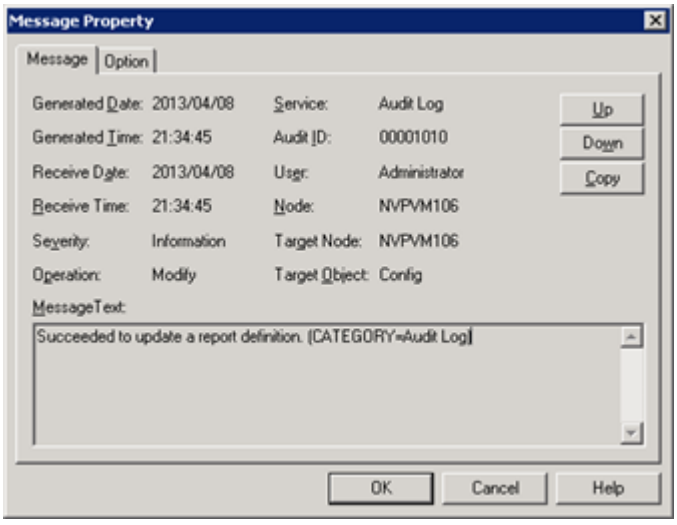
  Displays the name of the object that is the operation target.

Tip

In the configuration mode, the width and place of column such as **Severity**, etc. can be changed in the **Audit Log Online View** tab. These changes are also reflected in the Audit Log window.

2. Double-click an audit log to display the properties window for that audit log.

   Alternatively by right-clicking, you can copy or display the properties window for the currently selected audit log.



- **Message** tab

  Message Text

Displays the audit log message text.

- **Option** tab

  Displays additional audit log information.

- **UpDown** button

  Switches the audit log for which the properties are being displayed.

  The **Up** button moves to the next audit log up in the Audit Log window and displays its properties, the **Down** button moves to the next audit log down and displays its properties.

- **Copy** button

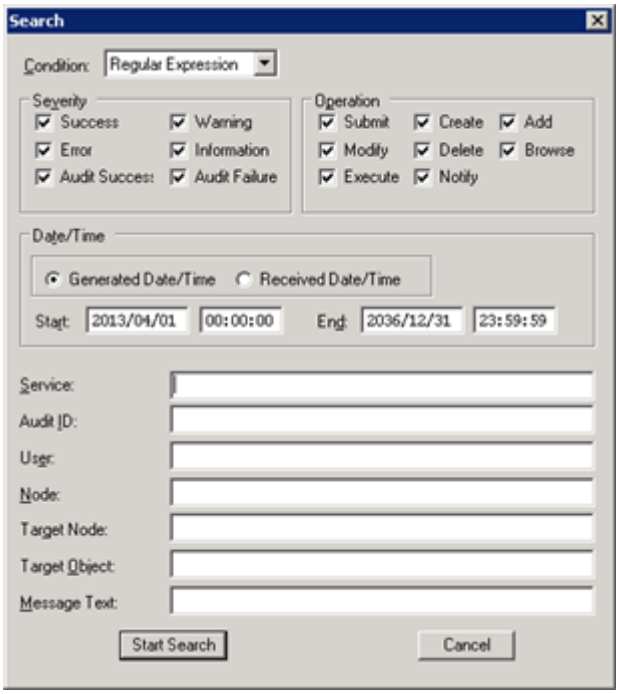
  Copies the audit log information to the clipboard.

5.16.2 Searching audit logs

You can search and narrow down audit logs.

This operation is only available to users belonging to a group with "Audit trail reference authority".

1. In the Audit Log window, click **Search** button.
2. In the Search dialog box, specify the conditions.



- **Condition**

  Select either "Wild Card" or "Regular Expression".

  The selected search conditions will be valid for the **Service**, **Audit ID**, **User**, **Node**, **Target Node**, **Target Object** and **Message Text**.

- **Severity**

  Searches audit logs for the selected severity levels.

- **Operation**

  Searches audit logs for the selected operations.

- **Date/Time**

  Specify a range for the **Generated Date/Time** or **Received Date/Time** for the audit log. Select whether you want to search by the **Generated Date/Time** or **Received Date/Time**.

- **Service**

  Specify the name of the service that generated the audit log using either a wild card or regular expression.

- **Audit ID**

  Specify the audit ID using either a wild card or regular expression.

- **User**

  Specify the name of the user who performed the operation using either a wild card or regular expression.

- **Node**

  Specify the name of the host that performed the operation using either a wild card or regular expression.

- **Target Node**

  Specify the host name of the operation target using either a wild card or regular expression.

- **Target Object**

  Specify the object name of the operation target using either a wild card or regular expression.

- **Message Text**

  Specify the message text using either a wild card or regular expression.

3. Click **Start Search** button.

   The search results are displayed in the Search Result window. You can sort the columns in the Search Result window.

5.16.3 Exporting audit logs to a file

Audit logs for particular categories can be output to a file in CSV format and used in other applications. The file output is performed from command lines (on machines installed with the manager function). For details, refer to "9.1.3 AuditTrailCmd CSV (page 688)".

1. Execute a command.

   ```
   > AuditTrailCmd.exe CSV 3 2011/02/14 C:\foo\bar.csv
   ```

   System category audit logs stored on February 14, 2011 is output to C:\foo\bar.csv on the manager.

5.16.4 Deleting audit logs within a category

Audit logs in a category can be deleted in one of two ways: either from the monitoring windows or from a command line (on machines installed with the manager function).

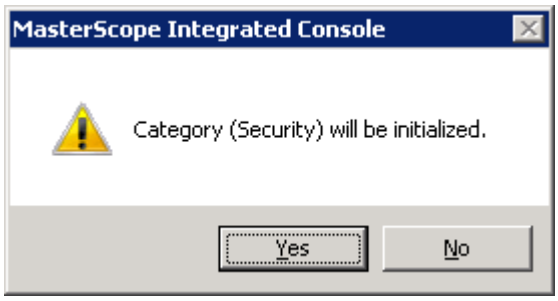
Deleted audit logs cannot be restored, regardless of which of the methods is used to delete them.

This section describes how to delete audit logs from the monitoring window. For the method performed from the manager command, refer to "9.1.1 AuditTrailCmd INIT (page 686)" and "9.1.2 AuditTrailCmd SWAP (page 687)".

This operation is only available to users belonging to a group with "Audit trail update authority".

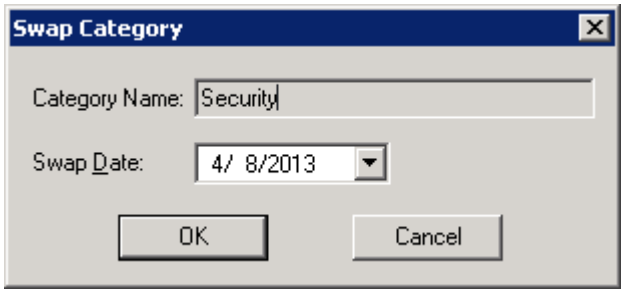
You must first change to the "configuration mode (page 27)".

- Deleting all audit logs within a category:
  1. In the tree view, select the category for the audit logs that you want to delete. Right-click and select **Initialize Category** menu.
  2. A window is displayed to confirm that you want to delete the audit logs. Click **Yes** button.



- Deleting audit logs within a category by specifying a date:

  Audit logs in the category that have a date earlier than the specified date are deleted.
  1. In the tree view, select the category for the audit logs that you want to delete. Right-click and select **Swap Category** menu.
  2. The Swap Category window is displayed. Specify a date and then click **OK** button.



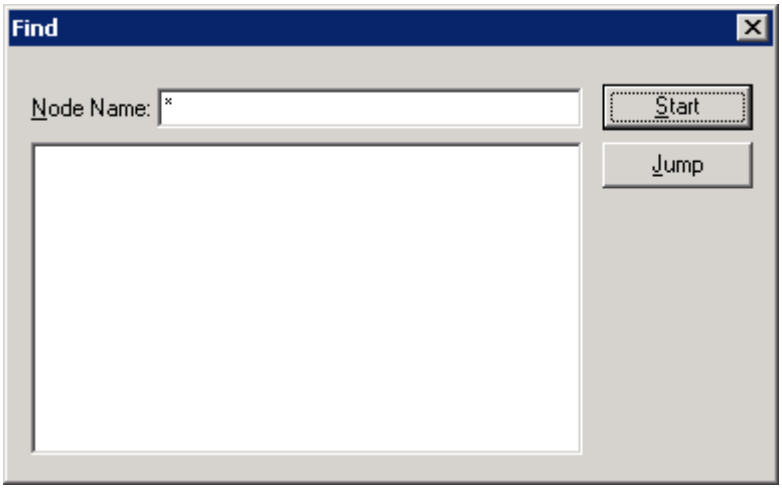
5.17 Searching for a Node

1. Display the Find dialog box in one of the following ways.
   - In the tree view, right-click and select **Find** menu.
   - Click the  icon on the toolbar.
2. In the Find dialog box, type the name of the node.

   Wildcards (*) can be used in the search.
3. Click **Start** button.

   The search result is displayed.

To display a node that has been found, double-click the node or select the node and click **Jump** button. The selected node is displayed.



5.18 Changing Window Appearance

5.18.1 Changing the method for positioning windows

To change the method for positioning windows, go to the **Window** menu.

- Cascading

  To display opened windows (Map View, Property View, monitoring windows) one on top of the other, select **Window**>**Cascade**.

- Side by side

  To display opened windows (Map View, Property View, monitoring windows) side by side, select **Window**>**Tile**.

- Aligning icons

  To align minimized windows (Map View, Property View, monitoring windows), select **Window**>**Arrange Icon**.

5.18.2 Showing or hiding the toolbar

To change the display status of the toolbar, select **View**>**Tool Bar**.

If the toolbar is currently being displayed, there will be a checkmark to the left of **Tool Bar** in the **View** menu.

5.18.3 Showing or hiding the status bar

To change the display status of the status bar, select **View**>**Status Bar**.

If the status bar is currently being displayed there will be a check mark on the left side of **Status Bar** of in the **View** menu.

5.19 Printing the Map View

Use one of the following methods to print the Map View image.

1. Display the Print dialog box in one of the following ways.
   - Display Map View image that you want to print. Select **File**>**Print**.
   - Display the Map View that you want to print, and click the  icon on the toolbar.
2. The Print dialog box is displayed. Configure the print setting.
   - To preview the print image:

     Display the Map View image that you want to print. In the main menu, select **File**>**Print Preview**.
   - To configure the printer settings:

     In the main menu, select **File**>**Printer Setting**. The Print Setup dialog box is displayed. Set each item and click **OK** button.
3. Click **OK** button.

Chapter 6. Menu Reference

Contents

6.1 Main Menus 560
6.2 Network View Menu 564
6.3 Audit Log menu 584
6.4 Common Menus for Background in the Map View 585
6.5 Common Menus for Objects (Icons) in the Map View 586
6.6 Common Menus in the Tree View 587

This chapter uses the following abbreviations in the availability of menu commands for user authority (reference authority and operation authority), each icon, and the web monitoring view. For details of the user authorities, refer to "2.4 User Access Rights (page 26)".

- Availability in each authority

Name	Abbreviation
Reference Authority	Ref.
Operation Authority (Normal mode)	Op. (Normal)
Operation Authority (Configuration mode)	Op. (Config)

- Availability in each icon type

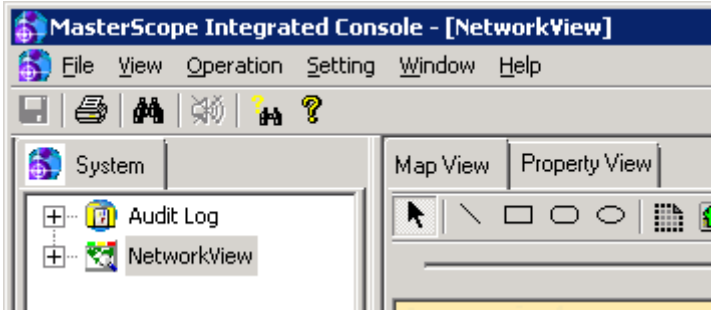
Icon Type	Abbreviation
NetworkView icon	
NetworkManagement icon	
Map icon	
Device icon	

- Availability in Web Monitoring View

Name	Abbreviation
Availability in Web Monitoring View	Web View

6.1 Main Menus

Commands for the entire system are executed from the main menu.



6.1.1 List of available main menu commands

The availability of main menu commands for user authority (reference authority and operation authority) and the web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

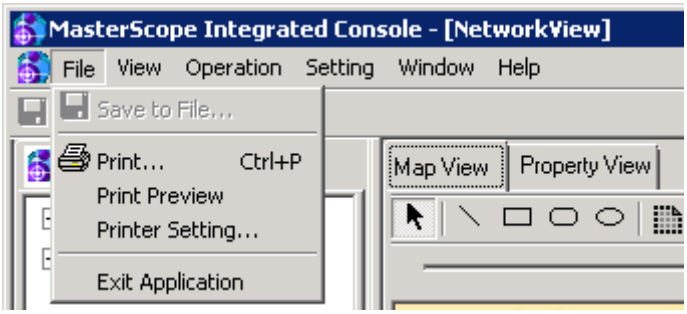
Menu Item	Ref.	Op. (Normal)	Op. (Config)	Web View
"File (page 561)"				

Menu Item	Ref.	Op. (Normal)	Op. (Config)	Web View
Save to File				
Print	o	o	o	o
Print Preview	o	o	o	o
Printer Setting	o	o	o	o
Exit Application	o	o	o	o
"View (page 562)"				
Tool Bar	o	o	o	o
Status Bar	o	o	o	o
"Operation (page 562)"				
Stop Sound	o	o	o	o
"Setting (page 563)"				
Configuration Mode			o	o
License Management			o 1)	o
Change Password	o	o	o	o
User Management			o 2)	o
Option			o	o
"Window (page 563)"				
Cascade	o	o	o	o
Tile	o	o	o	o
Arrange Icon	o	o	o	o
"Help (page 564)"				
Help Contents	o	o	o	o
About Version	o	o	o	o

1) This menu item is only available to users belonging to a group that has license management rights.

2) This menu item is only available to users belonging to a group that has user management rights.

6.1.2 File menu



- **Save to File**

  This menu item cannot be used in Network Manager. This menu is available if the system coexists with other MasterScope products.

- **Print**

  Opens the Print dialog box. In the Print dialog box, click **OK** button to print the Map View image.

  This menu item can only be used when the Map View window is the focus.

- **Print Preview**

  The Map View image is displayed as a print preview.

  In the Print Preview window, click **Close** button to return to the normal window.

  This menu item can only be used when the Map View window is the focus.

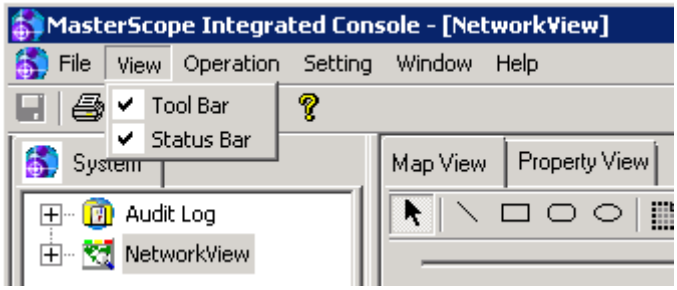
- **Printer Setting**

  Opens the Print Setup dialog box.

- **Exit Application**

  Closes the monitoring window.

6.1.3 View menu



- **Tool Bar**

  Displays or hides the toolbar. For details, refer to "5.18.2 Showing or hiding the toolbar (page 557)".

- **Status Bar**

  Displays or hides the status bar. For details, refer to "5.18.3 Showing or hiding the status bar (page 557)".

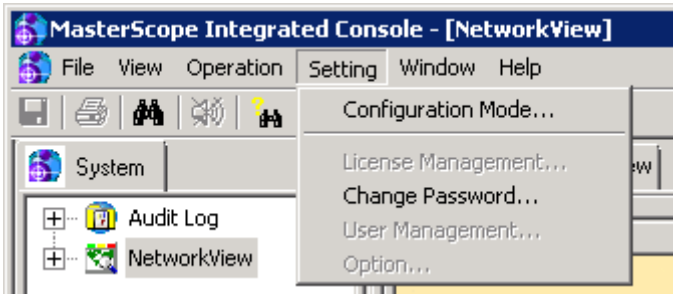
6.1.4 Operation menu

- **Stop Sound**

  Turns off the sound during an alarm. For details, refer to "5.1.2 Turning off sound during an alarm (page 449)".

  This menu item can only be used when an alarm is sounding.

6.1.5 Setting menu



- **Configuration Mode**

  Switches the operating mode of the monitoring terminal between monitoring mode and configuration mode. For details, refer to "2.5 Operation Modes (page 27)".

- **License Management**

  Registers and confirms licenses. For details, refer to "10.3 Registering Licenses (page 759)".

  This menu item is only available to users belonging to a group that has license management rights.

- **Change Password**

  Changes the password that is used for logging in to Network Manager.

- **User Management**

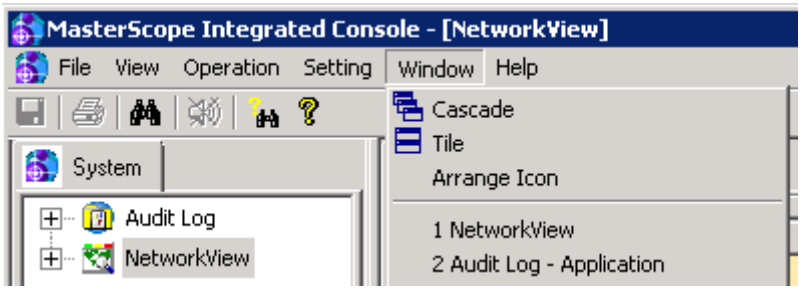
  Manages user information that is used in the system. For details, refer to "4.1 Managing Users and Groups (page 101)".

  Manages user information that is used in the system.

- **Option**

  Used to set system options.

6.1.6 Window menu



- **Cascade**

  Displays opened windows (Map View, Property View, monitoring windows) one on top of the other.

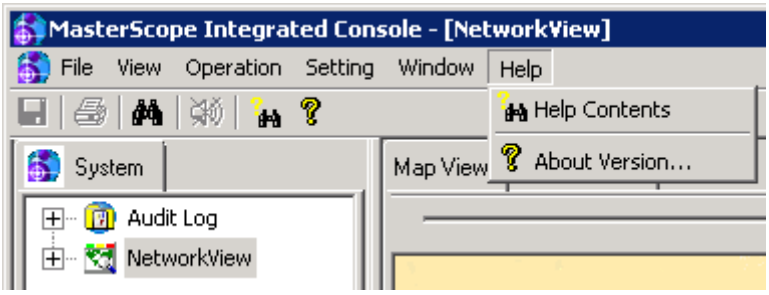
- **Tile**

  Displays opened windows (Map View, Property View, monitoring windows) side by side.

- **Arrange Icon**

  Arranges minimized windows (Map View, Property View, monitoring windows). For details, refer to "5.18.1 Changing the method for positioning windows (page 557)".

6.1.7 Help menu



- **Help Contents**

  Displays Help.

- **About Version**

  Shows the version information in the About Version dialog box.

6.2 Network View Menu

6.2.1 Configuration Management menu

The Configuration Management menu is used to perform operations relating to the configuration of target device information.

6.2.1.1 List of available Configuration Management menu commands

The availability of menu commands for different user authorities (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Menu Item	Ref.	Op. (Normal)	Op. (Config)					Web View
"Import and Export (page 566)"			o	o	o	o		
Autodiscover								
"TCP/IP Hosts (page 566)"			o		o	o		
"Network and Routers (page 566)"			o				o	
"Physical Topology (page 566)"			o		o	o	o [1)]	
"ProgrammableFlow Authentication Setting (page 567)"			o				o [2)]	
"ProgrammableFlow Topology (page 567)"			o				o [2)]	
"Nexus (page 567)"			o				o [3)]	
Update Property								

Menu Item	Ref.	Op. (Normal)	Op. (Config)					Web View
"Update Required Property (page 567)"			o		o	o	o	o
"Update All Property (page 568)"			o		o	o	o	o
"Check Topology (page 568)"			o				o	o
"Collect Routing Information (page 568)" 4)	o	o	o	o	o			
"Group List (page 568)"	o	o	o	o	o			o
"Group Member List (page 569)"	o	o	o	o	o			
Monitoring Mode								
"ON (page 569)"			o	o	o	o	o	
"OFF (page 569)"			o	o	o	o	o	
Monitoring-mode Schedule								
"Setting (page 569)"			o	o	o	o	o	
"Cancel (page 569)"			o	o	o	o	o	
"Property (page 570)"	o	o	o	o	o	o	o	o
"Login Information Setting (page 570)" 4)	o	o	o	o	o	o	o	o
"FTP/TFTP Server Setting (page 570)" 4)	o	o	o	o	o			
"Interface Property (page 570)" 4)	o	o	o				o	o
"Start Application (page 571)" 5)	o	o	o			o	o	
"Start Web browser (page 571)" 5)	o	o	o			o	o	o
"Command Creation (page 571)" 4)	o	o	o	o	o			
"Command Execution Result (page 571)"	o	o	o	o	o			
"Command Scheduling (page 571)" 4)	o	o	o	o	o	o	o	

1) This menu is available when the device icons of two or more supported target devices are selected in the Map View.

2) The menu is available when the device icon represents the ProgrammableFlow controller.

3) This menu is available for the Nexus 5000 icon.

4) The available range of operations changes depending on the user authorities (reference authority or operation authority).

5) This menu is made available by configuring settings in the Properties dialog box, under the **Functions** tab, in advance.

6.2.1.2 Import and Export menu

Imports (batch registration and deletion) or exports device information. For details, refer to "4.6 Batch Registering or Deleting Configuration Information (page 206)".

6.2.1.3 Autodiscover menu

TCP/IP Hosts menu

Discovers devices being operated within the specified network address and registers them. For details, refer to "4.2.1.1 Performing autodiscover (TCP/IP Hosts) (page 127)".

Preparation/Conditions

You need to register the map icon in the Map View under the **Network Management**.

Network and Routers menu

Uses the specified router as a base point to discover IP networks connected to that router, and routers in operation that are connected to that IP network, and registers them. For details, refer to "4.2.1.2 Performing autodiscover (networks and routers) (page 136)".

Preparation/Conditions

IP address information must be registered in the properties of the base device. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

Physical Topology menu

Collects topology information regarding a device icon under a selected map icon or regarding a selected device icon by the setting value of **Discovery Protocol** in the icon properties to display the connection relationship in the **Map View**. For details, refer to "4.2.3.2 Automatically detecting topology information (page 149)".

Preparation/Conditions

- Each device is required to run the neighboring protocol (CDP, OADP, FDP, or LLDP). For the configuration of each device, refer to the manual of the device.
- If a device specifies "1" (IP8800/700 series or ES8800/1700 series) in **Discovery Protocol**, configure the device-type of OADP to sysName. For details, refer to the manual of the device.
- For the icon properties of a targeted device, register **SNMP Community Name (get)** or **SNMPv3** tab information and create an environment that can carry out SNMP communication. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".
- Make the values of the sysName(1.3.6.1.2.1.1.5) of a device and the **sysName** in the icon properties consistent.
- Confirm if **Discovery Protocol** in the icon properties is properly specified. For details, refer to "4.2.3.1 Discovery Protocol (page 148)".

ProgrammableFlow Authentication Setting menu

Sets the authentication information to access Web API of the ProgrammableFlow controller. For details, refer to "4.2.4.1 Preparing for autodiscover of ProgrammableFlow physical topology (page 164)".

Preparation/Conditions

- The menu is available when the device icon represents the ProgrammableFlow controller.

ProgrammableFlow Topology menu

Checks the physical connection status of the ProgrammableFlow switch nodes in the same map to which the specified ProgrammableFlow controler icon belongs, and then draws the physical connection line. For details, refer to "4.2.4.2 Automatically detecting ProgrammableFlow physical topology (page 166)".

Preparation/Conditions

- The menu is available when the device icon represents the ProgrammableFlow controller.
- Web API needs to be valid on the target ProgrammableFlow controller.
- Perform "4.2.4.1 Preparing for autodiscover of ProgrammableFlow physical topology (page 164)" in advance.

Nexus menu

Checks the connection status of Nexus 2000 devices connected to a specified Nexus 5000 device, registers discovered Nexus 2000 devices, and draws connection lines. For details, refer to "4.2.5.1 Automatically detecting Nexus 2000 information (page 172)".

Preparation/Conditions

The SNMP community name (get) or SNMPv3 information must be registered in the properties of the specified Nexus 5000 device to perform SNMP communication with devices. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.1.4 Update Property menu

Update Required Property menu

Retrieves the most current information from all devices subordinate to the specified map node, or for the specified device node, and updates device information (properties) and interface property information that are required by Network Manager operation. For details, refer to "4.2.7 Updating device information via a network (page 179)".

Preparation/Conditions

The SNMP community name (get) or SNMPv3 information must be registered in the properties of the device node for which you are updating information to perform SNMP communication with devices. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

Update All Property menu

Retrieves the most current information from all devices subordinate to the specified map node, or for the specified device node, and updates device information (properties) and interface property information. For details, refer to "4.2.7 Updating device information via a network (page 179)".

Preparation/Conditions

The SNMP community name (get) or SNMPv3 information must be registered in the properties of the device node for which you are updating information to perform SNMP communication with devices. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.1.5 Check Topology menu

Compares physical topology information registered using the "connection-line manual register" function or the **Physical Topology** menu autodiscover function with the actual network and checks for inconsistencies. For details, refer to "4.2.3.4 Checking topology information (page 162)".

Preparation/Conditions

Only device nodes with registered connection-lines will be processed.

The SNMP community name (get) or SNMPv3 information must be registered in the properties of the target device node to perform SNMP communication with devices. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.1.6 Collect Routing Information menu

Collects L3 route information to be used in plotting a map between two devices. For details, refer to "4.7 Registering Routing Information for the Map between Two Nodes (page 231)".

Operations availability in operating modes:

- Normal mode

  The collection status of L3 routing information can be viewed.

- Configuration mode

  Operations for collecting L3 routing information can be performed.

Preparation/Conditions

The SNMP community name (get) or SNMPv3 information must be registered in the properties of the target device node to perform SNMP communication with devices. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.1.7 Group List menu

Displays a list of the registered groups.

A group is created when a device node belongs to the group, and is deleted when all device nodes have left the group.

Preparation/Conditions

To make device nodes belong to a group, register the **Group** item in the properties of device nodes. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.1.8 Group Member List menu

Displays a list of the nodes that belong to the specified groups.

The maximum number of members that can be displayed at a time is 20,000. If the number of members exceeds 20,000, narrows down target groups and then displays the list.

Preparation/Conditions

To make device nodes belong to a group, register the **Group** item in the properties of device nodes. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.1.9 Monitoring-mode menu

ON menu

Changes the monitoring mode status for all device nodes subordinate to the specified map node, or for specified device nodes, to ON. For details, refer to "5.13.1 Manually setting monitoring mode (page 506)".

Preparation/Conditions

If you are executing the command from a device node menu, this menu is available when the monitoring mode of the target device is OFF.

OFF menu

Changes the monitoring mode status for all device nodes subordinate to the specified map node, or for specified device nodes, to OFF. For details, refer to "5.13.1 Manually setting monitoring mode (page 506)".

Preparation/Conditions

If you are executing the command from a device node menu, this menu is available when the monitoring mode of the target device is ON.

6.2.1.10 Monitoring-mode Schedule menu

Setting menu

Sets a schedule for automatically switching the monitoring mode settings for specified map nodes or device nodes. For details, refer to "5.13.2 Setting and changing a monitoring mode schedule (page 506)".

Cancel menu

Cancels monitoring mode schedules set for specified map nodes or device nodes. For details, refer to "5.13.4 Canceling a monitoring mode schedule (page 510)".

Preparation/Conditions

This menu is available when monitoring mode schedules have been set for specified nodes.

Property menu

Displays the details of monitoring mode schedules set for specified map nodes or device nodes. For details, refer to "5.13.3 Viewing a monitoring mode schedule (page 509)".

Preparation/Conditions

This menu is available when monitoring mode schedules have been set for specified nodes.

6.2.1.11 Login Information Setting menu

Registers the information required for logging in to managed devices for performing operations such as remote login, device command execution, and using the Resource Manager function (config management and software management). For details, refer to "4.3 Registering Login Information (page 189)".

Operations availability in operating modes:

- Normal mode

  The registration status of login information can be viewed.

- Configuration mode

  Operations for registering and changing login information can be performed.

6.2.1.12 FTP/TFTP Server Setting menu

Configures settings for using file transfer servers that are located outside of Network Manager, in Resource Manager function (config management and software management) processes. For details, refer to "4.20.1 Registering an FTP or TFTP server (page 400)".

Operations availability in operating modes:

- Normal mode

  The settings information for the FTP/TFTP servers to be used can be viewed.

- Configuration mode

  Settings for the FTP/TFTP servers to be used can be configured.

6.2.1.13 Interface Property menu

Displays device interface information maintained by Network Manager in the Interface Properties dialog box. For details, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

Operations availability in operating modes:

- Normal mode

  The Interface Properties dialog box can be displayed, and interface information can be viewed.

- Configuration mode

  The Interface Properties dialog box can be displayed, and interface information can be updated (discovered).

  In addition, the default ports to be used in the status monitoring function and data collection function can be configured.

Preparation/Conditions

Devices that support SNMP are targeted.

When executed for the first time, SNMP communication with the devices is performed to collect device interface information. So, the SNMP community name (get) or SNMPv3 information must be registered in the properties of the device node to perform SNMP communication with devices. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.1.14 Start Application menu

Launches the applications that have already been specified. For details, refer to "4.5.1 Registering applications launched from icons (page 204)".

Preparation/Conditions

The **Application Path** item in the node properties must be registered in advance. This menu is available after the **Application Path** item has been registered. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.1.15 Start Web browser menu

Displays the previously specified URL in a web browser. For details, refer to "4.5.2 Registering web URLs launched from icons (page 205)".

Preparation/Conditions

The **URL** item in the node properties must be registered in advance. This menu is available after the **URL** item has been registered. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.1.16 Command Creation menu

Defines commands to be run on managed devices. For details, refer to "4.19.1 Defining commands (page 391)".

Operations availability in operating modes:

- Normal mode

  The details of created command definitions can be viewed.

- Configuration mode

  Command definitions can be created, edited, and deleted.

6.2.1.17 Command Execution Result menu

Records the execution results list for commands executed in the "Command Scheduling" function, in a CSV file. For details, refer to "5.10.3 Checking command execution results (page 484)".

6.2.1.18 Command Scheduling menu

Sets schedules for commands to be run on managed devices. For details, refer to "4.19.2 Scheduling command execution (page 398)".

Operations availability in operating modes and user authority:

- Normal mode

Reference authority:

The registration status of command schedules can be viewed.

Operation authority:

The registration status of command schedules can be viewed and the **Execute At Once** command can be performed for commands that have been registered.

- Configuration mode

  Command schedules can be registered and the **Execute At Once** command can be performed for commands that have been registered.

Preparation/Conditions

- Login information needs to be registered from the **Configuration Management**>**Login Information Setting** menu. For details, refer to "4.3 Registering Login Information (page 189)".
- Command definitions for execution schedules need to be created from the **Configuration Management**>**Command Creation** menu. For details, refer to "4.19.1 Defining commands (page 391)".

6.2.2 Fault Management menu

In the **Fault Management** menu, you can execute commands for managed devices, such as reporting and setting up monitoring.

6.2.2.1 List of available Fault Management menu commands

The availability of menu commands for different user authorities (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Menu Item	Ref.	Op. (Normal)	Op. (Config)					Web View
"State Monitoring (page 573)"	o	o	o	o	o			o
"Trap Definition Management (page 573)"	o	o	o	o	o			
"Alert Notification Setting (page 573)" 1)	o	o	o	o	o			o
"Show Route of 2 Devices (page 574)"	o	o	o	o	o		o	
"Ping (IPv4) (page 574)"		o	o				o	o
"Ping (IPv6) (page 574)"		o	o				o	o
"Remote Login (page 574)"		o	o				o	o
"Trace Route (IPv4) (page 574)"		o	o				o	o
"Trace Route (IPv6) (page 575)"		o	o				o	o

Menu Item	Ref.	Op. (Normal)	Op. (Config)					Web View
"Show Unrecovered Alert (page 575)"	o	o	o				o	o
"Show All Alert (page 575)"	o	o	o				o	o

1) The available range of operations changes depending on the user authorities (reference authority or operation authority).

6.2.2.2 State Monitoring menu

Displays the State Monitoring window and configures state monitoring settings. For details, refer to "4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function) (page 241)".

Operations availability in operating modes:

- Normal mode

  The State Monitoring window can be opened and the status of state monitoring can be viewed.

- Configuration mode

  The State Monitoring window can be opened, state monitoring rules can be configured, changed, and deleted, and new rules can be embedded.

6.2.2.3 Trap Definition Management menu

Displays the Trap Definition Management window to manage trap definitions. For details, refer to "4.11.3.1 Trap Definition Management window (page 265)".

Operations available in each operating mode:

- Normal mode

  The Trap Definition Management window can be started to view and search for trap definitions.

- Configuration mode

  The Trap Definition Management window can be started to add, change, and delete trap definitions, in addition to viewing and searching for them.

6.2.2.4 Alert Notification Setting menu

Sets the conditions and procedures for notifications when alerts occur (Patlite, e-mail, and execution of actions). For details, refer to "4.14 Settings for Sending Alert Reports (page 310)".

Operations availability in operating modes:

- Normal mode

  The report condition settings can be viewed.

- Configuration mode

  The conditions and procedures for notifications can be configured.

6.2.2.5 Show Route of 2 Devices menu

The PointToPoint Map window provides graphical illustration of the L3 route linking two specified network devices (including PC terminals). For details, refer to "5.7 Displaying Routing Information Map between Two Nodes (page 471)".

Preparation/Conditions

The collection of routing information must be performed from the **Configuration Management**>**Collect Routing Information** menu. For details, refer to "4.7 Registering Routing Information for the Map between Two Nodes (page 231)".

6.2.2.6 Ping (IPv4) menu

Executes the ping command for specified managed devices from the manager and displays the ICMP ECHO results for communication through IPv4. For details, refer to "5.5.1 Executing a ping command (page 468)".

Preparation/Conditions

IP address information must be registered in the properties of the device node that the menu command is being executing from. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.2.7 Ping (IPv6) menu

Executes the ping command for specified managed devices from the manager and displays the ICMP ECHO results for communication through IPv6. For details, refer to "5.5.1 Executing a ping command (page 468)".

Preparation/Conditions

IPv6 address information must be registered in the properties of the device node that the menu command is being executing from. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.2.8 Remote Login menu

Tests the remote login for a managed device. For details, refer to "5.5.3 Logging in to devices from the monitoring terminal (page 469)".

Preparation/Conditions

If you are registering login information from the **Configuration Management**>**Login Information Setting** menu, the window will open when the login process finishes. For details, refer to "4.3 Registering Login Information (page 189)".

6.2.2.9 Trace Route (IPv4) menu

Executes the traceroute command for specified managed devices from the manager and checks the communication path for IPv4 communication. For details, refer to "5.5.2 Executing a traceroute command (page 468)".

Preparation/Conditions

IP address information must be registered in the properties of the device node that the menu command is being executing from. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.2.10 Trace Route (IPv6) menu

Executes the traceroute command for specified managed devices from the manager and checks the communication path for IPv6 communication. For details, refer to "5.5.2 Executing a traceroute command (page 468)".

Preparation/Conditions

IPv6 address information must be registered in the properties of the device node that the menu command is being executed from. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

6.2.2.11 Show Unrecovered Aler menu

Displays the unrecovered alerts that have been published for a selected device node. For details, refer to "5.1.4 Managing alerts (page 456)".

6.2.2.12 Show All Alert menu

Displays all alerts that have been published for a selected device node. For details, refer to "5.1.4 Managing alerts (page 456)".

6.2.3 Performance Management menu

The **Performance Management** menu is used to collect performance information for managed devices, display graphs, and create reports.

6.2.3.1 List of available Performance Management menu commands

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Menu Item	Ref.	Op. (Normal)	Op. (Config)					Web View
"Data Collecting (page 576)" 1)	o	o	o	o	o			
"MIB Expression Creating (page 576)" 1)	o	o	o	o	o			
"Delete Report Cache on Console (page 576)"	o	o	o	o	o			
"Entry Information Import and Export (page 576)"			o	o	o			
"sFlow (page 576)"								

Menu Item	Ref.	Op. (Normal)	Op. (Config)					Web View
sFlow Agent List [1)]	o	o	o	o	o			
sFlow Data Setting [1)]	o	o	o	o	o			

1) The available range of operations changes depending on the user authority (reference authority or operation authority).

6.2.3.2 Data Collecting menu

Displays the Data Collecting Setting window for configuring data collection settings, graph display and report display. For details, refer to "4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices (page 334)".

Operations availability in operating modes:

- Normal mode

  The status of data collection settings can be viewed, collected data can be graphically displayed, and created reports can be viewed.

- Configuration mode

  Data collection can be set up and deleted, collected data can be displayed in the graph, and reports can be created and viewed.

6.2.3.3 MIB Expression Creating menu

Open the MIB Expression Creating window and create, edit, or delete an MIB expression. For details, refer to "4.16.3 Configuring MIB expressions (page 350)".

Operations availability in operating modes:

- Normal mode

  The definition of MIB expressions can be viewed.

- Configuration mode

  The definition of MIB expressions can be created, edited, deleted, and viewed.

6.2.3.4 Delete Report Cache on Console menu

Deletes temporary files transferred to the monitoring terminal from Manager for displaying reports.

6.2.3.5 Entry Information Import and Export menu

Import (batch registration and deletion) or export data collection settings information. For details, refer to "4.16.6 Batch registering data collection settings (page 359)".

6.2.3.6 sFlow Setting menu

sFlow Agent List menu

Displays the sFlow Agent List, and adds, deletes sFlow agents, and displays stored data in the graph. For details, refer to "4.17.1 Registering sFlow agents (page 373)".

Operations availability in operating modes:

- Normal mode

  Traffic flow under specified conditions can be displayed in the graph.

- Configuration mode

  The sFlow agents to be targeted for sFlow collection can be registered and the traffic flow under specified conditions can be displayed in the graph.

sFlow Data Setting menu

Displays the sFlow Data Received Setting dialog box and sets the collection method for flow data received from sFlow agents. For details, refer to "4.17.3 Setting duration of flow data retention (page 376)".

Operations availability in operating modes:

- Normal mode

  The settings information for the collection method can be viewed.

- Configuration mode

  The collection method can viewed and set up.

6.2.4 Device Config Management menu

The **Device Config Management** menu is used to perform operations relating to the management of configuration information for managed devices.

Resource Manager advanced function license needs to be applied to operate the items in this menu.

6.2.4.1 List of available Device Config Management menu commands

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Menu Item	Ref.	Op. (Normal)	Op. (Config)					Web View
"Alert Sending Setting (page 578)" 1)	o	o	o	o	o			
"Export Latest Config (page 578)" 1)	o	o	o	o	o			
"Schedule Information Import and Export (page 578)" 1)			o	o	o			
"Running-config Management (page 578)" 1)	o	o	o	o	o	o	o	
"Startup-config Management (page 579)" 1)	o	o	o	o	o	o	o	
"Check Configuration (page 579)" 1)	o	o	o	o	o	o	o	

1) The available range of operations changes depending on the user authority (reference authority or operation authority).

6.2.4.2 Alert Sending Setting menu

Displays each type of event detected by the command schedule and configuration management in the Network Manager Alert Management window. For details, refer to "4.20.5 Setting for sending an alert (page 414)".

Operations availability in operating modes:

- Normal mode

  Settings information can be viewed.

- Configuration mode

  Settings can be configured.

6.2.4.3 Export Latest Config menu

Exports the latest running-config to the manager. For details, refer to "4.20.4 Exporting the latest configuration (page 413)".

Operations availability in operating modes:

- Normal mode

  The export start/stop status and destination can be viewed.

- Configuration mode

  The export start/stop status can be changed and the destination can be set up.

6.2.4.4 Schedule Information Import and Export menu

Imports (batch registers) or exports change management schedule information. For details, refer to "4.20.2.4 Batch registration of change management schedule information (page 406)".

6.2.4.5 Running-config Management menu

Manages the running-config for managed devices. For details, refer to "5.14.1.1 Running-config Management window (page 512)".

Operations availability in operating modes:

- Normal mode

  The running-config change history can be viewed.

- Configuration mode

  Running-configs can be collected and distributed, and notes can be written in the change history.

Preparation/Conditions

Login information for target device nodes needs to be registered from the **Configuration Management**>**Login Information Setting** menu. For details, refer to "4.3 Registering Login Information (page 189)".

You need to assign a Resource Manager function license to target device nodes from the **NetMgr License Management** menu. For details, refer to "4.4 Managing the Advanced Functions License (page 201)".

6.2.4.6 Startup-config Management menu

Manages the startup-config for managed devices. For details, refer to "5.14.2.1 Startup-config Management window (page 520)".

Operations availability in operating modes:

- Normal mode

  The startup-config change history can be viewed.

- Configuration mode

  Startup-configs can be collected and distributed, and notes can be written in the change history.

Preparation/Conditions

Login information for target device nodes needs to be registered from the **Configuration Management**>**Login Information Setting** menu. For details, refer to "4.3 Registering Login Information (page 189)".

You need to assign a Resource Manager function license to target device nodes from the **NetMgr License Management** menu. For details, refer to "4.4 Managing the Advanced Functions License (page 201)".

6.2.4.7 Check Configuration menu

Monitors changes in the configuration of network devices. For details, refer to "4.20.2.1 Check Configuration window (page 404)".

Operations availability in operating modes:

- Normal mode

  Settings information for configuration change monitoring can be viewed and the locations of configuration changes can be verified.

- Configuration mode

  Configuration change monitoring can be set up and the locations of configuration changes can be verified.

Preparation/Conditions

Login information for target device nodes needs to be registered from the **Configuration Management**>**Login Information Setting** menu. For details, refer to "4.3 Registering Login Information (page 189)".

You need to assign a Resource Manager function license to target device nodes from the **NetMgr License Management** menu. For details, refer to "4.4 Managing the Advanced Functions License (page 201)".

6.2.5 Software Management menu

The **Software Management** menu is used to manage software for managed devices. Resource Manager advanced function license needs to be applied to operate the items in this menu.

6.2.5.1 List of available Software Management menu commands

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Menu Item	Ref.	Op. (Normal)	Op. (Config)					Web View
"File Management (page 580)" [1]	o	o	o	o	o			
"Software Upgrade (page 580)" [1]	o	o	o	o	o	o	o	

1) The available range of operations changes depending on the user authority (reference authority or operation authority).

6.2.5.2 File Management menu

Registers software deployed to managed devices in Network Manager. For details, refer to "5.15.1 Managing software files (page 531)".

Operations availability in operating modes:

- Normal mode

  Registered software information can be viewed.

- Configuration mode

  Software can be registered.

Preparation/Conditions

Resource Manager function license needs to be assigned to the node before registration information can be controlled from this menu item. For details, refer to "4.4 Managing the Advanced Functions License (page 201)".

6.2.5.3 Software Upgrade menu

Deploys software to managed devices. For details, refer to "5.15.2.1 Deploying a software file (page 543)".

Operations availability in operating modes:

- Normal mode

  The software version change history can be viewed.

- Configuration mode

  Software can be deployed and devices can be set to reboot.

Preparation/Conditions

- Login information for target device nodes needs to be registered from the **Configuration Management**>**Login Information Setting** menu. For details, refer to "4.3 Registering Login Information (page 189)".

- You need to assign a Resource Manager function license to target device nodes from the **NetMgr License Management** menu. For details, refer to "4.4 Managing the Advanced Functions License (page 201)".
- Software to be deployed must be registered in Network Manager from the **Software Management**>**File Management** menu. For details, refer to "5.15.1 Managing software files (page 531)".

6.2.6 NetMgr License Management menu

Allocates and cancels Node Manager function licenses and Resource Manager advanced function licenses for managed devices in the NetMgr License Manager dialog box. For details, refer to "4.4.1.1 NetMgr License Manager dialog box (page 202)". For details of the advanced function licenses, refer to "1.2 Network Manager Licenses (page 12)".

Menus displayed under different user permissions:

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Ref.	Op. (Normal)	Op. (Config)					Web View
o	o	o	o	o	o		o

Operations availability in operating modes:

- Normal mode

  The allocation status of licenses for managed devices can be viewed.
- Configuration mode

  Licenses for managed devices can be allocated and canceled.

Preparation/Conditions

If advanced function licenses are being allocated to managed devices, the advanced function licenses need to be activated in advance. For details, refer to "10.3 Registering Licenses (page 759)".

6.2.7 Environment Setting menu

Configures settings for the Network Manager operating environment. For details, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

Menus displayed under different user permissions:

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Ref.	Op. (Normal)	Op. (Config)					Web View
		o	o				o

6.2.8 Device Front Panel menu

Shows the front panel image for a node and displays various types of management and statistical information. For details, refer to "5.9 Displaying Device Front Panels (page 475)".

Menus displayed under different user permissions:

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Ref.	Op. (Normal)	Op. (Config)					Web View
o	o	o				o	

Operations availability in operating modes and user authority:

- Normal mode

  Reference authority:

  The device front panel can be displayed and all management and statistical information can be viewed.

  Operation authority:

  The device front panel can be displayed, all management and statistical information can be viewed, and interfaces using SNMP Set can be opened and closed.

- Configuration mode

  The device front panel display can be customized, all management and statistical information can be viewed, and interfaces using SNMP Set can be opened and closed.

Preparation/Conditions

- You need to allocate Node Manager function licenses to target device nodes from the **NetMgr License Management** menu. For details, refer to "4.4 Managing the Advanced Functions License (page 201)".
- The SNMP community name (get) or SNMPv3 information must be registered in the properties of the target device node to perform SNMP communication with devices. For details, refer to "4.2.9.1 Changing icon properties manually (page 184)".

  In addition, when performing controls such as opening and closing interfaces, the SNMP community name (set) information needs to be adapted and registered.

6.2.9 Property menu

Displays and makes changes to the properties of a selected node or connection line. For details regarding node properties, refer to "4.2.9.1 Changing icon properties manually (page 184)". For details regarding connection-line properties, refer to "4.2.9.2 Changing topology information manually (page 185)".

Menus displayed under different user permissions:

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Ref.	Op. (Normal)	Op. (Config)					Web View
o	o	o			o	o	o

Operations availability in operating modes:

- Normal mode

  Property information can be viewed.

- Configuration mode

  Property information can be changed.

6.2.10 Move menu

Moves a specified icon. For details, refer to "4.2.9.3 Moving an icon to another map (page 186)".

Menus displayed under different user permissions:

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Ref.	Op. (Normal)	Op. (Config)					Web View
		o			o	o	o

6.2.11 Copy menu

Copies a specified icon. When copied icon information is pasted into the Map View, a link to existing information is created.

Menus displayed under different user permissions:

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Ref.	Op. (Normal)	Op. (Config)					Web View
		o				o	o

6.2.12 Update menu

This menu is not used in Network Manager. (It will always be unavailable.)

6.2.13 Delete menu

Deletes specified nodes, connection lines, and other objects. For details, refer to "4.2.9.6 Deleting an icon (page 188)".

Menus displayed under different user permissions:

The availability of menu commands for different user authority (reference authority and operation authority), and each node icon and web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Ref.	Op. (Normal)	Op. (Config)					Web View
		o			o	o	o

6.3 Audit Log menu

Performs operations relating to audit logs.

The **Audit Log** node is only displayed in the tree view if the logged in user has a reference authority for audit logs. For details regarding user authority, refer to "4.1.3 Changing group authority (page 113)".

6.3.1 List of available Audit Log menu commands

The availability of main menu commands for different user authority (reference authority and operation authority) and the web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Menu Item	Ref.	Op. (Normal)	Op. (Config)	Web View
"Report Setting (page 584)"			o	o
"Initialize Category (page 584)"			o	o
"Swap Category (page 584)"			o	o

Tip

Audit log update authority is required to operate these menu items. For details, refer to "4.1.3 Changing group authority (page 113)".

6.3.2 Report Setting menu

Sets up reports for audit logs. For details, refer to "4.23.1 Defining report settings for audit logs (page 444)".

6.3.3 Initialize Category menu

Deletes all audit logs in a specified category (application, security, system, or audit log). For details, refer to "5.16.4 Deleting audit logs within a category (page 555)".

6.3.4 Swap Category menu

Deletes audit logs in a specified category (application, security, system, or audit log) in a specified date. For details, refer to "5.16.4 Deleting audit logs within a category (page 555)".

6.4 Common Menus for Background in the Map View

Performs operations relating to the background of the Map View.

6.4.1 List of available Common Background menu commands

The availability of main menu commands for different user authority (reference authority and operation authority) and the web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Menu Item	Ref.	Op. (Normal)	Op. (Config)	Web View
"Back (page 585)" 1)	o	o	o	o
"Up (page 585)" 1)	o	o	o	o
"Home (page 585)" 1)	o	o	o	o
"Select All (page 585)" 1)	o	o	o	o
"Manual Register (page 585)" 1)			o	o
"Paste (page 586)" 1)			o	o
"Port Name (page 586)" 1)			o	o
"Background Color (page 586)"			o	o
"Background Bitmap (page 586)"			o	o
"Grid (page 586)"			o	o
"Arrange Icon (page 586)"			o	o

1) Operations can only be performed for the Map View for map icons located below the **NetworkManagement** icon in the **NetworkView**.

6.4.2 Back menu

Displays the Map View for the previously displayed map. Displays up to 100 previous maps.

6.4.3 Up menu

Displays the Map View for maps one level up.

6.4.4 Home menu

Selects all icons. Displays the Map View of the **NetworkManagement** icon.

6.4.5 Select All menu

Selects all icons.

6.4.6 Manual Register menu

Manually registers device icons. For details, refer to "4.2.2 Manually registering devices and networks (page 138)".

6.4.7 Paste menu

Pastes copied icons into the Map View. Pasted icons are created as a link to existing information.

Preparation/Conditions

This menu becomes available when icons are copied.

6.4.8 Port Name menu

Displays the port names for connection line destination nodes and source nodes on the background of the Map View. For details, refer to "4.2.6.1 Changing the background of Map View (page 175)".

6.4.9 Background Color menu

Changes the background color of a specified Map View. For details, refer to "4.2.6.1 Changing the background of Map View (page 175)".

6.4.10 Background Bitmap menu

Inserts a bitmap to be used as the background in a specified Map View. For details, refer to "4.2.6.1 Changing the background of Map View (page 175)".

6.4.11 Grid menu

Displays grid lines on the background of a specified Map View. For details, refer to "4.2.6.1 Changing the background of Map View (page 175)".

6.4.12 Arrange Icon menu

Arranges the icons in a specified Map View.

6.5 Common Menus for Objects (Icons) in the Map View

Changes the method of displaying objects (icons) in the Map View. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Menu Item	Ref.	Op. (Normal)	Op. (Config)	Web View
Change Order				
"Move to Front (page 587)"			o	o
"Move to Back (page 587)"			o	o
"Move Forward (page 587)"			o	o
"Move Backward (page 587)"			o	o
Icon Text				
"Bottom (page 587)"			o	o
"Right (page 587)"			o	o
"Top (page 587)"			o	o

Menu Item	Ref.	Op. (Normal)	Op. (Config)	Web View
"Left (page 587)"			o	o

6.5.1 Change Order menu

6.5.1.1 Move to Front menu

Moves the selected icon to the front.

6.5.1.2 Move to Back menu

Moves the selected icon to the back.

6.5.1.3 Move to Forward menu

Moves the selected icon forward.

6.5.1.4 Move to Backward menu

Moves the selected icon backward.

6.5.2 Icon Text menu

6.5.2.1 Bottom menu

Displays text below the selected icon.

6.5.2.2 Right menu

Displays text to the right of the selected icon.

6.5.2.3 Top menu

Displays text above the selected icon.

6.5.2.4 Left menu

Displays text to the left of the selected icon.

6.6 Common Menus in the Tree View

Performs operations relating to the display of each node in the tree view.

6.6.1 List of available Tree View Common menu commands

The availability of main menu commands for different user authority (reference authority and operation authority) and the web monitoring view, is shown below. For abbreviation of the items, refer to "Chapter 6. Menu Reference (page 559)".

Menu Item	Ref.	Op. (Normal)	Op. (Config)	Web View
"Expand (page 588)"	o	o	o	o

Menu Item	Ref.	Op. (Normal)	Op. (Config)	Web View
"Collapse (page 588)"	o	o	o	o
"Find (page 588)"	o	o	o	o

6.6.2 Expand menu

Expands the specified tree node.

Preparation/Conditions

This menu becomes available when collapsed nodes are selected.

6.6.3 Collapse menu

Collapses the specified tree node.

Preparation/Conditions

This menu becomes available when expanded nodes are selected.

6.6.4 Find menu

Searches for a node. For details, refer to "5.17 Searching for a Node (page 556)".

Chapter 7. Supplemental Explanation for Monitoring Function

Contents

7.1 State Monitoring Rules 590
7.2 Data Collection Rules 622
7.3 Standard Specification Format 644
7.4 Adding MIBs 648
7.5 Monitoring Devices Using IPv6 662
7.6 SNMP Trap Identification Method 664
7.7 Notes on Counter-type and Counter64-type MIBs 666
7.8 Notes on Monitoring Nexus 5000 and 2000 Series 667

7.1 State Monitoring Rules

7.1.1 Rules for monitoring alive status

7.1.1.1 updown:UpDownCheck

Function description

Sends ICMP ECHO packets to the monitored device. If a response is obtained, the device is considered to be operating.

If a response is not obtained, it is considered to be down and a fault event is issued.

If **Response_Time** and **Repeat** arguments are specified, the response time is also checked when ICMP ECHO response is obtained.

Arguments

- **Response_Timeout[msec]**

  Specify the upper limit of the response time when the response for ICMP ECHO packet is obtained.

  If the response time repeatedly exceeds this value for the number of times specified in **Repeat** argument, a "Response Time Error" event is issued instead of a "Down" event.

  You can specify a value from 0 to 4,294,967,295 (unit: milliseconds). If this value is omitted or 0 is specified, a response time check is not performed.

- **Repeat**

  Specify how many times the **Response_Time** upper limit can be exceeded before a "Response Time Error" event notification is generated.

  If the response time repeatedly falls back below the **Response_Time** upper limit for the specified number of times, a "Response Time Recovery" event is issued.

  You can specify a value from 0 to 4,294,967,295. If this is omitted, the number of times is set to three. If the **Response_Time** upper limit is omitted, a response time check is not performed.

- **Communication_Failure_Repeat**

  Specify the number of consecutive times a down is detected before a fault event notification is to be issued.

  You can specify a value from 0 to 4,294,967,295. If this is omitted, the number of times is set to one. A fault event notification is issued as soon as the first down is detected.

For other setting items such as interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

If **Response_Time**t exceeds **Retry Interval** of SNMP/ICMP packets specified in the Environment Setting dialog box, the response time of ICMP ECHO will not be checked substantially.

Example:

If **Retry Interval** of SNMP/ICMP packets in the Environment Setting dialog box is set to "4 8" and **Response_Timeout** is set to "6000" (milli seconds), the first ICMP ECHO response time will not be checked and the second ICMP ECHO response time will be checked.

7.1.1.2 updownv6:ipv6UpDownCheck

Function description

Sends ICMPv6 ECHO packets to the monitored device. If a response is obtained, the device is considered to be operating. If a response is not obtained, it is considered to be down and a fault event is issued.

If **Response_Time** and **Repeat** arguments are specified, the response time is also checked when ICMPv6 ECHO response is obtained.

Arguments

- **Response_Timeout[msec]**

  Specify the upper limit of the response time when the response for ICMPv6 ECHO packet is obtained.

  If the response time repeatedly exceeds this value for the number of times specified in **Repeat** argument, a "Response Time Error" event is issued instead of a "Down" event.

  You can specify a value from 0 to 4294967295 (unit: milliseconds). If this value is omitted or 0 is specified, a response time check is not performed.

- **Repeat**

  Specify how many times the response time upper limit can be exceeded before a **Response_Time** Error event notification is generated.

  If the **Response_Time** repeatedly falls back below the response time upper limit for the specified number of times, a "Response Time Recovery" is issued.

  You can specify a value from 0 to 4294967295. If this is omitted, the number of times is set to three. If the **Response_Time** upper limit is omitted, a response time check is not performed.

- **Communication_Failure_Repeat**

  Specify the number of consecutive times a down is detected before a fault event notification is to be issued.

  You can specify a value from 0 to 4,294,967,295. If this is omitted, the number of times is set to one. A fault event notification is issued as soon as the first down is detected.

For other setting items such as interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

1. In the case of the upgrade from MasterScope Network Manager 2.0, this rule is registered as "Standing rule file". To use this rule, embed this rule first. For details, refer to "4.10.7 Embedding rule files (page 258)".
2. If **Respense_Timeout** exceeds **Retry Interval** of SNMP/ICMP packets specified in the Environment Setting dialog box, the response time of ICMP ECHO will not be checked substantially.

   Example:

   If **Retry Interval** of SNMP/ICMP packets in the Environment Setting dialog box is set to "4 8" and **Response_Timeout** is set to "6000" (milli seconds), the first ICMP ECHO response time will not be checked and the second ICMP ECHO response time will be checked.

7.1.1.3 snmpchk:SNMP_Check

Function description

Obtains the value of the monitored MIB (.system.sysUpTime.0) and, if a response is obtained, considers it to be operating. If the MIB value is not obtained, it is considered to be stopped and a fault event is issued.

This rule is valid for monitored targets on which the SNMP function on the TCP/IP is operating.

This rule can be used as alive monitoring for the devices that are set to block ICMP ECHO packets.

For setting items, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

1. If the SNMP function on the monitored targets is operating but a response is not obtained because the routing table is incorrectly set or SNMP communication between the monitored targets and Network Manager is not permitted, it is considered to be stopped.
2. If SNMP security settings (community name in SNMP v1/v2c, or user name, password, security level, authentication protocol/password, privacy protocol/password in SNMPv3) are incorrectly set, it is also considered to be stopped.

7.1.2 Rules for monitoring interface status

7.1.2.1 ifdown:InterfaceDown

Function description

Monitors the network interface for the monitored device and issues an alert if the interface is down when it should actually be up. Specifically, the following MIBs are monitored.

1. .interfaces.ifTable.ifEntry.ifAdminStatus
2. .interfaces.ifTable.ifEntry.ifOperStatus

The ".interfaces.ifTable.ifEntry.ifIndex" value is output as the event details.

Arguments

- **Interface_Number**

  Specify the interface numbers for the interfaces that you want to monitor.

  Use a number displayed in the **Index** column in the **IPv4** tab of the Interface Properties dialog box. To specify multiple interfaces, separate them using a comma.

  To select from the list of interfaces, click  button and select the interfaces in the Interface Number Select dialog box. For details regarding the Interface Number Select dialog box, refer to "4.10.2.3 Variable setting dialog box (page 247)".

  If this is omitted, the default target port is monitored. For details regarding the default target port or the available interface number, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

Caution

1. There are several important points to consider when monitoring Nexus 5000 and 2000 series devices. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".
2. While occurring an event relating to the interface specified in the **Interface_Number** column or the interface specified as the **Default Ports**, if the interface disappears for any reason, the occurring event cannot be canceled. If any inconsistency occurs in events, confirm the setting of the State Monitoring window or the setting of **Default Target Port** in the Properties dialog box of the target device.

7.1.2.2 ifDescr:UpDownCheck

Function description

Monitors the network interface for the monitored device and issues an alert if it is down when it should actually be up. Specifically, the following MIBs are monitored.

1. .interfaces.ifTable.ifEntry.ifAdminStatus
2. .interfaces.ifTable.ifEntry.ifOperStatus

The ".interfaces.ifTable.ifEntry.ifDescr" value is output as the event details.

Arguments

- **Interface_Number**

  Specify the interface numbers for the interfaces that you want to monitor.

  Use a number displayed in the **Index** column in the **IPv4** tab of the Interface Properties dialog box. To specify multiple interfaces, separate them using a comma.

  To select from the list of interfaces, click  button and select the interfaces in the Interface Number Select dialog box. For details regarding the Interface Number Select dialog box, refer to "4.10.2.3 Variable setting dialog box (page 247)".

  If this is omitted, the default target port is monitored. For details regarding the default target port or the available interface number, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

Caution

1. There are several important points to consider when monitoring Nexus 5000 and 2000 series devices. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".
2. While occurring an event relating to the interface specified in the **Interface_Number** column or the interface specified as the **Default Ports**, if the interface disappears for any reason, the occurring event cannot be canceled. If any inconsistency occurs in events, confirm the setting of the State Monitoring window or the setting of **Default Target Port** in the Properties dialog box of the target device.
3. Do not use this rule for monitoring the devices that do not support ".interfaces.ifTable.ifEntry.ifDescr" value.

7.1.2.3 ifName:UpDownCheck

Function description

Monitors the network interface for the monitored device and issues an alert if it is down when it should actually be up. Specifically, the following MIBs are monitored.

1. .interfaces.ifTable.ifEntry.ifAdminStatus
2. .interfaces.ifTable.ifEntry.ifOperStatus

The ".ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName" value is output as the event details.

Arguments

- **Interface_Number**

  Specify the interface numbers for the interfaces that you want to monitor.

  Use a number displayed in the **Index** column in the **IPv4** tab of the Interface Properties dialog box. To specify multiple interfaces, separate them using a comma.

  To select from the list of interfaces, click  button and select the interfaces in the Interface Number Select dialog box. For details regarding the Interface Number Select dialog box, refer to "4.10.2.3 Variable setting dialog box (page 247)".

  If this is omitted, the default target port is monitored. For details regarding the default target port or the available interface number, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

Caution

1. There are several important points to consider when monitoring Nexus 5000 and 2000 series devices. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".
2. While occurring an event relating to the interface specified in the **Interface_Number** column or the interface specified as the **Default Ports**, if the interface disappears for any reason, the occurring event cannot be canceled. If any inconsistency occurs in events, confirm the setting of the State Monitoring window or the setting of **Default Target Port** in the Properties dialog box of the target device.
3. Do not use this rule for monitoring the devices that do not support ".ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName" value.

7.1.2.4 ifOper:InterfaceStateCheck

Function description

If there are any changes in the interface of the managed component, an event is issued. If the status changes from a down status to a different down status, a cancel event is output first and then a new event is issued. Specifically, the following MIBs are monitored.

1. .interfaces.ifTable.ifEntry.ifAdminStatus
2. .interfaces.ifTable.ifEntry.ifOperStatus

Arguments

- **Interface_Number**

  Specify the interface numbers for the interfaces that you want to monitor.

  Use a number displayed in the **Index** column in the **IPv4** tab of the Interface Properties dialog box. To specify multiple interfaces, separate them using a comma.

  To select from the list of interfaces, click  button and select the interfaces in the Interface Number Select dialog box. For details regarding the Interface Number Select dialog box, refer to "4.10.2.3 Variable setting dialog box (page 247)".

  If this is omitted, the default target port is monitored. For details regarding the default target port or the available interface number, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

Caution

1. There are several important points to consider when monitoring Nexus 5000 and 2000 series devices. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".
2. While occurring an event relating to the interface specified in the **Interface_Number** column or the interface specified as the **Default Ports**, if the interface disappears for any reason, the occurring event cannot be canceled. If any inconsistency occurs in events, confirm the setting of the State Monitoring window or the setting of **Default Target Port** in the Properties dialog box of the target device.

7.1.2.5 ifup:InterfaceUp

Function description

Monitors the network interface for the monitored device and issues an alert if it is currently up when it should actually be down.

For example, this rule becomes effective if it is reported that the ISDN backup line is functioning. Specifically, ".interfaces.ifTable.ifEntry.ifOperStatus" is monitored.

Arguments

- **Interface_Number**

  Specify the interface numbers for the interfaces that you want to monitor.

  Use a number displayed in the **Index** column in the **IPv4** tab of the Interface Properties dialog box. To specify multiple interfaces, separate them using a comma.

  To select from the list of interfaces, click  button and select the interfaces in the Interface Number Select dialog box. For details regarding the Interface Number Select dialog box, refer to "4.10.2.3 Variable setting dialog box (page 247)".

  If this is omitted, the default target port is monitored. For details regarding the default target port or the available interface number, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

Caution

1. There are several important points to consider when monitoring Nexus 5000 and 2000 series devices. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".
2. While occurring an event relating to the interface specified in the **Interface_Number** column or the interface specified as the **Default Ports**, if the interface disappears for any reason, the occurring event cannot be canceled. If any inconsistency occurs in events, confirm the setting of the State Monitoring window or the setting of **Default Target Port** in the Properties dialog box of the target device.

7.1.2.6 nvtp-topchk:InterfaceDownCheck

Function description

Monitors whether the network interface for the monitored device is down. If it is down, an alert is issued for the registered connection line and the color of the connection line is changed. Specifically, the ".interfaces.ifTable.ifEntry.ifOperStatus" is monitored.

Arguments

- **Interface_Number**

  Specify the interface numbers for the interfaces that you want to monitor.

  Use a number displayed in the **Index** column in the **IPv4** tab of the Interface Properties dialog box. To specify multiple interfaces, separate them using a comma.

  To select from the list of interfaces, click  button and select the interfaces in the Interface Number Select dialog box. For details regarding the Interface Number Select dialog box, refer to "4.10.2.3 Variable setting dialog box (page 247)".

  If this is omitted, the default target port is monitored. For details regarding the default target port or the available interface number, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

Caution

1. This rule does not check the connection line which is registered as LAG (Link Aggregation) but is not supported in autodiscover function for topology information. For detail, refer to "4.2.3.2 Automatically detecting topology information (page 149)".
2. There are several important points to consider when monitoring Nexus 5000 and 2000 series devices. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".
3. While occurring an event relating to the interface specified in the **Interface_Number** column or the interface specified as the **Default Ports**, if the interface disappears for any reason, the occurring event cannot be canceled. If any inconsistency occurs in events, confirm the setting of the State Monitoring window or the setting of **Default Target Port** in the Properties dialog box of the target device.

7.1.2.7 nvtp-stpstat:STP_PortStateCheck

Function description

When the STP is operating, the STP Status of each port is checked, along with whether the port is in "Forwarding" status or not. If the port is in "Forwarding" status, an alert is issued for the registered connection line and the color of the connection line is changed.

This only can only be done with the following device types.

1. Cisco Systems Catalyst switches
2. NEC IP8800/700 Series and ES8800/1700 Series
3. NEC IP8800/S2400 Series, S3600 Series, S6300 Series and S6700 Series
4. NEC IP8800/S300 Series and S400 Series
5. NEC CX-uH24 (Physical ports only. Sharing ports are not supported.)
6. Foundry FDP support switches (Physical ports only. Trunk ports are not supported.)

Arguments

- **VLAN_Number.Port_Number**

  Specify the port that you want to monitor in the format of "vlan#.Port#". Multiple ports can be entered using comma separation.

  A range can be specified by using a hyphen (-) between the vlan numbers and port numbers (for example: "10-20.15-20").

  If this is omitted, all VLANs for all ports will be monitored.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

1. If the icon type of the target node is incorrect, this rule might not work. Specify the correct icon type. To modify the icon type or SNMP settings of the target node, stop the rules while modifying.
2. If the target is a Catalyst device, STP information must be acquired through SNMPv1 or v2c. For this reason, even if SNMPv3 settings are configured, specify the SNMP community name in the properties of the target node, and configure the device setting to be able to communicate by SNMPv1 or v2c.
3. For Catalyst devices, Network Manager cannot detect STP port status change when STP status changes from "forwarding" to "disabled" (link down). If you want to detect link down of physical ports, use "7.1.2.6 nvtp-topchk:InterfaceDownCheck (page 596)".

7.1.3 Rules for monitoring threshold

7.1.3.1 ifload64:InterfaceLoad_64bit

Function description

Monitors the input/output load of the high-speed network interface for monitored devices. This rule only applies to SNMPv2c or v3 compatible devices. Specifically, the following MIBs are monitored. For details regarding these counter-type MIBs, refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

1. .ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInOctets

2. .ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutOctets

Arguments

- **Interface_Number**

  Specify the interface numbers for the interfaces that you want to monitor.

  Use a number displayed in the **Index** column in the **IPv4** tab of the Interface Properties dialog box. To specify multiple interfaces, separate them using a comma.

  To select from the list of interfaces, click  button and select the interfaces in the Interface Number Select dialog box. For details regarding the Interface Number Select dialog box, refer to "4.10.2.3 Variable setting dialog box (page 247)".

  If this is omitted, the default target port is monitored. For details regarding the default target port or the available interface number, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

- **Upper_Limit[Mbps]**

  If the value exceeds the value specified here, a fault event is issued.

  Specify an integer from 0 to 18,446,744,073,709,551,615, in units of Mbps (Mbits/second).

  This value cannot be omitted. Only integer values can be specified.

- **Reset_Value[Mbps]**

  If the value falls below the value specified here, the fault is recovered.

  Specify an integer from 0 to 18,446,744,073,709,551,615, in units of Mbps (Mbits/second).

  This value cannot be omitted. Only integer values can be specified.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

Caution

1. There are several important points to consider when monitoring Nexus 5000 and 2000 series devices. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".
2. While occurring an event relating to the interface specified in the **Interface_Number** column or the interface specified as the **Default Ports**, if the interface disappears for any reason, the occurring event cannot be canceled. If any inconsistency occurs in events, confirm the setting of the State Monitoring window or the setting of **Default Target Port** in the Properties dialog box of the target device.

7.1.3.2 ifload:InterfaceLoad

Function description

Monitors the input/output load of the network interface for monitored devices.

Specifically, the following MIBs are monitored. For details regarding these counter-type MIBs, refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

1. .interfaces.ifTable.ifEntry.ifInOctets
2. .interfaces.ifTable.ifEntry.ifOutOctets

Arguments

- **Interface_Number**

  Specify the interface numbers for the interfaces that you want to monitor.

  Use a number displayed in the **Index** column in the **IPv4** tab of the Interface Properties dialog box. To specify multiple interfaces, separate them using a comma.

  To select from the list of interfaces, click  button and select the interfaces in the Interface Number Select dialog box. For details regarding the Interface Number Select dialog box, refer to "4.10.2.3 Variable setting dialog box (page 247)".

  If this is omitted, the default target port is monitored. For details regarding the default target port or the available interface number, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

- **Upper_Limit[Kbps]**

  If the value exceeds the value specified here, a fault event is issueed.

  Specify an integer from 0 to 4,294,967,295, in units of Kbps (Kbits/second).

  This value cannot be omitted. Only integer values can be specified.

- **Reset_Value[Kbps]**

  If the value falls below the value specified here, the fault is recovered.

  Specify an integer from 0 to 4,294,967,295, in units of Kbps (Kbits/second).

  This value cannot be omitted. Only integer values can be specified.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

1. There are several important points to consider when monitoring Nexus 5000 and 2000 series devices. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".
2. While occurring an event relating to the interface specified in the **Interface_Number** column or the interface specified as the **Default Ports**, if the interface disappears for any reason, the occurring event cannot be canceled. If any inconsistency occurs in events, confirm the setting of the State Monitoring window or the setting of **Default Target Port** in the Properties dialog box of the target device.

7.1.3.3 nvtp-bandchk:BandTraffic

Function description

Monitors traffic on devices, issues an alert when traffic exceeds a specified threshold value and changes the color of the relevant physical topology line. In addition, this rule separates some of the usage rate levels and allows users to recognize abnormal physical topology.

This rule monitors counter-type MIBs. For details regarding these counter-type MIBs, refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

Arguments

- **Interface_Number**

  Specify the interface numbers for the interfaces that you want to monitor.

Use a number displayed in the **Index** column in the **IPv4** tab of the Interface Properties dialog box. To specify multiple interfaces, separate them using a comma.

To select from the list of interfaces, click  button and select the interfaces in the Interface Number Select dialog box. For details regarding the Interface Number Select dialog box, refer to "4.10.2.3 Variable setting dialog box (page 247)".

If this is omitted, the default target port is monitored. For details regarding the default target port or the available interface number, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

- **Critical_Threshold**

  If the value exceeds the usage rate specified here, a critical state fault event is issued.

  This may be omitted.

  Specify a value from the usage rate of the next fault level down (1 if there are no lower levels) to 100.

- **Major_Threshold**

  If the value is between the usage rate specified here and the usage rate of the next fault level up (100 if there are no higher levels), a "Major Fault" event is issued.

  This may be omitted. If this is omitted, a "Major Fault" event is not issued.

  Specify a value between the usage rate of the next fault level down (1 if there are no lower levels), through to the next level up (100 if there are no higher levels).

- **Minor_Threshold**

  If the value is between the usage rate specified here and the usage rate of the next fault level up (100 if there are no higher levels), a "Minor Fault" event is issued.

  This may be omitted. If this is omitted, a "Minor Fault" event is not issued.

  Specify a value between the usage rate of the next fault level down (1 if there are no lower levels), and that of the next level up (100 if there are no higher levels).

- **Warning_Threshold**

  If the value is between the usage rate specified here and the usage rate of the next fault level up, a "Warning" fault event is issued.

  This may be omitted. If this is omitted, a "Warning" event is not issued.

  Specify a value between 1 and the usage rate of the next fault level up (100 if there are no higher levels).

- **InOut**

  Select "ifInOctets", "ifOutOctets" or to check both for the following values: Upper and lower case characters are treated the same in "IN" and "OUT".

  - "IN"

    Check "InOctets" only.

  - "OUT"

    Check "OutOctets" only.

  - "IN,OUT"

    Check both the "InOctets" and "OutOctets". If either matches a usage rate, the applicable event is issued. If there is a usage rate for both, the highest fault level is issued.

- "IN+OUT"

  Check the sum of "InOctets" and "OutOctets". Valid in duplex mode half.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

1. This rule does not check the connection line which is registered as LAG (Link Aggregation) but is not supported in autodiscover function for topology information. For details, refer to "4.2.3.2 Automatically detecting topology information (page 149)".
2. There are several important points to consider when monitoring Nexus 5000 and 2000 series devices. For details, refer to "7.8 Notes on Monitoring Nexus 5000 and 2000 Series (page 667)".
3. While occurring an event relating to the interface specified in the **Interface_Number** column or the interface specified as the **Default Ports**, if the interface disappears for any reason, the occurring event cannot be canceled. If any inconsistency occurs in events, confirm the setting of the State Monitoring window or the setting of **Default Target Port** in the Properties dialog box of the target device.

7.1.3.4 thresh:ThresholdValueCheck

Function description

Performs a general threshold value check.

Arguments

- **MIB_Name**

  Specify the MIB name for the monitoring target. (It is not possible to specify multiple MIBs using commas or braces.)

  Specifiable character is single-byte character.

  If you want to monitor counter-type MIBs, refer to the notes described in "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

- **Upper_Threshold**

  Specify the upper threshold value.

  Specify a value from -2,147,483,648 to 2,147,483,647.

- **Lower_Threshold**

  Specify the lower threshold value.

  Specify a value from -2,147,483,648 to 2,147,483,647.

- **Comparison_Method**

  Specify the comparison method (delta or absolute).

  delta: Comparing a value calculated as "(current value - previous value) / interval time (seconds)" with the upper and lower threshold values.

  absolute: Comparing a value directly with the upper and lower threshold values.

- **Event_Generating_Opportunity**

  Specify the warning trigger (rise or fall).

  rise: If you want an event report generated when the upper threshold value is exceeded.

fall: If you want an event report generated when the value falls below the lower threshold value.

If rise is set, the next fault event is not generated unless at some point the value falls below the lower threshold value. In the same way, if fall is set, the next fault event is not generated unless at some point the value exceeds the upper threshold value.

- **MIB_Name_Flag**

  Specify "1" to include the MIB name in the fault event. Specify "0" if you do not want to include the MIB name.

  Specifiable character is single-byte "1" or "0".

- **MIB_Value_Flag**

  Specify "1" to include the MIB value in the fault event. Specify "0" if you do not want to include the MIB value.

  Specifiable character is single-byte "1" or "0".

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

7.1.4 Rules for host resource monitoring

7.1.4.1 host_cpuload:CPU_LoadAvg_1min_HOST

Function description

Monitors the CPU usage rate of a host for the previous one minute.

This rule is only applicable to devices compatible with RFC 2790-compliant HOST-RESOURCES-MIB.

1. .host.hrDevice.hrDeviceTable.hrDeviceEntry.hrDeviceType
2. .host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad

Arguments

- **Upper_Limit**

  A fault event is issued if the 1-minute CPU usage rate exceeds the value specified here. You can specify a single-byte number between 1 and 100. The unit of measurement is percentages (%). This cannot be omitted.

- **Reset_Value**

  If the value falls below the value specified here, the fault is recovered. You can specify a single-byte number between 0 and 99.The unit of measurement is percentages (%). This cannot be omitted.

- **Comparison_Method**

  If there are multiple CPUs, compare the CPU usages with an upper limit value and a reset value using the comparison methods specified here.

  Select the value from the following.

  - average

    Compares the average of multiple CPUs usage rates with an upper limit value and a reset value.

- each

  Compares the each CPU usage rate with each upper limit value and reset value. A fault event is issued if the CPU usage exceeds the upper limit value in one or more CPUs. The fault event is recovered if the CPU usage falls below the reset value in all the CPUs.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

In the case of the upgrade from MasterScope Network Manager 2.0, this rule is registered as "Standing rule file". To use this rule, embed this rule first. For details, refer to "4.10.7 Embedding rule files (page 258)".

7.1.4.2 host_disk_usage:Disk_UsageRate

Function description

Monitors the usage rate of a local disk.

This rule is only applicable to devices compatible with RFC 2790-compliant HOST-RESOURCES-MIB.

1. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageType
2. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageDescr
3. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageAllocationUnits
4. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageSize
5. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageUsed

Arguments

- **Upper_Limit**

  A fault event is issued if the disk usage rate exceeds the value specified here. You can specify a single-byte number between 1 and 100. The unit of measurement is percentages (%). This cannot be omitted.

- **Reset_Value**

  If the value falls below the value specified here, the fault is recovered. You can specify a single-byte number between 0 and 99. The unit of measurement is percentages (%). This cannot be omitted.

- **Disk_Name**

  Specifies the name of the disk that you want to monitor. The disk that contains the character string specified in Disk_Name is monitored. If omitted, all the local disks of the node are monitored.

You can check the notation of the Disk_Name by acquiring monitored device MIB using the `NvPROAmibGetSvc` / `NvPROAmibGetMgr` command.

For details regarding these commands, refer to "9.7.1 NvPROAmibGetSvc/NvPROAmibGetMgr (page 712)".

Verifying the disk name

1. Check the device ID.

```
NvPROAmibGet(Svc|Mgr) -form "%C\t%-22AB\t\"%V\"\n"
 target_node .host.2.3.1.2
```

Example of execution result:

```
target_node hrStorageType.1
   ".host.hrStorage.hrStorageTypes.hrStorageFixedDisk"
target_node hrStorageType.2
   ".host.hrStorage.hrStorageTypes.hrStorageRam"
target_node hrStorageType.3
   ".host.hrStorage.hrStorageTypes.hrStorageVirtualMemory"
```

".host.hrStorage.hrStorageTypes.hrStorageFixedDisk" indicates the local disk. Use the value of *x* in "hrStorageType.*x*" to check the disk name in the next step.

In the result above, use "1" to check the disk name

2. Check the disk name.

```
NvPROAmibGet(Svc|Mgr) -form "%C\t%-22AB\t\"%V\"\n"
  target_node .host.2.3.1.3.x
```

Example of execution result:

```
target_node hrStorageDescr.1 "C:\ Label: Serial Number acdc64c4"
```

"C:\ Label: Serial Number acdc64c4" is the disk name in the result above.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

In the case of the upgrade from MasterScope Network Manager 2.0, this rule is registered as "Standing rule file". To use this rule, embed this rule first. For details, refer to "4.10.7 Embedding rule files (page 258)".

7.1.4.3 host_pmem_usage:PhysicalMemory_UsageRate

Function description

Monitors the usage rate of physical memory.

This rule is only applicable to devices compatible with RFC 2790-compliant HOST-RESOURCES-MIB.

1. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageIndex
2. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageType
3. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageAllocationUnits
4. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageSize
5. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageUsed

Arguments

- **Upper_Limit**

  A fault event is issued if the usage rate of the physical memory exceeds the value specified here. You can specify a single-byte number between 1 and 100. The unit of measurement is percentages (%). This cannot be omitted.

- **Reset_Value**

  If the value falls below the value specified here, the fault is recovered. You can specify a single-byte number between 0 and 99. The unit of measurement is percentages (%). This cannot be omitted.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

In the case of the upgrade from MasterScope Network Manager 2.0, this rule is registered as "Standing rule file". To use this rule, embed this rule first. For details, refer to "4.10.7 Embedding rule files (page 258)".

7.1.4.4 host_vmem_usage:VirtualMemory_UsageRate

Function description

Monitors the usage rate of virtual memory.

This rule is only applicable to devices compatible with RFC 2790-compliant HOST-RESOURCES-MIB.

1. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageIndex
2. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageType
3. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageAllocationUnits
4. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageSize
5. .host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageUsed

Arguments

- **Upper_Limit**

  A fault event is issued if the virtual memory usage rate exceeds the value specified here. You can specify a single-byte number between 1 and 100. The unit of measurement is percentages (%). This cannot be omitted.

- **Reset_Value**

  If the value falls below the value specified here, the fault is recovered. You can specify a single-byte number between 0 and 99. The unit of measurement is percentages (%). This cannot be omitted.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

In the case of the upgrade from MasterScope Network Manager 2.0, this rule is registered as "Standing rule file". To use this rule, embed this rule first. For details, refer to "4.10.7 Embedding rule files (page 258)".

7.1.4.5 host_process_check:ProcessCheck

Function description

Monitors the status of processes. This rule is only applicable to devices compatible with RFC 2790-compliant HOST-RESOURCES-MIB.

1. .host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName
2. .host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunPath
3. .host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunParameters
4. .host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunStatus

Arguments

- **Process_Name**

  Specifies the process name that you want to monitor.

- **Path**

  Specifies the launch path for the process to be monitored. This is optional. Specify if there are multiple processes with the same name. Processes with matching values are monitored.

- **Parameters**

  Specifies the parameters for launching the process to be monitored. This is optional. Specify if there are multiple processes with the same name. Processes with matching values are monitored.

You can check the notation of the Process_Name, Path, and Parameters by acquiring monitored device MIB using the `NvPROAmibGetSvc` / `NvPROAmibGetMgr`.

For details of command, refer to "9.7.1 NvPROAmibGetSvc/NvPROAmibGetMgr (page 712)".

Verifying the process information

- Check the process name.

```
NvPROAmibGet(Svc|Mgr) -form "%C\t%-22AB\t\"%V\"\n"
 target_node .host.4.2.1.2
```

Example of execution result:

```
target_node hrSWRunName.100 "notepad.exe"
```

In the results above, "notepad.exe" is the process name.

To verify the launch path and launch parameter of this process, use the value of *x* in "hrSWRunName.*x*" and follow the procedure below. A value of "100" is used in the results above.

- Check the process launch path.

```
NvPROAmibGet(Svc|Mgr) -form "%C\t%-22AB\t\"%V\"\n"
 target_node .host.4.2.1.4.x
```

Example of execution result:

```
target_node hrSWRunPath.100 "C:\WINDOWS\system32\"
```

In the results above, "C:\WINDOWS\system32\" is the launch path.

- Check the process launch parameters.

```
NvPROAmibGet(Svc|Mgr) -form "%C\t%-22AB\t\"%V\"\n"
 target_node .host.4.2.1.5.x
```

Example of execution result:

```
target_node hrSWRunParameters.100 " C:\log.txt"
```

In the results above, "C:\log.txt" is the launch parameters.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

1. In the case of the upgrade from MasterScope Network Manager 2.0, this rule is registered as "Standing rule file". To use this rule, embed it first. For details, refer to "4.10.7 Embedding rule files (page 258)".
2. If there are multiple processes that match all the values of the specified variables, monitoring cannot be performed correctly.

   The process to be monitored must be uniquely identifiable based on a set of specifications such as a process name, a launch path, and a launch parameter.
3. In this rule, an event is notified based on ".host.hrSWRun.hrSWRunTable.hrSWRunStatus" value.
   - Normal: running(1), runnable(2)
   - Abnormal: notRunnable(3), invalid(4), or process not found

7.1.5 Rules for specific device models

7.1.5.1 PortCheck_for_Catalyst2900:PortStateCheck_C2900PortEntry

Function description

Monitors the link status of the monitored device's port.

Products that can be monitored

- Layer 2 switches
- Catalyst2950T-24

  (Products equivalent to the Catalyst 2950 Series can be used)

Arguments

- **Port Number**

  Specify the port number being monitored.

  To specify multiple ports, separate them using a comma (for example: 0.1, 0.2, 0.3).

  To monitor all ports, omit the port number or specify an asterisk (*).

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

7.1.5.2 PortCheck_for_Catalyst:PortStateCheck_PortEntry

Function description

The PortStateCheck_PortEntry monitors the link status of the monitored port.

Products that can be monitored

Multi-layer switches

Catalyst3550-12T

(Products equivalent to the Catalyst 3550 Series can be used)

Arguments

- **Port Number**

  Specify the port number being monitored.

  To specify multiple ports, separate them using a comma (for example: 1.1, 1.2, 1.3).

  To monitor all ports, omit the port number or specify an asterisk (*).

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

7.1.5.3 AverageBusy5m_for_Catalyst:CPU_avgBusy5_CiscoIOS

Function description

Monitored device for the previous five minutes. By monitoring the average CPU busy rate, you can prevent faults in the monitored device. (Devices can be monitored if it is possible to obtain the average CPU busy rate for the past five minutes for that device using avgBusy5).

Products that can be monitored

- Catalyst2950T-24

  (Products equivalent to the Catalyst 2950 Series can be used)

- Catalyst3550-12T

  (Products equivalent with the Catalyst 3550 Series can be used)

Arguments

- **Upper_Limit**

  If the average CPU busy rate exceeds the value specified here, a fault event is issued. You can specify a value (%) from 0 to 100 (cannot be omitted).

- **Reset_Value**

  If the value falls below the value specified here, the fault is recovered. You can specify a value (%) from 0 to 100 (cannot be omitted).

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

7.1.6 Other rules

7.1.6.1 icmperrv6:ipv6ICMP_OutputErrorPackets

Function description

Monitors the number of ICMPv6 error packets output by the monitored device. This rule is valid if the router on the network is being monitored.

ICMPv6 error packets in this case include the following.

1. ICMP (IPv6) Destination Unreach (.ipv6IcmpMIB.ipv6IfIcmpOutDestUnreachs)
2. ICMP (IPv6) Time Exceeded (.ipv6IcmpMIB. ipv6IfIcmpOutTimeExcds)
3. ICMP (IPv6) Parameter Problem (.ipv6IcmpMIB. ipv6IfIcmpOutParmProblems)
4. ICMP (IPv6) PacketTooBig (.ipv6IcmpMIB. ipv6IfIcmpOutPktTooBigs)

By monitoring the occurrence of the abovementioned ICMPv6 error packets, you can prevent network failures and unnecessary traffic.

The number of errors listed in the details of event occurrence box is not the total over a one minute period, but rather, it is the total of each error that occurred within the specified interval. MIBs listed above are Counter-type MIBs, so also refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)" for monitoring.

Arguments

- **IPv6Index_Number**

  Specify the index of IPv6 interface you want to monitor the error packets.

  Use a number displayed in the **IPv6 Index** column in the **IPv6** tab of the "4.2.8.1.1 Interface Properties dialog box (page 181)". To specify multiple interfaces, separate them using a comma.

  To monitor all IPv6 interfaces of the device, omit the IPv6 interface index or specify an asterisk (*).

- **Upper_Limit**

  If the number of ICMPv6 output error packets per minute exceeds the number specified here, a fault event is issued.

  These events are manual recovery events. For this reason, a recovery report is not generated.

  You can specify a value from 0 to 4,294,967,295. If a value is not specified, it will automatically be set to 1.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

⚠ Caution

In the case of the upgrade from MasterScope Network Manager 2.0, this rule is registered as "Standing rule file". To use this rule, embed this rule first. For details, refer to "4.10.7 Embedding rule files (page 258)".

7.1.6.2 icmperr:ICMP_OutputErrorPackets

Function description

Monitors the number of ICMP error packets output by the monitored device.

This rule is valid if the router on the network is being monitored. ICMP error packets in this case include the following.

1. ICMP Destination Unreach (.icmp.icmpOutDestUnreachs.0)
2. ICMP Time Exceeded (.icmp.icmpOutTimeExcds.0)
3. ICMP Parameter Problem (.icmp.icmpOutParmProbs.0)
4. ICMP Redirects (.icmp.icmpOutRedirects.0)

By monitoring the occurrence of the abovementioned ICMP error packets, you can prevent network failures and unnecessary traffic.

The number of errors listed in the details of event occurrence box is not the total over a one minute period, but rather, it is the total of each error that occurred within the specified interval. MIBs listed above are Counter-type MIBs, so also refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)" for monitoring.

Arguments

- **Upper_Limit**

  If the number of ICMP output error packets per minute exceeds the number specified here, a fault event is issued.

  These events are manual recovery events. For this reason, a recovery report is not generated.

  You can specify a value from 0 to 4,294,967,295. If a value is not specified, it will automatically be set to 1.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

7.1.6.3 valchange:ValueChange

Function description

If the MIB value for the monitoring target has changed compared to the previous time, an alert is issued.

Arguments

- **MIB_Name**

  Specify the MIB for the monitored device. Only ascii characters can be used.

For other setting items such as the interval, refer to "4.10.2.1 Rule Entry Settings dialog box (page 244)".

7.1.7 Creating new rules

7.1.7.1 Rule file format

One rule is written in the following format.

```
main ruleFuncName(arg, ...) {
    initialize-section
    statement-list
}
```

The function name (rule ID) that identifies the rule is specified in ruleFuncName.

In Network Manager, one rule is identified by the ".rl" extracted from the rule file name (for example, nvrule.rl) and the character string that is connected to ruleFuncName by a colon (:) ("nvrule:ruleFuncName").

For the arguments of functions (arg), the value of the variable set in the Rule Entry Settings dialog box in the State Monitoring window is set and the rule is run.

Initialize-section is run only once when the rule is started, and then statement-list is run at intervals.

Immediately before statement-list is run, information is obtained each time from the MIB that is specified to the system reserved variable MIBNAME. If you specify the MIB that contains large amount of data in MIBNAME, the MIB data collection may time out before all MIBs are obtained completely. In this case, statement-list is run using partial MIB data that has been obtained before the timeout, and then the process may not work correctly. To avoid this case, adjust **Retry Interval** value in the Environment Setting dialog box. For details, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

Tip

- For a rule file name and ruleFuncName, you cannot use spaces. In addition, you cannot specify a ruleFuncName consisting only of digits.
- Given the display limits of in the State Monitoring window, the specification of a name of up to 259 characters for "Rule file name: ruleFuncName" is recommended.
- Usually, to view the MIB in statement-list, use the MIB access functions, such as value() and test(), for the MIB (MIB specified in MIBNAME) acquired immediately before statement-list.
- If you want to obtain or set MIB data from MIBs that are not specified in MIBNAME, use MIB access functions such as getvalue() or setvalue().
- In a rule file, up to 4095 characters can be defined on one line.

7.1.7.2 Initializing (Initialize-section)

Initializing (initialize-section) is run only once before running a rule (prior to polling).

This is where you state that you want to configure initial settings for the MIB names, levels when issuing an event, and the messages before starting polling. The initialize-section can be omitted.

The initialize-section is written in the following format.

```
{
    statement-list
}
```

7.1.7.3 Rule grammar

Rule grammar is similar to the C language.

The rules are configured from one or more statement-lists. A statement-list is configured from one or more statements. The statements can be any of the following.

Any lines beginning with "#" are assumed to be comment lines.

```
expression;
while (expression) statement
if (expression) statement
if (expression) statement else statement
{ statement-list }
continue;
break;
return;
```

Expressions can be any of the following.

```
constant
variable
function
expression op expression
```

"constant" is a constant, "variable" is a variable, "function" is a function, and "op" is an operator.

Constants

The following constant types are possible.

- Integers

  Decimals with no decimal point, hexadecimals beginning with "0x", and octals beginning with "0" are handled as integer constants.

- Real numbers

  Digit strings containing decimal points (.) are handled as real numbers.

- Character strings

  Characters strings enclosed in double quotation marks (") are considered to be character string constants.

Variables

Reserved words and character strings, excluding embedded function names, that are used in constants, operators and control statements are handled as variables. Values substituted in variables are also saved at the time a rule is run for the next polling. The initial value of a variable is 0.

A variable name can contain alphanumeric characters and following symbols.

_ . ' ` : [ ] $? @

There are system reserved variables as follows.

- STATUS

  The variable is used to specify whether or not to run a rule.

  If 1 is specified, the rule is executed.

If 0 is specified, the rule is not executed.

- COMPNAME

  The component that applies a rule is set.

- MIBNAME

  The MIB set in this variable is polled.

- INTERVAL

  This is the interval at which polling is performed (in seconds).

- LEVEL

  This variable is used to set the level when an event is issued.

  It is set based on the **Fault Level** set in the Rule Entry Settings dialog box in the State Monitoring window.

- TIME

  This is the current time.

In addition to the constant values above, variables can also be set using list type data.

For information regarding list data, refer to the list data manipulation functions for the intrinsic functions. If the key is specified immediately after the variable name definition, the argument can be specified easily by the dialog box or combo box.

The keys are reserved words so cannot be used as variable name. Refer to the following table for details.

Key	Details
[MIB]	Argument can be specified by the "4.16.1.3 Managed Item Selection Dialog dialog box (page 340)". Multiple MIBs cannot be selected.
[MIBS]	Argument can be specified by the "4.16.1.3 Managed Item Selection Dialog dialog box (page 340)". Multiple MIBs can be selected.
[IF]	Argument can be specified by the "4.16.1.2 Interface Number Select dialog box (page 340)".
[SELECT:...]	Argument can be specified by the combo box. • To display multiple strings in a combo box, separate strings by a colon (:). Example: If "[SELECT:A:B:C]" is specified, "A","B","C" are displayed in a combo box. • If [SELECT:] is specified, a text box is displayed instead of a combo box.

If a variable name contains square brackets ([ ]) used for specifying a key, a variable name is determined as following rules.

- A string in square brackets ([ ]) is considered as a normal variable. Neither dialog box nor combo box will be displayed.
- A string before the key is considered as a variable name. Any strings after a right square bracket ( ]) are omitted.
- If a key exists but a variable name is omitted, a key is considered as a variable name.
- If a string in square brackets ([ ]) is not matched any keys, it is considered as a normal variable.

Operators

You can use the following operators. The definition of operators here is the same as the definition in the C language.

- Arithmetic operators

  *, /, +, -, %

- Relational operators

  >, >=, <, <=, ==, !=

- Logical operators

  <<, >>, &, ^, |, &&, ||

- Assignment operators

  =

⚠ Caution

The "<<" and ">>" 64-bit data operators are not supported.

Control statements

You can use the following control statements.

- while

  Controls loops. This is used in the same way it is used in the C language.

- if, else

  Describes conditions. This is used in the same way it is used in the C language.

- break

  When used within a loop control, this control provides a break in the loop. When used outside of the loop control, it stops running the rule for that component.

- continue

  When used within a loop control, this control provides a break in the loop. When used outside of the loop control, it stops running the rule for that component.

- return

  Terminates user-defined functions.

  Return statements are:

  ```
  return;
  ```

  or,

  ```
  return(expression);
  ```

  Either of these formats is acceptable. When using the latter, the expression value is returned as the return value of the function.

Functions

- User-defined functions

  User-defined functions can be defined in the following format.

```
defun subFuncName(arg, ...) {
    statement-list
}
```

The function name (subFuncName) and argument (arg) are defined after defun and statement-list is inserted inside the {}.

Of the variables that are used within functions, the variables with the same name as variables used within the main function are treated the same as the variables within the main function. Values from return statements can also be returned.

- Built-in functions

  You can use the following built-in functions.

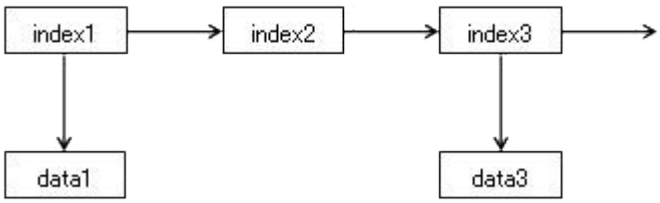
  - "7.1.7.3.5.1 List handling functions (page 615)"
  - "7.1.7.3.5.2 Data handling functions (page 616)"
  - "7.1.7.3.5.3 MIB access functions (page 617)"
  - "7.1.7.3.5.4 Event handling functions (page 618)"
  - "7.1.7.3.5.5 Other functions (page 619)"

List handling functions

By using the following functions, you can manipulate list-type data.

- List-type data

  List-type data is data that is valid when separate data is handled as one unit, and data which is structured with one or more index/data units, as shown below.



  Character strings can be used in indexes. Integers, decimals, character strings, and list-type data can be used in data. Indexes may be omitted.

- `nextindex`(*value*, *index*)

  Within list-type data indicated by *value*, the index of the data following the data indicated by *index* is returned. If 0 is specified in *index*, the index of the data at the start of *value* is returned.

- `addlist`(*valuelist*, *value*[, *index*])

  In list-type data indicated by *valuelist*, the data *value* with the index *index* is added.

- `dellist`(*valuelist*[, *index*])

  From list-type data indicated by *valuelist*, data with the index *index* is deleted. If *index* is omitted, the data at the start of the list is deleted.

- `getlist`(*valuelist*[, *index*])

  From list-type data indicated by *valuelist*, data with the index *index* is returned. If there is no data with *index*, "0" is returned. If *index* is omitted, the data at the start of the list is returned.

- `getlistindex`(*valuelist*[, *index*])

From list-type data indicated by *valuelist*, if there is data with the index *index*, that index is returned. If there is no data with *index*, "0" is returned. If *index* is omitted, the index of the data at the start of the list is returned.

- `listnum`(*valuelist*)

  This function returns the number of data items in the *valuelist* list data. If *valuelist* is not list-type data, "0" is returned. If a variable is specified that has no assigned value, then "-1" is returned.

Data handling functions

- `ipaddr2str`(*ipaddr*)

  This function converts the IpAddress-type value *ipaddr* to a character string and returns it.

- `tticks2str`(*tticks*)

  This function converts the TimeTicks-type value *tticks* to a character string and returns it.

- `uxtime2str`(*uxtime*)

  This function converts the time *uxtime* set in the variable "TIME" to a character string and returns it.

- `str2int`(*str*)

  This function converts the character string *str* into a signed integer and returns it.

- `str2uint`(*str*)

  This function converts the character string *str* into an unsigned integer and returns it.

- `str2uint64`(*str*)

  This function converts the character string *str* into an unsigned 8-byte (64-bit) integer and returns it.

- `str2oct`(*str*)

  This function converts the character string *str* into OctetString-type data and returns it. *str* character strings are in hexadecimal form and each octet is separated by a colon or a space. It is also possible for the character string to start with "0x".

- `str2tticks`(*str*)

  This function converts the character string *str* into TimeTicks and returns it. The *str* character string is in the following format: [[hh:][mm:]]ss[:uu]

- `str2ipaddr`(*str*)

  This function converts the character string *str* into IpAddress and returns it. The *str* character string is decimal notation separated by four periods (.) or hexadecimal notation beginning with "0x".

- `int`(*x*)

  This function converts the real number *x* (excluding 64-bit data) into an integer-type value and returns it.

- `float`(*i*)

  This function converts the integer *i* (excluding 64-bit data) into a real number and returns it.

- `suboct`(*oct*, *m*, *n*)

This function returns a value of *n* bytes in length starting from the *m* position of the OctetString-type value *oct*. The first byte of *oct* is calculated as byte one. If *n* is 4 or less, the value is returned as an integer.

- `substr`(*str*, *m*, *n*)

  This function returns a character string of *n* characters from the *m* position of a *str* character string. The first character of the *str* is calculated as character one.

- `strcat`(*str1*, *str2*[, *str3*, ...])

  This function returns a character string that combines character string *str2*, .. at the end of character string *str1*.

- `split`(*str*, *c*)

  This function returns a list-type value that splits the *str* character string with the separator character *c*. Stringed numbers from 1 to the number of units are used in the index.

- `sprint`(*arg1*[, *arg2*, ...])

  This function strings the *arg1*, *arg2*, .. values and returns a character string that combines these values.

- `strmatch`(*str1*, *str2*)

  This function searches from the beginning of the *str1* character string and returns the position of the first match for the *str2* character string. If there is no match, "0" is returned.

- `strrmatch`(*str1*, *str2*)

  This function searches from the end of the *str1* character string and returns the position of the first match for the *str2* character string. If there is no match, "0" is returned.

- `regmatch`(*reg*, *str*)

  This function determines if the *str* character string matches the regular matching format *reg*. If there is a match, "1" is returned. If there is no match, "0" is returned.

MIB access functions

- `value`(*mib*)

  This function returns the value of management items specified in the *mib* MIB name.*mib* must be set in the "MIBNAME" variable.

  In addition to complete character string-type MIB names (expressed numerically), *mib* can be specified with an asterisk ("*") (wildcard) at the end of the MIB name. In this case, a list-type value is returned and the index value is the character string that matches the "*" portion.

- `test`(*mib*)

  If management items that are specified in the *mib* MIB name are obtained, a "1" is returned. Otherwise, a "0" is returned. *mib* must be set in the "MIBNAME" variable.

  In addition to complete character string-type MIB names (expressed numerically), *mib* can be specified with an asterisk ("*") (wildcard) at the end of the MIB name. In this case, if one or more matching management items are obtained, a "1" is returned. If no management items are obtained, a "0" is returned.

- `getvalue`(*mib*[, *compname*])

  This function returns the value of management items specified in the *mib* MIB name.

In addition to complete character string-type MIB names (expressed numerically), *mib* can be specified with an asterisk ("*") (wildcard) at the end of the MIB name. In this case, a list-type value is returned and the index value is the character string that matches the "*" portion.

This function differs from `value`() in that `getvalue`() retrieves the value at the time that the function is run. As a result, it is possible to specify the MIB name *mib* even though it was not set in the "MIBNAME" variable.

If the *compname* component name is omitted, it is assumed to be the component that is currently applying the rule. If an error occurs indicating that the value cannot be retrieved, the current rule is terminated.

- `setvalue`(*mib*, *value*[, *compname*])

  Sets the value, *value*, in the *mib* MIB name of the component with the *compname* component name (when omitted, it is assumed to be the component currently applying the rule).

- `setrawvalue`(*mib*, *type*, *value*[, *compname*])

  Sets the syntax *type* value, *value*, in the *mib* MIB name of the component with the *compname* component name (when omitted, it is assumed to be the component currently applying the rule). Any of the following character strings are specified in *type*.

  INTEGER

  OctetString

  ObjectID

  IpAddress

  Counter

  Counter64

  Gauge

  TimeTicks

  DisplayString

  PhysAddress

Event handling functions

- `eventsend`(*level*, *msgnum*[:*msgfile*], *dtmsg*[, *compname*])

  On the component with the component name *compname*, creates an event with the level *level*, the message number *msgnum*, and the detailed message *dtmsg*.

  Specify the fault event file name in *msgfile*. If *msgfile* is omitted, this defaults to "nvbase.msg".

  When this intrinsic function is run, an ID is returned to identify the event that was created. An ID is necessary to clear the auto recovery type event through `eventcancel`(). For this reason, you must save the returned value.

  Here, the *level* can be "L1", "L2", "L3", "L4", "M1", "M2", "M3","M4".

  The levels beginning with "L" issue an auto recovery type event and those beginning with "M" issue a manual recovery type event. Beginning with 1, the levels correspond to Warning, Minor Fault, Major Fault and Critical State.

- `eventcancel`(*eventid*, *msgnum*[:*msgfile*], *dtmsg*)

  An auto recovery type event is returned to its original state.

Clear the event corresponding to the *eventid* that is the returned value of `eventsend`(), attach the message number *msgnum* and the detailed message *dtmsg* and send a notification.

Specify the fault event file name(Refer to "7.1.7.6 Customizing fault event message files (page 620)".) in *msgfile*. If *msgfile* is omitted, this defaults to "nvbase.msg".

Other functions

- `getrelation`(*compname*, *relname*, *direct*)

  This function returns the component that has the relationship *relname* with the component *compname*. Specify the direction of the relationship in *direct*. The *relname* can be specified using the following character strings.

  "map-icon", "icon-obj", "obj-if"

  If *direct* is a right-directed relationship where *compname* is the base point, specify "1". If it is a left-directed relationship, specify `"0"`.

- `valuesize`(*value*)

  This function returns the size (length) of the value specified in *value*.

- `print`(*arg1*[, *arg2*, ...])

  This function outputs the values for *arg1*, *arg2*.. to a log file. This function is primarily used for debugging rules.

7.1.7.4 Embedding new rule files

This section describes how to add rule files.

You must first change to the "configuration mode (page 27)".

1. Store the newly created rule files in the folder shown below.

   <On the manager, %installfolder%>`\Manager\sg\NvPRO\NVWORK\local\rules`

2. In the State Monitoring window, add the file to the list of rules.

   Rule files are embedded in the Embedded Rule File dialog box on the monitoring terminal. For more information regarding the Embedded Rule File dialog box, refer to "4.10.7 Embedding rule files (page 258)". When you open the Embedded Rule File dialog box, the newly created rule file is displayed in the **Standing rule file** list. Add the files to the rule list by pressing the **<- Add** button.

   Caution

   If there are syntax errors in the newly created rule file, the following results may occur. In such cases, fix the rule file and embed it again.

   - The newly created rule file is not displayed in the Embedded Rule File dialog box under the **Standing rule file** list.
   - An error message is generated when you click the **<- Add** button.

7.1.7.5 Debugging new rule files

To debug newly created rule files, output logs according to the procedure outlined below.

You must first change to the "configuration mode (page 27)".

1. Create the following definition file.

Definition file:

<On the manager, %installfolder%>\Manager\sg\NvPRO\NvpLog.ini

Settings:

```
[LogLevel]
DEFALUT=ALERT
83=INFO
[LogFile]
AUTO_FLUSH=INFO
```

2. Run the following command to load the definition content.

   <On the manager, %installfolder%>\Manager\bin\FlushNvpLog.exe

3. Install the created rules.

   For instructions on how to install a rule, refer to "4.10.7 Embedding rule files (page 258)".

4. Create new state monitoring rules and execute the rules.

   For instructions on how to create and execute a rule, refer to "4.10.2 Creating new state monitoring rule entries (page 243)".

When the procedure above completes, output results for print statements contained in the state monitoring rules are recorded in the log file below.

<On the manager, %installfolder%>\Manager\log\NvpLot.txt

After completing the debug tasks, always follow the steps below to stop log output.

1. Delete the following definition file that was created for the debug log.

   <On the manager, %installfolder%>\Manager\sg\NvPRO\NvpLog.ini

2. Run the following command to apply the settings for stopping log output.

   <On the manager, %installfolder%>\Manager\bin\FlushNvpLog.exe

3. If necessary, stop or delete the target rule.

7.1.7.6 Customizing fault event message files

When using event handling functions, select the message that you want to display by specifying the line numbers from the fault event file. The fault event message files are stored in the following directory on the manager.

- Detailed messages

  <On the manager, %installfolder%>\Manager\sg\NvPRO\NVWORK\public\locale\0409

- Summary messages

  <On the manager, %installfolder%>\Manager\sg\NvPRO\NVWORK\public\locale\0409\SUMMARY

Create "user.msg" to define a new fault event or change the contents of an existing event.

1. Create new files named "user.msg" in the directories in which the detailed messages and summary messages are stored.

   Create files using the encoding formats below.

OS	BOM	Encoding	Linefeed
Windows	o	UTF-16 Little-Endian	CRLF
Linux	-	UTF-8	LF

Caution

a. The names of the detailed message and summary message files must be the same.

b. A new fault message file can be created with any file name other than "user.msg". However, it is recommended to use the name "user.msg" because the system may overwrite at the future version upgrades.

2. In the "user.msg" files, write the message that you want to display in the alert.

   The line numbers that define the messages must be the same for detailed messages and summary messages. If the line numbers are different, message cannot be displayed correctly.

Caution

Do not make edits directly in the system message file "nvbase.msg". During version upgrades, the system message file is overwritten and the edits are deleted.

3. Reflect the contents of the fault event file "user.msg" in Network Manager.

   Execute the NvPROReloadDefFileMgr command and reflect the results onto Network Manager.

```
> NvPROReloadDefFileMgr
```

   For details, refer to "9.5.4 NvPROReloadDefFileMgr (page 699)".

4. When using fault event files that have been customized in new rules, specify them as shown below.

```
eventsend(level,"1:user.msg","");
```

   In this case, the message in the first line of "user.msg" is set up to be output.

7.1.7.7 Examples of rule descriptions

Following is an explanation based on an example description of a simple rule. The following rule is used to:

1. Send ICMP ECHO packets to a target device.
2. Issue an important-state event if a response is not obtained.
3. If a response is obtained from the target device, clear the important state status.

```
 1: main icmpCheck()
 2: {
 3:     {
 4:         icmpmib = "icmpmib.icmpEcho.0";
 5:         MIBNAME = icmpmib;
 6:         level = strcat("L", sprint(LEVEL));
 7:
 8:     }
 9:     if (!test(icmpmib)) {
10:         #
11:         # The ICMP ECHO is not obtained.
12:         #
```

```
13:         if (!eventid) {
14:             #
15:             # The component is down.
16:             #
17:             eventid = eventsend(level, 1026, "");
18:         }
19:     } else if (eventid) {
20:         #
21:         # The ICMP ECHO is obtained,
22:         # clears the DOWN event.
23:         #
24:         eventcancel(eventid, 1027, "");
25:         eventid = 0;
26:     }
27: }
```

- Line 1

  The rule name is defined as "icmpCheck".

- Line 4 and 5

  The name of the MIB being polled is specified. To send ICMP ECHO packets, Network Manager extension MIB is specified.

- Line 6

  Creates the parameters for publishing an event.

  The "LEVEL" variable is set based on the fault level set in the Rule Entry Settings dialog box in the State Monitoring window.

- Line 8

  Everything up to this point is run in the initializing process prior to commencing polling.

- Line 9

  Checking whether or not the ICMP ECHO has been obtained.

- Line 13-18

  If the ICMP ECHO is not obtained, an event will be published if one has not already been published.

  The ID for clearing published events is stored in the eventid variable.

- Line 19-26

  This is the process for clearing an event in the case that the ICMP ECHO is obtained and an event has already been published.

7.2 Data Collection Rules

7.2.1 Traffic of the specific host

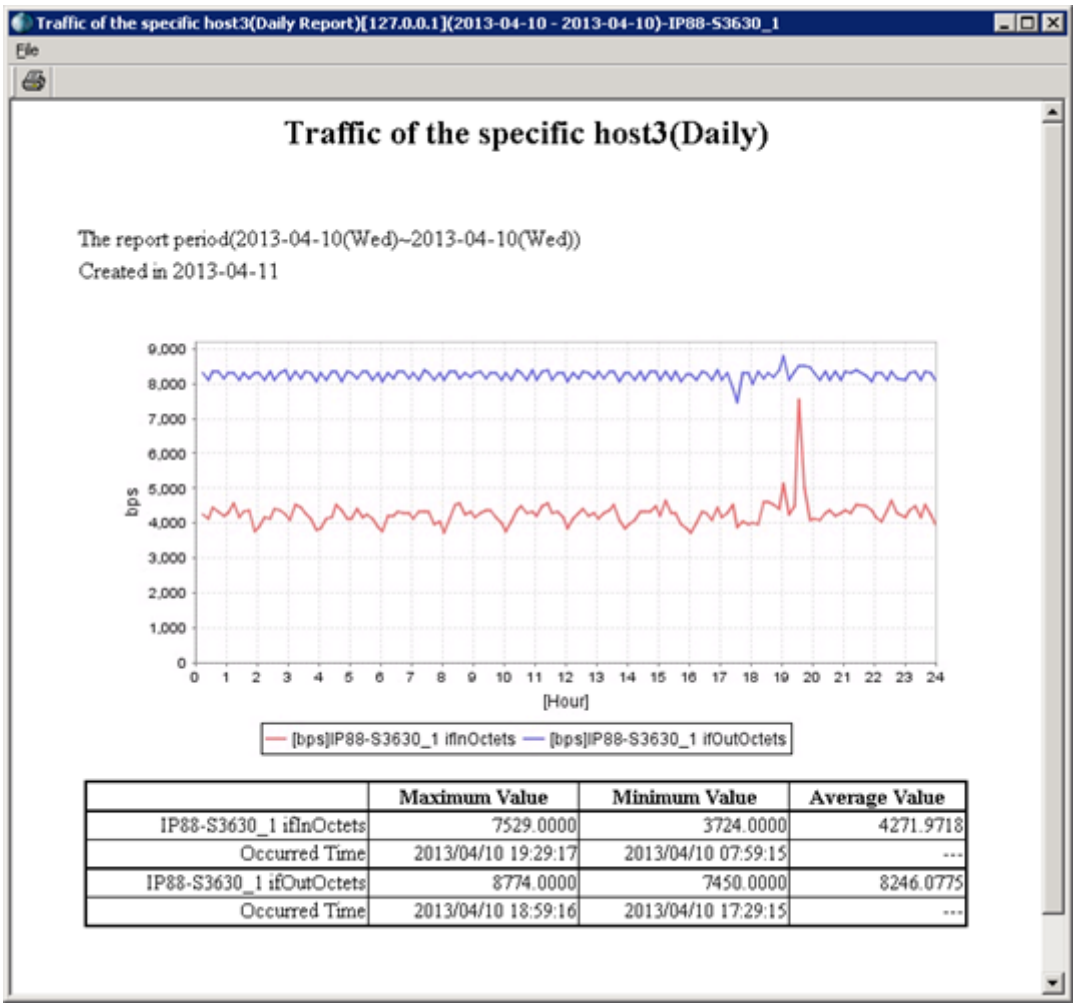
Summary

This rule collects data for the purpose of assessing trends in load concentration and data volume and determining whether throughput is adequate. It is effective at collecting data for nodes that tend to accumulate load, such as servers.

This rule collects Counter-type MIBs. For details regarding the counter-type MIBs, refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

For other setting items such as the interval, refer to "4.16.1 Data Collecting Setting window (page 334)".

Report sample



	Maximum Value	Minimum Value	Average Value
IP88-S3630_1 ifInOctets	7529.0000	3724.0000	4271.9718
Occurred Time	2013/04/10 19:29:17	2013/04/10 07:59:15	---
IP88-S3630_1 ifOutOctets	8774.0000	7450.0000	8246.0775
Occurred Time	2013/04/10 18:59:16	2013/04/10 17:29:15	---

CSV file format

;UNIXTIME	ManagerName: Compname	ifInOctets()	ifOutOctets()
;		bps	bps
Collecting time	:Node name	Collected incoming size	Collected outgoing size

7.2.2 Traffic of the specific hub port (64bit)

Preconditions

The target device must support SNMPv2c or SNMPv3. SNMPv2c or SNMPv3 communication between Network Manager and the target device must be possible.

Summary

This rule collects data for the purpose of assessing trends in data volume for the specified port of the specified hub, and determining whether the input-output volume for the specified port of the specified hub is adequate.

This rule collects Counter64-type MIBs. For details regarding the counter-type MIBs, refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

Items to set

- **Port Number**

  Specify the port number for the hub for which you want to collect data.

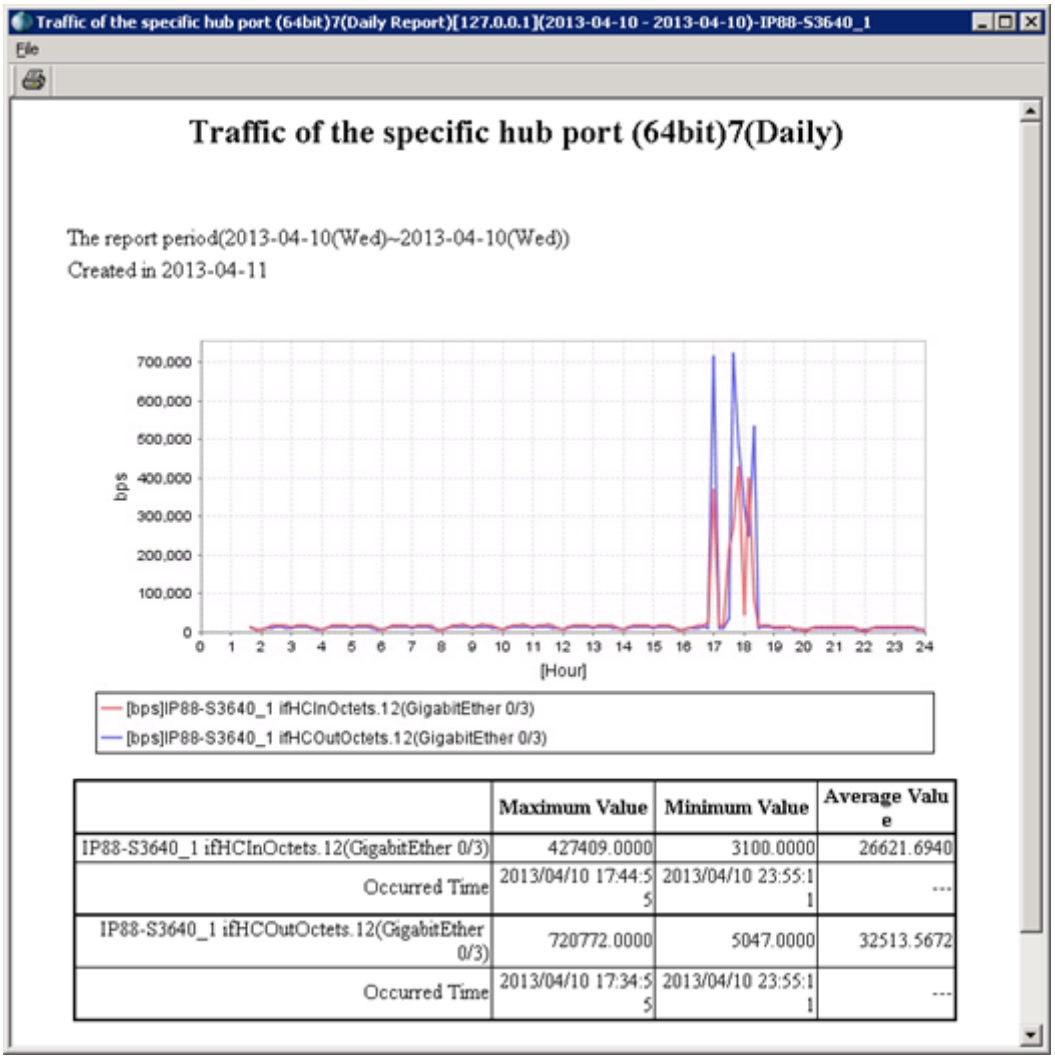
  Multiple ports can be specified. To specify multiple ports, separate the ports using a comma (,).

  A value may not be obtained for some devices if a large number of port numbers are listed using comma separation. In this case, specify an asterisk (*) for the port number to retrieve the default target port value. (The asterisk (*) must be a single-byte character).

  For details regarding the default target port, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.16.1 Data Collecting Setting window (page 334)".

Report sample



	Maximum Value	Minimum Value	Average Value
IP88-S3640_1 ifHCInOctets.12(GigabitEther 0/3)	427409.0000	3100.0000	26621.6940
Occurred Time	2013/04/10 17:44:55	2013/04/10 23:55:11	---
IP88-S3640_1 ifHCOutOctets.12(GigabitEther 0/3)	720772.0000	5047.0000	32513.5672
Occurred Time	2013/04/10 17:34:55	2013/04/10 23:55:11	---

CSV file format

;UNIXTIME	ManagerName :Compname	ifHCInOctets.#1 (name#1)	ifHCOutOctets.#1 (name#1)	...
;		bps	bps	...
Collecting time	:Node name	Incoming size of port index 1	Outgoing size of port index 1	...

⚠ Caution

The number of ifHCInOctets and ifHCOutOctets increases and decreases according to the number of ports.

7.2.3 Traffic of the specified hub port

Summary

This rule collects data for the purpose of assessing trends in data volume for the specified port of the specified hub, and determining whether the input-output volume for the specified port of the specified hub is adequate.

This rule collects Counter-type MIBs. For details regarding the counter-type MIBs, refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

Items to set

- **Port Number**

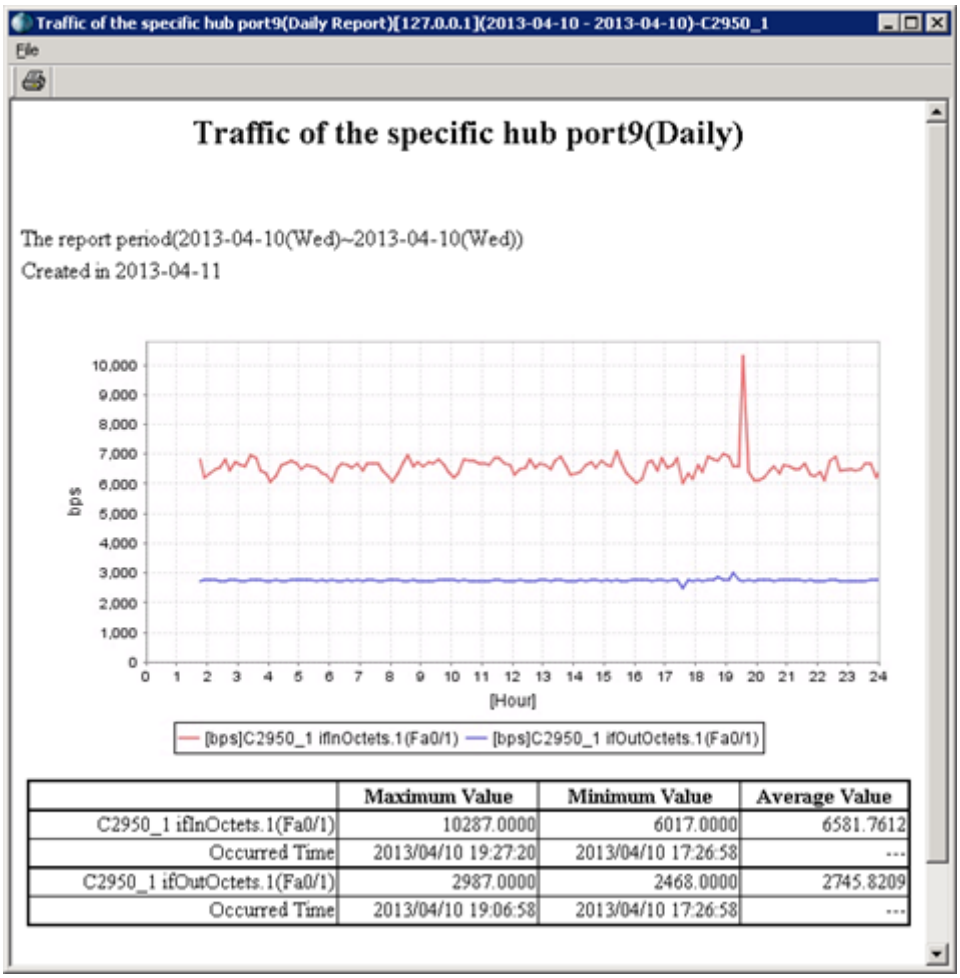
  Specify the port number for the hub for which you want to collect data. Multiple ports can be specified. To specify multiple ports, separate the ports using a comma (,).

  A value may not be obtained for some devices if a large number of port numbers are listed using comma separation. In this case, specify an asterisk (*) for the port number to retrieve the default target port value. (The asterisk (*) must be a single-byte character).

  For details regarding the default target port, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.16.1 Data Collecting Setting window (page 334)".

Report sample



	Maximum Value	Minimum Value	Average Value
C2950_1 ifInOctets.1(Fa0/1)	10287.0000	6017.0000	6581.7612
Occurred Time	2013/04/10 19:27:20	2013/04/10 17:26:58	---
C2950_1 ifOutOctets.1(Fa0/1)	2987.0000	2468.0000	2745.8209
Occurred Time	2013/04/10 19:06:58	2013/04/10 17:26:58	---

CSV file format

;UNIXTIME	ManagerName :Compname	ifInOctets.#1 (name#1)	ifOutOctets.#1 (name#1)	...
;		bps	bps	...
Collecting time	:Node name	Incoming size of port index 1	Outgoing size of port index 1	...

Caution

The number of ifInOctets and ifOutOctets increases and decreases according to the number of ports.

7.2.4 WAN Traffic (64bit)

Preconditions

The target device must support SNMPv2c or SNMPv3. SNMPv2c or SNMPv3 communication between Network Manager and the target device must be possible.

Summary

This rule collects data for the purpose of assessing trends in data volume and determining whether the capacity of the specified WAN is adequate.

This rule collects Counter64-type MIBs. For details regarding the counter-type MIBs, refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

Items to set

- **Interface_Number**

  Specify the interface number for the router for which you want to collect data.

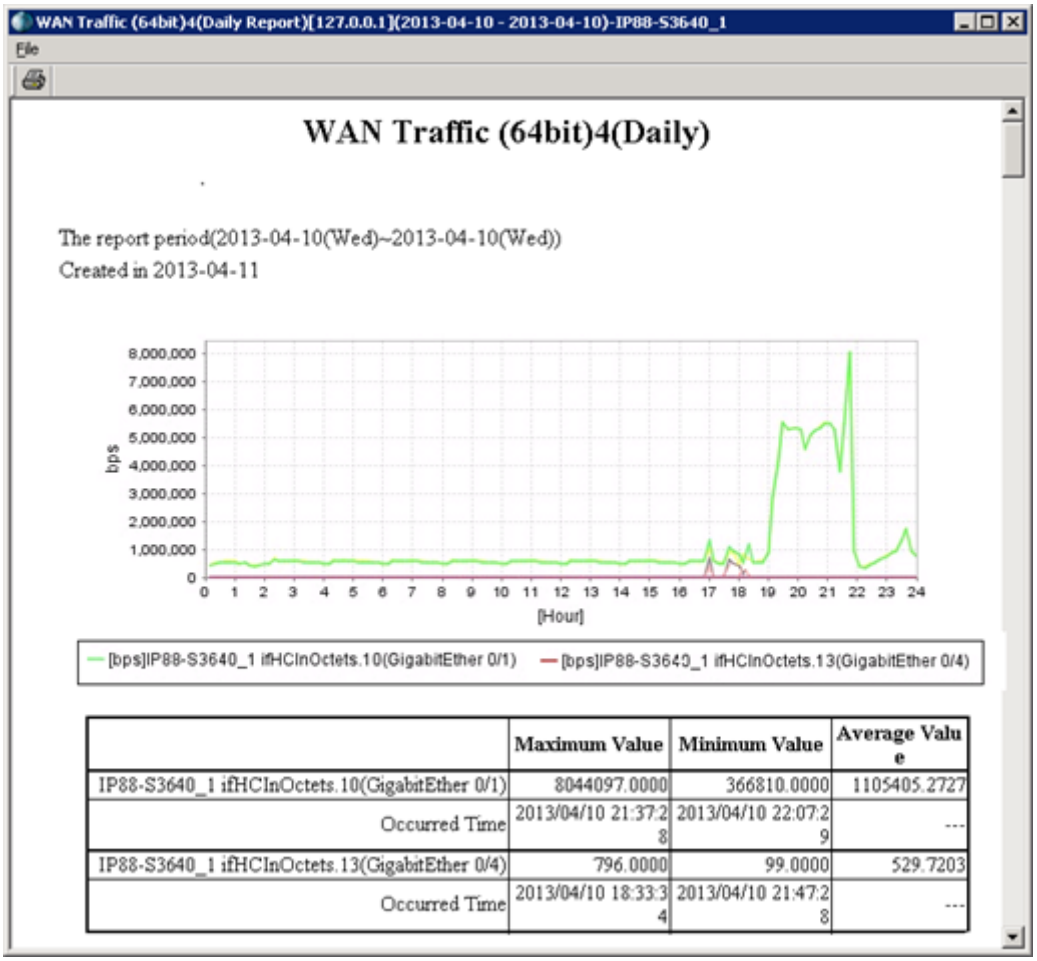
  Traffic is collected for the WAN connected to the specified interface number. It is possible to specify multiple interface numbers. To specify multiple ports, separate the ports using a comma (,).

  To specify multiple ports, separate the ports using a comma (,). A value may not be obtained for some devices if a large number of interface numbers are listed using comma separation. In this case, specify and asterisk (*) for the interface number to retrieve the default target port value. (The asterisk (*) must be a single-byte character.)

  For details regarding the default target port, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.16.1 Data Collecting Setting window (page 334)".

Report sample



	Maximum Value	Minimum Value	Average Value
IP88-S3640_1 ifHCInOctets.10(GigabitEther 0/1)	8044097.0000	366810.0000	1105405.2727
Occurred Time	2013/04/10 21:37:28	2013/04/10 22:07:29	---
IP88-S3640_1 ifHCInOctets.13(GigabitEther 0/4)	796.0000	99.0000	529.7203
Occurred Time	2013/04/10 18:33:34	2013/04/10 21:47:28	---

CSV file format

;UNIXTIME	ManagerName :Compname	ifHCInOctets.#1 (name#1)	ifHCOutOctets.#1 (name#1)	...
;		bps	bps	...
Collecting time	:Node name	Incoming size of port index 1	Outgoing size of port index 1	...

Caution

The number of ifHCInOctets and ifHCOutOctets increases and decreases according to the number of ports.

7.2.5 WAN Traffic

Summary

This rule collects data for the purpose of assessing trends in data volume and determining whether the capacity of the specified WAN is adequate.

This rule collects Counter-type MIBs. For details regarding the counter-type MIBs, refer to "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

Items to set

- **Interface_Number**

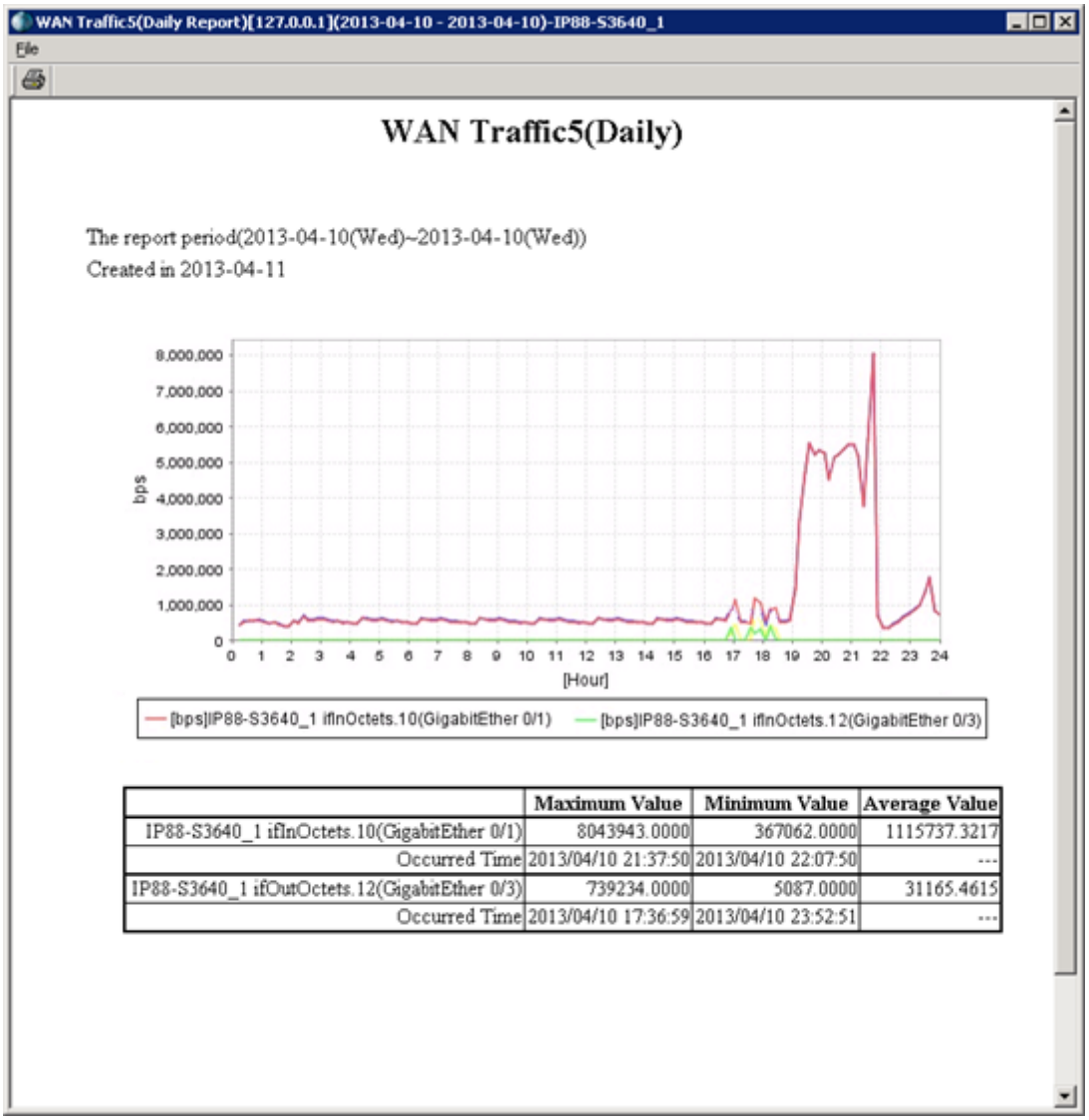
  Specify the interface number for the router for which you want to collect data. Traffic is collected for the WAN connected to the specified interface number. It is possible to specify multiple interface numbers. To specify multiple ports, separate the ports using a comma (,).

  A value may not be obtained for some devices if a large number of interface numbers are listed using comma separation. In this case, specify and asterisk (*) for the interface number to retrieve the default target port value. (The asterisk (*) must be a single-byte character.)

  For details regarding the default target port, refer to "4.2.8.1.1 Interface Properties dialog box (page 181)".

For other setting items such as the interval, refer to "4.16.1 Data Collecting Setting window (page 334)".

Report sample



	Maximum Value	Minimum Value	Average Value
IP88-S3640_1 ifInOctets.10(GigabitEther 0/1)	8043943.0000	367062.0000	1115737.3217
Occurred Time	2013/04/10 21:37:50	2013/04/10 22:07:50	---
IP88-S3640_1 ifOutOctets.12(GigabitEther 0/3)	739234.0000	5087.0000	31165.4615
Occurred Time	2013/04/10 17:36:59	2013/04/10 23:52:51	---

CSV file format

;UNIXTIME	ManagerName : Compname	ifInOctets.#1 (name#1)	ifOutOctets.#1 (name#1)	...
;		bps	bps	...
Collecting time	:Node name	Incoming size of port index 1	Outgoing size of port index 1	...

Caution

The number of ifInOctets and ifOutOctets increases and decreases according to the number of ports.

7.2.6 Server load

Summary

This rule collects data to assess the load being incurred by a server machine with NEC ESMPRO Agent installed and creates a report to analyze the load.

The load information collected from the NEC ESMPRO Agent includes the host CPU, memory, and page file usage rates.

This rule does not support the operation of monitoring threshold.

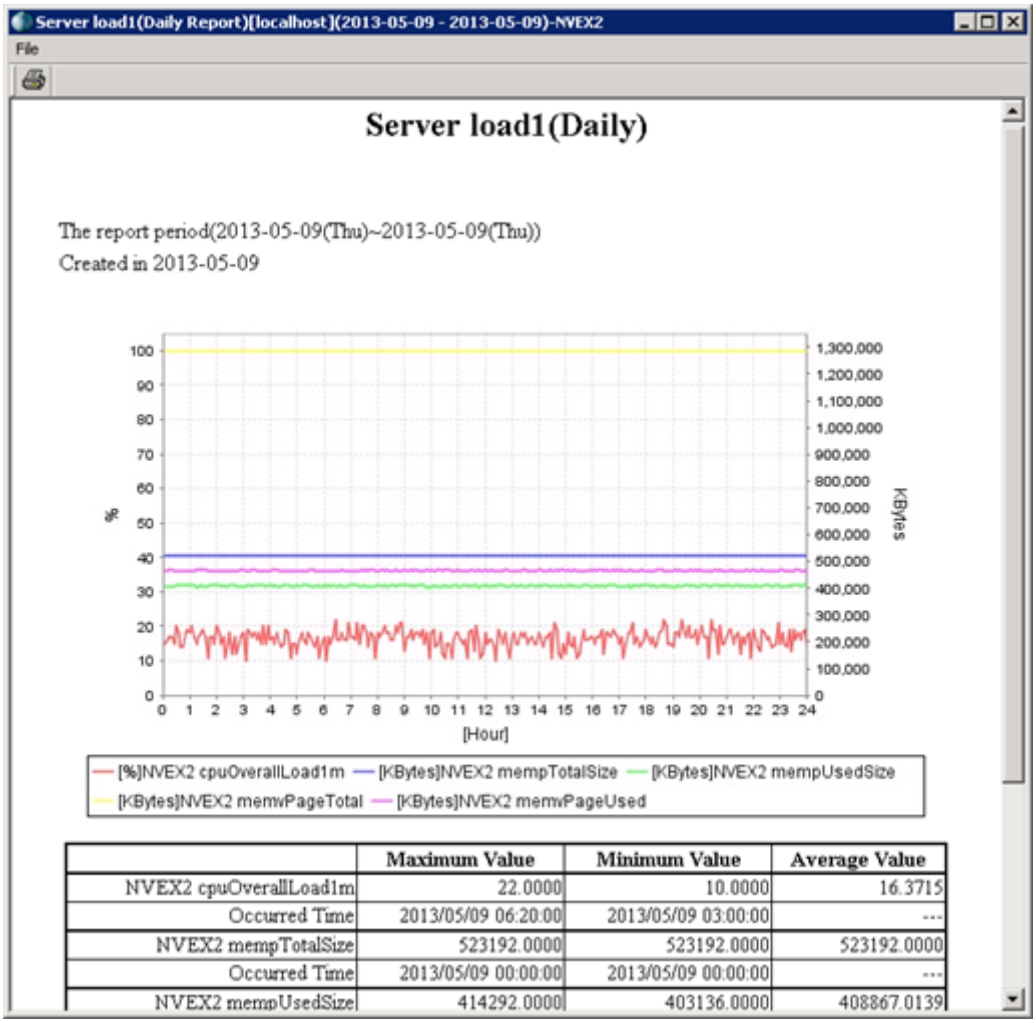
Items to set

- **Target Server**

  Specify the server for which you want to collect data. This can be specified using a character string with up to 63 single-byte characters.

For other setting items such as the interval, refer to "4.16.1 Data Collecting Setting window (page 334)".

Report sample



	Maximum Value	Minimum Value	Average Value
NVEX2 cpuOverallLoad1m	22.0000	10.0000	16.3715
Occurred Time	2013/05/09 06:20:00	2013/05/09 03:00:00	---
NVEX2 mempTotalSize	523192.0000	523192.0000	523192.0000
Occurred Time	2013/05/09 00:00:00	2013/05/09 00:00:00	---
NVEX2 mempUsedSize	414292.0000	403136.0000	408867.0139

CSV file format

;UNIXTIME	ManagerName: Compname	cpuOverall Load1m()	mempTotal Size()	mempUsed Size()	memvPage Total()	memvPage Used()
;		%	KBytes	KBytes	KBytes	KBytes
Collecting time	:Node name	CPU busy rate	Memory total size	Memory usage size	Page total size	Page Usage size

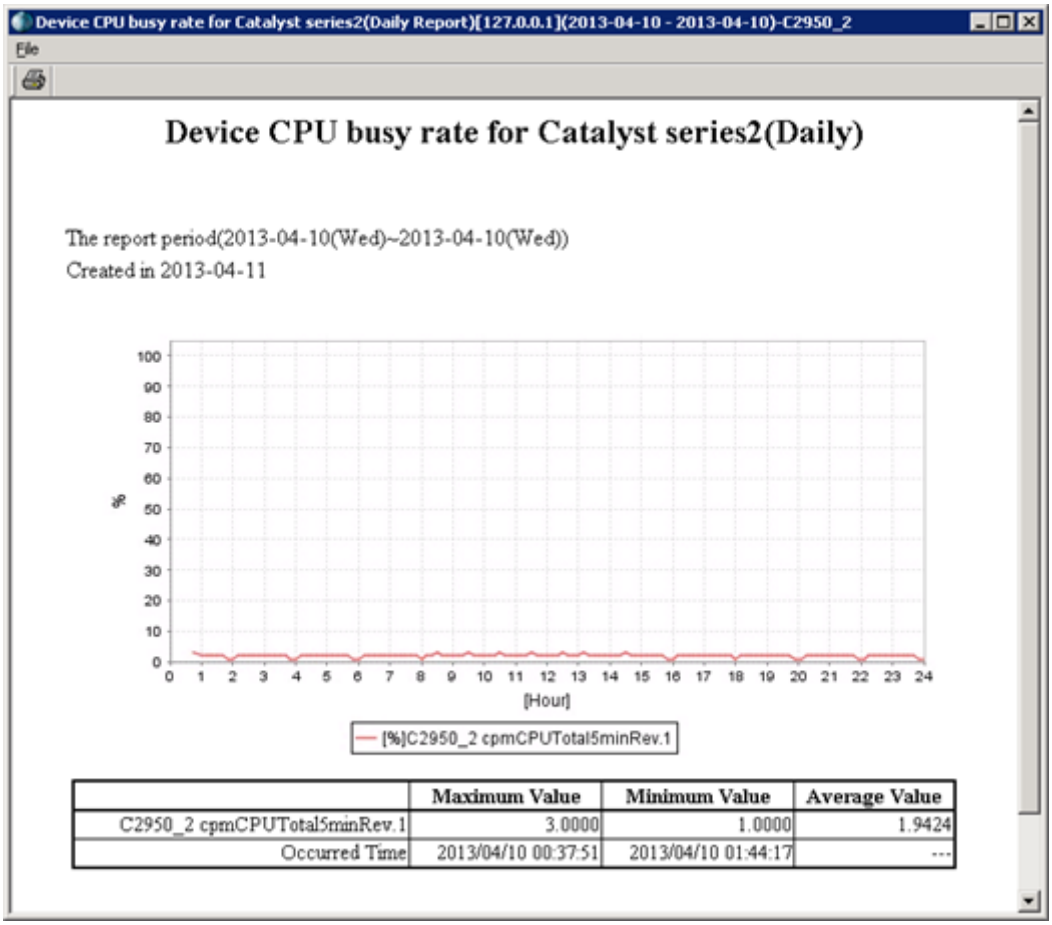
7.2.7 Device CPU busy rate for Catalyst series

Summary

This rule collects data for the CPU busy ratio for Cisco Catalyst Series, Cisco Router Series, Cisco Nexus Series, and Cisco ASA5500 Series devices.

For other setting items such as the interval, refer to "4.16.1 Data Collecting Setting window (page 334)".

Report sample



	Maximum Value	Minimum Value	Average Value
C2950_2 cpmCPUTotal5minRev.1	3.0000	1.0000	1.9424
Occurred Time	2013/04/10 00:37:51	2013/04/10 01:44:17	---

⚠ Caution

This CPU busy rate is data at intervals of five minutes. It is recommended that the interval is set to 5 minutes or more.

CSV file format

UNIXTIME	ManagerName:Compname	avgBusy5()
;		
Collecting time	:Node name	CPU busy rate

7.2.8 MIB Expression

Summary

Collect data according to the definition of the specified MIB expression and monitor the values calculated by that MIB expression.

If you specify the definition of a MIB expression that contains multiple expressions in one definition and you set threshold monitoring on it, all calculated values are subject to threshold checking.

Items to set

- **Rule**

Specify the rule name to identify the MIB expression definition.

If you want to collect counter-type MIBs, refer to the notes described in "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

- **Instance**

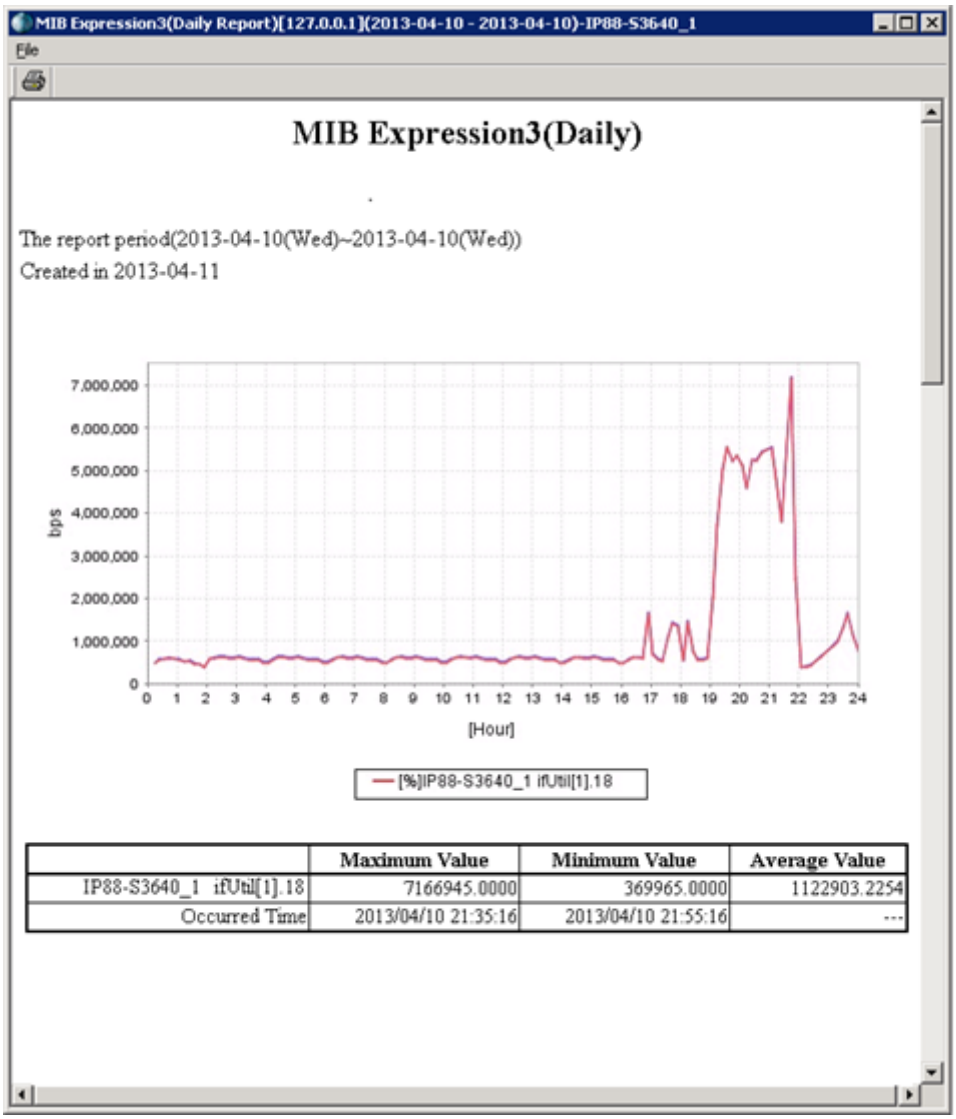
  Specify the instance number of the management item.

  The specified value is added as the last element of the management item specified by "MIB Expression" rule.

  If this item is not specified, MIB that can be recognized is the obtainable target, based on the management item specified by "MIB Expression" rule. However, note that the target MIB varies depending on embedding status of MIB or what element of OID is specified.

For other setting items such as the interval, refer to "4.16.1 Data Collecting Setting window (page 334)".

Report sample



CSV file format

;UNIXTIME	ManagerName:Compname	MIB name
;		%
Collecting time	:Node name	Outputs the value calculated using the MIB expression specified in the **Rule** name in the Data Collecting Setting window.

Caution

MIB specified as the monitoring item does not support MIB of character string type.

7.2.9 General

Function description

This rule collects data for the purpose of assessing information such as changes over time in items for a specified MIB. It is possible to retrieve up to three MIB items at the same time in one data collection entry.

Items to set

- **Management Item Name**

  Select the MIB item that you want to collect and register it. Up to three items can be registered. A character string of up to 4095 characters can be entered in one entry box.

  If you want to collect counter-type MIBs, refer to the notes described in "7.7 Notes on Counter-type and Counter64-type MIBs (page 666)".

  Caution

  1. When displaying the data obtained in the report in a single graph, it may be difficult to interpret the graph if a large quantity of management items were specified.

     For example, if specifying, "iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets" target only the necessary interfaces so that it becomes (iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets.interface_number)
  2. The data processing unit of graph display or CSV output is specified per entry. MIB items of which units are different should be managed in the different entries.
  3. "Default Target Ports" setting of the icon properties is enabled only for monitoring the following MIBs.
     - iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable (1.3.6.1.2.1.2.2)
     - iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable (1.3.6.1.2.1.31.1.1)

- **Output CSV Data Unit**

  Specify "bps", "pps", "%", "Differential", or "No Processing" as the processing unit for outputting CSV file and creating a report.

  - bps

    When an interval t1 value is val1 and the next interval t2 value is val2, the following calculation is performed.

    bps = (val2 - val1) * 8 / (t2 - t1)

This processed method is valid for MIB representing octet figure such as MIB name ".interfaces.ifTable.ifEntry.ifInOctets", etc.

- pps

  When an interval t1 value is val1 and the next interval t2 value is val2, the following calculation is performed.

  pps = (val2 - val1) / (t2 - t1)

  This processed method is valid for MIB representing packet figure such as MIB name ".interfaces.ifTable.ifEntry.ifInUcastPkts", etc.

- Difference

  Calculates the simple difference of values at intervals. When an interval t1 value is val1 and the next interval t2 value is val2, the following calculation is performed.

  Difference = val2 - val1

  Caution

  When there is missing data due to a load, etc., the difference between data before and after the missing data is displayed. For this reason, the data looks prominent.

- %, No processing

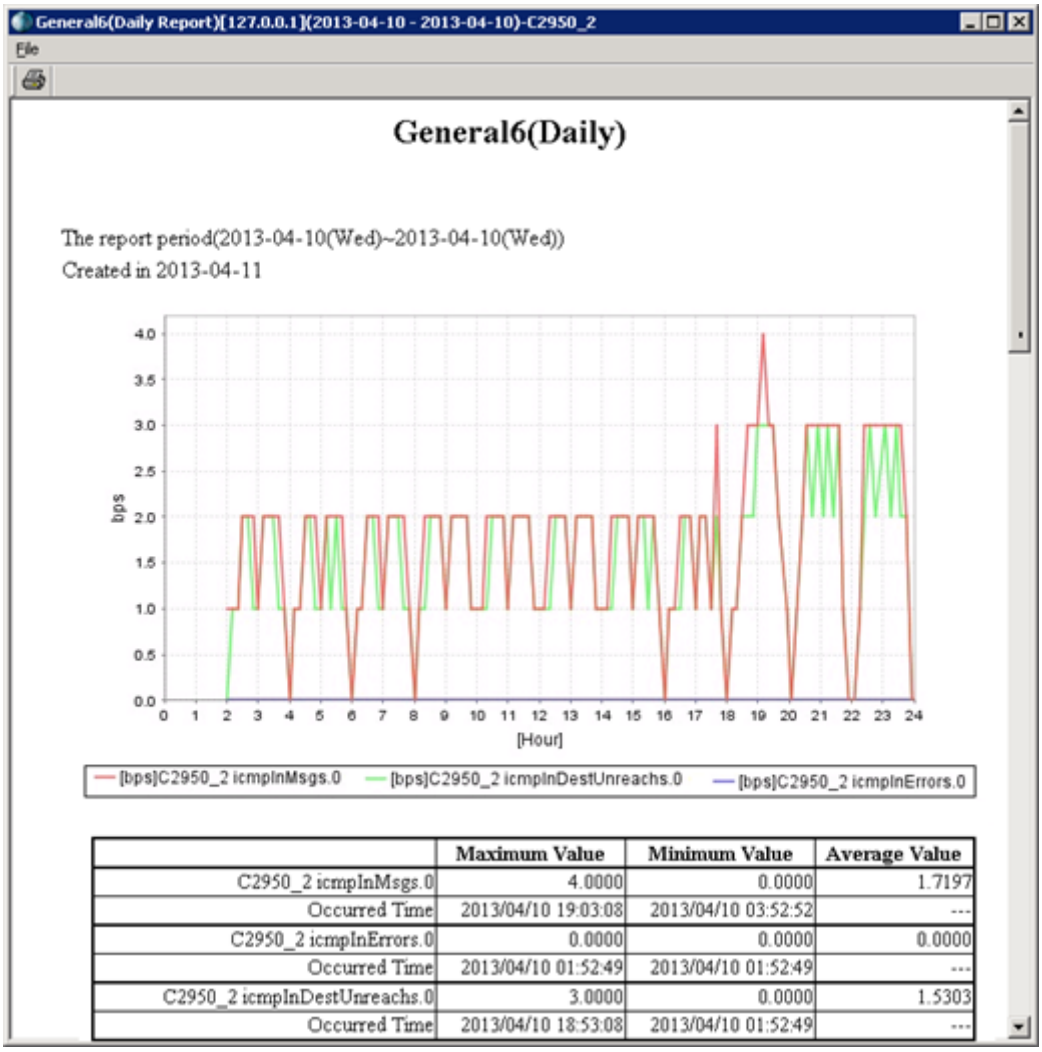
  The obtained value is not processed.

Caution

If the MIB-type is counter-type, because it is an accumulation value, "No Processing" is a value with no meaning as an output data.

For other setting items such as the interval, refer to "4.16.1 Data Collecting Setting window (page 334)".

Report sample



	Maximum Value	Minimum Value	Average Value
C2950_2 icmpInMsgs.0	4.0000	0.0000	1.7197
Occurred Time	2013/04/10 19:03:08	2013/04/10 03:52:52	---
C2950_2 icmpInErrors.0	0.0000	0.0000	0.0000
Occurred Time	2013/04/10 01:52:49	2013/04/10 01:52:49	---
C2950_2 icmpInDestUnreachs.0	3.0000	0.0000	1.5303
Occurred Time	2013/04/10 18:53:08	2013/04/10 01:52:49	---

CSV file format

;UNIXTIME	ManagerName:Compname	MIB name
;		"bps", "pps", or "diff"
Collecting time	:Node name	Output data from the MIB specified in the management item name of the Data Collecting Setting window.

Caution

1. The number of MIB name increases and decreases according to the number of specified managed items (MIBs). "bps", "pps", or "diff" is output in the unit set in the **Output CSV Data Unit** of the Data Collecting Setting window.
2. MIB specified as the monitoring item does not support MIB of character string type.

7.2.10 Built-in MIB Expression rules

This section describes details of the built-in MIB Expression rules in Network Manager.

Tip

The built-in MIB expression rules have appropriate **Type of data**, and the collected data can be displayed on the Web Console.

7.2.10.1 Rules for interfaces

Collects MIBs provided by the IF-MIB and calculates the following data related to the interfaces.

Interface Utilization (IN)

Collects MIBs of the specified input interfaces of the specified device and calculates the bandwidth utilization for input interfaces.

Rule name	Support device
builtin:ifInUtil	The devices supporting IF-MIB
builtin:ifInUtil64bit	The devices supporting IF-MIB and running SNMP v2c or SNMP v3 agent

In this rule, **ifInUtil** is set as the **Type of data**.

Interface Utilization (OUT)

Collects MIBs of the specified output interfaces of the specified device and calculates the bandwidth utilization for output interfaces.

Rule name	Support device
builtin:ifOutUtil	The devices supporting IF-MIB
builtin:ifOutUtil64bit	The devices supporting IF-MIB and running SNMP v2c or SNMP v3 agent

In this rule, **ifOutUtil** is set as the **Type of data**.

Packet Loss Rate (IN)

Collects MIBs of the specified input interfaces of the specified device and calculates the percentage of packets discarded for inbound packets.

Rule name	Support device
builtin:ifInDiscards	The devices supporting IF-MIB

In this rule, **ifInDiscards** is set as the **Type of data**.

Packet Loss Rate (OUT)

Collects MIBs of the specified output interfaces of the specified device and calculates the percentage of packets discarded for outbound packets.

Rule name	Support device
builtin:ifOutDiscards	The devices supporting IF-MIB

In this rule, **ifOutDiscards** is set as the **Type of data**.

Packet Error Rate (IN)

Collects MIBs of the specified input interfaces of the specified device and calculates the percentage of error packets for inbound packets.

Rule name	Support device
builtin:ifInErrors	The devices supporting IF-MIB

In this rule, **ifInErrors** is set as the **Type of data**.

Packet Error Rate (OUT)

Collects MIBs of the specified output interfaces of the specified device and calculates the percentage of error packets for outbound packets.

Rule name	Support device
builtin:ifOutErrors	The devices supporting IF-MIB

In this rule, **ifOutErrors** is set as the **Type of data**.

7.2.10.2 Rules for QX series

Collects MIBs provided by the QX series and calculates the following data.

CPU Utilization

Collects MIBs related to the CPUs provided by the QX series and calculates the CPU utilization of the system or slot.

Rule name	Support device
builtin:QxSystemCpu	S800E series, S1000G series, S2109T-PW, S2110P-I, S3100TP series, S3300TP series, S3400F series, S3800 series, S4000P series, S4100G series, S5200G series, S5300 series, S5300G series, S5400 series, S5500 series, S5500G series, S5600G series, S5828T, S5900 series, S6600 series, S6832QP, W1000 series, W2000 series
builtin:QxSlotCpu	S800E series, S2109T-PW, S2110P-I, S3400F series, S3800 series, S4100G series, S5200G series, S5300 series, S5300G series, S5400 series, S5500 series, S5500G series, S5600G series, S5828T, S5900 series, S6600 series, S6832QP, S7500 series, W1000 series, W2000 series

In this rule, **cpuUtil** is set as the **Type of data**.

Memory Utilization

Collects MIBs related to the memory provided by the QX series and calculates the memory utilization of the system.

Rule name	Support device
builtin:QxMemory	S1000G series, S3100TP series, S3300TP series, S3400F series, S3800 series, S4000P series, S4100G series, S5200G series, S5300 series, S5300G series, S5400 series, S5500 series, S5500G series, S5600G series, S5828T, S5900 series, S6600 series, S6832QP, W1000 series, W2000 series

In this rule, **memoryUtil** is set as the **Type of data**.

7.2.10.3 Rules for IX series

Collects MIBs provided by the IX series and calculates the following data.

CPU Utilization

Collects MIBs related to the CPUs provided by the IX series and calculates the CPU utilization of the system.

Rule name	Support device
builtin:Ix1000Ix2000Ix3000Cpu	1000 series, 2000 series, 3000 series

In this rule, **cpuUtil** is set as the **Type of data**.

Memory Utilization

Collects MIBs related to the memory provided by the IX series and calculates the memory utilization of the system.

Rule name	Support device
builtin:Ix1000Ix2000Ix3000Memory	1000 series, 2000 series, 3000 series

In this rule, **memoryUtil** is set as the **Type of data**.

7.2.10.4 Rules for IP8800 series and ALAXALA Networks devices

Collects MIBs provided by the IP8800 series or ALAXALA Networks devices and calculates the following data.

CPU Utilization

Collects MIBs related to the CPUs provided by the IP8800 series or ALAXALA Networks devices and calculates the CPU utilization of the system.

Rule name	Support device
builtin: Ip8800S8kR8kBcuCpu	IP8800/S8600, S8300, R8600 series, AX8600S, 8300S, 8600R series
builtin:Ip8800R8kPruCpu	IP8800/R8600 series, AX8600R series
builtin:Ip8800S8kPsuCpu	IP8800/S8600, S8300 series, AX8600S, 8300S series

Rule name	Support device
builtin:Ip8800S6700Cpu	IP8800/S6700 series, AX6700S series
builtin:Ip8800S6600Cpu	IP8800/S6600 series, AX6600S series
builtin:Ip8800S6300Cpu	IP8800/S6300 series, AX6300S series
builtin:Ip8800S4600Cpu	IP8800/S4600 series, AX4600S series
builtin:Ip8800S3800Cpu	IP8800/S3800 series, AX3800S series
builtin:Ip8800S3660Cpu	IP8800/S3660 series, AX3660S series
builtin:Ip8800S3650Cpu	IP8800/S3650 series, AX3650S series
builtin:Ip8800S3640Cpu	IP8800/S3640 series, AX3640S series
builtin:Ip8800S2500Cpu	IP8800/S2500 series, AX2500S series
builtin:Ip8800S2200Cpu	IP8800/S2200 series, AX2200S series
builtin:Ip8800S2100Cpu	IP8800/S2100 series, AX2100S series
builtin:Ip8800S1250Cpu	IP8800/S1250 series, AX1250S series
builtin:Ip8800S1240Cpu	IP8800/S1240 series, AX1240S series
builtin:Ip8800A260Cpu	IP8800/A260 series, AX260A series

In this rule, **cpuUtil** is set as the **Type of data**.

Memory Utilization

Collects MIBs related to the memory provided by the IP8800 series or ALAXALA Networks devices and calculates the memory utilization of the system.

Rule name	Support device
builtin: Ip8800S8kR8kBcuMemory	IP8800/S8600, S8300, R8600 series, AX8600S, 8300S, 8600R series
builtin:Ip8800R8kPruMemory	IP8800/R8600 series, AX8600R series
builtin:Ip8800S8kPsuMemory	IP8800/S8600, S8300 series, AX8600S, 8300S series
builtin:Ip8800S6700Memory	IP8800/S6700 series, AX6700S series
builtin:Ip8800S6600Memory	IP8800/S6600 series, AX6600S series
builtin:Ip8800S6300Memory	IP8800/S6300 series, AX6300S series
builtin:Ip8800S4600Memory	IP8800/S4600 series, AX4600S series
builtin:Ip8800S3800Memory	IP8800/S3800 series, AX3800S series
builtin:Ip8800S3660Memory	IP8800/S3660 series, AX3660S series
builtin:Ip8800S3650SMemory	IP8800/S3650 series, AX3650S series
builtin:Ip8800S3640Memory	IP8800/S3640 series, AX3640S series
builtin:Ip8800S2500Memory	IP8800/S2500 series, AX2500S series
builtin:Ip8800S2200Memory	IP8800/S2200 series, AX2200S series
builtin:Ip8800S2100Memory	IP8800/S2100 series, AX2100S series
builtin:Ip8800S1250Memory	IP8800/S1250 series, AX1250S series
builtin:Ip8800S1240Memory	IP8800/S1240 series, AX1240S series

Rule name	Support device
builtin:Ip8800A260Memory	IP8800/A260 series, AX260A series

In this rule, **memoryUtil** is set as the **Type of data**.

7.2.10.5 Rules for PF series

Collects MIBs provided by the PF series and calculates the following data.

CPU Utilization

Collects MIBs related to the CPUs provided by the PF series and calculates the CPU utilization of the system.

Rule name	Support device
builtin:Pf6800Cpu	PF6800, PF6800 Software
builtin:Pf6800 NetworkCoordinatorCpu	PF6800 Network Coordinator
builtin:Pf5200Cpu	PF5200 series
builtin:Pf5300Cpu	PF5300 series

In this rule, **cpuUtil** is set as the **Type of data**.

Memory Utilization

Collects MIBs related to the memory provided by the PF series and calculates the memory utilization of the system.

Rule name	Support device
builtin:Pf6800Memory	PF6800, PF6800 Software
builtin:Pf6800 NetworkCoordinatorMemory	PF6800 Network Coordinator
builtin:Pf5200Memory	PF5200 series
builtin:Pf5300Memory	PF5300 series

In this rule, **memoryUtil** is set as the **Type of data**.

7.2.10.6 Rules for SV series

Collects MIBs provided by the SV series and calculates the following data.

CPU Utilization

Collects MIBs related to the CPUs provided by the SV series and calculates the CPU utilization of the system.

Rule name	Support device
builtin:Sv7000Sv8500Sv9500Cpu	7000 series, 8500 series, 9500 series

In this rule, **cpuUtil** is set as the **Type of data**.

7.2.10.7 Rules for BX series and AudioCodes devices

Collects MIBs provided by the BX series or AudioCodes devices and calculates the following data.

CPU Utilization

Collects MIBs related to the CPUs provided by the BX series or AudioCodes devices and calculates the CPU utilization of the system.

Rule name	Support device
builtin:BxDataCpu	BX series, Mediant series
builtin:BxVoIpCpu	BX series, Mediant series

In this rule, **cpuUtil** is set as the **Type of data**.

Memory Utilization

Collects MIBs related to the memory provided by the BX series or AudioCodes devices and calculates the memory utilization of the system.

Rule name	Support device
builtin:BxDataMemory	BX series, Mediant series
builtin:BxVoIpMemory	BX series, Mediant series

In this rule, **memoryUtil** is set as the **Type of data**.

7.2.10.8 Rules for Cisco Systems devices

Collects MIBs provided by Cisco Systems devices and calculates the following data.

CPU Utilization

Collects MIBs related to the CPUs provided by Cisco Systems devices and calculates the CPU utilization of the system.

Rule name	Support device
builtin: CiscoWirelessLanControllerCpu	Cisco Wireless LAN Controller (2500 series, 3500 series, 5500 series, 8500 series)

In this rule, **cpuUtil** is set as the **Type of data**.

Tip

For CPU utilization of Cisco Systems devices other than the Cisco Wireless LAN Controller, use the Data Collection Rule **Device CPU busy rate for Catalyst series**.

Memory Utilization

Collects MIBs related to the memory provided by Cisco Systems devices and calculates the memory utilization of the system.

Rule name	Support device
builtin:CatalystMemory	Cisco Catalyst series, Cisco Router series, Cisco ASA5500 series

Rule name	Support device
builtin:NexusMemory	Cisco Nexus series
builtin: CiscoWirelessLan ControllerMemory	Cisco Wireless LAN Controller (2500 series, 3500 series, 5500 series, 8500 series)

In this rule, **memoryUtil** is set as the **Type of data**.

7.2.10.9 Rules for Fortinet devices

Collects MIBs provided by Fortinet devices and calculates the following data.

CPU Utilization

Collecting MIBs related to the CPUs provided by Fortinet and calculates the CPU utilization of the system, or the CPU utilization of each processor of the device with multiple CPUs. And calculates the CPU utilization of each cluster member when configuring the Cluster (High Availability).

Rule name	Support device
builtin:FortiGateSystemCpu	FortiGate series
builtin:FortiGateProcessorCpu	FortiGate series
builtin:FortiGateHaCpu	FortiGate series (Cluster (High Availability) configuration)
builtin:FortiManagerCpu	FortiManager series

In this rule, **cpuUtil** is set as the **Type of data**.

Memory Utilization

Collecting MIBs related to the memory provided by Fortinet and calculates the memory utilization of the system, or the memory utilization of Low memory(used by the kernel). And calculates the memory utilization of each cluster member when configuring the Cluster (High Availability).

Rule name	Support device
builtin:FortiGateSystemMemory	FortiGate series
builtin:FortiGateLowMemMemory	FortiGate series
builtin:FortiGateHaMemory	FortiGate series (Cluster (High Availability) configuration)
builtin:FortiManagerMemory	FortiManager series

In this rule, **memoryUtil** is set as the **Type of data**.

7.2.10.10 Rules for A10 Networks devices

Collects MIBs provided by A10 Networks devices and calculates the following data.

CPU Utilization

Collects MIBs related to the CPUs provided by A10 Networks devices and calculates the CPU utilization of the control CPU or the data CPU.

Rule name	Support device
builtin:A10ControlCpu	A10 Thunder series, AX series
builtin:A10DataCpu	A10 Thunder series, AX series

In this rule, **cpuUtil** is set as the **Type of data**.

Memory Utilization

Collects MIBs related to the memory provided by A10 Networks devices and calculates the memory utilization of the system.

Rule name	Support device
builtin:A10Memory	A10 Thunder series, AX series

In this rule, **memoryUtil** is set as the **Type of data**.

7.3 Standard Specification Format

7.3.1 Overview of Standard Specification Format

Standard specification format is the naming rule for "component name" and "AMIB". This section describes the standard specification format in detail.

Tip

AMIB (Abstract Management Information Base) is the original concept extended from the Internet standard MIB. AMIB is extended from original MIB by adding two concepts: "Component" and "Time". "Component" is identified by the component type and component name.

7.3.2 Standard Matching Specification Format

When specifying a component-type name or component name, you can use the "standard matching specification format".

In matching, the asterisk (*), question mark (?), left bracket ([), right bracket (]), hyphen (-) and backslash (or yen symbol) (\) have meanings. These characters with meanings are referred to as metacharacters.

1. The asterisk (*) matches any character string of zero or more characters.
   - Example: Switch*

     This example matches any name starting with "Switch", such as "Switch1" or "SwitchABC".
   - Example : *

     This example matches all registered names.
2. The question mark (?) matches any single character.
   - Example: Router?

     This example matches any five-letter name starting with "Router", such as "Router1" or "RouterA".
3. Brackets match any characters contained within the brackets.
   - Example: Host[123]

This example matches "Host1", "Host2" or "Host3".

When there are two characters connected by a hyphen (-) within the brackets, any characters within that character range are matched. These characters can be specified using alphabetic characters. Multiple specifications are also possible.

- Example: Host[1-3]

  This example matches "Host1", "Host2" and "Host3".

- Example: Host[a-zA-Z0-9]

  This example matches any name that starts with "Host" and ends with one alphanumeric character, such as "SwitchA" or "Switch1".

7.3.3 Standard Component Name Specification Format

When specifying a component, you can use the standard component name specification format. The standard component name specification format is a format with combination of the component-type name and component name, and is followed by the rules below.

1. The component-type name is delimited from the component name by (:).

   - Example: node:Switch1

   Component type name has the following types.

   - node

     Device icon name registered in the Map View

   - grp

     Group name specified in the **Group** column of the Properties dialog box

   - map

     Map icon name registered in the Map View

   You can use standard matching specification format expressions such as the asterisk (*) to specify component-type names or component names.

   - Example: node:Switch*

     This example indicates node components, all of which names begin with "Switch".

   - Example: grp:Group*

     This example indicates group components, all of which names begin with "Group".

2. Multiple components can be specified by connecting component names with a comma (,).

   - Example: node:Node1,node:Node2,grp:Group*,node:Node3

     This example indicates node components of which names are "Node1", "Node2", and "Node3", and a group component of which name begins with "Group".

3. Component type can be omitted. When the specified beginning of the component type is omitted, it is considered as a node component type. When a component type connected by comma (,) is omitted, it is considered as a type equal to the previous component.

   - Example: Node1,Node2

     This example indicates node component of which name is "Node1" and "Node2".

   - Example: grp:Group1,Group2

     This example indicates a group component of which name is "Group1" and "Group2"

- Example : *

  This example indicates all node components.

- Example: Node1,grp:Group*,node:HostNode*

  This example indicates node component of which name is "Node1", node component of which name begins with "HostNode", and all group components of which names begin with "Group".

  In this example, "node" before "HostNode*" can not be omitted. If it is omitted, the result is the same as when "grp:HostNode*" is specified, then it indicates not node but group component.

4. A colon (:) or comma (,) must not be preceded or followed with a space.
   - Incorrect: Host32, Host33, Host34

7.3.4 Standard AMIB Name Specification Format

This section describes the method for specifying names where an AMIB name is entered in an item.

Following is the example of the AMIB name.

- iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0

The "iso" and "org" are each referred to as an AMIB entry name. An entry name that appears at the end, such as "sysDescr" above, is referred to as a leaf AMIB entry name. The "0" at the end is referred to as an instance variable or simply an index.

Each AMIB entry name is related to a numerical value. For this reason, they can be entered using either numerical characters or name characters. If all entry names are specified using name characters they are referred to as complete name string type AMIB. If the entry names are specified using numerical characters they are referred to as complete numerical string type AMIB. The following examples express the same name.

- iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0
- 1.3.6.1.2.1.1.1.0
- iso.3.dod.1.mgmt.1.system.1.0

If the name begins with a period (.), it is assumed to begin with "iso.org.dod.internet.mgmt.mib-2". The following examples express the same name.

- iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0
- .system.sysDescr.0

If the name begins with a tilde (~) it is assumed to begin with "iso.org.dod.internet.private.enterprises". The following examples express the same name.

- iso.org.dod.internet.private.enterprises.nec.necProduct.pc-9801
- ~nec.necProduct.pc-9801

It is possible to specify multiple AMIBs using comma separation (,). (Commas must not be preceded or followed by a space.)

- .system.sysDescr.0,.system.sysLocation.0

Multiple AMIBs can be specified by surrounding them with braces ({}). A comma can also be specified within braces ({,}). The first three examples below express the same name.

- .system.sysDescr.0,.system.sysLocation.0

- .system.{sysDescr,sysLocation}.0
- .system.sys{Descr,Location}.0
- .interfaces.ifTable.ifEntry.if{In{Octets,Discards},OutOctets}.{3,4,5}

If an asterisk (*) is shown or the AMIB entry name at the end is omitted, all AMIBs below the specified AMIB entry are displayed. An asterisk (*) cannot be used in the middle of an AMIB entry name.

- .system.* --> all below ".system"
- .system --> all below ".system"
- .system.sys* --> error

7.3.5 Standard AMIB Value Specification Format

Use the following "standard AMIB value specification format" in items specifying AMIB values.

INTEGER-Type:

Specify a numeric value between "-2,147,483,648" and "2,147,483,647".

Counter-Type Gauge-Type:

Specify a numeric value between "0" and "4,294,967,295".

Counter64-Type:

Specify a numeric value between "0" and "18,446,744,073,709,551,615".

TimeTicks-Type:

Specify a value in "12:34:56.78" format (12 hours 34 minutes 56.78 seconds). The hour, minute and millisecond can be omitted.

UnixTime-Type:

pecify a value in "2008/12/25.12:00:00" format (2008-12-25.12:00hrs), "2008/12/25" format (2008-12-25 0hrs), or "12:00:00" (today at 12:00 hrs) format. Use a dot (.) between the date and time. Whitespace characters must not be entered before or after dots (.), slashes (/), or colons (:). The year and second may be omitted.

IpAddress-Type NetworkAddress-Type:

Specify a value in "127.0.0.1" format made up of four numeric values between "0" and "255" linked using dots (.). Alternatively, use hexadecimal notation starting with 0x, such as "0x7f000001".

IpxAddress-Type:

Specify a value in "1a00:4c05353d" (network number:node number) format using hexadecimal notation. The network number is in hexadecimal notation with a maximum of 8 digits. The node number has a maximum of 12 digits. For NetWare servers, specify internal network numbers for the network numbers and "1" for the node number. In this case, the node number may be omitted. Additionally, you can omit the leading "0" from the network numbers and node numbers.

OctetString-Type PhysAddress-Type Opaque-Type:

Specify in "0x7f:56:3b:0a" format (starting with 0x and separated by a colon (:) or in "7f 56 3b 0a" format (separated by whitespace characters) and using hexadecimal notation. Specify a numerical value of 0 to f using 2 digits, such as 00-0f.

DisplayString-Type:

Specify a normal text string such as "Network Manager". In accordance with the SNMP specification, non-ASCII characters should not be used, however, non-ASCII characters seems to be used.

ObjectID-Type:

Specify in standard AMIB name specification format, such as ".system.sysDescr.0".

NULL-Type:

Since this type has no values, there is no need to specify a value.

Ipv6Address-Type:

Specify an IPv6 address such as "fe80::230:13ff:fe85:3169".

Ipv6AddressPrefix-Type:
Ipv6AddressIfIdentifier-Type:

Currently there are no values to be specified.

7.4 Adding MIBs

Network Manager comes with the MIB file definition information required to use each function, but it is necessary to add new definition information from MIB files published by RFC or device vendors to perform the following operations:

- If monitoring SNMP traps for specific device types and want to create a Network Manager trap definition from an MIB file published by a device vendor.
- When monitoring and managing device-specific MIBs or new MIBs published by RFC.

Use the Trap Definition Management window to create trap definitions. For details, refer to "4.11.6.2 Automatically creating a trap definition from an MIB file (page 295)".

To add definition information for monitoring and managing MIBs, incorporate a definition file, created by using the `NvPROMib2Amib` command, into Network Manager. With the `NvPROMib2Amib` command, you can create the following four definition files.

For information about the `NvPROMib2Amib`, refer to "9.5.1 NvPROMib2Amib (page 695)".

1. AMIB definition file (basic file)

   This file defines information about the MIB tree structure and the data types for MIB objects connected to the tree. It forms the basis of all definition files generated from an MIB file.

   The AMIB definition files that are provided by Network Manager are installed in the following directory:

   `<On the manager, %installfolder%>\Manager\sg\NvPRO\NVWORK\local\amib\`

   When adding new AMIB definition file, store the AMIB definition file into the following directory:

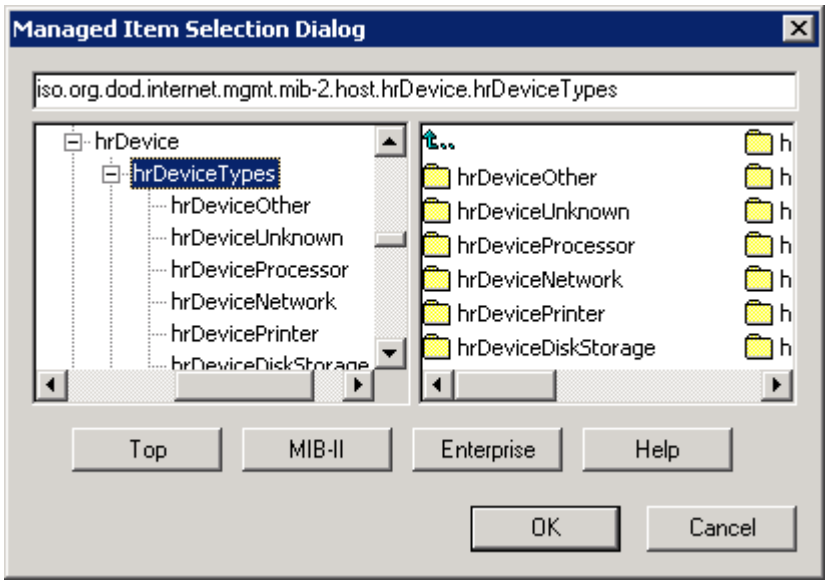
   `<On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\public\amib\`

   - Benefits of incorporating the file

     By understanding the tree structure and object types of a newly added MIB, it is possible to perform tasks that are appropriate for the MIB. In addition, it is possible to express the MIB name using a name (text string) instead of just a number.

The inserted MIB tree information also reflects in the "4.16.1.3 Managed Item Selection Dialog dialog box (page 340)" used when specifying MIBs in the State Monitoring and Data Collection functions.

Example of an MIB tree display:



For instructions on how to incorporate a file, refer to "7.4.1.1 Procedure for incorporating an AMIB definition file and type definition file (page 652)".

2. Type definition file (NetvisorEx.tc)

   This is the file that defines extended data types that are different from the standard data types (INTEGER, OCTET STRING, etc). It is incorporated in conjunction with the AMIB definition file.

   - Benefits of incorporating the file

     If new extended data types different from the standard data types are used in the content of AMIB definition files (in an MIB object definition), an error occurs when the file is incorporated.

     To incorporate a definition of the extended data type first, Network Manager can understand the contents of the AMIB definition and the file can be incorporated without errors.

   When using the `NvPROMib2Amib` command to create an AMIB definition file, if there is a TEXTUAL-CONVENTION macro definition that shows the new data type in the specified MIB file, the new type definition is automatically added to NetvisorEx.tc and stored in the folder below.

   Store destination:

   <On the manager, %sharedfolder%>`\Manager\sg\NvPRO\NVWORK\public\amib\`

   For instructions on how to incorporate a file, refer to "7.4.1.1 Procedure for incorporating an AMIB definition file and type definition file (page 652)".

3. AMIB help file

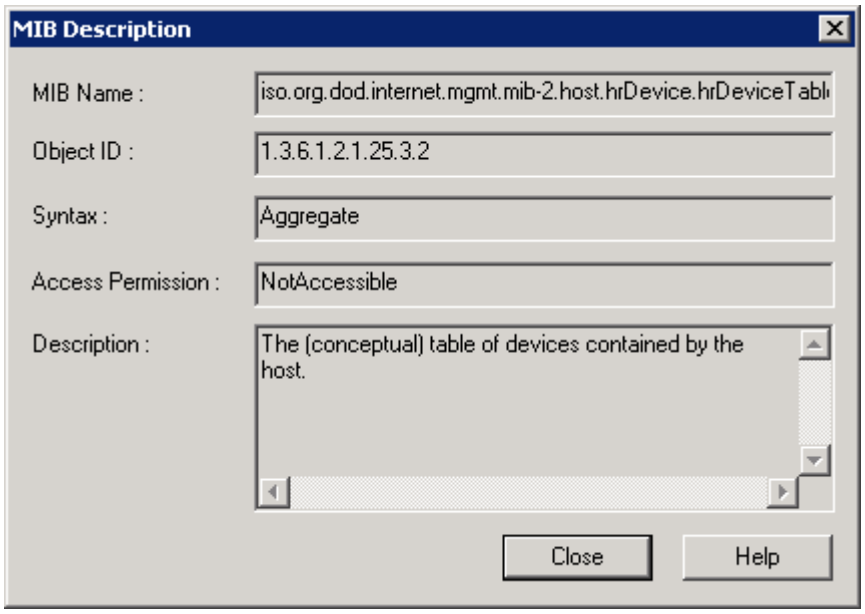
   Contains descriptions (DESCRIPTION) of MIB objects extracted from an MIB file. Incorporated in conjunction with the AMIB definition file, as needed.

   - Benefits of incorporating the file

The incorporated descriptions display in the "4.16.1.4 MIB Description dialog box (page 341)".

(Open by clicking the **Help** button in the "4.16.1.3 Managed Item Selection Dialog dialog box (page 340)" dialog box used to specify MIBs in the State Monitoring function and Data Collection function.)

Example of an MIB description:



If an AMIB help file has not been incorporated or there is no description in the MIB file, the **Description** column in the MIB Description dialog box is empty. For instructions on how to incorporate a file, refer to "7.4.1.2 Procedure for incorporating an AMIB help file (page 654)".

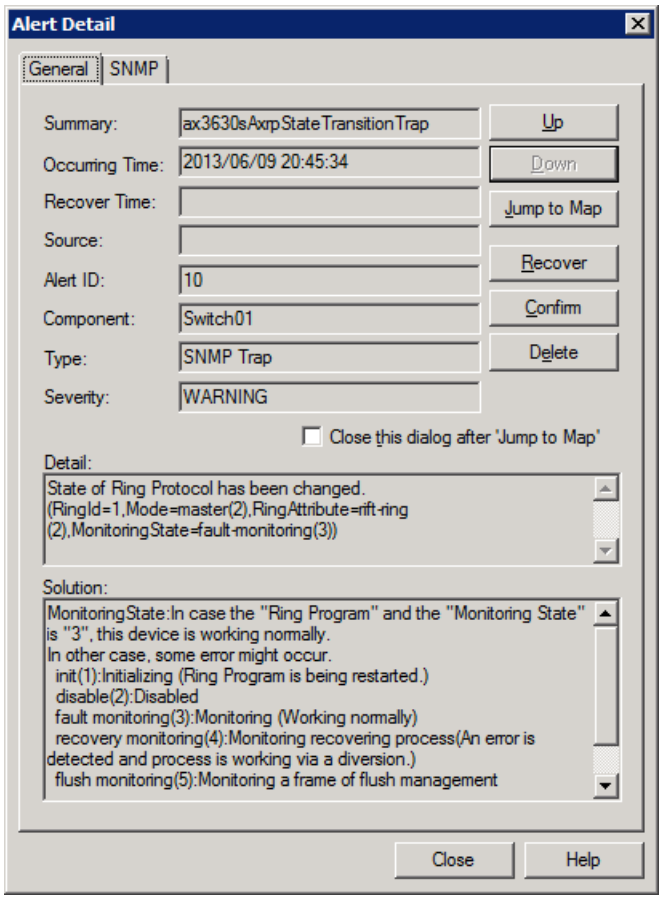
4. Trap definition file

   This is the file that defines the alert notification content when an SNMP trap is received. Automatically create the file based on the definitions in an MIB file (TRAP-TYPE macro or NOTIFICATION-TYPE macro).

   - Benefits of incorporating the file

     When receiving SNMP traps or acquire MIBs by methods such as the `NvPROAmibGetMgr` command, numeric MIB values are converted to symbolic names.

     Example: when an AMIB enumeration definition is incorporated (alert details display):



If an AMIB enumeration file is not incorporated, only numeric values display. For instructions on how to incorporate a file, refer to "7.4.1.3 Procedure for incorporating an AMIB enumeration (page 655)".

7.4.1 Procedure for adding an MIB

Follow the procedure below before integrating a new MIB into Network Manager.

1. Investigate the MIB file to be integrated and obtain the MIB file.

   To obtain the MIB file, contact the vendor of the target device.

2. Verify that there are no unnecessary strings in the obtained MIB file that are not part of the OBJECT-TYPE macro definition.

   If there are any unnecessary strings, delete them.

   - OBJECT-TYPE macro definition refers to the following descriptive section:

     ```
     <MIB name> DEFINITIONS ::= BEGIN
         :
     END
     ```

     If there are multiple OBJECT-TYPE macros in a MIB file, save each macro as the different file.

   - Lines starting with "--" are comment lines. These lines are ignored when creating a definition file in Network Manager.
   - Below are some examples of unnecessary strings.
     - SNMP Working Group [Page 13]

- ^L
- RFC 1213 MIB-II March 1991

3. Make sure that the extension of the MIB file is ".MIB".
4. Check the following important points when adding a MIB definition.
   a. An error will occur when adding the definition if a definition has not been added for the MIB file indicated in the "FROM" field in the "IMPORTS" definition that comes after "<MIB name> DEFINITIONS ::= BEGIN".

      ```
      <MIB name> DEFINITIONS ::= BEGIN
      IMPORTS
          <Object definition> FROM <MIB name>
      ;
      ```

      (The terminating ";" indicates the end of the "IMPORTS" definition.) Prepare the files, including the MIB file indicated in "FROM", and add the files in order, starting from the definition for the MIB file indicated in "FROM".
   b. For information about the MIB files (AMIB definition files) that come with Network Manager, refer to "Appendix C. Embedded MIB File List (page 814)".
   c. If a large number of MIB files (AMIB definition files) are added, Manager will take longer to start up. Only add the files to perform the required work.
   d. When adding an MIB file, errors may occur and some confirmations may be required. For this reason, batch execution is not recommended.
   e. In the case of the upgrade from MasterScope Network Manager 4.0 or older version, MIB file definitions that were manually added might become disabled. Check the following log file after upgrading.

      ```
      <On the manager, %installfolder%>\Manager\log\NvPROAmibDefFile.log
      ```
   f. In the MIB tree, if the different object IDs (OIDs) have same name, NvPRO Base Manager service may fail to start. Check the following log file and remove the AMIB definition file which causes the fault.

      ```
      <On the manager, %installfolder%>\Manager\log\NvPROAmibDefFile.log
      ```

RELATED LINKS

7.4.1.1 Procedure for incorporating an AMIB definition file and type definition file (page 652)
7.4.1.2 Procedure for incorporating an AMIB help file (page 654)
7.4.1.3 Procedure for incorporating an AMIB enumeration (page 655)

7.4.1.1 Procedure for incorporating an AMIB definition file and type definition file

The procedure below shows how to create an AMIB definition file from an obtained MIB file, add a type definition to a type definition file (NetvisorEx.tc), and incorporate the files into Network Manager.

When incorporating multiple MIB files, first incorporate the MIB that is listed in **FROM** of the **IMPORT** section in the MIB file. For example, if the MIB file has the following definitions,

incorporate ABC-MIB first. If XYZ-MIB is incorporated first, an error will occur because the xyz definition in ABC-MIB cannot be resolved.

```
XYZ-MIB DEFINITIONS ::= BEGIN
IMPORTS
    xyz FROM ABC-MIB
;
```

1. Start the command prompt (terminal) and change the current directory.

   ```
   > cd <On the manager, %installfolder%>\Manager\bin\
   ```

2. Run the following command for the MIB file.

   ```
   > NvPROMib2Amib -amib <MIB file name>.MIB
   ```

   For details, refer to "9.5.1 NvPROMib2Amib (page 695)".

   - The following message may be displayed while running the command.

     ```
     WARNINIG: The parent definition of [MIB definition] is ambiguous.
     ```

     The definition of MIB might be wrong. Check the relevant MIB definition, and contact with the vendor who provided the MIB file. If there is no problem, no adverse affect will be caused by incorporation of the MIB. Ignore the message.

   - If the definition file is created successfully, the following message is displayed.

     ```
     Succeeded in generating the definition file.
     (file name specified for an argument)
     ```

   - If an error occurs, the following message is displayed.

     ```
     Failed to generate the definition file.
     (file name specified for an argument)
     ```

     Resolve the error by referring to "7.4.2 Handling errors (page 656)", and run the `NvPROMib2Amib` command again.

3. Confirm that the created AMIB definition file does not affect operations of Network Manager.

   Network Manager may not perform monitoring correctly depending on the contents of the created AMIB definition file.

   Check the contents of the created AMIB definition file by using the `nvpamibcheck` command.

   ```
   > nvpamibcheck <AMIB definition file name>
   ```

   For details, refer to "9.5.2 nvpamibcheck (page 697)".

   If the following message is displayed, check the contents of the log file. Add *"#"* to the beginning of the definitions that will affect operations of Network Manager in the log file, so that the definition will not be incorporated.

   ```
   There are some illegal definitions.
   (result: 1 illegal definitions)
   Check the operation log for details:
   <On the manager, %installfolder%>\Manager\log
   \yyyyMMddHHmmssSSS_nvpamibcheck.log
   ```

4. Run the `NvPROReloadDefFileMgr` command to incorporate the AMIB definition file to Network Manager.

```
> NvPROReloadDefFileMgr
```

For details, refer to "9.5.4 NvPROReloadDefFileMgr (page 699)".

You can incorporate multiple AMIB definition files into Network Manager at a time by using the `NvPROReloadDefFileMgr` command. When incorporating multiple MIB files, convert them all to AMIB definition files and then run the `NvPROReloadDefFileMgr` command.

- If the files are incorporated successfully, the following message is displayed.

```
AMIB definition file <AMIB definition file name> reload succeeded.
NvPROStringconv.inf reload succeeded.
Please refer to the operation LOG.
<On the manager, %installfolder%>\Manager\log
\NvPROAmibDefFile.log
Notification of AMIB definition file reload is sent.
Notification of ICON definition file reload is sent.
exdll nvalanlz.dll reload succeeded
exdll NvPROAlertConvKnowledgeAPI.dll reload succeeded
exdll NvPROTrapCmdAPI.dll reload succeeded
exdll NvPROAlertAnalyzerAPI.dll reload succeeded
```

- If an error occurs, a message indicating the error is displayed.

  Resolve the error by referring to "7.4.2 Handling errors (page 656)", and run the `NvPROReloadDefFileMgr` command again.

Tip

MIBs incorporated to Network Manager by the `NvPROReloadDefFileMgr` command are listed in the following file. Information such as error messages issued during incorporation processing is also registered in this file.

<On the manager, %installfolder%>\Manager\log\NvPROAmibDefFile.log

MIBs defined as the OctetString type in the AMIB definition file are treated as the DisplayString type at incorporation. They are converted into a character string if possible. If they cannot be converted into character strings, binary data is displayed in hexadecimal.

If you want to display a MIB defined as the OctetString type in the AMIB definition file in hexadecimal, specify the target MIB in the NvPROStringconv.inf file. For details on setting, refer to "7.4.1.4 MIB Definition hexadecimal notation setting procedure (page 655)".

7.4.1.2 Procedure for incorporating an AMIB help file

The procedure below shows how to create an AMIB help file from an obtained MIB file and incorporate the file into Network Manager.

First add the AMIB definition file corresponding to the AMIB help file. For instructions, refer to "7.4.1.1 Procedure for incorporating an AMIB definition file and type definition file (page 652)".

1. Open the command prompt (terminal) and change the current directory.

```
> cd <On the manager, %installfolder%>\Manager\bin\
```

2. Run the following command for the MIB file.

```
> NvPROMib2Amib -desc <MIB file name>.MIB
```

For details, refer to "9.5.1 NvPROMib2Amib (page 695)".

- If the definition file is created successfully, the following message is displayed.

```
Succeeded in generating the definition file. (output file name)
```

- If an error occurs, the following message is displayed.

```
Failed to generate the definition file. (output file name)
```

Refer to "7.4.2 Handling errors (page 656)" to resolve the error, and run the `NvPROMib2Amib` command again.

7.4.1.3 Procedure for incorporating an AMIB enumeration

The procedure below shows how to create an AMIB enumeration file from an obtained MIB file and incorporate the file into Network Manager.

First add the AMIB definition file corresponding to the AMIB help file. For details, refer to "7.4.1.1 Procedure for incorporating an AMIB definition file and type definition file (page 652)".

1. Open the command prompt (terminal) and change the current directory.

```
> cd <On the manager, %installfolder%>\Manager\bin\
```

2. Run the following command for the MIB file.

```
> NvPROMib2Amib -enum <MIB file name>.MIB
```

For details, refer to "9.5.1 NvPROMib2Amib (page 695)".

- If the definition file is created successfully, the following message is displayed.

```
Succeeded in generating the definition file. (output file name)
```

- If an error occurs, the following message is displayed.

```
Failed to generate the definition file. (output file name)
```

Refer to "7.4.2 Handling errors (page 656)" to resolve the error, and run the `NvPROMib2Amib` command again.

7.4.1.4 MIB Definition hexadecimal notation setting procedure

MIB that should be displayed in hexadecimal notation is included in the MIB definition defined in the OctetString format in the AMIB definition file. In this case, MIB can be displayed in hexadecimal notation. The setting procedure is described below.

1. Create NvPROStringconv.inf in the following folder.

   <On the manager, %sharedfolder%>`\Manager\sg\NvPRO\NVWORK\public\amib\`

   If the file already exists, do not need to create a new file.

   The character encoding of `NvPROStringconv.inf` should be as follows:

OS of Manager	Character Code
Windows	UTF-16 (with BOM) (recommended) or OS multi-byte character encoding
Linux	UTF-8 (without BOM) (recommended) or UTF-16 (with BOM)

2. Open `NvPROStringconv.inf` and add the contents in the following format.

```
AMIB name<TAB>Hex
```

The *AMIB name* should be specified in the complete name string format or the complete numeric string format.

After editing, save and close the file.

3. Run the `NvPROReloadDefFileMgr` command to reflect the settings.

```
> cd <On the manager, %installfolder%>\Manager\bin\
> NvPROReloadDefFileMgr
```

For details, refer to "9.5.4 NvPROReloadDefFileMgr (page 699)".

7.4.2 Handling errors

When running the `NvPROMib2Amib` command to create a definition file for addition, or when running the `NvPROReloadDefFileMgr` command to apply the MIB addition, one or more of the error messages below may be generated, depending on the state of the execution environment. If an error message generates, refer to the information below to resolve the error.

During command execution checks

The following types of messages generate for errors occurring when starting each type of process:

Error Message	Meaning
Illegal command arguments	Message generated when an argument is incorrect. Check for problems with the argument specification. For example, -amib and -enum might have been specified at the same time.
Cannot connect to NvPRO Base Manager	Message generated when the connection to NvPRO Base Manager (NvPROBaseMgr) fails during the initialization process. Check if NvPRO Base Manager has stopped.
Failed to open a file	Message generated when a file cannot be opened. Make sure there is write access to the specified file. If "-out" option is not specified and a file name automatically output is too long, fails to open a file. Specify a output file in "-out" option and execute a command.
No such file or directory	Message generated when the specified file does not exist. Check if there are any errors in the file name or path name.
ERROR: Another process is running. Retry after the process has been finished.	`NvPROMib2Amib` or `NvPROReloadDefFileMgr` command is running in another process. Try again after running process is finished.

When analyzing MIB files

The following table lists the messages displayed if an error occurs when analyzing a MIB file, and the causes and solutions of the errors.

Regarding errors in the MIB file syntax, it is recommended to obtain a MIB file including properly corrected definitions from the vendor that supplied the MIB file. However, if unable to get a new file, perform the steps below to resolve the problem.

⚠ Caution

There might actually be an error in a line earlier than the indicated line number. If there is not a problem in the vicinity of the line number, check for a problem in the code before the line.

Error Message	Cause and Solution
ERROR: In *MIB module name*(*MIB filename*): The parent definition [*parent-MIB*] of [*definition-whose-parent-MIB-is-unknown*] was not found.	The MIB definition that is necessary for definition file analysis has not been found. Confirm whether the MIB definition that defines <*parent-MIB*> is incorporated or not.
ERROR: In *MIB module name*(*MIB filename*): The parent definition [*parent-MIB*] of [*definition-whose-parent-MIB-is-unknown*] is ambiguous.	The upper (parent) MIB definition was not uniquely found. Select an adequate number when candidates for a definition are displayed under the error message. If an adequate definition is unknown, confirm with the vendor that supplied the MIB file.
ERROR: Unknown access rights. Specify access rights using the words listed bellow. read-only,read-write, read-create, write-only not-accessible, accessible-for-notify	Definitions other than the following are specified as an access rights definition. read-only, read-write, read-create, write-only, not-accessible, accessible-for-notify Confirm the access rights definition and change to any of the above adequate access rights.
ERROR: Illegal MIB name "*MIB-name*". "*invalid-character-string*" is invalid character.	The displayed *"MIB-name"* does not comply with the following MIB definition rules. • A MIB-name must start with a lowercase letter. • A MIB-name must consist of uppercase and lowercase letters, numbers, and hyphens ("-"). Correct the corresponding definition in the source MIB file with names by complying with the above rules.
ERROR: Illegal MIB name "*MIB-name*". Specify the MIB name using up to 64 characters.	The displayed *"MIB-name"* does not comply with the following MIB definition rules. • A MIB-name must consist of up to 64 letters. Correct the corresponding definition in the source MIB file with names by complying with the above rules.
ERROR: SYNTAX element is already defined.	SYNTAX is redundantly defined in one definition. Decide which definition is appropriate, and delete unnecessary definitions.
ERROR: ACCESS element is already defined.	ACCESS or MAX-ACCESS is redundantly defined in one definition. Decide which definition is appropriate, and delete unnecessary definitions.
ERROR: LAST-UPDATED element is already defined.	LAST-UPDATED is redundantly defined in one definition. Decide which definition is appropriate, and delete unnecessary definitions.
ERROR: DISPLAY-HINT element is already defined.	DISPLAY-HINT is redundantly defined in one definition. Decide which definition is appropriate, and delete unnecessary definitions.
ERROR: DESCRIPTION element is already defined.	DESCRIPTION is redundantly defined in one definition. Decide which definition is appropriate, and delete unnecessary definitions.
ERROR: Illegal token "*invalid-character-string*". Double quotation mark (") is expected.	The definitions for DESCRIPTION, DISPLAY-HINT, and LAST-UPDATED are not enclosed in double quotation marks ("). Check for the definition in the vicinity near <*invalid-character-string*> and enclose the description in double quotation marks (").
ERROR:	There is an unnecessary opening brace ("{") between the opening and closing braces ("{}").

Error Message	Cause and Solution
Token "{" is redundant. Do not place more than one "{". "{ <*MIB name*> <*number*> }" format is expected.	Delete the unnecessary opening brace ("{").
ERROR: There is no token between "{" and "}". "{ <*MIB name*> <*number*> }" format is expected.	There is no definition between the opening and closing braces ("{}"). Delete the corresponding definition (described below). *MIB-name* OBJECT-TYPE : ::= {}
ERROR: There is no number definition between "{" and "}". "{ <*MIB name*> <*number*> }" format is expected.	There is no number (in the <*number*> section) between the opening and closing braces ("{}"). Delete the corresponding definition (described below). *MIB-name* OBJECT-TYPE : ::= { *xxx* }
ERROR: Invalid MIB name "*MIB-name*". MIB name must start with a lower-case letter.	The displayed *"MIB-name"* does not comply with the following MIB definition rule. • MIB name must start with a lowercase letter. Change the first letter of the MIB name to a lowercase letter.
ERROR: <*MIB name*> "*MIB-name*" can be specified only the beginning. "{ <*MIB name*> <*number*> }" format is expected.	The definition format between the opening and closing braces ("{}") is invalid in the MIB definition "::= { *xxx* <*number*> }". If you define MIB names between the opening and closing braces ("{}"), you can define only one MIB name at the beginning. Replace MIB names located other than at the beginning with the corresponding numbers.
ERROR: Do not use the following characters in "{ <*MIB name*> <*number*> }" . ; " ::=	There are semicolons (;), double quotations (") or "::=" in the MIB definition "::= { *xxx* <*number*> }". Delete the unnecessary symbols.
ERROR: Illegal token between "{" and "}". Token must be like "<*symbol name*>(<*number*>)".	The enumeration type format is invalid. Correct it into the following format: SYNTAX *type-name* { *symbol-name(number)*, : *symbol-name(number)* }
ERROR: Illegal token "*invalid-character-string*" between "{" and "}". Use the following format. SYNTAX <type name>{ <*symbol name*>(<*number*>), <*symbol name*>(<*number*>) }	The enumeration type format is invalid. There are semicolons (;), double quotations ("), or "::=" between the opening brace ({) and the closing brace (}). There are semicolons (;), double quotations (") or "::=" in the enumeration type definition. Correct it into the following format: SYNTAX *type-name* { *symbol-name(number)*, : *symbol-name(number)* }
ERROR:	Delete any unnecessary symbols. There are semicolons (;), double quotations (") or "::=" in the enumeration type definition after SYNTAX.

Error Message	Cause and Solution
Illegal token "*invalid-character-string*" after SYNTAX.	Delete the unnecessary symbols. `SYNTAX type-name {` `  symbol-name(number),` `  :` `  symbol-name(number)` `}`
ERROR: Illegal syntax "SYNTAX OBJECT". "SYNTAX OBJECT IDENTIFIER" is expected.	The type definition (SYNTAX) is invalid. Replace it with OBJECT IDENTIFIER.
ERROR: Illegal syntax "SYNTAX OCTET". "SYNTAX OCTET STRING" is expected.	The type definition (SYNTAX) is invalid. Replace it with "OCTET STRING".
ERROR: Illegal token "*invalid-character-string*" after "SEQUENCE". "SEQUENCE OF ..." or "SEQUENCE { ... }" is expected.	The format of the enumeration type definition starting from "SEQUENCE" is invalid. Correct it into the following format: `SEQUENCE OF type-name` Or `SEQUENCE {...}`
ERROR: Invalid sequence type "*invalid-definition*" after "SEQUENCE OF". Sequence type must start with an upper-case letter.	The type name following "SEQUENCE OF" does not comply with the following MIB definition rule: • A type name must start with an uppercase letter. Change the first letter of the type name to an uppercase letter.
ERROR: Parenthesis is not closed. Token ")" is expected.	In the type definition (SYNTAX), the format which defines a value range is invalid. Correct it into the following format: `SYNTAX type-name (lower-limit..upper-limit)`
ERROR: Illegal token "*invalid-character-string*". Definitions or macros must start with alphabetic character string.	The first letter of each definition is not a letter. Replace the invalid letters with appropriate ones.
ERROR: Illegal token "*invalid-character-string*". An Upper-case letter is expected.	"*invalid-character-string*" must start with an uppercase letter. Change the first letter to an uppercase letter. Change the first letter to an uppercase letter.
ERROR: Illegal token "*invalid-character-string*". "::=" is expected.	"*invalid-character-string*must be "::=". Replace it with "::=".
ERROR: Illegal token "*invalid-character-string*". "BEGIN" is expected.	"*invalid-character-string*" must be "BEGIN". Replace it with "BEGIN ".

Error Message	Cause and Solution
ERROR: Illegal token "*invalid-character-string*". "::=" or "MACRO" is expected.	"*invalid-character-string"* must be "::=" or "MACRO". Replace it with a correct character string.
ERROR: Illegal token "*invalid-character-string*". Specify one of the words listed bellow. MODULE-IDENTITY, OBJECT-IDENTITY, OBJECT-TYPE, TRAP-TYPE, NOTIFICATION-TYPE, OBJECT-GROUP, MODULE-COMPLIANCE, AGENT-CAPABILITIES, OBJECT, NOTIFICATION-GROUP	"*invalid-character-string* must be one of the following definitions: MODULE-IDENTITY, OBJECT-IDENTITY, OBJECT-TYPE, TRAP-TYPE, NOTIFICATION-TYPE, OBJECT-GROUP, MODULE-COMPLIANCE, AGENT-CAPABILITIES, OBJECT, NOTIFICATION-GROUP
ERROR: Illegal token "invalid-character-string". "{" is expected.	An opening brace ("{") is missing. Add an opening brace ("{") in an appropriate place.
ERROR: Reached the end of file while parsing a definition. A definition seems to not be finished correctly.	The definition might not complete. All the entire definitions of the MIB file (MIB module) must be enclosed by "BEGIN" to "END". `<MIB-module-name> DEFINITIONS ::= BEGIN` `  :` `END` Each MIB definition must start with a lowercase letter and end with "::= { <*MIB name*> <*number*> }" `ifSpecific OBJECT-TYPE` `  :` `::= { ifEntry 22 }` Check if the definition is complete, there is no redundancy, or if the line break position is valid. In addition, the MIB file might contain a character code that is not supported. The supported character codes are as follows. Convert to the supported character code if necessary. Windows : ASCII or SJIS Linux : ASCII or UTF-8(without BOM)

When outputting various files

Error messages that may be output during the creation of analysis results include the following.

Error Message	Cause and Solution
"<*unsolved-data-type-name*>" can't be interpreted. Error: A part of amib definition file(<*AMIB-definition-file-name*>) wasn't generated.	This may be displayed during AMIB definition file creation. This error occurs because the definition of the type-name indicated by <*unsolved-data-type-name*> is not incorporated. First, incorporate the definition in the MIB file contained in the IMPORTS clause, and then perform the work again using this MIB file.

Error Message	Cause and Solution
	If the error occurs again even after you incorporate the definition in the MIB file contained in the IMPORTS clause (after you execute `NvPROReloadDefFileMgr`) first, confirm if there are any errors in the definition for <*unsolved-data-type-name*> and correct them if any.

When executing the `NvPROReloadDefFileMgr` command

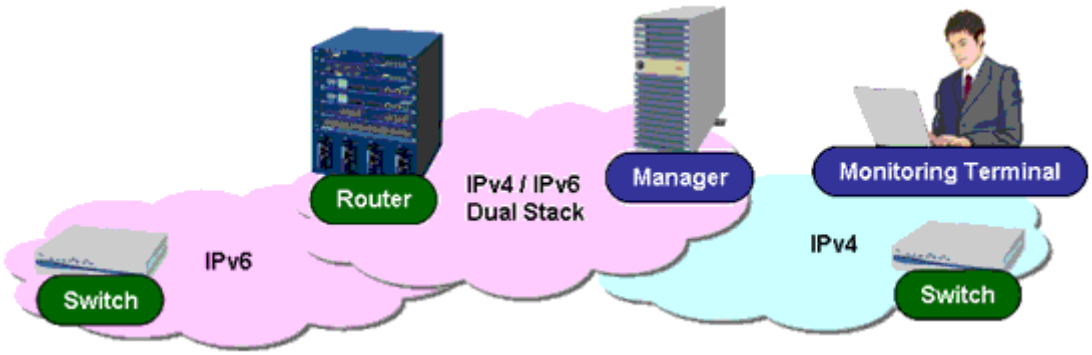
The following describes the messages displayed if errors occur during AMIB definition file incorporation (`NvPROReloadDefFileMgr` command execution), as well as their causes and solutions.

Error Message	Cause and Solution
ERROR: <*AMIB-definition-file-name*> (Line: <*line-number*>) The specified AMIB-name is illegal.	The definition on the displayed line in the AMIB definition file may violate the following rules for MIB definitions. • An MIB-name must start with a lower-case alphabetic character. • An MIB-name must consist of alphabetic characters (uppercase and lowercase), digits, and a hyphen ("-"), and must not exceed 64 characters in length. In this case, the definition in the original MIB file has a rule violation. Replace all occurrences of the relevant character string in the AMIB definition file at once with a name that satisfies the above rules, and then execute `NvPROReloadDefFileMgr` again.
ERROR: <*AMIB-definition-file-name*> (Line: <*line-number*>) The parent AMIB-name is illegal.	In the definition on the displayed line in the AMIB definition file, the MIB tree cannot be created because the parent AMIB definition is not found. If the error line appears as shown below, the bbbb portion is the parent-MIB name. `aaaa bbbb.cc AMIBNONE not-accessible SNMP-ACS` Search for the MIB file defining bbbb through the IMPORTS clause, create an AMIB definition file from the MIB file, incorporate it, and then execute `NvPROReloadDefFileMgr`again.
ERROR: <*AMIB-definition-file-name*> (Line: <*line-number*>) The same AMIB number already exists.	An AMIB definition with the same object ID already exists, but the AMIB-nameor data type is contradictory to the AMIB definition. This may occur if you attempt to incorporate a new, updated version of MIB definition into an environment into which the old MIB definition is incorporated. In this case, delete the AMIB definition file containing the old MIB definition and new AMIB definition file which you attempted to incorporate by moving them to separate folders or by other means, and then reboot the manager.Then, place the new AMIB definition in the folder, and execute `NvPROReloadDefFileMgr` again.
ERROR: <*AMIB-definition-file-name*> (Line: <*line-number*>) The same AMIB name already exists.	The specified MIB-name already exists in the same file. The following rule for MIB definitions may have been violated. • An MIB-name must be unique in the MIB file. In this case, the definition in the original MIB file has a rule violations. Replace all occurrences of the relevant character string in the AMIB definition file at once with another name, and then execute `NvPROReloadDefFileMgr` again.
ERROR:Another process is running. Retry after the process has been finished.	The `NvPROMib2Amib` command or the `NvPROReloadDefFileMgr` command is being executed in another process. Execute it again after the end of the process.

7.5 Monitoring Devices Using IPv6

7.5.1 Using the IPv6 function

You can perform IPv6-based alive monitoring and receive traps for managed devices by setting up IPv6 global unicast addresses in addition to IPv4 addresses on machines that have the manager of Network Manager installed. The configuration of the system is shown below.



Tip

Use IPv4 communications between the manager and the monitoring terminal function.

The configuration method for IPv6 address settings vary depending on the OS. Check the following.

Windows Manager (Windows Server 2008 or later):

There is no special installation procedure required because the IPv6 function is installed based on OS defaults.

Linux Manager:

There is no special installation procedure required because the IPv6 function is installed based on OS defaults.

The term "IPv6 global unicast addresses" refers to all addresses that do not match the addresses listed below.

Type	Address
Unspecified addresses	::
Loopback addresses	::1
Multicast addresses	FF00::/8
Link-local addresses	FE80::/10
IPv4-compatible addresses	0000:0000:0000:0000:0000:0000::/96
IPv4-mapped addresses	0000:0000:0000:0000:0000:FFFF::/96
6to4 addresses	2002::/16
ISATAP addresses	xxxx:xxxx:xxxx:xxxx:0000:5EFE:xxxx:xxxx (xxxx is any address)
NSAP addresses	0200::/7
IPX addresses	0400::/7
Reserved addresses	0000::/8

For information on how to set up IPv6 addresses, refer to the manual for the relevant OS. After you have set up IPv6 addresses, restart the manager function (refer to "10.2 Starting and Stopping the Manager Function (page 757)").

⚠ Caution

1. If you have upgraded MasterScope Network Manager from version 2.0, IPv6 interface information is not registered in the registered managed devices. In addition, IPv6 interface information is not registered immediately after manual registration and batch registration (see "4.6 Batch Registering or Deleting Configuration Information (page 206)"), so IPv6 address-based traps cannot be received.

   For this reason, when receiving traps based on IPv6, you must select **Update Property** in the popup menu for the relevant device or the map that the device is registered in, and update the device information.

2. When performing registration using autodiscovery (see "4.2.1.1 Performing autodiscover (TCP/IP Hosts) (page 127)"), IPv6 addresses are not configured automatically in the property information of the devices. Therefore, when performing IPv6 address-based alive monitoring or router autodiscovery, you must open the Properties dialog box of the target devices and configure IPv6 addresses individually.

7.5.2 IPv6-compatible functions

When management is carried out using IPv6 communications alone, only the following functions are available. Note that by using IPv4 and IPv6 communication together, you can use all management functions for the devices that have a dual-stack configuration.

IPv6 communication-compatible functions:

- SNMP trap receipt ("5.1 Checking Alert Information (page 448)")

  Receives SNMP traps and issues alert notifications.

- State monitoring ("4.10 Monitoring the States of Devices at Regular Interval (State Monitoring Function) (page 241)")

  Performs monitoring MIBs using SNMP and alive monitoring using ICMPv6 ECHO. Use the "7.1.1.2 updownv6:ipv6UpDownCheck (page 591)".

- Data collection function ("4.16 Collecting, Storing and Monitoring Threshold of Performance Data (MIB) from Devices (page 334)")

  Collects the MIBs of managed devices via SNMP, displays data in the graph form, and creates reports.

- Device front panel display ("5.9 Displaying Device Front Panels (page 475)")

  Displays images of the front panels of managed devices and displays current up/down status information for ports in a way that is easy to understand.

- Display of interface properties ("4.2.8.1.1 Interface Properties dialog box (page 181)")

  All interface information for managed devices can be verified.

- Updating device information ("4.2.7 Updating device information via a network (page 179)")

  Acquires the latest information from the managed devices and updates registered device information and interface information.

- Discovery of physical topology ("4.2.3.2 Automatically detecting topology information (page 149)")

Acquires physical connection information from the managed devices and draws their topological configuration in the Map View.

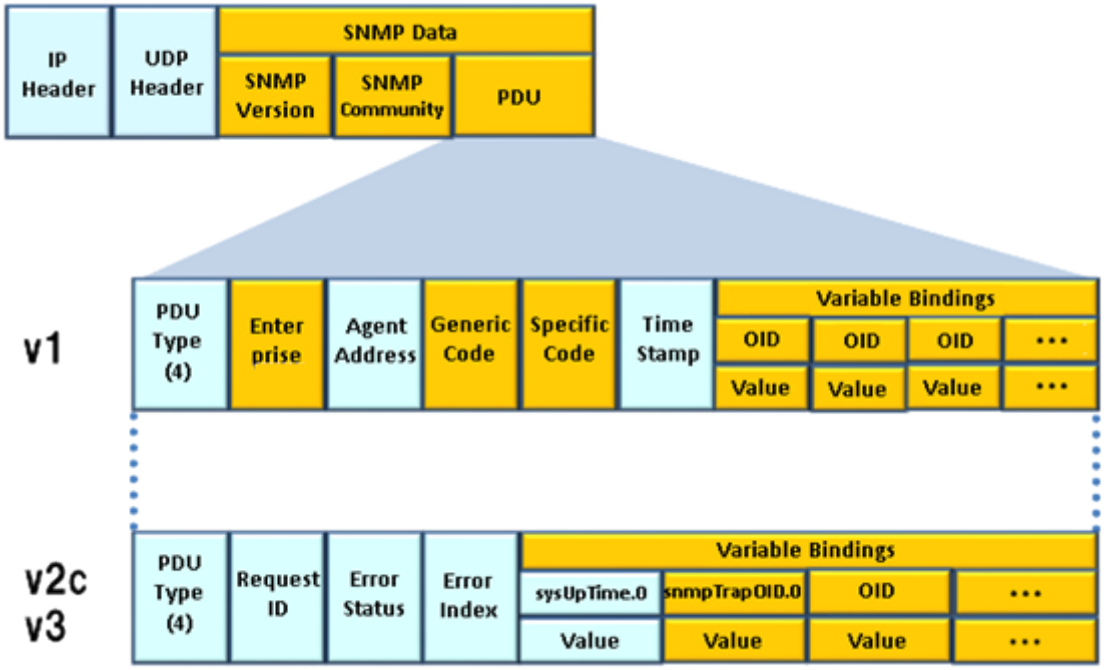
- Discovery of networks and router ("4.2.1.2 Performing autodiscover (networks and routers) (page 136)")

  Searches for unregistered routers and networks and registers discovered router and network information in the Map View.

7.6 SNMP Trap Identification Method

Network Manager can monitor SNMPv1/v2c/v3 traps, identify their contents, and issue alert notifications. The following describes the method of Network Manager to identify SNMP traps.

As shown in the figure below, the SNMPv1 trap and the SNMPv2c/v3 traps differ in the data structure of the PDU (Protocol Data Unit). Network Manager determines the data structure from the "SNMP version" information, identifies the contents of all the SNMPv1/v2c/v3 traps, and processes them.



SNMPv1 trap identification method

The contents of the SNMP trap are identified from the values of "Enterprise", "SpecificCode", and "GenericCode" in the PDU, and an alert notification is issued in accordance with the relevant trap definition. For details on the trap definitions, refer to "4.11.2 Trap definitions (page 260)".

SNMPv2c/v3 trap identification method

The contents of the SNMP trap are identified from value (OID) of "snmpTrapOID.0" in the PDU.

Network Manager divides this value (OID) according to RFC3584, and converts it into the same "Enterprise", "SpecificCode", and "GenericCode" formats as those used for SNMPv1. The details are provided below.

- For a standard trap

If the value of "Value" is in 1.3.6.1.6.3.1.1.5.x format (snmpTraps.x), the trap is judged to be a standard trap, and the value is converted as follows.

- Enterprise (vendor identifier)

  "1.3.6.1.6.3.1.1.5", with the last digit (x) removed, is regarded as being Enterprise.

- SpecificCode (specific-trap code)

  There is no value for a standard trap. It is indicated by a hyphen (-) when displayed.

- GenericCode (generic-trap code)

  The value (0 to 5) resulting from subtracting 1 from the last digit (x: 1 to 6) is regarded as being GenericCode.

Example: For a linkDown trap (1.3.6.1.6.3.1.1.5.3)

- Enterprise: 1.3.6.1.6.3.1.1.5
- SpecificCode: -
- GenericCode: 2

- For a vendor-extended trap

  If the value of "Value" is in a format other than that of a standard trap, the trap is judged to be a vendor-extended trap, and the value is converted as below.

  - Enterprise (vendor identifier)

    The value with the last digit removed is regarded as being Enterprise. If the last digit of the value is "0" after the last digit is removed, this "0" is also removed.

  - SpecificCode (specific-trap code)

    The last digit is regarded as being SpecificCode.

  - GenericCode (generic-trap code)

    This is always "6".

  Example: For a ciscoEnvMonTemperatureNotification trap (1.3.6.1.4.1.9.9.13.3.0.3)

  - Enterprise: 1.3.6.1.4.1.9.9.13.3
  - SpecificCode: 3
  - GenericCode: 6

Alert notifications are processed in accordance with the contents of trap definitions, after being converted to the same format as that of SNMPv1 traps. For this reason, the format of the trap definitions is the same as that of the SNMPv1 traps. For details on the trap definitions, refer to "4.11.2 Trap definitions (page 260)".

Caution

When different traps are interpreted as the same "Enterprise", "SpecificCode", "GenericCode" pair as a result of OID value conversion according to RFC 3584 method, notifications of the one type of trap is supported.

7.7 Notes on Counter-type and Counter64-type MIBs

In Counter-type and Counter64-type MIBs, accumulated values are stored from the time that a device is started. For this reason, these numeric values alone have no meaning, but are valued according to variance, or amount of change per time unit.

SNMP agents store integers from 0 to 4,294,967,295 for Counter-type MIBs and from 0 to 18,446,744,073,709,551,615 for Counter64-type MIBs, but if the maximum values are exceeded the number returns to 0. Normally packet numbers and octet counts are handled as Counter-type or Counter64-type. Counter32-type is equivalent to Counter-type.

In the state monitoring rules below, Counter-type and Counter64-type MIB values are monitored.

- ifload64:InterfaceLoad_64bit : Counter64-type
- ifload:InterfaceLoad : Counter-type
- nvtp-bandchk: BandTraffic :

  Counter64-type if Counter64-type is supported, Counter-type if not
- icmperr:ICMP_OutputErrorPackets : Counter-type
- icmperrv6:ipv6ICMP_OutputErrorPackets : Counter-type

The data collection rules below refer to Counter-type and Counter64-type MIB values.

- Traffic of the specified host : Counter-type
- Traffic of the specified hub port (64-bit) : Counter64-type
- Traffic of the specified hub port : Counter-type
- WAN Traffic (64-bit) : Counter64-type
- WAN Traffic : Counter-type

Network Manager can calculate difference correctly, even if accumulated values return to 0 between monitoring intervals.

However, if accumulated values return to 0 two or more times between monitoring intervals, it is not possible to calculate difference correctly.

For example, when traffic (octet counts) is managed as accumulated value of 32 bit, under the environment that 100Mbps communication continues, accumulated values return to 0 in $2^{32} * 8 / 100,000,000$ (bps) = 343.6 (seconds), that is to say less than 6 minutes. When these values are collected every 10 minutes, accumulated values may return to 0 two times between monitoring intervals. Therefore, correct difference value may not be calculated.

In this case, take countermeasures as follows:

- If managed devices support SNMPv2c or SNMPv3, use 64 bit-compatible collection rules and state monitoring rules.
- Shorten the monitoring interval than the interval that accumulated value returns to 0. (In the above example, 343 or less seconds)

7.8 Notes on Monitoring Nexus 5000 and 2000 Series

When monitoring Nexus 5000 and 2000 Series devices, you must configure your environment as follows.

1. To receive traps from Nexus 5000 devices, you must first set the main address of the Nexus 5000 to the address of the management port. (if the version of NX-OS is 4.1 (3)N2 (1a))
2. To send traps from the Nexus 5000, you must first connect the management port to a real network.
3. The Nexus 2000 cannot be monitored directly. To monitor the Nexus 2000, the Nexus 5000 that the Nexus 2000 is connected to must be first registered as the monitored component.
4. While monitoring the Nexus 5000, if you made changes to the configuration of the Nexus 2000 that is subordinate to the monitored Nexus 5000, you must update device information for the Nexus 5000. In this case, you need to turn off the monitoring mode and then turn it on again. If you do not do this, monitoring cannot be performed successfully.

When monitoring the Nexus 2000, there are the following restrictions.

1. Connecting lines between the Nexus 5000 and the Nexus 2000 that are drawn during auto-discovery (Nexus), are simple lines. Therefore, they do not change color based on alerts.
2. When alerts occur between devices connected below the Nexus 2000, the colors of the connection-lines between the Nexus 2000 and those devices do not change. In this case of "7.1.3.3 nvtp-bandchk:BandTraffic (page 599)", alerts are issued for Nexus 2000 nodes, not the connection-lines.
3. If the FEX IDs of Nexus 2000 icons are invalid, the color of the Nexus 2000 icons does not change even if there is a failure.
4. When the Nexus 5000 that the Nexus 2000 is connected to is registered manually, you must update icon properties for Nexus 5000. If this is not done, the Nexus 2000 icons will not change to the error color when faults occur.
5. If the monitoring mode of the Nexus 5000 that the Nexus 2000 is connected to is set to "OFF", the Nexus 2000 cannot be monitored even if the monitoring mode of the Nexus 2000, which is subordinate to the Nexus 5000, is "ON".
6. If multiple Nexus 2000 devices with the same FEX ID are registered, monitoring is not performed correctly.

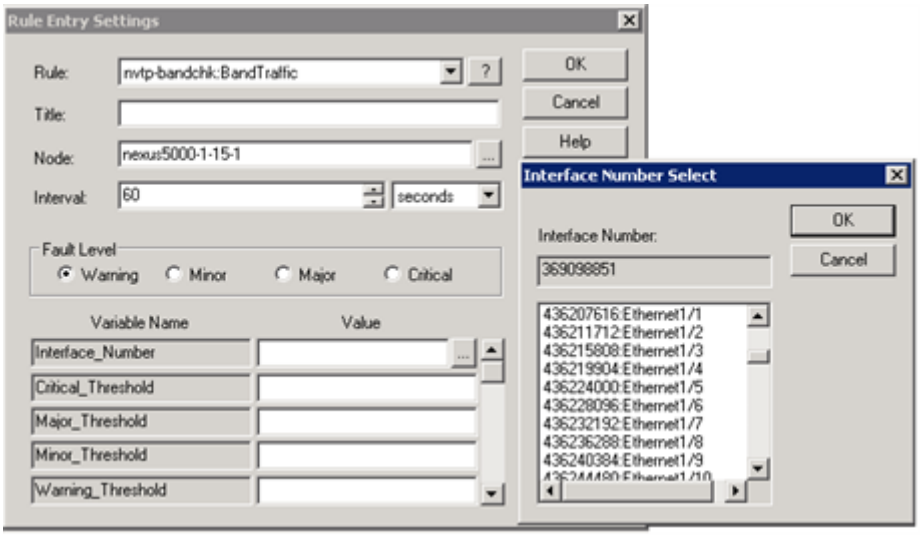
When applying monitoring rules to the Nexus 2000, you can use the following rules.

- ifDescr:UpDownCheck
- ifdown:InterfaceDown
- ifload:InterfaceLoad
- ifload64:InterfaceLoad_64bit
- ifName:UpDownCheck
- ifOper:InterfaceStateCheck
- ifup:InterfaceUp
- nvtp-bandchk:BandTraffic

If you want to monitor a specific port on the Nexus 2000, the description of the index will be as follows.

Example: If you want to monitor Port 3 of Slot 1 on a Nexus 2000 with a FEX ID=100.

In the figure, you can see "Ethernet100/1/3 (*Interface Name+FEX ID*/*Slot number*/*Port number*)".



To display a list of interface numbers, click ... button on right of the **Interface_Number**. In the list, specify the interface number with the same name that is shown in the description above.

Chapter 8. Supplemental Explanation for Resource Manager and Device Access

Contents

8.1 Resource Manager Supplemental Explanation 670
8.2 Supplemental Explanation for Device Access 675

8.1 Resource Manager Supplemental Explanation

8.1.1 Error Codes in Resource Manager function

Error codes to be displayed when using the Resource Manager and related functions are shown below.

Error code	Meaning
-1	Internal error.
-2	Invalid parameter.
-3	Memory allocation error.
-4	Internal communication error of Resource Manager (Connection error).
-6	Internal communication error of Resource Manager (Data sending error).
-7	Internal communication error of Resource Manager (Data receiving error).
-8	Timeout error for completion latency of execution (10 minutes).
-101	File I/O error.
-102	Invalid data within a file.
-103	Maximum number of simultaneous processes exceeded error.
-104	Access to the same target device error.
-105	Internal error.
-106	Database access error.
-107	Zero access information items.
-108	The device is not registered.
-109	Login information is not registered for the specified device.
-110	Failed to add device information (duplicate device identifier).
-111	The specified config history does not exist.
-112	Telnet connection error.
-113	Telnet-login error for the target device.
-114	Enable-login error for the target device.
-115	Command execution error.
-116	Device driver not detected error (**OS Type** or **Software Version** in the icon properties may be incorrect).
-117	Failed to obtain config from the device.
-118	TFTP connection information is not defined.
-119	FTP connection information is not defined.
-120	Failed to set TFTP connection information.
-121	Failed to set FTP connection information.
-122	Another TFTP server is running in the same host.
-137	The number of requests to the same device exceeded error.
-138	The number of simultaneous processes on multiple device exceeded error.
-141	Authorized host public key does not match the host public key.

Error code	Meaning
-142	SSH function is not implemented.
-201	Invalid parameter.
-202	Invalid model name/model number mapping table.
-203	Invalid device IP address.
-204	Invalid Network Manager environment.
-205	Invalid device name.

8.1.2 Supported Devices in Resource Manager function

In the Resource Manager function, the range of function to be supported and the file transfer protocol to be used for config/software management depends on the specification of the device. The following is a list of the supported device list in Resource Manager function.

- Marks for the supported functions:

  "o" : supported

  None : not supported

- Marks for the supported file transfer type:

  None: device operates as FTP client or TFTP client.

  "FC": device operates as FTP client.

  "TC": device operates as TFTP client.

  "FS": device operates as FTP server.

  "TS": device operates as TFTP server.

⚠ Caution

If the file transfer type is FS (the device operates as FTP server), the login user name of Telnet/SSH server needs to be same with that of FTP server. Configure the device settings in advance.

Device Model	running-config mgmt	startup-config mgmt	config change mgmt	software mgmt	file transfer type
NEC					
IP8800/S2400, S3600, S3800, S4630, S6300, S6700 series	o 6) 11)	o	o	o 13) 17)	
IP8800/SS1200, S2200 series	o 1) 9)	o	o	o 2) 7) 13)	FS
IP8800/S2500 series	o 1) 9)	o	o	o 2) 7) 13)	FS
IP8800/S8300 series	o 1)	o	o	o 13)	
IP8800/S8600 series	o 1)	o	o	o 13)	
QX-S series 10)	o 1) 9)	o	o	o	
QX-S3400F series 10)	o 1) 16)	o	o	o	
QX-S4100G series 10)	o 1) 16)	o	o	o	
QX-S5200G series 10)	o 1) 16)	o	o	o	
QX-S5500G series 10)	o 1) 16)	o	o	o	

Device Model	running-config mgmt	startup-config mgmt	config change mgmt	software mgmt	file transfer type
QX-S5900/PF5459 series [10]	o [1] [16]	o	o	o	
QX-S6600 series [10]	o [1] [16]	o	o	o	
QX-S800E series, S2109T-PW, S2110P-I [10]	o [1] [9]	o	o	o	TC
IX1000, 2000, 3000 series	o [1] [9]	o	o	o	TC
PF6800	o	o [1]	o		FS
PF5200 series	o [6]	o	o	o [13]	
PF5820	o	o [1]	o		TC
WA series	o [1] [16]	o	o	o	
Express5800/110Ba-e3, 120Ba-4	o [1]	o	o	o [2]	TC
Express5800/ 120Ba-SWM-BNT	o		o	o	TC
SIGMABLADE SwitchModule, SwitchModule(10G)	o		o	o	TC
QX-R series	o [1] [9]	o	o	o	TC
IP8800/S300, S400, R400 series	o [4]	o [5]	o	o [7] [13]	FC
IP8800/700 series	o	o	o	o	
ES8800/1700 series	o	o	o	o	
IP8800/620 series	o	o	o	o	TC
IX5000 series	o [1] [9]		o	o	FS
IX5500 series	o [1] [9]	o	o	o	FS
CX2610	o		o	o [2]	FC
CX-Hammernet uH24	o [1] [9]	o	o	o	
CX2600/220	o	o	o	o [2]	FC
MA155MX/4E	o	o	o	o	TC
Cisco Systems					
Cisco router, Catalyst series (IOS)	o	o	o	o	
Cisco Catalyst series (Catalyst OS)	o	o [3]	o	o	
Cisco Catalyst series (IOS-XE)	o	o	o	o	
Cisco Nexus3000 series	o	o [1]	o		
Cisco Nexus5000 series	o	o [1]	o	o	
Cisco Nexus7000 series	o	o [1]	o	o	
Cisco Nexus7000 series	o	o [1]	o		

Device Model	running-config mgmt	startup-config mgmt	config change mgmt	software mgmt	file transfer type
(VDC)					
Cisco Nexus9000 series	o	o [1)]	o		
Cisco ASR920, 1000 series	o	o	o	o	
Cisco ASA5500 series	o	o [8)]	o	o	
Cisco ASA5500 series (ADMIN-CONTEXT)	o	o [8)]	o	o	
Cisco ASA5500 series (CONTEXT)	o		o		
Cisco PIX Firewall series	o		o	o [2)]	TC
Cisco Aironet1100, 1200 series	o	o	o	o [7)]	
Brocade Communications Systems					
Brocade VDX 6700 series	o	o	o		FC
Brocade ICX 6000 series	o [1)]	o	o	o [12) 14)]	TC
Brocade FastIron SX, WS series	o [1)]	o	o	o [12) 14)]	TC
Brocade TurboIron 24X	o [1)]	o	o	o [12) 14)]	TC
Brocade FCX series	o [1)]	o	o	o [12) 14)]	TC
Brocade NetIron CES/CER 2000 series	o	o	o		TC
Brocade NetIron XMR, MLX, MLXe series	o	o	o		TC
Brocade ServerIron, FastIron Edge X, BigIron series	o	o	o	o	TC
F5 Networks					
BIG-IP V11, V12, V13 series (TMOS)	o		o		FC
BIG-IP V9, V10 series	o [9)]		o		FC
A10 Networks					
AX series	o	o	o	o [2)]	
Thunder ADC series	o	o	o	o [2)]	
Juniper Networks					
EX4200 series	o		o	o [2)]	FC
EX2200, EX3200, EX3300, EX4500, EX6200, EX8200 series	o		o		FC
Fortinet					

Device Model	running-config mgmt	startup-config mgmt	config change mgmt	software mgmt	file transfer type
FortiGate series		o			TC
Hitachi Metals					
APRESIA series	o [9]	o	o	o [2]	TC
Citrix Systems					
Citrix NetScaler MPX series	o [1]	o	o	o [2]	
YAMAHA					
RT series	o		o	o [2] [7]	TS
Allied Telesis					
CentreCOM 8216XL2, 8224SL, 8324XL, 8724SL CentreCOM GS908M, GS916M, GS924M	o [1]	o	o		
HP					
HP Procurve2510	o [1]	o	o	o	TC
HP A3100-8 v2 EI Switch, HP A3100-16 v2 SI Switch, HP A5120-24G SI Switch [10] [15]	o [1] [16]	o	o	o	
HP BL10e	o		o	o [2] [7]	TC
HP BL20p	o		o	o	TC
HP BL20p	o		o	o	TC
Extreme Networks					
Summit24, 1i	o [1]		o	o [2]	TC
Seiko Instruments					
NS series		o		o [7]	FC
Lucent Technologies					
MAX series	o [1] [9]	o	o	o [2] [7]	TC

1) Only collecting function is supported. It is not possible to upload the config file.

2) Only software distributing function is supported. It is not possible to backup the software.

3) Only Catalyst (IOS) with the layer 3 module is supported.

4) Startup-config is overwritten after uploading running-config.

5) Running-config is overwritten after uploading startup-config.

6) According to the device specification, after uploading running-config, operated ports are automatically restarted and communication failure might occur temporarily.

7) According to the device specification, the device is rebooted automatically while distributing the software.

8) According to the device specification, after uploading startup-config, communication failure might occur temporarily.

9) When collecting running-config, startup-config is modified temporary. Finally, startup-config is restored to the original.

10) To use each function, configure one of the following settings in the login setting.
- Set the login information for the user with user-level 3.
- If the user-level is 2 or less, specify the super password for elevating to user-level 3 in the "super" field.

11) In the stack configuration, uploading running-config is not supported due to the device specification.

12) Only Flash Code can be deployed. Boot Code cannot be deployed.

13) The device uses the software file with the fixed name. Therefore, when distributing software, current software cannot be left on the device. The software file is always overwritten.

14) When managing the software files, select "ICX6450" to make a setting for an additional model.

15) Stack configurations are not supported.

16) You cannot use external FTP/TFTP servers while running-config is collected.

17) Only "Deploy to master switch" is supported for stack configurations,. While switching the master switch by rebooting, deploy software to all the switches making up a stack.

8.2 Supplemental Explanation for Device Access

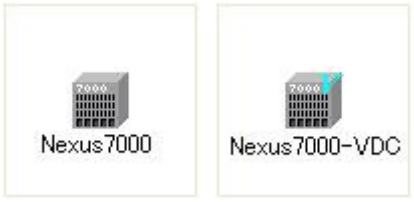
8.2.1 Device-specific operations

8.2.1.1 Managing Cisco Nexus 7000 Virtual Device Context (VDC) configuration

To manage an environment using the Virtual Device Context (VDC) feature of the Nexus 7000 series, configure the following settings in Network Manager.

1. Treat each VDC as a single node when registering node information in Network Manager. Assign a Resource Manager advanced functions license (RM license) to each VDC.
2. If registering nodes using autodiscovery, the "Nexus7000" icon type is used for all VDCs when registering the node information.

   For VDCs other than the default VDC, manually change the icon type to "Nexus7000-VDC".



Default VDC Other VDC

3. In the icon properties for each VDC, make sure that the value of **OS Type** is set to the following:
   - Default VDC: Nexus7000
   - Other VDC: Nexus7000-VDC

When performing operations, consider the important points below.

1. Software deployment cannot be performed for VDCs other than the default VDC.
2. The default name of the VRF (Virtual Routing and Forwarding) for the Cisco Nexus 7000 copy commands used in file transfers is set to "management".

For how to change the specified VRF name, refer to "8.2.2 Extended Settings for the Resource Manager Function (page 682)".

8.2.1.2 Managing Cisco ASA 5500 redundant/multiple context mode configuration

Managing in a redundant configuration

When using an ASA 5500 series device in a redundant configuration, consider the following important points:

1. When you perform running-config and startup-config collections, the primary config and secondary config display and are managed in a single window as images divided by separators.

   Image for a redundant configuration:

```
********** system <Primary> config START **********
      <primary device config image>
********** system <Primary> config END **********
********** system <Secondary> config START **********
      <secondary device config image>
********** system <Secondary> config END **********
```

2. When running-configs are uploaded, images containing both the corrected primary and corrected secondary configs are uploaded to active devices only. When startup-configs are uploaded, images containing both the corrected primary and corrected secondary configs are uploaded to both active and standby devices.
3. When uploading software, uploaded the same software to both active and standby devices. To enable the newly uploaded software, restart both the active and standby devices.

Managing in a multiple context configuration

To manage an environment using the multiple context mode feature of the ASA 5500 series, configure the following settings in Network Manager.

1. Treat each context as a single node when registering node information in Network Manager. Assign a Resource Manager advanced functions license (RM license) to each context.
2. If registering nodes using autodiscovery, use the "ASA5500" icon type for all contexts when registering the node information. When using multiple context mode, manually change the following icon types.

ASA5500-ADMIN-CONTEXT

ASA5500-CONTEXT

3. In the icon properties for each context, make sure that the value of **OS Type** is set to the following:
   - Admin context: ASA5500-ADMIN-CONTEXT
   - General context: ASA5500-CONTEXT
4. To manage startup-configs of general contexts, configure the following settings:

- In the device side setting, set the context name of the general context to the hostname of the general context.
- In Network Manager, register an admin context node, assign an RM license to it, and configure login settings of it.
- In the **Function** tab of the general context node properties, configure as follows:
  - **Administration Node Name**: Specify the node name of the admin context.
  - **sysName**: Specify the context name of the general context that is configured on ASA 5500.

When using an ASA 5500 series device in multiple context mode, consider the following important points:

1. When running-configs are collected, the running-config image is managed in the following ways.
   - In an admin context, obtained context images display and are managed with the system config (in a redundant configuration there are both primary and secondary configs) and admin context config combined in a single window divided by separators.
   - In a general context, obtained config images display and are managed in the unchanged form.

   Admin context (ASA5500-ADMIN-CONTEXT) image:

```
********** system <Primary> config START **********
      <running-config image for the primary device system>
********** system <Primary> config END **********
********** system <Secondary> config START **********
      <running-config image for the secondary device system>
********** system <Secondary> config END **********
********** admin-context <admin> config START **********
      <running-config image for the admin context>
********** admin-context <admin> config END **********
```

2. Upload system running-configs but not running-configs in an admin context or general context.
3. When startup-configs are collected, the startup-config image is managed in the following ways.
   - In an admin context, obtained context images display and are managed with the system config (in a redundant configuration there are both primary and secondary configs) and admin context config combined in a single window divided by separators.
   - In a general context, obtained config images display and are managed in the unchanged form.

   Admin context (ASA5500-ADMIN-CONTEXT) image:

```
********** system <Primary> config START **********
      <startup-config image for the primary device system>
********** system <Primary> config END **********
********** system <Secondary> config START **********
      <startup-config image for the secondary device system>
********** system <Secondary> config END **********
********** admin-context <admin> config START **********
      <startup-config image for the admin context>
********** admin-context <admin> config END **********
```

4. To reboot a general context after uploading a startup-config to it, instead of rebooting the device directly, execute "clear configure all" command and "copy startup-config running-config" command.
5. It is possible to only upload software to the admin context.

Switching the management method for startup-configs of general contexts

You can switch the management method for startup-configs of general contexts to the method of MasterScope Network Manager 5.1.

By switching the management method, the following points will change.

1. When startup-configs are collected, the startup-config image is managed in the following ways.
   - In an admin context, obtained context images display and are managed with the system config (in a redundant configuration there are both for primary and secondary configs), admin context configs, and general context configs combined in a single window divided by separators.
   - In a general context, it is not possible to obtain startup-configs directly. They are obtained and managed through the admin context.

   Admin context (ASA5500-ADMIN-CONTEXT) image:

```
********** system <Primary> config START **********
      <startup-config image for the primary device system>
********** system <Primary> config END **********
********** system <Secondary> config START **********
      <startup-config image for the secondary device system>
********** system <Secondary> config END **********
********** admin-context <admin> config START **********
      <startup-config image for the admin context>
********** admin-context <admin> config END **********
********** context <contextA> config START **********
#********** context <contextA> Reload **********
      <startup-config image for the general context>
********** context <contextA> config END **********
********** context <contextB> config START **********
#********** context <contextB> Reload **********
      <startup-config image for the general context>
********** context <contextB> config END **********
```

2. To upload startup-configs to a general context, edit and upload the general context image in the config image for the admin context. It is not possible to upload startup-configs directly to a general context.

   Upload startup-configs of the admin context, general contexts, and system from the admin context.
3. To reboot after uploading a startup-config to a general context, instead of rebooting the device directly, delete the pound character "#" at the beginning of the "#~context~" field in the first line of the general context image in the config image of the admin context node. Then perform the upload on the edited image. Network Manager then starts the reboot process.

   The startup-config image distributed when restarting a general context:

```
********** context <contextA> config START **********
********** context <contextA> Reload **********
 (Image with the "#" deleted from the beginning)
      <startup-config image for the general context>
 (Can be omitted if only restarting)
********** context <contextA> config END **********
********** context <contextB> config START **********
********** context <contextB> Reload **********
 (Image with the "#" deleted from the beginning)
      <startup-config image for the general context>
 (Can be omitted if only restarting)
********** context <contextB> config END **********
```

4. It is not necessary to set the **Administration Node Name** and **sysName** properties in a general context node.

To switch the management method to the older one, perform the following steps.

1. Rename *<On the manager, %sharedfolder%>*`\Manager\sg\NvPRO\ResourceManager\NvPROResourceManagerMgr.ini.org` to `NvPROResourceManagerMgr.ini`.
2. Open `NvPROResourceManagerMgr.ini` and rewrite "CiscoASAStartup=1" to "CiscoASAStartup=0". After editing, save the change.
3. Restart the manager function. For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)"

8.2.1.3 Managing Juniper EX4200 Virtual Chassis (VC) configuration

To manage the environment using Virtual Chassis (VC) feature of the Juniper EX4200 series, configure the following settings in Network Manager.

1. Configure the following setting in order to synchronize the update of configuration on the master device with all devices.

```
# set system commit synchronize
# commit
```

2. If you reboot the master device after deploying software, all devices will be rebooted.

8.2.1.4 Managing UNIVERGE WA series

For WA1020/2020/2021, multiple users who have the administrator authority cannot login to the device at the same time. For this reason, if a user with the administrator authority has already logged in the device, operations from Network Manager will fail (login error).

8.2.1.5 Managing the PF5459 series, QX-S series

When collecting running-config of the following device models, Network Manager uses the results of executing the "display current-config" device command.

- PF5459 series
- QX-S3400F series
- QX-S4100G series
- QX-S5200G series
- QX-S5500G series

- QX-S5900 series
- QX-S6600 series

Because of the specifications of this device command, the collected running-config contains a line break code (0x0D 0x0A) on each line. Even if line break codes are contained, they do not influence each of the functions for running-config management (such as history management, change management, viewing differences, and exporting).

8.2.1.6 Managing the BIG-IP series

Device connection

For a BIG-IP, the default method of authentication in an SSH connection is "challenge and response authentication". Network Manager does not support "challenge and response authentication", so change the setting to "plaintext authentication".

Example of setting for changing the authentication method:

```
# modify sys sshd { include "PasswordAuthentication yes" }
# save sys config
```

Managing the BIG-IP V9 and V10 series

To use the Resource Manager function on the BIG-IP V9 and V10 series, you must set the **OS Type** icon property to **BIG-IP_V9**. After executing autodiscover or updating the device information (**Update All Property**), confirm the value of the icon property **OS Type** and manually update it to **BIG-IP_V9** if necessary.

Managing the BIG-IP V11, V12, V13 series (TMOS)

When using the Resource Manager function on the BIG-IP V11, V12, V13 series, note the following.

1. If logs are output to the console during the execution of a command from Network Manager, the command execution results cannot be recognized correctly. Therefore, make the setting for suppressing the output of logs to the console in advance.

   Example of setting for suppressing the output of logs to the device console:

   ```
   # modify sys syslog console-log disabled
   # save sys config
   ```

2. When using running-config Management, note the following:
   a. An SCF text file is handled as running-config. For this reason, information about the settings related to GTM/ASM and other product modules, licenses, and SSL certificates are not managed.
   b. During Deploy running-config, Network Manager executes the load sys config file command. If the device is rebooted after deployment of running-config, rebooting is performed by updating startup-config due to the device specifications.
   c. When replacing a device due to a device failure or other causes, it may not be possible to deploy the running-config collected before device replacement directly on the new device.

      After device replacement, collect running-config on the new device. Then, edit the newly collected config file and deploy running-config.
3. When managing BIG-IPs in a redundant configuration, note the following:

a. A virtual IP address cannot be assigned to the BIG-IP management interface (Management Port) because of the device specifications. For this reason, you must register the two BIG-IPs in the redundant configuration with individual icons on the map and manage them.

b. Network Manager does not automatically synchronize the configuration when deploying running-config. It is recommend that you make the auto sync setting to manage BIG-IPs in a redundant configuration. If you do not make the auto sync setting, execute config-sync manually after deploying config file.

   auto sync setting example:

```
# modify cm trust-domain Root save-on-auto-sync true
# modify cm device-group <device-group> auto-sync enabled
# save sys config
```

   For <device-group>, specify the device-group name of the redundant configuration.

8.2.1.7 Managing the AX series and the Thunder ADC series

Settings for using the software deployment function (common to the AX series and the Thunder ADC series)

The Resource Manager function detects the end of a software deployment process by receiving the axSystemRestart trap from the device. For this reason, when using the software deployment function, make the setting for sending an axSystemRestart trap on the device.

Example of setting for sending the axSystemRestart trap:

```
(config)# snmp-server enable traps system restart
(config)# write memory
```

Settings for enabling the simultaneous setting of the device (Thunder ADC series)

The Thunder ADC series allows multiple users to simultaneously access the device and make settings. To avoid collision of settings when they access the device from the Resource Manager function to make changes, it is recommended that you enable this feature to allow simultaneous setting by multiple users.

Example of setting for enabling simultaneous settings:

```
(config)# multi-config enable
(config)# write memory
```

Action to be taken upon the occurrence of a Thunder ADC series defect

The Thunder ADC series with a specific 2.7.2 version (2.7.2-P5 or earlier) has a defect whereby the MIB (sysObjectID) for identifying a model returns an invalid value. For this reason, Network Manager cannot identify models appropriately if the autodiscover of **TCP/IP Hosts** or the **Update Property** is executed.

If you are using the Resource Manager function with a Thunder ADC series that contains this defect, manually change the following items of the icon properties of the device to appropriate values.

- **OS Type**

Specify "A10Thunder".

- **SW Version**

  Specify "2.7.2".

8.2.1.8 Managing the FortiGate series

The FortiGate series supports the VDOM (virtual UTM) function, which enables you to create multiple virtual FortiGates on a single FortiGate appliance.

The Resource Manager function operates on the assumption that the VDOM function is enabled. Thus, to use the Resource Manager function, enable VDOM on the FortiGate side in advance.

Example of setting for enabling VDOM:

```
#config system global
(global)#set vdom-admin enable
(global)#end
```

If you are not using the Resource Manager function, perform this operation by changing the icon property **OS Type** from **FortiGate** to **OtherSwitch**.

8.2.1.9 Managing the IP8800/S8300 and IP8800/S8600 series

For the IP8800/S8300 series and IP8800/S8600 series, the data reception rate of the device is limited to protecting the device. If the device receives data transferred at a speed faster than the defined reception rate, packets will be discarded according to the device specifications.

To prevent operations from being affected by the device specifications, it is recommended that FTP is used as the file transfer method of the device.

For how to set File Transfer Protocol, refer to "4.3.5 Setting external server information (page 195)".

8.2.2 Extended Settings for the Resource Manager Function

In some operating environments, it is possible to configure detailed settings for communication with devices. Configure the settings with the configuration file.

Configuration file for communication with devices

<On the manager, %sharedfolder%>\Manager\sg\NvPRO\RMAPI\nvrmapi.ini

parameters can be set

Parameter	Description
yamahaTftpMod=1	This setting is specific to communication with YAMAHA RT series devices. When transferring files with a YAMAHA RT device, the device-side config settings for the tftp server used by Network Manager are set automatically. Be careful with the above operations because the device configuration changes automatically.
IXRouterCopyMod=1	This setting is specific to communication with NEC IX series devices. When communication between Network Manager and an IX device takes place through a VPN, the IP address for tftp transfers on the IX side is not always the same as the IP address on the VPN. A different interface IP address is sometimes used. (This depends on the rules for determining an address.)

Parameter	Description
	If this situation occurs, setting this parameter allows for changing the handling so it is possible to explicitly specify the IX-side IP address for the IX copy command used during file transfers and perform proper communication.
Nexus7000vrfName=<*vrf name*>	This setting is specific to communication with Cisco Nexus 7000 series devices. The default name of the VRF (Virtual Routing and Forwarding) for the Cisco Nexus 7000 copy commands used in file transfers is set to "management". To use a name other than the default VRF name, specify <*vrf name*> with this field. Note that this name needs to be unique in the system.
tftpClientIpAddress=<*tftp client IP address*>	Specifies the source node IP address for when Network Manager communicates with devices as a tftp client.
tftpAnsIpAddress=<*reply IP address of tftp server*>	Specifies the source node IP address for sending reply packets when Network Manager communicates with devices as a tftp server.
tftpIpAddress=<*tftp server IP address*>	Specifies the tftp server IP address when Network Manager communicates with devices as a tftp server.
ftpClientIpAddress=<*ftp client IP address*>	Specifies the source node IP address for when Network Manager communicates with devices as an ftp client.
ftpIpAddress=<*ftp server IP address*>	Specifies the ftp server IP address when Network Manager communicates with devices as an ftp server.
PF5200TelnetLoginRetry=1	This setting is specific to communication with the PF5200 series. Due to a defect in the PF5200 series, it may not be possible to display the login prompt in the login process. This can be avoided by sending an Enter code (0x0D 0A) to the PF5200. By setting this parameter, the defect in the PF5200 can be avoided by sending an Enter code (0x0D 0A) to the PF5200 the specified number of times and at the specified interval in the login process.
PF5200TelnetLoginRetryCount=<*execution count*>	This is effective provided the following is specified: PF5200TelnetLoginRetry=1. Specifies the number of times the Enter code (0x0D 0A) is to be sent to the PF5200. You can specify a single-byte number from "1" to "10". The default is "3".
PF5200TelnetLoginRetryInterval=<*execution interval*>	This is effective provided the following is specified: PF5200TelnetLoginRetry=1. Specifies the time interval (seconds) at which to send an Enter code (0x0D 0A) to the PF5200. You can specify a single-byte number from "1" to "60". The default is "2".

To apply the settings in nvrmapi.ini, restart the manager function.

Configuration file for the manager process

*<On the manager, %installfolder%>*Manager\sg\NvPRO\RMAPI\jservice.ini

parameters can be set

Section	Parameter	Description
JAVA	Xmx=<*Maximum memory size*>	Specify the maximum memory size reserved by Resource Manager function. The unit is MB. When the value is omitted, The default value is as follows: • Windows: 256MByte • Linux: 512MByte

The apply the settings in jservice.ini, restart the manager function. For the cluster system, justify the setting of jservice.ini of the active host and the waiting host.

When updating MasterScope Network Manager from the version 5.1 or earlier, [JAVA] section may not exist in service.ini. In such the case, add the section to jservice.ini as follows.

Example of addition (when the maximum memory size is 512MB.)

```
[JAVA]
Xmx=512
```

Chapter 9. Command Reference

Contents

9.1 Commands for Audit Log (AuditTrailCmd) 686
9.2 Commands for Alert Report History (ReportCmd) 689
9.3 Commands for License Registration (LicenseCmd) 690
9.4 Alert Information Output Command (NvPROAlertPrint) 693
9.5 Definition Files Operation Command 695
9.6 Trap Definition Operation Commands 700
9.7 SNMP Access Command 712
9.8 Command for Sending SNMP Traps 717
9.9 Command for Issuing Alert Events (nvpalertsend) 720
9.10 Configuration Information Operation Command 722
9.11 Status Monitoring Config Command (nvpstsmonconf) 731
9.12 Data Collection Config Command 734
9.13 File Code Conversion Command (nvpfileconv) 739
9.14 Command for Executing Device Commands (nvpdevcmdexe) 741
9.15 Backup and Restore Function 744

Network Manager provides not only operations from the monitoring window, but also provides commands that can be executed manually for the part of functions. When executing commands, consider the following important points.

1. Execute a command as an Administrator (as a root user for Linux).

   For Windows, you need to launch a command propmp by **Run as administrator** menu.

2. In the Windows, a command execution may fail if specifying a path name for the input and output file that includes "nul" (either uppercase or lowercase). Specify a path name that does not contain "nul" (either uppercase or lowercase).

3. In the Linux , the following preparatory steps are necessary before running these commands.

   - Library path settings

     Add the following to the LD_LIBRARY_PATH environment variable.

     <On the manager, %installfolder%>/Manager/bin

   - Language settings

     Set the LANG environment variable to UTF-8 locales.

     Example:

     ```
     env LC_ALL=ja_JP.utf8 LD_LIBRARY_PATH=/opt/UMF/Operations
     /Manager/bin:${LD_LIBRARY_PATH} /opt/UMF/Operations/Manager/bin/
     NvPROReloadDllMgr
     ```

     (Do not insert a linefeed while inputting commands.)

4. In the Linux, commands must be run with absolute path, except the one with the special description. It is not possible to run with relative path.

5. In the Linux, if you want to execute commands with multi-byte characters, use the UTF-8 encoding for input characters. Note that you should configure your terminal emulator settings to use the UTF-8 encoding.

6. In the Linux, if many commands are executed simultaneously, "`The winapidaemon is not running`" message may be displayed and the commands may not start correctly. In this case, decrease the number of commands that start at the same time, and then execute again.

9.1 Commands for Audit Log (AuditTrailCmd)

9.1.1 AuditTrailCmd INIT

This command deletes all audit logs within a category.

Path

<On the manager, %installfolder%>\Manager\bin\AuditTrailCmd.exe

Specification method

```
AuditTrailCmd.exe INIT categoryID
```

Description

Deletes all audit logs in the category specified in *categoryID* argument. If the argument is omitted or invalid, help is displayed.

Arguments

categoryID

Specify the ID of the category in which the target audit logs are stored.

Category IDs are as follows:

1: Application category

2: Security category

3: System category

4: Audit log category

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

1. Deleted audit logs cannot be restored.
2. To delete an audit log for a specified date, use the `SWAP` option.

9.1.2 AuditTrailCmd SWAP

This command deletes all audit logs within a category in relation to a specified date.

Path

<On the manager, %installfolder%>`\Manager\bin\AuditTrailCmd.exe`

Specification method

```
AuditTrailCmd.exe SWAP categoryID date
```

Description

Deletes audit logs, in the category specified in *categoryID* argument, older than or equal to the date specified in *date* argument. If the argument is omitted or invalid, help is displayed.

Arguments

categoryID

Specify the ID of the category in which the target audit logs are stored.

Category IDs are as follows:

1: Application category

2: Security category

3: System category

4: Audit log category

date

Specify the date in the format "YYYY/MM/DD".

Specification example

```
AuditTrailCmd.exe SWAP 3 2011/02/14
```

This command deletes the audit logs in the system category, received at February 14, 2011 or older.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

1. Deleted audit logs cannot be restored.
2. To delete all audit logs, use the `INIT` option.

9.1.3 AuditTrailCmd CSV

This command outputs audit logs within a category to a file.

Path

<On the manager, %installfolder%>\Manager\bin\AuditTrailCmd.exe

Specification method

```
AuditTrailCmd.exe CSV categoryID date csvfile [-U [-B]] [-T]
```

Description

Outputs audit logs within the audit logs in the category specified in *categoryID* category_id argument, that are in the date category specified in *date* argument, to a CSV file on Manager. Specify the name of the output file in *csvfile* argument.

If the argument is omitted or invalid, help is displayed.

Arguments

CategoryID

Specify the ID of the category in which the target audit logs are stored.

Category ID are as follows:

1: Application category

2: Security category

3: System category

4: Audit log category

Date

Specify the date in the format "YYYY/MM/DD".

CSVFile

Specify the file name by its absolute path. If the specified directory does not exist, the command will be ignored.

-U

If this option is specified, Unicode is output when outputting in Windows (the default output is ASCII).

-B

If this option is specified, when the `-U` option is specified in Windows and Unicode is output, BOM (Byte Order Mark) is not attached to the output file (BOM is attached by default). If the `-U` option is not specified, this option is not enabled.

-T

If this option is specified, TAB separation is used in the CSV file (comma separation is the default).

Specification example

```
AuditTrailCmd.exe CSV 3 2011/02/14 C:\foo\bar.csv
```

This command outputs the audit logs in the system category, received at February 14, 2011, to the file named 'C:\foo\bar.csv'.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

9.2 Commands for Alert Report History (ReportCmd)

9.2.1 ReportCmd INIT

This command deletes all report history.

Path

<On the manager, %installfolder%>`\Manager\bin\ReportCmd.exe`

Specification method

```
ReportCmd.exe INIT
```

Description

Deletes all notification history. If the argument is omitted or invalid, help is displayed.

Arguments

None

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

1. Deleted notification history cannot be restored.
2. To delete notification history for a specified date, use the `SWAP` option.

9.2.2 ReportCmd SWAP

This command deletes all notification history in relation to a specified date.

Path

<On the manager, %installfolder%>\Manager\bin\ReportCmd.exe

Specification method

```
ReportCmd.exe SWAP date
```

Description

Deletes report history older than or equal to the date specified in the *date* argument.

If the argument is omitted or invalid, help is displayed.

Arguments

date

Specify the date in the format "YYYY/MM/DD".

Specification example

```
ReportCmd.exe SWAP 2011/02/14
```

This command deletes the notification history at February 14, 2011 or older.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

1. Deleted notification history cannot be restored.
2. To delete all notification history, use the `INIT` option.

9.3 Commands for License Registration (LicenseCmd)

9.3.1 LicenseCmd ADD

This is the command for adding license keys.

Path

<On the manager, %installfolder%>\Manager\bin\LicenseCmd.exe

Specification method

```
LicenseCmd.exe ADD productcode licensekey
```

Description

productcode argument is used to enter a product code, and *licensekey* argument is used to enter a license key.

If the license key is correct, a codeword request code is displayed.

If the arguments are omitted or invalid, help is displayed.

Arguments

productcode

Specify the product code of a license.

licensekey

Specify the license key being registered.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

This command can only be run while the manager is in a stopped state. If the manager is running, register the license from the monitoring terminal.

9.3.2 LicenseCmd DELETE

This is the command for deleting license keys.

Path

<On the manager, %installfolder%>\Manager\bin\LicenseCmd.exe

Specification method

```
LicenseCmd.exe DELETE licensekey
```

Description

Enter the license key to delete as the *licensekey* argument.

If the argument is omitted or invalid, help is displayed.

Arguments

licensekey

Specify the license key to delete.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

This command can only be run while the manager is in a stopped state. If the manager is running, delete the license from the monitoring terminal.

9.3.3 LicenseCmd LIST

This command outputs a list of registered licenses.

Path

<On the manager, %installfolder%>\Manager\bin\LicenseCmd.exe

Specification method

```
LicenseCmd.exe LIST [-R]
```

Description

Outputs registered licenses.

Arguments

-R

If this option is specified, only licenses with unregistered codewords are displayed.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

Output format

```
ProductCode : [Product code]
LicenseKey : [License key]
RequestCode : [Request code]
Codeword : [Codeword]
```

If you are using a trial license, the license key is displayed as "Trial License Key" and the request code is displayed as "Trial Version".

⚠ Caution

This command can only be run while the manager is in a stopped state. If the manager is running, register the license from the monitoring terminal.

9.3.4 LicenseCmd REGISTER

This command registers a codeword.

Path

<On the manager, %installfolder%>\Manager\bin\LicenseCmd.exe

Specification method

```
LicenseCmd.exe REGISTER licensekey codeword
```

Description

licensekey argument is used to enter a license key and *codeword* argument is used to enter a codeword.

If the arguments are omitted or invalid, help is displayed.

Arguments

licensekey

Specify a registered license key.

codeword

Specify an acquired codeword.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

This command can only be run while the manager is in a stopped state. If the manager is running, register the license from the monitoring terminal.

9.4 Alert Information Output Command (NvPROAlertPrint)

This command outputs alert information accumulated in a database to a file.

Path

<On the manager, %installfolder%>\Manager\bin\NvPROAlertPrint[.exe]

Specification method

```
NvPROAlertPrint -o ofile [-c code] [-s size] [-r] [-m count]
 [-q] [-i] [-cs] [-h]
```

Description

The working directory when executing this command must be: *<On the manager, %installfolder%>*\Manager\bin.

Alert information stored in a database is output to the file specified in the -o *ofile* argument.

By running the command and leaving the specification as the created file -o *ofile*, you can output and add alert information generated after the last alert of the previous output.

It is possible to specify the output character encoding in -c *code*.

It is possible to specify the output file size with `-s` *size*. Before outputting the alerts, check the file size. If it exceeds the specified size, rename the old file, create a new file, and output the alert information.

If the argument is omitted or invalid, help is displayed.

Arguments

-o ***ofile***

Specify the alert information I/O file name.

-c ***code***

Specify the output character code for the alert display image. Codes that can be specified: "ansi", "utf-16" and "utf-8". If this is omitted and you are using Windows, the default code is "ansi". If you are using Linux, the default code is "utf-8".

-s ***size***

Specify the maximum size for the alert information file in kilobytes. Before outputting the alert information, check the size of the existing file. If exceeding the size specified in `-s`, rename the existing file and create a new alert output file (log file rotate). When renaming a file, the system searches from 001 for "*ofile*.*nnn*" (decimals from 001-999), and assigns the first available number that is found. (New files are created in the order *.001, *.002, ... , *.999)

-r

The file naming rules for log file rotation change as follows. When renamed, file names become "*ofile*.001". If the file already exists, sequential renaming is done by adding a 1 to the "*.nnn*" portion. (New files are created in the order *.999, ... , *.002, *.001)

-m ***count***

Specify the maximum number of alert information files in decimal numbers from 2-999. This is only valid if `-s` has been specified. The number of files includes all alert information files and rotation files. If `-r` has not been specified and the maximum number of files is reached, the data is added to the alert information file without performing a log rotation. If `-r` has been specified and the maximum number of files is reached, the oldest file is deleted.

-q

Does not display anything while the command is running. If omitted, the alert information and execution status are displayed.

-i

Displays the status of the current number of alerts and the last alert ID for the specified alert information file, without outputting alert information.

-c

Replace a linefeed code (CRLF or LF) with a white space in alert information.

-h

Displays Help.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

Output format

```
%EventId% %OccurTime% Severity=%Severity% %CompType% "%CompName%" %IpAddres
s% Sender="%Sender%" Summary="%Summary%" Detail="%Detail%" Action="%Action%
"
```

Item	Description
%EventId%	Event ID
%OccurTime%	Time of occurrence
%Severity%	Importance level (Normal:1, Unknown: 2, Warning: 4, MINOR: 6, MAJOR: 7, Fatal: 8)
%CompType%	Component type
%CompName%	Component name
%IpAddress%	IP address of the device on which the alert occurred
%Sender%	Name of the function which detected the alert
%Summary%	Alert summary message
%Detail%	Alert detailed message
%Action%	Alert handling method

Specification example

The following is an example for outputting alert information to "alert_file.txt" with UTF-8 encoding.

```
NvPROAlertPrint -o alert_file.txt -c utf-8 -cs
```

9.5 Definition Files Operation Command

9.5.1 NvPROMib2Amib

This command creates the definition files for Network Manager from a new MIB published by the RFC, or a vendor extension MIB published by a device vendor.

Path

<On the manager, %installfolder%>\Manager\bin\NvPROMib2Amib[.exe]

Specification method

```
NvPROMib2Amib {-amib|-desc|-enum} file [-silent] [-out ofile]
```

```
NvPROMib2Amib -help
```

Description

If the argument is omitted or invalid, help is displayed. For details, refer to "7.4 Adding MIBs (page 648)".

Arguments

-amib

Create an AMIB definition file.

For details of the output location, refer to the explanation of `-out` *ofile*.

For instructions on how to incorporate an AMIB definition file, refer to "7.4.1.1 Procedure for incorporating an AMIB definition file and type definition file (page 652)".

If the MIB file contains a type definition (TEXTUAL-CONVENTION macro), add the type definition to the following file.

`<On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\public\amib\NetvisorEx.tc`

-desc

Create an AMIB help file.

For details of the output location, refer to the explanation of `-out` *ofile*.

For instructions on how to incorporate an AMIB help file, refer to "7.4.1.2 Procedure for incorporating an AMIB help file (page 654)".

An AMIB help file is a file containing MIB object descriptions extracted from an MIB file. View from the "4.16.1.4 MIB Description dialog box (page 341)".

-enum

Create an AMIB enumeration file.

For details of the output location, refer to the explanation of `-out` *ofile*.

For instructions on how to incorporate an AMIB enumeration file, refer to "7.4.1.3 Procedure for incorporating an AMIB enumeration (page 655)".

An AMIB enumerated file is a file containing correlation information for symbol names corresponding to numeric values extracted from an MIB file. This is used to convert numeric value-type MIB values into symbol names and display them.

file

Specify the name of the MIB file that you want to convert.

-out ofile

Specify the name of the output file for the conversion results.

Specify extensions as follows:

- AMIB definition file: def
- AMIB help file: dsc
- AMIB enumeration file: enm

If `-out` *file* is not determined, output file is automatically determined.

Output file name:

MIB_module-SMI_version- Last_update_date.Extension

- If the last update date is not described, *Last_update_date* is omitted.
- *SMI_version* is "v1" if SMIv1, or "v2" if SMIv2.

The file output destination depends on types of definition file.

`<On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\public\`

- AMIB definition file: amib

- AMIB help file: amib\locale\0409
- AMIB enumeration file: amib

-silent

Specify this argument to run the command in silent mode.

The task confirmation display during command execution is hidden in silent mode. For this reason, no input operations are required while the command is running. If the output file such as specified in `-out` *ofile* exists, it is overwritten.

In cases where an user needs to input, the process ends in an error. In this case, nothing is output even if `-out` *file* is specified. When the process ends in an error, execute again without `-silent` option.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

1. If an error occurs when running the command, refer to "7.4.2 Handling errors (page 656)" for a solution.
2. Cannot run simultaneously with `NvPROReloadDefFileMgr` command.

9.5.2 nvpamibcheck

This command checks whether the AMIB definition file includes definitions affecting operations of Network Manager before the AMIB definition file is incorporated to Network Manager.

If the AMIB definition file including MIB definitions defining objects in an MIB object index is incorporated to Network Manager as in the example below, the MIB value of the MIB object index cannot be obtained correctly.

- Example:

```
sysUpTimeInstance OBJECT IDENTIFIER ::= { sysUpTime 0 }
```

In the above example, the “0” connected to sysUpTime defines the object named sysUpTimeInstance. If this definition is incorporated to Network Manager, Network Manager cannot obtain a value for sysUpTime.0 (1.3.6.1.2.1.1.3.0) properly.

Use this command to prevent definitions from being incorporated to Network Manager.

Path

<On the manager, %installfolder%>`\Manager\bin\nvpamibcheck[.exe]`

Specification method

```
nvpamibcheck [file]
```

Description

This command inspects whether the AMIB definition file specified for *file* includes any definition that can affect operations of Network Manager.

If *file* is not specified, this command inspects all AMIB definition files (*.def) stored under the following path.

<On the manager, %installfolder%>\Manager\sg\NvPRO\NVWORK\public\amib\

If the inspection finds there are no definitions affecting operations of Network Manager in the AMIB definition file, the following message is displayed.

```
Succeeded in checking AMIB definitions.
```

If the AMIB definition file contains any definitions affecting operations, the detailed description is output to the log file in addition to the following message.

```
There are some illegal definitions.
```

Log file output destination:

<On the manager, %installfolder%>\Manager\log\yyyyMMddHHmmssSSS_nvpamibcheck.log

The definition affecting operations is described in the log file as "ERROR: *file name* (*line number*):". Add *"#"* to the beginning of the relevant definition in the AMIB definition file so that the definition will not be read.

Arguments

file

Specify the AMIB definition file to be inspected.

Return values

Return value	Type	Description
0	Normal	Normal end
1	Normal	Detected any definition that causes Network Manager behave abnormally.
2	Warning	Processing interrupted due to user action (e.g. pressing CTRL+C).
101	Fatal	Invalid argument
104	Fatal	Failed to connect to NvPROBaseMgr.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
113	Fatal	Input file does not exist.
114	Fatal	File I/O error.
115	Fatal	File contents are incorrect. (It is not in the format of AMIB definition file.)

⚠ Caution

This command can only be used while the manager is running.

9.5.3 NvPROReloadDllMgr

This command applies the added and updated definitions to Network Manager without stopping the services.

Path

<On the manager, %installfolder%>\Manager\bin\NvPROReloadDllMgr[.exe]

Specification method

```
NvPROReloadDllMgr
```

Arguments

None

Description

The items shown below can be reloaded while the system is running, without stopping the services.

- Definition files used for displaying details of SNMP traps
- Command definition files that are executed when SNMP traps are received

Return value

When successful, 0 is returned. When unsuccessful, a value other than 0 is returned.

9.5.4 NvPROReloadDefFileMgr

This command applies the added and updated definitions to Network Manager without stopping the services.

Path

<On the manager, %installfolder%>\Manager\bin\NvPROReloadDefFileMgr.[exe]

Specification method

```
NvPROReloadDefFileMgr
```

Arguments

None

Description

The items shown below can be reloaded while the system is running, without stopping the services.

- Definition files used for displaying details of SNMP traps
- Command definition files that are executed when SNMP traps are received
- AMIB definition files
- Fault event files

For details of the command definition files executed when SNMP traps are received, refer to "4.15 Settings for Executing Device Commands When Alerts Occur (page 333)".

For details regarding AMIB definition files, refers to "7.4 Adding MIBs (page 648)".

For details of the fault event files, refer to "7.1.7.6 Customizing fault event message files (page 620)".

AMIB definitions that were incorporated by `NvPROReloadDefFileMgr` command can be confirmed in the following file.

<On the manager, %installfolder%>/Manager/log/NvPROAmibDefFile.log

Return value

When successful, 0 is returned. When unsuccessful, a value other than 0 is returned.

⚠ Caution

1. After executing this command, the communication with the monitoring terminal terminates. Restart the monitoring terminal window.
2. When error occurs on executing this command, refer to "7.4.2 Handling errors (page 656)".
3. Cannot run with simultaneously with `NvPROMib2Amib` command.

9.6 Trap Definition Operation Commands

The following describes the commands for operating the trap definitions used to monitor SNMP traps/informs.

For details of trap definitions, refer to "4.11.2 Trap definitions (page 260)".

9.6.1 Trap definition batch registration command (nvptrapdefconf)

This command adds, edits, or deletes (imports) trap definitions as a batch, or it outputs (exports) a list of trap definitions to external files for preparation prior to batch registration.

Path

<On the manager, %installfolder%>\Manager\bin\nvptrapdefconf[.exe]

Specification method

```
nvptrapdefconf export [-silent] [-log <logfile>]
               [-only-notapplied] <fileprefix>
nvptrapdefconf import [-silent] [-log <logfile>] <file>
nvptrapdefconf apply
nvptrapdefconf -help
```

Description

This command adds, edits, or deletes trap definitions as a batch, or it outputs a list of trap definitions, on the manager.

This command registers trap definitions from an external file to Network Manager as a batch, or it updates or deletes them as a batch. The trap definitions to be registered, updated, or deleted enter the unapplied or delete state in Network Manager. By performing an application operation on them in this state with `nvptrapdefconf`, they are reflected in the trap reception process. It can also output those trap definitions currently registered in Network Manager to an external file.

- export mode

Registered trap definitions are output to a file. The output is divided into multiple files according to definition category as below.

- User definition: *fileprefix*`.user.def`
- System definition: *fileprefix*`.system.def`
- MIB original definition: *fileprefix*`.original.def`
- Incomplete definition: *fileprefix*`.unknown.def`

For details regarding trap definition categories, refer to "4.11.2.1 Trap definition categories (page 261)".

The command progress is output to the standard output and to the file specified for *logfile*.

The command execution results are displayed in the standard output and the standard error output. They are also output to the file specified for *logfile*.

- import mode

  The information in the file specified for *file* is handled as the trap definition and added to, updated on, or deleted from Network Manager. When added or updated, trap definitions are stored in the "Not Applied" state. Trap definitions to be deleted are stored in the "Deleting" state. Trap definitions in the "Not Applied" or "Deleting" state are reflected in the operation of Network Manager by executing the command in the apply mode.

  The command progress is output to the standard output and to the file specified for *logfile*.

  The command execution results are displayed in the standard output and the standard error output. They are also output to the file specified for *logfile*.

- apply mode

  Changes (additions, changes, and deletions) made in import mode are confirmed and reflected in the operation of Network Manager.

Arguments

export

Specify this argument to output trap definitions to an external file.

import

Specify this argument to add or edit trap definitions from an external file or to delete trap definitions.

apply

Reflects trap definitions in the "Not Applied" or "Deleting" state on the operation of Network Manager.

-silent

Specify this argument to run the command in silent mode.

The task confirmation display during command execution is hidden in silent mode. For this reason, no input operations are required while the command is running, and the command works as follows:

- When exporting
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file matching the file name prefix specified in *fileprefix* exists, it is overwritten.

- When importing
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file specified in *file* contains definitions with format errors, only those definitions with the correct format are processed.
  - If the file specified in *file* contains trap definitions that have already been registered, those definitions are overwritten.

-log *logfile*

Specifies a relative path or absolute path as the output destination for the command execution results file.

- If the path contains a space, enclose it in double quotation marks (").
- The execution results log is also saved to the following default folder, regardless of whether it is specified. (*nnn* is a sequence number.)

  <On the manager, %installfolder%>\Manager\log\nvptrapdefconf*nnn*_nvptrapdefconf.txt
- The maximum number of alphanumeric characters that can be specified is 255 for Windows and 1,023 for Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

-only-notapplied

For export, outputs only those definitions that are in the "Not Applied" state. You can use this to determine those definitions for which any changes have not been reflected.

file

Specifies a relative path or absolute path as the trap definition file to import.

- If the path contains a space, enclose it in double quotation marks (").
- The maximum number of alphanumeric characters that can be specified is 255 for Windows and 1,023 for Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

fileprefix

Specifies the file name prefix of the trap definition file to export.

Not only the file name but also path information (relative or absolute path) can be included. The actual file is output with this name plus the name representing the category and an extension.

- If the path contains a space, enclose it in double quotation marks (").
- The maximum number of alphanumeric characters that can be specified is 242 for Windows and 1010 for Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

Example:

If you specify out/nec, the following four files are output. If there is not a single definition in a category, the file for that category is not created.

- out/nec.user.def (User definition)
- out/nec.system.def (System definition)
- out/nec.original.def (MIB original definition)

- out/nec.unknown.def (Incomplete definition)

-help

Displays a description of the command.

Return value

Value	Type	Description
0	Normal	Normal end.
1	Warning	Termination with part of the processing skipped due to user action (e.g. when registration is skipped for records containing errors during an import operation).
2	Warning	Processing interrupted due to user action (e.g., pressing CTRL+C).
100	Fatal	Processing of all records failed.
101	Fatal	Invalid argument.
102	Fatal	Failed to change to the configuration mode failed.
103	Fatal	Failed to connect to SysMonMgr.
104	Fatal	Failed to connect to NvPROBaseMgr.
105	Fatal	Communication with SysMonMgr was disconnected.
106	Fatal	Communication with NvPROBaseMgr was disconnected.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
112	Fatal	File could not be saved due to insufficient available disk space.
113	Fatal	Input file does not exist.
114	Fatal	File I/O error.

Caution

1. This command can only be run while the manager is running.
2. Configuration mode is acquired during the execution of this command. If the monitoring terminal or other commands are running in configuration mode, first release configuration mode and then run the command.
3. If optional parameters are specified in the command multiple times, then only the last parameter to be specified is used.
4. Do not specify the same file in *logfile* and *file*. If the same file is specified, the file may corrupt such that command execution does not terminate normally.

   Similarly, in *logfile* and *fileprefix*, specify path names that are not duplicated when category names and extensions are added.
5. If a definition could not be registered during an import operation as a result of an error or some other cause, that definition is saved as an error definition file with "TMP" + "*import_file_name*".

   If a file with the same name as this "error definition file" exists, it is overwritten.
6. In Linux, if multi-byte characters (such as Japanese) are used in file names, use UTF-8 for the file name character encoding.

9.6.1.1 Trap definition batch registration file format

Description rules

The description rules of the trap definition batch registration information file are as follows.

- The following file formats are supported.

  When creating a trap definition file manually, create it using the following character codes.

OS of manager	Character code
Windows	UTF-16 (with BOM) (recommended) or SJIS
Linux	UTF-8 (without BOM) (recommended) or UTF-16 (with BOM)

- Write one item per line. Separate the item name from the value with a colon (:).
- Lines beginning with the "#" symbol are treated as comment lines.
- You can specify multiple SNMP trap definitions in a single trap definition file. Start a trap definition with Enterprise.

Description format

The description format of the trap definition file is as follows.

Tip

- Prior to processing, Network Manager converts the identification information for SNMPv2c/v3 traps into the same format as that for SNMPv1 traps. For details, refer to "7.6 SNMP Trap Identification Method (page 664)".
- If you omit a value during editing, the relevant item is not updated. The value that has been set is used.

Item name	Description
Enterprise	Specifies the definition item corresponding to the value (OID) of the "Enterprise" of the SNMP trap, using a "complete numerical string type (page 646)" or a single character "*" which represents anything. To make an addition, this item must be specified. If you specify a tilde (~) at the beginning, it is treated as *"1.3.6.1.4.1."*. For example, if you specify *"~119"*, *"1.3.6.1.4.1.119"* is registered. If you specify a dot (.) at the beginning, it is treated as *"1.3.6.1.2.1"*. For example, if you specify *".14.16"*, *"1.3.6.1.2.1.14.16"* is registered. **Tip** • If you specify a tilde (~) or a dot (.) at the beginning, it is not treated as a single character but as *"1.3.6.1.4.1."* Or *"1.3.6.1.2.1."* for a word count after expansion. • If the input value ends with ".0", it can be registered if the number of characters excluding ".0" is 598 or less.
GenericCode	Indicates the definition item corresponding to the value of "GenericCode" of the SNMP trap. Specify one of the following single characters. • * • 0 (coldStart) • 1 (warmStart) • 2 (linkDown) • 3 (linkUp) • 4 (authentificationFailure)

Item name	Description
	• 5 (egpNeighborLoss) • 6 (enterpriseSpecific) To make an addition, this item must be specified.
SpecificCode	Specifies the definition item corresponding to the value of the "SpecificCode" of the SNMP trap, using a numeric value or a single character "*" which represents anything. You can specify a single-byte number from *"-2147483648"* to *"2147483647"*. To make an addition, this item must be specified.
Node	Indicates the definition of the specific node or group to which the trap definition is to be applied in the "standard component name specification format (page 645)". You can enter up to 128 characters. Specify them in the "standard component name specification format (page 645)". **Caution** • In this item, you cannot specify multiple components concatenated with a comma (,), which is supported by the "standard component name specification format (page 645)". • Even if you specify the node by explicitly adding the node component type (node:), it is registered in the format in which the node component type is omitted when the trap definition is registered. If you omit this value during addition, an asterisk "*" representing all nodes is set.
Severity	Specifies the severity of the alert notification to be issued when an SNMP trap matching the definition items specified for Enterprise, GenericCode, SpecificCode, and Node is received. Normal: `2` or `n` Unknown: `u` Warning: `3` or `w` MINOR : `mi` MAJOR : `ma` Fatal: `4` or `f` This item is required if you specify `1` for Logging.
Summary	Specifies the character string of the summary information of an alert to be issued when an SNMP trap matching the definition items specified for Enterprise, GenericCode, SpecificCode, and Node is received. You can enter up to 128 characters. A Unicode surrogate pair character is counted as two characters. You can specify a substitute string for displaying the varBindList value of the received SNMP trap individually. For details regarding substitute strings, refer to "Display of varBindList information (page 288)". **Tip** • If you specify a substitute string, you must define it so that the number of characters in the string after substitution in the alert message does not exceed 128. • If the input value contains a double-byte or single-byte space at the end, it is registered by deleting the space. This item is required if you specify `1` for Logging.

Item name	Description
Detail	Specifies the character string as the alert detail information notification to be issued when an SNMP trap matching the definition items specified for Enterprise, GenericCode, SpecificCode, and Node is received. You can enter up to 2,000 characters. A Unicode surrogate pair character is counted as two characters. You can define a notification containing line breaks and tabs. A line break is counted as two characters and a tab as one character. In addition, you can specify the substitute strings for displaying the varBindList value of the received SNMP trap individually, as well as the substitute string for displaying all varBindList values sequentially. For details regarding substitute strings, refer to "Display of varBindList information (page 288)". **Tip** • If you specify a substitute string, you must define it so that the number of characters in the string after substitution in the alert message does not exceed 2,000. • To enter a line break character, specify `\CARRIAGE\\NEWLINE\`. • To enter a tab character, specify `\HORIZTAB\`. • If the input value contains a double-byte or single-byte space at the end, it is registered by deleting the space.
Action	Specifies the text string indicating the action information of an alert to be reported when an SNMP trap that matches the specified Enterprise, SpecificCode, GenericCode, and Node definition settings is received. You can enter up to 1,280 characters. A Unicode surrogate pair character is counted as two characters. You can define a notification containing line breaks and tabs. A line break is counted as two characters and a tab as one character. In addition, you can specify a substitute string for displaying the varBindList value of the received SNMP trap individually. For details regarding substitute strings, refer to "Display of varBindList information (page 288)". **Tip** • If you specify a substitute string, you must define it so that the number of characters in the string after substitution in the alert message does not exceed 1,280. • To enter a line break character, specify `\CARRIAGE\\NEWLINE\`. • To enter a tab character, specify `\HORIZTAB\`. • If the input value contains a double-byte or single-byte space at the end, it is registered by deleting the space.
RecoveryNo	Indicates the definition of the number for identifying the trap definition to form a pair for auto recovery control. Network Manager executes auto recovery control, using two trap definitions having the same number as a set. For trap definitions having the same RecoveryNo, the one with a severity of "normal ("`2`" or "`n`")" is regarded as the definition for recovery alert notification, while the other with a severity other than "normal" is regarded as the definition for abnormal alert notification. If an abnormal alert is reported and then followed by a recovery alert with the same RecoveryNo, the alert is automatically recovered. Specify a single-byte number from *"1"* to *"4,294,967,295"*. Set the same RecoveryNo for those trap definitions that correspond to alert and recovery SNMP traps for the same incident.

Item name	Description
	Caution If RecoveryNo or RecoveryCondition is changed during an operation, an alert reported before the change cannot be automatically recovered. In such a case, recover it manually.
RecoveryCondition	Shows the definition setting of the varBindList number condition used to identify whether an SNMP trap is the automatic recovery control target. Use this if it is not possible to determine, with RecoveryNo alone, that an SNMP trap to form a pair has been received. In the case of a linkDown or linkUp SNMP trap, "ifIndex", which is contained in the first information of varBindList, indicates the interface on which the incident occurred. Therefore, in this case, the first value in varBindList is used to determine if the SNMP trap forms a pair. You can use this parameter to automatically recover from such an SNMP trap alert. Specify the n-th value of varBindList with a single-byte number to determine if the trap forms a pair. To determine the other part of the pair using multiple varBindList values, delimit them with a comma (,). Example: 1,3 If RecoveryNo is not set, this parameter value is ignored.
Logging	Specifies whether to issue an alert notification. `1`: Issues an alert notification (default value). `0`: Does not issue an alert notification (discard). If you omit this value during addition, the default value is set.
ExternFun	Indicates the definition of the alert notification control for specific devices. Select one of the following. Normally, specify nothing. • Blank (Nothing specified) Special alert notification control is not performed. • ChangeCompByIfIndex This is a parameter for monitoring Nexus 2000 and reporting an alert to the target Nexus 2000 icon when a linkDown or linkUp SNMP trap is received.
Id	ID for uniquely identifying a trap definition. This specification is required to perform an update or deletion.
DeleteFlag	Specify this argument to delete the trap definition. Specify either of the following values. Usually, this specification can be omitted, except in the case of deletion. `1`: Deletes it. `0`: Does not delete it (default value).

The following items are output as reference information if output in export mode. For an explanation of the meaning of each item, refer to the description of the relevant item in "4.11.3.1 Trap Definition Management window (page 265)" and "4.11.5.1 Add/Edit/Properties of Trap Definition dialog box (page 282)".

They are ignored if specified in import mode.

Item name	Description
Category	The contents of **Category** are output.
Imported	The contents of **Import Date** are output.
LastModified	The contents of **Last Modified Date** are output.

Item name	Description
MibFileName	The contents of **MIB File Name** are output.
MibModuleName	The contents of **MIB Module Name** are output.
MibLastUpdated	The contents of **MIB File Last Updated** are output.
StatusOfEditing	The contents of the **Status** column are output.

Trap definition samples

- Updating the contents of an MIB original definition

  A file output in export mode (Category being Original) is saved, and a copy of the file is edited. The Id line is deleted.

```
Enterprise: 1.3.6.1.4.1.21839.1.2.18
GenericCode: 6
SpecificCode: 1
Severity: 2
Summary: ax2230sSystemMsgTrap
Detail: A system message is output.\CARRIAGE\\NEWLINE\%all
Logging: 1
Action:
RecoveryNo:
RecoveryCondition:
Node:*
ExternFun:
Description:
#MibModuleName:
#Imported:
#LastModified: 2017/02/15 11:25
#MibLastUpdated:
#MibFileName:
#Category:Original
#StatusOfEditing: NotApplied
DeleteFlag: 0
```

Tip

1. You can also update the definition of the product definition category in a similar way.
2. You must not specify *"Id"*. Otherwise, registration will fail.
3. You cannot update those trap definitions for which the category is MIB original definition (Original) or system definition (System). They must be newly registered as user definitions.
4. If Logging is `1`, Enterprise, GenericCode, SpecificCode, and Summary must be specified. They cannot be omitted.

- Updating registered user definitions

  A file output in export mode (Category being User) is edited. The Id line is not deleted.

```
Enterprise: 1.3.6.1.4.1.21839.1.2.18
GenericCode: 6
SpecificCode: 1
Severity: 2
Summary: A system message trap is generated.
Detail: A system message is output.\CARRIAGE\\NEWLINE\%all
Logging: 1
```

```
Action:
RecoveryNo:
RecoveryCondition:
Node:*
ExternFun:
Description:
#MibModuleName:
#Imported:
#LastModified: 2017/02/15 11:25
#MibLastUpdated:
#MibFileName:
#Category:User
#StatusOfEditing: NotApplied
Id: 00001
DeleteFlag: 0
```

Tip

- Be sure to specify *"Id"*. If you do not specify *"Id"*, it is registered as a new user definition.
- If Logging is `1`, Enterprise, GenericCode, SpecificCode, and Summary must be specified. They cannot be omitted.

- Deleting unnecessary trap definitions

  A file output in export mode is edited. *1* is specified for *"DeleteFlag"*.

```
Enterprise: 1.3.6.1.4.1.21839.1.2.18
GenericCode: 6
SpecificCode: 1
Severity: 2
Summary: ax2230sSystemMsgTrap
Detail: A system message is output.\CARRIAGE\\NEWLINE\%all
Logging: 1
Action:
RecoveryNo:
RecoveryCondition:
Node:*
ExternFun:
Description:
StatusOfEditing: NotApplied
Id: 00001
DeleteFlag: 1
```

Tip

- Be sure to specify *"Id"*. If you do not specify *"Id"*, the definition is registered as a new one.
- Any items other than *"Id"* and *"DeleteFlag"* are ignored.

- Adding new, un-incorporated definitions manually

```
Enterprise: 1.3.6.1.4.1.9.9.82.2.0
GenericCode: 6
SpecificCode: 1
Severity: 2
Summary: Spanning tree conflict
Detail: A conflict is discovered on a port of the VLAN spanning tree.\
CARRIAGE\\NEWLINE\%D1%
Logging: 1
```

Tip

- You must not specify *"Id"*. Otherwise, registration may fail or an existing definition may be updated.
- If Logging is `1`, Enterprise, GenericCode, SpecificCode, and Summary must be specified. They cannot be omitted.

9.6.2 Trap definition auto generation command (nvpmib2trapdef)

This command automatically creates trap definitions by importing MIB files published by RFC and device vendors.

Path

<On the manager, %installfolder%>\Manager\bin\nvpmib2trapdef[.exe]

Specification method

```
nvpmib2trapdef [-silent] [-encode {utf8|sjis}] [-with-incomplete]
               [-log <logfile>] <folder>
```

```
nvpmib2trapdef -help
```

Description

On the manager, analyzes an MIB file, automatically creates trap definitions, and registers them as MIB original definitions. Trap definitions to be registered enter the "Not Applied" state. For details regarding registration items, refer to "4.11.6.3 Description of a trap definition automatically created from an MIB file (page 296)".

Edit the trap definitions that are automatically generated upon the execution of this command as needed, using the `nvptrapdefconf` command and other commands. Then, reflect them onto Network Manager, using the `nvptrapdefconf apply` command.

Arguments

-encode {utf8|sjis}

Specifies the character code used to encode the MIB file to import. The default is `utf8`.

- `ttf8`: UTF-8 (without BOM)
- `sjis`: Shift-JIS

-with-incomplete

If the MIB file for creating trap definitions is insufficient or if the descriptions in the MIB file contain a syntax error, it may not be possible to determine the value of the OID of the Enterprise ID appropriately, resulting in incomplete trap definitions. In such cases, specify whether to register incomplete trap definitions.

If you specify this, trap definitions are registered even if they are incomplete.

-silent

Specify this argument to run the command in silent mode.

The task confirmation display during command execution is hidden in silent mode. For this reason, no input operations are required while the command is running, and any trap definitions that result in errors and warnings in analysis are skipped unconditionally.

In addition, if the file specified in `-log` *logfile* exists, it is overwritten.

Tip

- Usually, if trap definitions are automatically created from an MIB file, they are registered with the category of the trap definitions being "MIB original definition". If they are incomplete trap definitions, they are registered with the category being "incomplete definition".
- Trap definitions registered in the category of "incomplete definition" cannot serve as trap definitions unless the value of the OID of the Enterprise ID is edited appropriately. Acquire appropriate MIB files from device vendors and execute auto creation again. Alternatively, confirm the appropriate value of the OID of the Enterprise ID and manually edit the trap definitions.

-log *logfile*

Specifies a relative path or absolute path as the output destination for the command execution results file.

- If the path contains a space, enclose it in double quotation marks (").
- The execution results log is also saved to the following default folder, regardless of whether it is specified. (*nnn* is a sequence number.)

  <On the manager, %installfolder%>`\Manager\log\nvpmib2trapdef\`*nnn*`_nvpmib2trapdef.txt`
- The maximum number of alphanumeric characters that can be specified is 255 for Windows and 1,023 for Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

folder

Specifies a relative path or absolute path of the folder to which to save the MIB file to import.

Specifies the folder that stores the MIB file to import.

- If the path contains a space, enclose it in double quotation marks (").
- The maximum number of alphanumeric characters that can be specified is 255 for Windows and 1,023 for Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

⚠ Caution

- Do not place files other than MIB files in the specified folder. If a file is identified as a non-MIB file, the analysis of the file is stopped and the next file is analyzed. Depending on the contents of the file, however, the entire processing may be affected.
- Any files in any subfolders under the specified folder are not processed.

  If any of the files in the specified folder has a name that satisfies any of the following conditions, such a file is also not processed.
  - The file name starts with a dot (.).
  - The file name starts or ends with the "#" symbol.
  - The file name ends with a tilde (~).

Return value

Value	Type	Description
0	Normal	Normal end.
1	Warning	Termination with part of the processing skipped due to user action (e.g. when registration is skipped for records containing errors during an import operation).
2	Warning	Processing interrupted due to user action (e.g., pressing CTRL+C).
100	Fatal	Processing of all records failed.
101	Fatal	Invalid argument.
102	Fatal	Failed to change to the configuration mode failed.
103	Fatal	Failed to connect to SysMonMgr.
104	Fatal	Failed to connect to NvPROBaseMgr.
105	Fatal	Communication with SysMonMgr was disconnected.
106	Fatal	Communication with NvPROBaseMgr was disconnected.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
112	Fatal	File could not be saved due to insufficient available disk space.
113	Fatal	Input file does not exist.
114	Fatal	File I/O error.

Caution

1. This command can only be run while the manager is running.
2. Configuration mode is acquired during the execution of this command. If the monitoring terminal or other commands are running in configuration mode, first release configuration mode and then run the command.
3. If optional parameters are specified in the command multiple times, then only the last parameter to be specified is used.
4. In Linux, if multi-byte characters (such as Japanese) are used in folder names, use UTF-8 for the folder name character encoding.
5. If an event that requires the confirmation of the validity of a process or an error occurs after the start of this command, a message indicating the details of the process is output to the file specified in `-log` *logfile*. Confirm the contents of the output message, and if there is a problem, contact NEC Customer Support Center or the device vendor who supplied the MIB file.

   For details regarding the contents of the message, refer to "4.11.6.4 Messages output during MIB file analysis (page 297)".

9.7 SNMP Access Command

9.7.1 NvPROAmibGetSvc/NvPROAmibGetMgr

These commands acquire MIB values from specified nodes or acquire AMIB values from the internal components of Network Manager.

Path

<On the monitoring terminal, %installfolder%>`\Svc\bin\NvPROAmibGetSvc.exe`

```
<On the manager, %installfolder%>\Manager\bin\NvPROAmibGetMgr[.exe]
```

Specification method

```
NvPROAmibGet(Svc|Mgr) [-form output_format] [-tout time_out] [-snmpnext]
 [-diff] [-file output_filename] component [mib_name [mib_time]]
```

Description

Acquires MIB values from the node specified in *component* or AMIB values from the Network Manager internal component, and outputs them as text. If the argument is omitted or invalid, help is displayed.

Tip

1. "Component" is the collective term of the managed nodes and Network Manager internal information.
2. AMIB mostly indicates information of the Network Manager internal components.

Arguments

-form *output_format*

Specify the output format. The following alternate strings can be used.

%T

Replaced with a component type name (node, map, logEnt, etc.).

%C

Replaced with a component name.

%AN

Replaced with a complete numeric string-type MIB or AMIB name.

%AS

Replaced with a complete name string-type MIB or AMIB name.

%AB

Replaced with a MIB or AMIB leaf name.

%QN

Replaced with a request time expressed numerically.

%QS

Replaced with a request time expressed as a string.

%QD

Replaced with a request time character string expressed using the standard date command format for UNIX.

%SN

Replaced with a response time expressed numerically.

%SS

Replaced with a response time expressed as a string.

%SD

Replaced with a character string representing a request time in the standard UNIX date command format.

%W

Replaced with an acquired value. OctetString types are converted to hexadecimal notation (in a colon (:)-separated format that starts with 0x).We recommend using this parameter when retrieving OctetString Type MIBs or AMIBs.

%V

Replaced with an acquired value. OctetString types are converted to ASCII characters.

Example: Acquired value: 0x4142 -> conversion result: AB

If conversion is not possible, this works in the same manner as %W.

%%

Replaced with a percentage character (%).

In addition, you can specify the width of the display by specifying a numeric value (from -4,096 to 4,096) after the percentage (%).

If the numeric value starts with a minus (-), the display is aligned to the right, if not, it is aligned to the left. To include a space, include quotation marks (") on both sides.

If omitting the `-form` option, the same output is generated when you spacify as follows:

- *mib_time* specified : `-form` "%C\t%QS\t%-22AB\t%V\n"
- *mib_time* unspecified : `-form` "%C\t%-22AB\t%V\n"

-tout *time_out*

Specify the timeout time when acquiring information from the SNMP agent, in units of seconds.

This value can be between a minimum of 1 second to a maximum of 300 seconds. If omitted, the default is 300 seconds.

If the retry timeout for SNMP packets and ICMP packets specified in the operating environment settings occurs, timeout errors may be generated prior to the timeout time specified here.

-snmpnext

Use the SNMP GetNextRequest function to acquire the MIB value of the next name of the specified MIB names, in dictionary order.

-diff

If the interval is specified using *mib_time*, and the MIB specified in *mib_time* is a counter-type, used for counting the number of packets, the average values per unit time (second) are displayed, rather than the raw data acquired using SNMP.

-file *output_file*

Creates a file with the specified name and outputs command results to the file.

component

Specifies component names using the standard component name specification format. If you want to specify a node name starting with a hyphen (-), always specify it in "node:*node_name*" format.

If you want to specify a port number for SNMP communication, specify the component name in "*node_name@port*" format. If a port number is not specified, the port number specfied in the **SNMP Port** property of the node is used.

mib_name

Specify a MIB or AMIB name using the standard AMIB name specification format. If omitted, an appropriate name is selected in accordance with the component type.

mib_time

Specify intervals for acquiring AMIB values. If the interval is omitted, values are only acquired once.

Specification example

- Acquires node "switch1" configuration information from the manager.

```
NvPROAmibGetMgr node:switch1
```

- Acquires MIB values below ".system" in node "switch1" from the monitoring terminal.

```
NvPROAmibGetSvc node:switch1 .system
```

- Acquires the number of node "switch1" input packets, every 5 seconds.

```
NvPROAmibGetMgr -diff node:switch1 .ip.ipInReceives.0 5
```

- Changes the display format to "Response time + value" only.

```
NvPROAmibGetMgr -diff -form "%QS %W\n" node:switch1
 .ip.ipInReceives.0 5
```

- Acquires interface information from node "switch1" and writes it to a file.

```
NvPROAmibGetMgr node:switch1 .interfaces -file switch1_interfaces.txt
```

- Acquires MIB values below ".system" in node "switch1" using 16161/udp port.

```
NvPROAmibGetMgr node:switch1@16161 .system
```

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

1. In the Linux environment, when an asterisk (*), question mark (?), or backslash (\) are specified in a component name, the shell may recognize them as wildcard characters and try to expand them. In this case, the component name cannot be specified correctly. To avoid the wildcard processing, specify as follows:

   NvPROAmibGetMgr "node:*"

   NvPROAmibGetMgr 'node:*'

   NvPROAmibGetMgr node:*

2. In the Linux environment, to obtain accurate output when specifying a format string using the `-form` option, enclose the format string in single quotes(').

   Example:

   ```
   ./NvPROAmibGetMgr -form '%C\t%AB\n' switch1 .system
   ```

3. If a file specified using the `-file` option already exists, it will be overwritten.
4. If format string parsing fails, "(format_error)" is displayed.
5. If an interval was specified using the *mib_time* option, press the CTRL + C key to stop continuous MIB value acquisition. In addition, if an interval time is specified short (e.g. 1) because it takes some

time to complete the command processing, MIB value acquisition may continue until the command processing is completed.

6. When a file is output using `-file` option to a directory of which amount of space is not full, writing may fail.
7. If any non-ASCII character is included in the obtained data, they may not be displayed correctly. If they are not displayed correctly, set the **SNMP Character Code** property and retry the operation.

9.7.2 NvPROAmibSetMgr

This command sets MIB values of specified nodes.

Path

<On the manager, %installfolder%>\Manager\bin\NvPROAmibSetMgr[.exe]

Specification method

```
NvPROAmibSetMgr component mib_name value
```

```
NvPROAmibSetMgr -file file_name
```

Description

Sets *mib_name* as the MIBs of nodes specified in the *component* argument, or as the AMIB of internal Network Manager function components, overwriting with the value specified in *value*.

Tip

"Component" is the collective term of the managed nodes and Network Manager internal information. This command can be used for node components.

Arguments

component

Specifies component names using the standard component name specification format. If you want to specify a node name starting with a hyphen (-), always specify it in "node:*node_name*" format.

mib_name

Specify a MIB using the standard AMIB name specification format.

First incorporate an MIB file that defines the type of MIB to specify. For instructions on how to incorporate a file, refer to "7.4.1.1 Procedure for incorporating an AMIB definition file and type definition file (page 652)".

value

Specifies the value that will be set in the specified MIB.

-file *file_name*

Specifies the *file_name* containing the specified component name, specified MIB name, and the value to be set. Use this option for specifying characters that cannot be specified using arguments of the command line (for example, Unicode surrogate pair characters), as a component name, MIB name, or value.

The maximum length of the file path specified in `-file` option is 259 for Windows, 1,023 for Linux or HP-UX.

For the file specification, use spaces to separate each argument.

```
Component_name MIB_name New_value
```

The maximum number of characters per line of the specified file is 8,189 characters.

You can include more than one of the specifications above. If any line uses an incorrect format, an error message is generated and the operation ends.

Return value

When successful, 0 is returned. When unsuccessful, 1 is returned.

⚠ Caution

1. There is a limit to how much data to set each time you run `NvPROAmibSetMgr`. If the error below occurs, reduce the number of specified components and try again.

   ```
   NvPROAmibSetMgr: Data size exceeds buffer size
   ```

2. In the Linux or HP-UX environment, when an asterisk (*), question mark (?), or backslash (\) are specified in a component name, the shell may recognize them as wildcard characters and try to expand them. In this case, the component name cannot be specified correctly. To avoid the wildcard processing, specify as follows:

   NvPROAmibSetMgr "node:*" ...

   NvPROAmibSetMgr 'node:*' ...

   NvPROAmibSetMgr node:* ...

3. In the Windows environment, if configuring settings for multiple nodes in a single execution of the `NvPROAmibSetMgr` command as in the example below, the `"Failed to get/set (a part of) data"` error may display.

   Example:

   - Sets the MIB value for all components.

     ```
     NvPROAmibSetMgr.exe "*" mib_name
     ```

   - Configures settings based on the large file content.

     ```
     NvPROAmibSetMgr.exe -file large_file_name
     ```

   In these cases, separate the command into multiple execution runs.

4. Even when the configuration of MIB settings are permitted in the MIB definition, configure may still not be possible, depending on the specifications and settings of the target device type.
5. The wait time to receive a response from a node after an MIB configuration request is 300 seconds. If the system is in a state that does not allow communication with target nodes, commands may not terminate for 300 seconds.

9.8 Command for Sending SNMP Traps

9.8.1 NvPROTrapSend

To send SNMP traps from Network Manager, specify the information below in the action report.

Path

<On the manager, %installfolder%>\Manager\bin\NvPROTrapSend[.exe]

Specification method

```
NvPROTrapSend [-v 1|2c] [-p port] [-c community] [-a ipaddress]
 -ip ipaddress -o1 "YYYY/MM/DD HH:MM:SS" -o2 "ipaddress"
 -o3 severity -o4 "summary" -o5 "detail" -o6 "solution"
```

Arguments

-v 1|2c

Specifies a version of the SNMP traps to be sent.

This is optional. The default is 1 (version 1).

-p *port*

Specifies a send port number between 1 and 65,535 for SNMP traps to be sent.

This is optional. The default value is 162.

-c *community*

Specifies a community name with a maximum of 16 single-byte characters for SNMP traps to be sent.

This is optional. The default is "Network Manager".

-a *agentaddress*

Specifies a SNMP agent address for SNMP traps to be sent, using an IPv4 address in decimal dot notation.

This is optional. The default value is the IPv4 address of the manager.

Only valid for SNMP version 1 traps.

-ip *ipaddress*

Specifies the send source for SNMP traps, using an IPv4 address in decimal dot notation.

This parameter is mandatory.

-o1 "*YYYY/MM/DD HH:MM:SS*"

Specifies the date and time that alerts are received.

Specify up to 19 characters. The excess characters will be truncated.

When specifying as action report options, specify "$OCCURTIME$". This parameter is replaced by the received date and time of alert.

-o2 "*ipaddress*"

Specifies the TCP/IP address of the device on which the alert occurred, using an IPv4 address in decimal dot notation.

Specify up to 39 characters. The excess characters will be truncated.

When specifying as action report options, specify "$IPADDRESS$". This parameter is replaced by the IP address of the node where the alert occurred.

-o3 "*severity*"

Specifies the severity of the alert that has occurred. Specify up to 64 characters. The excess characters will be truncated.

When specifying as action report options, specify "$SEVERITY$". This parameter is replaced by the alert severity in the alert view (NORMAL, UNKNOWN, WARNING, MINOR, MAJOR,FATAL).

-o4 "*summary*"

Specifies the summary text for the alert that has occurred. Specify up to 128 characters. The excess characters will be truncated.

When specifying as action report options, specify "$SUMMARY$". This parameter is replaced by the alert summary text in the alert view.

-o5 "*detail*"

Specifies the details text for the alert that has occurred.

Specify up to 1,024 characters. The excess characters will be truncated.

When specifying as action report options, specify "$DETAIL$". This parameter is replaced by the alert details text in the alert view.

-o6 "*solution*"

Specifies the processing text for the alert that has occurred.

Specify up to 640 characters. The excess characters will be truncated.

When specifying as action notification options, specify "$ACTION$". This parameter is replaced by the alert solution text in the alert view.

⚠ Caution

1. If space is included in arguments like `-o1` to `-o6`, the entire character string of argument needs to be enclosed in double quotation marks ("").
2. You can specify only the ASCII or Shift-JIS characters.
3. The source IP address of the trap is determined by OS, because it is not set in this command when sending the trap.

9.8.2 Sending SNMP trap format

The trap formats that Network Manager sends are shown below.

Enterprise-ObjectID

.1.3.6.1.4.1.119.2.3.143.2

Generic-Trap

6

Specific-Trap

11

variable-bindings

.1.3.6.1.4.1.119.2.3.143.1.1	Date and time when the alert is received
.1.3.6.1.4.1.119.2.3.143.1.2	IP address of the node where the alert occurred
.1.3.6.1.4.1.119.2.3.143.1.3	Alert severity (NORAML, UNKNOWN, WARNING, MINOR, MAJOR, FATAL)

.1.3.6.1.4.1.119.2.3.143.1.4	Alert summary text
.1.3.6.1.4.1.119.2.3.143.1.5	Alert details text
.1.3.6.1.4.1.119.2.3.143.1.6	Alert solution text

Tip

The MIB file defining the format of SNMP trap sent by Network Manager is stored in the following location:

<On the manager, %installfolder%>\Manager\sg\NvPRO\NetworkManagerMIB\NetworkManager.mib

9.9 Command for Issuing Alert Events (nvpalertsend)

This command issues failure alert events and pseudo SNMP traps to the manager itself.

Path

*<On the manager, %installfolder%>*Manager\bin\nvpalertsend[.exe]

Specification method

```
nvpalertsend alert msgnum [-level level] [-msgfile msgfile]
 [-optmsg optmsg] [-action actmsg] node
```

```
nvpalertsend trap trapoid [-varbind oid type value ...] node
```

```
nvpalertsend -help
```

Description

On the manager, issues alert events and pseudo SNMP traps to the manager itself.

Alert events and pseudo SNMP traps issued by this command are proceeded as usual, so you can use it to confirm the correctness of alert notification settings or SNMP trap alert definitions.

This command cannot issue the alert events and pseudo SNMP traps to other managers.

Arguments

alert *msgnum*

Issues the alert with the specified message number *msgnum*.

The message number means the line number in the fault event message file specified by -msgfile.

For details how to create fault event message files, refer to "7.1.7.6 Customizing fault event message files (page 620)".

trap *trapoid*

Issues the pseudo SNMP trap with OID specified by *trapoid*.

Tip

To issue an enterprise-specific trap of SNMP v1, concatinate the value of "Enterprise" and "SpecificCode" with dot (.) in order to specify as one OID value.

Example: Enterprise:1.3.6.1.4.1.119, GenericCode:6, SpecificCode:1

```
trap 1.3.6.1.4.1.119.1
```

node

Specifies the alert occurrence source node.

-help

Displays a description of the command.

Optional arguments (when "alert" is specified)

-level *level*

Specifies the alert severity level. Specify one of the following: w(Warning), mi(MINOR), ma(MAJOR), f(Fatal). If omitted, interpreted as w(Warning).

-msgfile *msgfile*

Specifies the fault event message file name. If omitted, the file name is interpreted as `user.msg`. For details how to create fault event message files, refer to "7.1.7.6 Customizing fault event message files (page 620)".

-optmsg *optmsg*

Specifies additional information appended to the **Detail** field of the alert.

-action *actmsg*

Specifies the message text displayed in the **Solution** field of the alert.

Optional arguments (when "trap" is specified)

-varbind *oidtypevalue*

Specifies the variable bindings (varBind) information for the pseudo SNMP trap.

To specify multiple variable bindings, repeat the set "*oid type value*".

Example:

```
-varbind 1.3.6.1.2.1.2.2.1.1.1 INTEGER 1 1.3.6.1.2.1.2.2.1.1.1 INTEGER 2
```

Specify one of the followings MIB types in *type*.

- INTEGER, COUNTER, COUNTER64, GAUGE, TIMETICKS, UNIXTIME, IPADDRESS, PHYADDRESS, OCTETSTRING, DISPLAYSTRING, OBJECTID

If the MIB specified by *oid* is incorporated in Network Manager, incorporated MIB type is given priority over specified *type*.

Return value

Value	Type	Description
0	Normal	Normal end.
100	Fatal	Failed to send an alert.

Value	Type	Description
101	Fatal	Invalid argument.
104	Fatal	Failed to connect to NvPROBaseMgr.
106	Fatal	Communication with NvPROBaseMgr was disconnected.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
114	Fatal	File I/O error.

Specification example

1. Issue the warning alert event defined at the first line in `user.msg`.

```
nvpalertsend alert 1 -level w Switch1
```

2. Issue the coldStart trap.

```
nvpalertsend trap 1.3.6.1.6.3.1.1.5.1 Switch1
```

Caution

1. This command is only executed while Manager is running.
2. If optional parameters are specified multiple times in the command, then the last specified parameter is chosen.
3. This command may take about one second or more to complete. When running the command repeatedly, consider one second or more as a guide of an interval of each command.

9.10 Configuration Information Operation Command

9.10.1 Configuration information batch registration command (nvpnodeconf)

This command registers device information and map information in Network Manager from an external file. It also allows exporting currently registered device information and map information to an external file and deletes device information registered in Network Manager.

Path

*<On the manager, %installfolder%>*Manager\bin\nvpnodeconf[.exe]

Specification method

```
nvpnodeconf {export|import} [-silent] [-map map|-mapbyfile]
 [-log logfile] file
```

```
nvpnodeconf -help
```

Description

Batch registers or exports device information and map information in Manager. Also batch deletes device information.

- export mode

  Exports device information and map information to the file specified in *file*.

  The progress status of the command is written to standard output and to the file specified in *logfile*.

  The command results are written to standard output and standard error. They are also exported to the file specified in *logfile*.

- import mode

  Registers or deletes the information from the file specified in *file* as configuration information in Network Manager.

  The progress status of the command is written to standard output and to the file specified in *logfile*.

  The command results are written to standard output and standard error. They are also exported to the file specified in *logfile*.

Arguments

export

Specify this argument when exporting device information and map information to an external file.

import

Specify this argument when registering device information and map information in Network Manager from an external file or delete device information from Network Manager.

-silent

Specify this argument to run the command in silent mode.

The task confirmation display during command execution is hidden in silent mode. For this reason, no input operations are required while the command is running, and the command works as follows:

- When exporting:
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file specified in *file* exists, it is overwritten.
- When importing:
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file specified in *file* contains records with format errors, only records with the correct format are processed.
  - If the file specified in *file* contains the device or map information that has already been registered, those settings are overwritten.

-map *map* / -mapbyfile

Specifies the map that will be the reference point. If a map name contains characters that cannot be specified from a terminal, use `-mapbyfile` instead of `-map` *map*.

Be sure to specify a map that has been registered in Network Manager. If omitted, "NetworkManagement" is used as the reference point.

When exporting, the device information and map information in the specified map is exported.

When importing, devices are registered under the specified map.

When using `-mapbyfile` option, specify the map name in the following file on the manager.

1. Change the following setting file name. Delete the end ".org".

   <On the manager, %sharedfolder%>`\Manager\sg\NvPRO\NvPROCsvIOConfig\nvpnodeconf.ini.org`

2. Specify the map name after "MAP=".

   The following is an example to specify "mapA".

```
[nvpnodeconf]
MAP=mapA
```

When specify `-map` option and `-mapbyfile` option simultaneously, the one specified later is enabled.

-log *logfile*

Specifies a relative path or absolute path as the output destination for the command execution results file.

- If the path contains spaces, enclose it in double quotation marks (").
- The execution results log is also saved to the following default folder, regardless of whether it is specified: (*nnn* is a sequence number)

  <On the manager, %installfolder%>`\Manager\log\nvpnodeconf\`*nnn*`_ImportExportLog.txt`

- The maximum number of alphanumeric characters that can be specified is 255 for the Windows and 1,023 for the Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

file

Specifies a relative path or absolute path for the export destination file or the import source file.

- If the path contains spaces, enclose it in double quotation marks (").
- The maximum number of alphanumeric characters that can be specified is 255 for the Windows and 1,023 for the Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

For information about formats for input and output files, refer to "4.6.1.1 Configuration information file format (page 207)".

-help

Displays a description of the command.

Return value

Value	Type	Description
0	Normal	Normal end.

Value	Type	Description
1	Warning	Termination with part of the processing skipped due to user action (e.g. when registration is skipped for records containing errors during an import operation).
2	Warning	Processing interrupted due to user action (e.g. pressing CTRL+C).
100	Fatal	Processing of all records failed.
101	Fatal	Invalid argument.
102	Fatal	Failed to change to the configuration mode failed.
103	Fatal	Failed to connect to SysMonMgr.
104	Fatal	Failed to connect to NvPROBaseMgr.
105	Fatal	Communication with SysMonMgr was disconnected.
106	Fatal	Communication with NvPROBaseMgr was disconnected.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
112	Fatal	File could not be saved due to insufficient available disk space.
113	Fatal	Input file does not exist.
114	Fatal	File I/O error.
115	Fatal	File contents are incorrect.
116	Fatal	No license.

Caution

1. This command is only executed while Manager is running.
2. Configuration mode is acquired during the execution of this command. If the monitoring terminal or other commands are running in configuration mode, release configuration mode and then run the command.
3. If optional parameters are specified multiple times in the command, then the last specified parameter is used.
4. Do not specify the same file in *logfile* and *file*. If specifying the same file, the file might become corrupted and the command might not terminate normally.
5. If a record could not be registered during the import operation due to an error or some other cause, that line is saved as an error record file ("TMP" + *import_file_name*).

   If a file with the same name as this error record file exists, it is overwritten.
6. In the Linux, if multi-byte characters are used in file names, use UTF-8 for the file name character encoding.

9.10.2 Configuration information update command (nvpnodeup)

This command updates the configuration management information in Network Manager.

Path

<On the manager, %installfolder%>\Manager\bin\nvpnodeup[.exe]

Specification method

```
nvpnodeup [all|interface|interface-all] [-silent] [-log logfile]
    {-node node|-map map|-file file}
```

```
nvpnodeup -help
```

Description

If any of `all`, `interface`, or `interface-all` is not specified, only required items shown below are updated.

Required system information items	Required interface information items
• Agent type • Software version • Routing control • SNMP engine ID • sysName	• Interface information (ifTable, IPv4, IPv6) • Fex ID (only if OS type is NX-OS)

For the file format of the file specified in the `-file` option, refer to "9.10.2.1 Format of files that specify the target devices of `nvpnodeup` command (page 728)".

Arguments

all

Updates all system information and interface information.

interface

When specified, only required interface information items are updated.

interface-all

When specified, all interface information items are updated.

-silent

Specify this argument to run the command in silent mode.

The task confirmation display during command execution is hidden in silent mode. For this reason, no input operations are required while the command is running. If the file specified in `-log` *logfile* exists, it is overwritten.

-log *logfile*

Specifies a relative path or absolute path as the output destination for the command execution results file.

- If the path contains spaces, enclose it in double quotation marks (").
- The execution results log is also saved to the following default folder, regardless of whether it is specified(*nnn* is a sequence number):

  <On the manager, %installfolder%>`\Manager\log\nvpnodeup\`*nnn*`_nvpnodeup.txt`
- The maximum number of alphanumeric characters that can be specified is 255 for the Windows and 1,023 for the Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

-node *node* / -map *map* / -file *file*

Use one of the following to specify target nodes for device information updates.

- `-node` *node*

  If specifying more than one node, use a comma to separate them. When including node names containing white spaces, enclose the entire list in double quotation marks (").

- `-map` *map*

  Targets nodes in the specified map for device information updates. If specifying more than one map, use a comma to separate them. When including map names containing white spaces, enclose the entire list in double quotation marks (").

- `-file` *file*

  Specifies the file containing the target node/map names for device information updates. Specify a relative or absolute path. For information about file formats, refer to "9.10.2.1 Format of files that specify the target devices of `nvpnodeup` command (page 728)".

If target node names/map names contain characters that cannot be specified from a command line, specify them in a file instead.

If no target nodes have been specified for device information updates, the command processing ends in the error code 100.

-help

Displays a description of the command.

Return value

Value	Type	Description
0	Normal	Normal end.
1	Warning	Some device information updates failed.
2	Warning	Processing interrupted due to user action (e.g. pressing CTRL+C).
100	Fatal	Specified node or map is invalid (not found).
101	Fatal	Invalid argument.
102	Fatal	Failed to change to the configuration mode.
103	Fatal	Failed to connect to SysMonMgr.
104	Fatal	Failed to connect to NvPROBaseMgr.
105	Fatal	Communication with SysMonMgr was disconnected.
106	Fatal	Communication with NvPROBaseMgr was disconnected.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
112	Fatal	File could not be saved due to insufficient available disk space.
113	Fatal	Input file does not exist.
114	Fatal	File I/O error.
115	Fatal	File contents are incorrect.

⚠ Caution

1. This command is only executed while Manager is running.
2. Configuration mode is acquired during the execution of this command. If the monitoring terminal or other commands are running in configuration mode, release configuration mode and then run the command.
3. If optional parameters are specified multiple times in the command, then the last specified parameter is chosen. If `-node`, `-map`, or `-file` are specified several times, the command ends in an error.
4. Do not specify the same file in *logfile* and *file*. If specifying the same file, the file might become corrupted and the command might not terminate normally.
5. In the Linux, if multi-byte characters are used in file names, use UTF-8 for the file name character encoding.
6. If an abort request takes place while device information is being updated, the abort is performed after information of the device that is being processed has been updated. For this reason, if an abort is requested while devices with a large number of interfaces are being processed, it might take some time for the command to terminate.
7. If any non-ASCII character is included in the property information to be updated, they may not be displayed correctly. If they are not displayed correctly, set the **SNMP Character Code** property and retry the operation.

9.10.2.1 Format of files that specify the target devices of `nvpnodeup` command

This section describes the format for files used to specify target nodes and maps when running the device information update command (`nvpnodeup`).

Create a file for the device information to update using the following encoding.

Manager OS	Encoding
Windows	UTF-16(with BOM) or standard OS multi-byte character encoding with CRLF line break code
Linux	UTF-8(with BOM) with LF line break code

File format details:

- Lines beginning with the "#" symbol are treated as comment lines.
- Write one node name/map name per line. Use the standard matching specification format.
- When specifying a node name, write the [node] keyword at the start of the line.

  When specifying a map name, write the [map] keyword at the start of the line.

  A section is defined as a single block from keyword to keyword, and lines outside of the section are ignored.
- When specifying either a node or map, if there is extra white space(space or tab) before or after the node name or map name, the name is considered to contain white spaces. (This allows you to include multibyte spaces in a node or map name.)

Example with only nodes specified:

```
[node]
# this is a comment line
Node?
nvp*Router
Node220
```

Example with a combination of nodes and maps specified:

```
This line is ignored,because it is outside of the section.
[map]
192.168.?.*
192.168.10.*
192.168.20.*
[node]
NodeA
NodeB
Router*
```

Tip

1. If the specified file does not exist, the command processing ends in the error code 113 (input file does not exist).
2. If reading a specified file failed, the command processing ends in the error code 114 (file I/O error).

9.10.3 XML file output command (NvPROExportCmd)

This is a command to export configuration management information stored in Network Manager to a CMDB-compatible XML-format file.

Path

*<On the manager, %installfolder%>*Manager\bin\NvPROExportCmd[.exe]

Specification method

```
NvPROExportCmd [-node node_name_list | -ip ip_address_list]
 [-out outputfile]
```

Arguments

-node *node_name_list*

Specify the node name to export. When specifying more than one, use comma separation.

-ip *ip_address_list*

Specify the IP address of the node to be exported in decimal dot notation. When specifying more than one, use comma separation.

-out *outputfile*

Specify either the absolute or relative path for the file name of the XML file to be exported.

If omitted, a file with the name `nvpexport.xml` will be created in the current directory .

Enclose the path in double quotation marks (") if it includes a space.

Specification example

- Configuration information for the node of the specified IP address will be output to the current directory.

```
NvPROExportCmd -ip 192.168.0.1,192.168.0.3
```

- Node configuration information for the specified node name will be output to the following file: C:\export\nvexp.xml

```
NvPROExportCmd -node Sirius,Orion -out C:\export\nvexp.xml
```

Return value

When finishing successfully, results will be output in standard output. If ending abnormally, an error message will be returned in standard error output.

Return value	Description
0	Normal end.
1	Invalid argument.
2	Failed to acquire configuration management information.
3	Failed to convert to XML or create file.
4	Unknown error.

Caution

1. `-node` and `-ip` cannot be specified at the same time.
2. When there is no specification for `-node` or `-ip`, the target will be all nodes.
3. If more than one specification is made for `-node` or `-ip`, specify without inserting a space before or after commas.
4. This command can only be executed under *<On the manager, %installfolder%>*`Manager\bin` directory.

9.10.4 VLAN/Load Balancer setting information export command (NvPRODCImportExportCmd)

This is a command to export VLAN and Load Balancer setting information stored in Network Provisioning function to a TAB-separated Unicode text file format (TSV-format file).

For details regarding output TSV-format, refer to "4.21.6 Checking configuration status of Network Provisioning (page 424)".

Path

<On the manager, %installfolder%>`\Manager\bin\NvPRODCImportExportCmd.exe`

Specification method

```
NvPRODCImportExportCmd.exe {-vlan|-lb} -export -file filename
```

Arguments

-vlan

Export VLAN settings. This option cannot be specified with `-lb`.

-lb

Export LB settings. This option cannot be specified with `-vlan`.

-file *filename*

Specify the output file name.

Return value

Always return 0.

9.11 Status Monitoring Config Command (nvpstsmonconf)

This command registers or deletes state monitoring setting information, or to export the information.

Path

<On the manager, %installfolder%>\Manager\bin\nvpstsmonconf[.exe]

Specification method

```
nvpstsmonconf { export | import} [-rule rule] [-silent][-log logfile] file
```

```
nvpstsmonconf -help
```

Description

Batch registers or exports state monitoring setting information. Also batch deletes the information.

- export mode

  Exports state monitoring setting information to the file specified in *file*.

  The progress status of the command is written to standard output and the file specified in *logfile*.

  The command results are written to standard output and standard error. They are also output to the file specified in *logfile*.

- import mode

  Batch registers or deletes the state monitoring setting information from the file specified in *file*.

  The progress status of the command is written to standard output and the file specified in *logfile*.

  The command results are written to standard output and standard error. They are also output to the file specified in *logfile*.

Arguments

export

Specify this argument to export configured state monitoring setting information to an external file.

import

Specify this argument to register or delete state monitoring setting information in Network Manager from an external file.

-rule *rule*

Specify rule names (rule file names without extension) to apply to setting information targeted for export. The command results are written to standard output and standard error. They are also output to the file specified in.

Example:

When specifying the "icmperr:ICMP_OutputErrorPackets" and "ifName:UpDownCheck" rule names, specify as follows.

-rule icmperr,ifName

When specifying a rule name that contains a space, enclose the entire rule in double quotation marks (").

-rule "abc rule,ifName"

Do not insert any spaces before or after a comma.

This specification is disabled when specifying `import` as the processing mode.

When this is omitted, all rules are exported.

-silent

Specify this argument to run the command in silent mode.

The task confirmation display during command execution is hidden in silent mode. For this reason, no input operations are required while the command is running, and the command works as follows:

- When exporting:
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file specified in *file* exists, it is overwritten.
- When importing:
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file specified in *file* contains records with format errors, only records with the correct format are processed.
  - If the file specified in *file* contains the setting information that has already been registered, the setting information is overwritten or deleted while monitoring is stopped. If monitoring is being performed, the information is neither overwritten nor deleted but an error is recorded.
  - If the rules contained in the *file* specified in file have been incorporated, "removal flag" is set to "1 (remove)" and there is no state monitoring entry information that the rule on removal, the rules are removed. If there is state monitoring entry information that specifies the rule on removal, the rules are not removed but an error is recorded.

-log *logfile*

Specifies a relative path or absolute path as the output destination for the command execution results file.

- If the path contains spaces, enclose it in double quotation marks (").
- The execution results log is also saved to the following default folder, regardless of whether it is specified: (*nnn* is a sequence number)

  <On the manager, %installfolder%>\Manager\log\nvpstsmonconf*nnn*_nvpstsmonconf.txt
- The maximum number of alphanumeric characters that can be specified is 255 for the Windows and 1,023 for the Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

file

Specifies a relative path or absolute path for the export destination file or the import source file.

- If the path contains spaces, enclose it in double quotation marks (").
- The maximum number of alphanumeric characters that can be specified is 255 for the Windows and 1,023 for the Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

For information about formats for input and output files, refer to "4.10.6.1 State monitoring setting file format (page 251)".

-help

Displays a description of the command.

Return value

Value	Type	Description
0	Normal	Normal end.
1	Warning	Termination with part of the processing skipped due to user action (e.g. when registration is skipped for records containing errors during an import operation).
2	Warning	Processing interrupted due to user action (e.g., pressing CTRL+C).
100	Fatal	Processing of all records failed.
101	Fatal	Invalid argument.
102	Fatal	Failed to change to the configuration mode failed.
103	Fatal	Failed to connect to SysMonMgr.
104	Fatal	Failed to connect to NvPROBaseMgr.
105	Fatal	Communication with SysMonMgr was disconnected.
106	Fatal	Communication with NvPROBaseMgr was disconnected.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
112	Fatal	File could not be saved due to insufficient available disk space.
113	Fatal	Input file does not exist.
114	Fatal	File I/O error.
115	Fatal	File contents are incorrect.

Caution

1. This command is only executed while Manager is running.
2. Configuration mode is acquired during the execution of this command. If the monitoring terminal or other commands are running in configuration mode, release configuration mode and then run the command.
3. If optional parameters are specified multiple times in the command, then the last specified parameter is used.
4. If a record could not be registered during the import operation due to an error or some other cause, that line is saved as an error record file (*import_file_name* + "TMP" + *extension*).If a file with the same name as this error record file exists, it is overwritten.
5. Do not specify the same file in *logfile* and *file*. If specifying the same file, the file might become corrupted and the command might not terminate normally.

6. In the Linux, if multi-byte characters are used in file names, use UTF-8 for the file name character encoding.

9.12 Data Collection Config Command

9.12.1 Data Collection Config Command (nvpdatacolconf)

This command registers or deletes data collection setting information, or to export the information.

Path

<On the manager, %installfolder%>\Manager\bin\nvpdatacolconf[.exe]

Specification method

```
nvpdatacolconf { export | import } [-silent][-log logfile] file
```

```
nvpdatacolconf -help
```

Description

Batch registers or exports data collection setting information. Also batch deletes the information.

- export mode

  Exports data collection setting information to the file specified in *file*.

  The progress status of the command is written to standard output and the file specified in *logfile*.

  The command results are written to standard output and standard error. They are also output to the file specified in *logfile*.

- import mode

  Batch registers or deletes the data collection setting information from the file specified in *file*.

  The progress status of the command is written to standard output and the file specified in *logfile*.

  The command results are written to standard output and standard error. They are also output to the file specified in *logfile*.

Arguments

export

Specify this argument to export configured state monitoring setting information to an external file.

import

Specify this argument to register or delete the collection entry information in Network Manager from an external file.

-silent

Specify this argument to run the command in silent mode.

The task confirmation display during command execution is hidden in silent mode. For this reason, no input operations are required while the command is running, and the command works as follows:

- When exporting:
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file specified in *file* exists, it is overwritten.
- When importing:
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file specified in *file* contains records with format errors, only records with the correct format are processed.
  - If the file specified in *file* contains the setting information that has already been registered, those settings are overwritten or deleted when the entry is stopped, or process for the entry is failed when the entry is running.

-log *logfile*

Specifies a relative path or absolute path as the output destination for the command execution results file.

- If the path contains spaces, enclose it in double quotation marks (").
- The execution results log is also saved to the following default folder, regardless of whether it is specified: (*nnn* is a sequence number)

  <On the manager, %installfolder%>`\Manager\log\nvpdatacolconf\`*nnn*`_ImportExportLog.txt`
- The maximum number of alphanumeric characters that can be specified is 255 for the Windows and 1,023 for the Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

file

Specifies a relative path or absolute path for the export destination file or the import source file.

- If the path contains spaces, enclose it in double quotation marks (").
- The maximum number of alphanumeric characters that can be specified is 255 for the Windows and 1,023 for the Linux.
- It is not possible to specify a path that contains surrogate pair characters.

For information about formats for input and output files, refer to "4.16.6.1 Data collection settings file format (page 359)".

-help

Displays a description of the command.

Return value

Value	Type	Description
0	Normal	Normal end.
1	Warning	Termination with part of the processing skipped due to user action (e.g. when registration is skipped for records containing errors during an import operation).
2	Warning	Processing interrupted due to user action (e.g. pressing CTRL+C).
100	Fatal	Processing of all records failed.
101	Fatal	Invalid argument.

Value	Type	Description
102	Fatal	Failed to change to the configuration mode failed.
103	Fatal	Failed to connect to SysMonMgr.
104	Fatal	Failed to connect to NvPROBaseMgr.
105	Fatal	Communication with SysMonMgr was disconnected.
106	Fatal	Communication with NvPROBaseMgr was disconnected.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
112	Fatal	File could not be saved due to insufficient available disk space.
113	Fatal	Input file does not exist.
114	Fatal	File I/O error.
115	Fatal	File contents are incorrect.

Specification example

1. Export registered data collection settings information to a file.

```
> nvpdatacolconf.exe export -silent "C:\tmp\temp.csv"
```

2. Batch register data collection settings information from an input file.

```
> nvpdatacolconf.exe import -silent "C:\tmp\temp.csv"
```

⚠ Caution

1. This command is only executed while Manager is running.
2. Configuration mode is acquired during the execution of this command. If the monitoring terminal or other commands are running in configuration mode, release configuration mode and then run the command.
3. If optional parameters are specified multiple times in the command, then the last specified parameter is used.
4. If a record could not be registered during the import operation due to an error or some other cause, that line is saved as an error record file ("TMP_" + *import file name*). If a file with the same name as this error record file exists, it is overwritten.
5. Do not specify the same file in *logfile* and *file*. If specifying the same file, the file might become corrupted and the command might not terminate normally.
6. In the Linux, if multi-byte characters are used in file names, use UTF-8 for the file name character encoding.

9.12.2 Data Collection Filter Operation Command (nvpdatacolfilter)

This command configures filter settings for performace data passed to other MasterScope products.

Path

<On the manager, %installfolder%>\Manager\bin\nvpdatacolfilter[.exe]

Specification method

```
nvpdatacolfilter {enable|disable|status}
```

```
nvpdatacolfilter {export|import} [-silent] [-log logfile] file
```

```
nvpdatacolfilter -help
```

Description

Batch registers, deletes, or exports filter setting information. And enables or disables the data filter function.

- export mode

  Exports filter setting information to the file specified in *file*.

  The progress status of the command is written to standard output and the file specified in *logfile*.

  The command results are written to standard output and standard error. They are also output to the file specified in *logfile*.

- import mode

  Batch registers or deletes the filter setting information from the file specified in *file.*

  The progress status of the command is written to standard output and the file specified in *logfile*.

  The command results are written to standard output and standard error. They are also output to the file specified in *logfile*.

Arguments

enable

Specify this argument to enable the data filter function.

disable

Specify this argument to disable the data filter function.

status

Specify this argument to display the status of the data filter function.

export

Specify this argument to export the filter setting information to an external file.

import

Specify this argument to batch register the filter setting information from an external file.

-silent

Specify this argument to run the command in silent mode.

The task confirmation display during command execution is hidden in silent mode. For this reason, no input operations are required while the command is running, and the command works as follows:

- When exporting:
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file specified in *file* exists, it is overwritten.

- When importing:
  - If the file specified in `-log` *logfile* exists, it is overwritten.
  - If the file specified in *file* contains records with format errors, only records with the correct format are processed.
  - If the file specified in *file* contains the setting information that has already been registered, those settings are overwritten.

-log *logfile*

Specifies a relative path or absolute path as the output destination for the command execution results file.

- If the path contains spaces, enclose it in double quotation marks (").
- The execution results log is also saved to the following default folder, regardless of whether it is specified: (*nnn* is a sequence number)

  <On the manager, %installfolder%>\Manager\log\nvpdatacolfilter*nnn*_ImportExportLog.txt
- The maximum number of alphanumeric characters that can be specified is 255 for the Windows and 1,023 for the Linux.
- It is not possible to specify a path that contains Unicode surrogate pair characters.

file

Specifies a relative path or absolute path for the export destination file or the import source file.

- If the path contains spaces, enclose it in double quotation marks (").
- The maximum number of alphanumeric characters that can be specified is 255 for the Windows and 1,023 for the Linux.
- It is not possible to specify a path that contains surrogate pair characters.

For information about formats for input and output files, refer to ""4.16.8.5 File format of the data filter settings (page 372)""

-help

Displays a description of the command.

Return value

Value	Type	Description
0	Normal	Normal end.
1	Warning	Termination with part of the processing skipped due to user action (e.g. when registration is skipped for records containing errors during an import operation).
2	Warning	Processing interrupted due to user action (e.g. pressing CTRL+C).
100	Fatal	Processing of all records failed.
101	Fatal	Invalid argument.
102	Fatal	Failed to change to the configuration mode failed.
103	Fatal	Failed to connect to SysMonMgr.
104	Fatal	Failed to connect to NvPROBaseMgr.
105	Fatal	Communication with SysMonMgr was disconnected.

Value	Type	Description
106	Fatal	Communication with NvPROBaseMgr was disconnected.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
112	Fatal	File could not be saved due to insufficient available disk space.
113	Fatal	Input file does not exist.
114	Fatal	File I/O error.
115	Fatal	File contents are incorrect.

Specification example

1. Export registered filter setting information to a file.

```
> nvpdatacolfilter.exe export -silent "C:\tmp\temp.csv"
```

2. Batch register the filter setting information from an input file.

```
> nvpdatacolfilter.exe import -silent "C:\tmp\temp.csv"
```

⚠ Caution

1. This command is only executed while Manager is running.
2. Configuration mode is acquired during the execution of this command. If the monitoring terminal or other commands are running in configuration mode, release configuration mode and then run the command.
3. If optional parameters are specified multiple times in the command, then the last specified parameter is used.
4. If a record could not be registered during the import operation due to an error or some other cause, that line is saved as an error record file ("TMP_" + *import file name*). If a file with the same name as this error record file exists, it is overwritten.
5. Do not specify the same file in *logfile* and *file*. If specifying the same file, the file might become corrupted and the command might not terminate normally.
6. In the Linux, if multi-byte characters are used in file names, use UTF-8 for the file name character encoding.
7. If the data filter function is enabled, only the data that matches the filter condition is passed to other MasterScope products. Therefore, if the data filter function is enabled but no filter conditions are imported, no data is passed to other MasterScope products.

9.13 File Code Conversion Command (nvpfileconv)

Converts the character encoding and line break code in a file.

Path

<On the monitoring terminal, %installfolder%>\Svc\bin\nvpfileconv.exe

Specification method

```
nvpfileconv.exe fromcode tocode fromfile tofile [-linefeed tolinefeed]
```

```
nvpfileconv.exe -help
```

Description

This command converts the character encoding and line break code in a file. For example, use it in the following cases:

- To edit a file exported using the Linux configuration information batch register command on the Windows.
- To import a file edited on the Windows using the Linux configuration information batch register command.

The command results are written to standard output and standard error.

Arguments

fromcode

Specifies the character code in the conversion source file as "utf8" or "utf16le".

Loads the *fromfile* with the character encoding specified in *fromcode*.

tocode

Specifies the character code in the conversion destination file as "utf8" or "utf16le".

Writes the *tofile* with the character encoding specified in *tocode*.

fromfile

Specifies the conversion source file using a relative path or absolute path.

If the path contains spaces, enclose it in double quotation marks (").

tofile

Specifies the conversion destination file using a relative path or absolute path.

If the path contains spaces, enclose it in double quotation marks (").

-linefeed *tolinefeed*

Specifies the line break code in the conversion destination file as "crlf" or "lf".

If specifying this argument and specifying the same character encoding for both the *fromcode* and *tocode*, character code conversion is not performed but linefeed code conversion is performed.

-help

Displays a description of the command.

Specification example

- To edit a file exported from Linux in Windows:
  1. Export using the Linux Manager command.

     The data is exported to a file using UTF-8 character encoding, the LF linefeed code, and TAB separator characters.
  2. Transfer the exported file to Windows.
  3. Run the command (`nvpfileconv`). The file character encoding is converted from UTF-8 to UTF-16 and the line break code is converted from LF to CRLF.

```
> cd "C:\Program Files (x86)\NEC\UMF\Operations\Svc\bin"
> nvpfileconv.exe utf8 utf16le "C:\work\input.txt"
  "C:\work\output.txt" -linefeed crlf
```

4. Edit the converted file.

- To import a file edited in Windows into Linux:

1. Create the import file in Windows.

   Set the character encoding to UTF-16, the linefeed code to CRLF, and the separator character to TAB.

2. Run the command (`nvpfileconv`). The file character encoding is converted from UTF-16 to UTF-8 and the linefeed code is converted from CRLF to LF.

```
>cd "C:\Program Files (x86)\NEC\UMF\Operations\Svc\bin"
> nvpfileconv.exe utf16le utf8 "C:\work\input.txt"
  "C:\work\output.txt" -linefeed lf
```

3. Transfer the converted file to Linux.
4. Import using the appropriate manager command on Linux.

Return value

Value	Type	Description
0	Normal	Normal end.
101	Fatal	Invalid argument.
110	Fatal	Internal error (other error).
113	Fatal	Input file does not exist.
114	Fatal	File I/O error

Caution

1. Do not specify the same file in *fromfile* and *tofile*. If specifying the same file, the file may become corrupted and the command may not terminate normally.
2. If optional parameters are specified multiple times in the command, then the last specified parameter is used.

9.14 Command for Executing Device Commands (nvpdevcmdexe)

Login to a device and execute device commands defined in the external command file.

The login settings must be performed in advance for a target device on which a device command will be executed. For details, refer to "4.3 Registering Login Information (page 189)".

Path

<On the manager, %installfolder%>\Manager\bin\nvpdevcmdexe.exe

Specification method

```
nvpdevcmdexe {-node node|-nodefile file} -cmdfile cmdfile [-silent]
 [-log logfile] [-retry count]
```

```
nvpdevcmdexe -help
```

Description

Login to a target device and execute arbitrary device commands described in the command file specified by `-cmdfile`. In the command file, you can use not only device commands but also simple scripts such as control flow statements.

Arguments

-node *node* / -nodefile *file*

Specifies the target node for the command execution from a command line or file. Use `-nodefile` option to specify the node name with a character that cannot be specified from a terminal.

When using `-nodefile`, create the file as follows:

- Use Unicode (Windows) or UTF-8 (Linux) for the character encoding.
- Specify only one node name into the file.
- Do not put line break.

If the path contains spaces, enclose it in double quotation marks (").

-cmdfile *cmdfile*

Specifies the command file in which device commands were written.

If the path contains spaces, enclose it in double quotation marks (").

Create the command file as follows:

- Use only ASCII characters. Do not use other encoding characters such as Unicode.
- Use CRLF as line break.
- File size must be less than 100KB.

The command file format is the same as described in "4.19.1 Defining commands (page 391)". The simple script can be used. For details regarding simple scripts, refer to "4.19.1.1 Simple scripts (page 393)". When creating a command file, refer to "4.19.1.2 Precautions in creating commands (page 395)".

-silent

Specify this argument to run the command in silent mode.

The task confirmation display during command execution is hidden in silent mode. For this reason, no input operations are required while the command is running. If the file specified in `-log` *logfile* exists, it is overwritten.

-log *logfile*

Specifies a relative path or absolute path as the output destination for the command execution results file.

If omitted, the command execution results are not outputted to a file.

The execution result is not output when the execution failed before logging in to the device.

If the path contains spaces, enclose it in double quotation marks (").

-retry *count*

Specifies the retry count for connecting to the device. Specify the number from 1 to 10. If omitted, interpreted as 1.

-help

Displays a description of the command.

Return value

Value	Type	Description
0	Normal	Normal end.
2	Warning	Processing interrupted due to user action (e.g. pressing CTRL+C).
100	Fatal	Fatal error.
101	Fatal	Invalid argument.
110	Fatal	Internal error (other error).
111	Fatal	Memory allocation failed.
114	Fatal	File I/O error.
115	Fatal	File contents are incorrect. For example: • The command file contains any characters other than ASCII. • Character encoding of the file specified in `-nodefile` is incorrect.
117	Fatal	Node name does not exist.
201	Fatal	Command script returned 1 by *END.
202	Fatal	Command script returned 2 by *END.
203	Fatal	Command script returned 3 by *END.
204	Fatal	Command script returned 4 by *END.
205	Fatal	Command script returned 5 by *END.
206	Fatal	Command script returned 6 by *END.
207	Fatal	Command script returned 7 by *END.
208	Fatal	Command script returned 8 by *END.
209	Fatal	Command script returned 9 by *END.
221	Fatal	Failed to connect to the device.
222	Fatal	Failed to login to the device.
223	Fatal	Failed to change to the enable mode.
224	Fatal	Command execution error.
225	Fatal	Failed to connect to the manager process.

If the return value of command is 110 to 115, 221 to 225, error codes of the Resource Manager function is output to the standard output. For details, refer to "8.1.1 Error Codes in Resource Manager function (page 670)".

Caution

If executing multiple `nvpdevcmdexe` commands simultaneously for the same node, the command process that was executed later is started after all preceding commands have been finished. If the `nvpdevcmdexe` command process has not been started within 5 minutes, this command process is terminated with an error.

9.15 Backup and Restore Function

This function helps to back up the setting files and definition files and the configuration information in the database, without stopping the manager function. This function makes it possible to back up the setting information without stopping the system operation.

For details of the backup command, refer to "9.15.1 Backup command (page 744)".

When restoring setting information from the backup, the manager services need to be stopped. The restore procedures is described in "9.15.4 Restore command (restore procedure) (page 748)".

Caution

Restoring can only be performed on the same environment where the backup was made. The environment where the restoring is performed needs to satisfy the following conditions.

1. In the destination environment of the restoration, Network Manager must be installed with the same version and same installation parameters (install folder, etc.) when the backup was made.

   In addition, the configuration of the database (type, version, install folder, etc.) cannot be changed. Especially when using the external database, you must install the database software with the same version into the same folder.
2. You must assign the same hostname and IP address where the backup was made.

Backup Targets

The backup targets are the contents that were set from the monitoring view and the definition files placed on the manger. Note that the operational data, such as the alert information, audit logs, and report histories, are not backed up.

However, the histories of Resource Manager function (device config management, device software management) are backed up because they are closely related to the function settings.

Tip

If you want to backup all the information including what this command is not backup (alert information or audit log, etc.), refer to "Backup and Restore Procedures" section in "MasterScope Network Manager Setup Guide".

Caution

When any other product that uses framework such as MasterScope SystemManager G is installed in the same folder, the setting information of that product is backed up and restored at the same time.

9.15.1 Backup command

This command backs up the definition files on the manager.

For details of the backup targets, refer to "9.15 Backup and Restore Function (page 744)".

Path

<On the manager, %installfolder%>\Manager\bin\SysMonMgr[.exe]

Specification method

```
SysMonMgr -backup
```

For cluster system only:

```
SysMonMgr -backup [-L|-S|-B]
```

Description

Backs up setting information such as definition files.

If backup is successful, information about the path to the backup folder is output to the standard output.

Backups are created in the following locations. If you did not specify **Data Directory** during installation, <*On the manager, %installfolder%*> becomes the same folder as <*On the manager, %installfolder%*> .

- Backup of the install folder

  <*On the manager, %installfolder%*>\Manager\backup*nnn*

- Backup of data folder

  <*On the manager, %sharedfolder%*>\Manager\backup*nnn*

If you want to save backups to removable media, etc., save the data under each of the above *nnn* directories as a batch.

It is recommended that you use an appropriate archiver (such as tar or zip) to save file attributes, etc.

⚠ Caution

1. *nnn* is a 3-digit integer. It starts with 001.
2. Upper bound of *nnn* is limited to 10 by default.

   In order to change the upper bound of *nnn*, add MaxIndex key under [Backup] section to `SysMonMgr.ini`. (Valid MaxIndex ranges are 001 - 999.)

   If necessary, add a new section and then describe as shown below.

   Example: Limiting *nnn* range to 000 - 050.

   ```
   [Backup]
   MaxIndex=50
   ```

3. If *nnn* exceeded the limit specified by MaxIndex key, *nnn* is reset to 000. Following backup operation will increment and overwrite old backups.

Arguments

In the cluster system, you can use the `-L`, `-S`, or `-B` option to specify the backup target scope.

-L

Backs up the definition files and databases saved in <*On the manager, %installfolder%*>. Use this option when backing up the standby host of the cluster system.

-S

Backs up only the definition files that are saved on a <*On the manager, %sharefolder%*>. This option is not used for Network Manager backup.

-B

Backs up the definition files that are saved on both a <*On the manager, %installfolder%*> and a <*On the manager, %sharefolder%*>. Use this option when backing up the active host of the cluster system.

If the option is omitted, `-B` is specified. For non-clustering systems, do not use the backup target scope options above.

Return value

When successful, 0 is returned. When unsuccessful, 2 is returned.

Caution

1. Before executing this command, some settings such as library path are needed. Refer to "the notes (page 685)".
2. When executing the backup operation, the manager services must be running.
3. This command moves on to configuration mode and starts the backup process.

   For this reason, this command will fail if a monitoring terminal is in configuration mode. You cannot execute multiple instances of this command at the same time.
4. Do not create files or directories in the backup directory.

9.15.2 Backup list command

This command lists the backups that are currently held on the manager.

Path

<On the manager, %installfolder%>`\Manager\bin\SysMonMgr[.exe]`

Specification method

```
SysMonMgr -listbackup
```

Description

Outputs the backup list information to the standard output. When you want to restore definition files from the backup or delete the backup, you must specify the corresponding backup identifier that is displayed in the list.

Description of each displayed column:

- for a non-cluster system:

[TimeStamp]	The date and time when the backup was created. The date and time is displayed in the ISO 8601 format.
[L DirName]	The backup identifier on the local disk.
[S DirName]	The backup identifier on the shared disk.
[HostName]	The hostname where the backup was created.

- for a cluster system:

[TimeStamp]	The date and time when the backup was created. The date and time is displayed in the ISO 8601 format.
[L DirName]	Display the backup identifier if the backup created by `-B` or `-L` option. Display '---' if the backup created by `-S` option.

[S DirName]	Display the backup identifier if the backup created by -B or -S option. Display '---' if the backup created by -L option.
[HostName]	The hostname where the backup was created.

Return value

When successful, 0 is returned. When unsuccessful, 2 is returned.

⚠ Caution

Before executing this command, some settings such as library path are needed. Refer to "the notes (page 685)".

9.15.3 Backup delete command

This command deletes the specified backup that is currently held on the manager, or all of them.

Path

<On the manager, %installfolder%>\Manager\bin\SysMonMgr[.exe]

Specification method

```
SysMonMgr -deletebackup [-f] -all
```

```
SysMonMgr -deletebackup [-f] backup_id
```

For cluster system only:

```
SysMonMgr -deletebackup [-f] [-L|-S|-B] -all
```

```
SysMonMgr -deletebackup [-f] [-L|-S|-B] backup_id
```

Description

Deletes the specified backup, or all the backups.

When you specify -all with a cluster configuration, a confirmation window is displayed if the backup on *<On the manager, %installfolder%>* does not correspond to the backup on *<On the manager, %sharedfolder%>*.

Arguments

In the cluster system, you can use the -L, -S, or -B option to specify the deletion target scope.

-f

The deletion process will continue as if "Y" is typed in the confirmation.

-all

Deletes all the backups.

backup_id

Specify the backup you want to delete. It corresponds to one of the backup identifiers that will be displayed with the backup list command.

-L / -S / -B

Specify one of `-L`, `-S`, or `-B` for the target scope. Each of them has the same meaning as in the "backup command (page 745)".

Return value

When successful, 0 is returned. When unsuccessful or canceled, 2 is returned.

⚠ Caution

Before executing this command, some settings such as library path are needed. Refer to "the notes (page 685)".

9.15.4 Restore command (restore procedure)

This section describes how to restore from the backup on the manager.

Refer to the following sections according to your environment.

- For Windows environment, refer to "9.15.4.1 Restore procedure for Windows (page 748)".
- For Linux environment, refer to "9.15.4.2 Restore procedure for Linux (page 751)".

9.15.4.1 Restore procedure for Windows

This section describes how to restore from the backup on the Windows manager.

Place saved backups in advance so that they have the same configuration as in environment in which they were acquired. When placing backup data, remove the read-only attributes from the files and directories and make other changes, as needed, so that the files and directories are write-enabled.

Backups are placed in the following locations. If you did not specify **Data Directory** during installation, *<On the manager, %sharedfolder%>* becomes the same folder as *<On the manager, %installfolder%>*.

- Install folder

  <On the manager, %installfolder%>\Manager\backup*nnn*

- Data folder

  <On the manager, %sharedfolder%%>\Manager\backup*nnn*

⚠ Caution

nnn is a 3-digit integer. The *nnn* portion of the directory name can be changed to any number between 000 - 999.

1. Stop manager functions.

   For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

2. Delete following two data on Manager from a command prompt.

```
> rmdir /q /s <On the manager, %sharedfolder%>\Manager\sg\NvPRO
\RMAPI\db
> rmdir /q /s <On the manager, %sharedfolder%>\Manager\sg\NvPRO
\ResourceManager\work
```

3. Execute restore command (`SysMonMgr -restore`).

   - Path

     <On the manager, %installfolder%>\Manager\bin\SysMonMgr[.exe]

- Specification method

```
SysMonMgr -restore [-f] -latest
```

```
SysMonMgr -restore [-f] backup_id
```

For cluster system:

```
SysMonMgr -restore [-f] [-L|-S|-B] -latest
```

```
SysMonMgr -restore [-f] [-L|-S|-B] backup_id
```

- Description

Restore the definitions from the specified backup.

- Arguments

-f

The restoration process will continue as if "Y" is typed in the confirmation.

-latest

Select the latest backup.

backup_id

Specify the backup from which you want to restore. It corresponds to one of the backup identifiers that will be displayed with the backup list command.

-L / -S / -B

Specify one of `-L`, `-S`, or `-B` for the target scope. Each of them has the same meaning as in the "backup command (page 745)".

- To perform restore to the active host in a cluster configuration, use `-B`.

  If backups are collected with the same timing but the backup identifier differs between <*On the manager, %installfolder%*> and <*On the manager, %sharedfolder %*>, you can specify a combination of `-L` and `-S`, instead of `-B`. Be sure to specify backups collected at the same timing.

- To restore to the standby host, use `-L`.

- Return value

When successful, 0 is returned. When unsuccessful or canceled, 2 is returned.

⚠ Caution

a. Before executing this command, some settings such as library path are needed. Refer to "the notes (page 685)".

b. You cannot execute multiple instances of restore concurrently. Therefore, do not attempt to execute multiple instances at the same time.

c. A folder named restore*nn* is created under backup folder when restoring. These folders can be removed after restore finished successfully.

4. Execute the restore procedure of the database.

In case of the cluster system, execute this procedure only in the active host.

- When using the internal database, open a command prompt and execute commands as follows.

```
> cd "<On the manager, %installfolder%>\Manager\bin"
> WfdbCtlStart.bat
> cd ..\sql\postgres"
> DR_TBL.bat
> WfdbRestore_pos.bat
```

Caution

When `WfdbRestore_pos.bat` is executed, the following error or warning message is displayed, however the restored data has no problem.

```
ERROR:  schema "wfdb" already exists
WARNING:  no privileges could be revoked for "public"
WARNING:  no privileges could be revoked for "public"
WARNING:  no privileges were granted for "public"
WARNING:  no privileges were granted for "public"
```

- When using SQL Server, open a command prompt and execute commands as follows.

```
> cd "<On the manager, %installfolder%>\Manager\sql\sqlserver"
> WfdbDropDB.bat <database name> <server name> <instance name>
> WfdbRestore_sql.bat <database name> <server name>
 <instance name>
```

For details regarding the arguments of `WfdbDropDB.bat`, refer to "Uninstalling the Database" section in "MasterScope Network Manager Setup Guide".

For `WfdbRestore_sql.bat`, specify the same arguments as `WfdbDropDB.bat` execution.

Caution

If SQL Server is installed into different folder from when the backup was created, the restore will fail. Install SQL Server into the same folder where SQL Server was installed at the backup time.

5. Execute the post-processing of the restoration.

   In case of the cluster system, execute this procedure only in the active host.

   Open a command prompt and execute commands as follows.

```
> cd "<On the manager, %installfolder%>\Manager\bin"
> NvPRORestoreDataC.bat
```

6. In the EXPRESSCLUSTER X environment and using external database (SQL Server), the additional procedure is required in order to make SID of the database login user same between the active host and the standby host.

   To make same SID, execute step 9 and 11 in "Restore procedure" section for external databases in "MasterScope Network Manager Setup Guide for the cluster environment".

7. When using internal database, stop the database service for CMDB.

   In case of the cluster system, execute this procedure only in the active host.

   Open a command prompt and execute commands as follows.

```
> cd "<On the manager, %installfolder%>\Manager\bin"
> WfdbCtlStop.bat
```

8. Start manager functions.

   For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

Example of restore procedure

The execution example to restore from the latest backup is shown as below. In this example, it is assumed that Network Manager is installed in the default install path and the default database parameters, in non-clustering system.

- With internal database:

  Stop manager functions, and then open a command prompt.

```
> cd "C:\Program Files (x86)\NEC\UMF\Operations\Manager"
> rmdir /q /s sg\NvPRO\RMAPI\db
> rmdir /q /s sg\NvPRO\ResourceManager\work
> cd bin
> SysMonMgr.exe -restore -latest
> WfdbCtlStart.bat
> cd ..\sql\postgres
> DR_TBL.bat
> WfdbRestore_pos.bat
> cd ..\..\bin
> NvPRORestoreDataC.bat
> WfdbCtlStop.bat
```

  Start manager functions.

- With external SQL Server:

  Stop manager functions, and then open a command prompt.

```
> cd "C:\Program Files (x86)\NEC\UMF\Operations\Manager"
> rmdir /q /s sg\NvPRO\RMAPI\db
> rmdir /q /s sg\NvPRO\ResourceManager\work
> cd bin
> SysMonMgr.exe -restore -latest
> cd ..\sql\sqlserver
> WfdbDropDB.bat
> WfdbRestore_sql.bat
> cd ..\..\bin
> NvPRORestoreDataC.bat
```

  Start manager functions.

9.15.4.2 Restore procedure for Linux

This section describes how to restore from the backup on the Linux manager.

Place saved backups in advance so that they have the same configuration as in environment in which they were acquired. When placing backup data, remove the read-only attributes from the files and directories and make other changes, as needed, so that the files and directories are write-enabled.

Backups are placed in the following locations. If you did not specify **Data Directory** during installation, *<On the manager, %sharedfolder%>* becomes the same folder as *<On the manager, %installfolder%>*.

- Install folder

  On the manager, %installfolder%/Manager/backup/*nnn*

- Data folder

  On the manager, %sharedfolder%/Manager/backup/*nnn*

Caution

nnn is a 3-digit integer. The *nnn* portion of the directory name can be changed to any number between 000 - 999.

1. Stop manager functions.

   For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

2. Delete following two data on Manager from command line.

```
# rm -rf <On the manager, %sharedfolder%>/Manager/sg/NvPRO/RMAPI/db/*
# rm -rf <On the manager, %sharedfolder%>/Manager/sg/NvPRO
/ResourceManager/work/*
```

3. Execute the restore command (`SysMonMgr -restore`).

   - Path

     On the manager, %installfolder%`/Manager/bin/SysMonMgr`

   - Specification method

```
SysMonMgr -restore [-f] -latest
```

```
SysMonMgr -restore [-f] backupID
```

     For a cluster configuration:

```
SysMonMgr -restore [-f] [-L|-S|-B] -latest
```

```
SysMonMgr -restore [-f] [-L|-S|-B] backupID
```

   - Description

     Restores setting information from a specified backup.

   - Arguments

     -f

     Continues restore by assuming that Y is entered in the confirmation window.

     -latest

     Selects the latest backup.

     backupID

     Specifies a restore target. It corresponds to the backup identifier displayed with the backup list command.

     -L or -S or -B

     Not used in a non-cluster configuration. For a cluster configuration, specify any one of `-L`, `-S`, and `-B` as the target range. The meaning of each option is the same as for the "Backup command (page 745)".

     - To restore to the active host in a cluster configuration, use `-B`.

       If backups are collected with the same timing but the backup identifier differs between <*On the manager, %installfolder%*> and <*On the manager, %sharedfolder %*>, you can specify a combination of `-L` and `-S`, instead of `-B`. Be sure to specify backups collected at the same timing.

     - To restore to the standby host, use `-L`.

- Return value

  When successful, 0 is returned. When unsuccessful or canceled, 2 is returned.

Caution

a. Before executing this command, some settings such as library path must be made. Refer to "notes on Command Reference (page 685)".

b. You cannot execute multiple instances of restore concurrently. Therefore, do not attempt to execute multiple instances at the same time.

c. In the restore process, restore*nn* directories are created as work directories in the backup directory. These directories are not necessary after the completion of restore. Delete them.

4. Execute the restore procedure of the database.

   In case of the cluster system, execute this procedure only in the active host.

   - When using the internal database, execute commands as follows.

```
# cd <On the manager, %installfolder%>/Manager/bin
# ./WfdbCtlStart.sh
# cd ../sql/postgres
# ./DR_DB.sh
# ./WfdbRestore_pos.sh
```

   - When using PostgreSQL, execute commands as follows.

```
# cd <On the manager, %installfolder%>/Manager/sql/postgres
# ./DR_DB.sh <database name> <PGSQL_HOME> <PGPORT> <PGSQL_ADMIN>
# ./WfdbRestore_pos.sh <database name> <PGSQL_HOME> <PGPORT>
 <PGSQL_ADMIN>
```

   For details regarding the arguments of `DR_DB.sh`, refer to "Uninstalling the Database" section in "MasterScope Network Manager Setup Guide".

   For `WfdbRestore_pos.sh`, specify the same arguments as `DR_DB.sh` execution.

Caution

When `WfdbRestore_pos.sh` is executed, the following error or warning message is displayed, however the restored data has no problem.

```
ERROR:  schema "wfdb" already exists
WARNING:  no privileges could be revoked for "public"
WARNING:  no privileges could be revoked for "public"
WARNING:  no privileges were granted for "public"
WARNING:  no privileges were granted for "public"
```

5. Execute the post-processing of the restoration.

   In case of the cluster system, execute this procedure only in the active host.

   - When using the internal database, execute commands as follows.

```
# cd <On the manager, %installfolder%>/Manager/bin
# ./NvPRORestoreDataC.sh
```

   - When using PostgreSQL, execute commands as follows.

```
# cd <On the manager, %installfolder%>/Manager/bin
# ./NvPRORestoreDataC.sh <PGSQL_HOME>
```

   Specify PostgreSQL installation directory to the argument <*PGSQL_HOME*>.

6. When using internal database, stop the database service for CMDB.

   In case of the cluster system, execute this procedure only in the active host.

   Execute commands as follows.

```
# cd <On the manager, %installfolder%>/Manager/bin
# ./WfdbCtlStop.sh
```

7. Start manager functions.

   For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

Example of restore procedure

The execution example to restore from the latest backup is shown as below. In this example, it is assumed that Network Manager is installed in the default install path and the default database parameters, in non-clustering system.

- With internal database:

```
# /etc/init.d/UMFOperationsManager_1 stop
# rm -rf /opt/UMF/Operations/Manager/sg/NvPRO/RMAPI/db/*
# rm -rf /opt/UMF/Operations/Manager/sg/NvPRO/ResourceManager/work/*
# LC_ALL=C.utf8 LD_LIBRARY_PATH=/opt/UMF/Operations/Manager/bin
  :${LD_LIBRARY_PATH}
 /opt/UMF/Operations/Manager/bin/SysMonMgr -restore -latest
# cd /opt/UMF/Operations/Manager/bin
# ./WfdbCtlStart.sh
# cd ../sql/postgres
# ./DR_DB.sh
# ./WfdbRestore_pos.sh
# cd ../../bin
# ./NvPRORestoreDataC.sh
# ./WfdbCtlStop.sh
# /etc/init.d/UMFOperationsManager_1 start
```

- With PostgreSQL:

```
# /etc/init.d/UMFOperationsManager_1 stop
# rm -rf /opt/UMF/Operations/Manager/sg/NvPRO/RMAPI/db/*
# rm -rf /opt/UMF/Operations/Manager/sg/NvPRO/ResourceManager/work/*
# LC_ALL=C.utf8 LD_LIBRARY_PATH=/opt/UMF/Operations/Manager/bin
  :${LD_LIBRARY_PATH}
 /opt/UMF/Operations/Manager/bin/SysMonMgr -restore -latest
# cd /opt/UMF/Operations/Manager/sql/postgres
# ./DR_DB.sh wfdb /usr/local/pgsql
# ./WfdbRestore_pos.sh wfdb /usr/local/pgsql
# cd ../../bin
# ./NvPRORestoreDataC.sh /usr/local/pgsql/
# /etc/init.d/UMFOperationsManager_1 start
```

Chapter 10. System Maintenance

Contents

10.1 Checking Version Information....756
10.2 Starting and Stopping the Manager Function....757
10.3 Registering Licenses....759
10.4 Changing System Environment....764

10.1 Checking Version Information

10.1.1 Checking the version of the manager function

Check the contents of the following definition file.

[Definition File]

<On the manager, %installfolder%>\Manager\sg\SysMonMgr.ini

[Verification procedure]

1. Find the section [Product*NNN*] which contains the key "DisplayName=MasterScope Network Manager", where *NNN* is a 3-digit number.

   There may be multiple [Product*NNN*] sections.

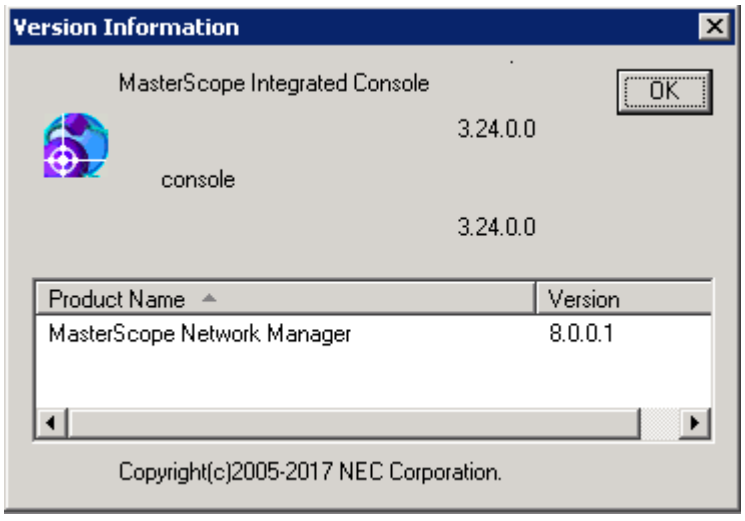
2. Check the "Version" value in this section.

```
  : (omit)

[Product001]
ProductID=5
DisplayName=MasterScope Network Manager
DisplayVersion=9.0.0.11
Version=9.0.0.11
HomeRegistry=SOFTWARE\NEC\WebSAM\NetvisorPro\Manager

  : (omit)
```

10.1.2 Checking the version of a monitoring terminal

You can check the version of a monitoring terminal function using one of the following three methods.

- In the main menu, select **Help**>**About Version**, and confirm the version from the displayed Version Information dialog box.
- Click  on the tool bar and check the version in the displayed Version Information dialog box.



- Check the contents of the following definition file.
  - Definition File

    <On the monitoring terminal, %installfolder%>\Svc\sg\SysMonSvc.ini
  - Verification procedure
    1. Find the section [Product*NNN*] which contains the key "DisplayName=MasterScope Network Manager", where *NNN* is a 3-digit number.

       There may be multiple [Product*NNN*] sections.
    2. Check the "Version" value in this section.

```
  : (omit)

[Product001]
ProductID=5
DisplayName=MasterScope Network Manager
DisplayVersion=9.0.0.11
Version=9.0.0.11
Copyright=Copyright(c)2007-2019 NEC Corporation.
HelpFile=C:\Program Files (x86)\NEC\UMF\Operations\Svc\bin\NvP
RO.chm
HomeRegistry=SOFTWARE\NEC\WebSAM\NetvisorPro\Svc

  : (omit)
```

10.2 Starting and Stopping the Manager Function

After installing the manager function of Network Manager, restart the required services (daemons) by rebooting the machine. Follow the steps below to stop and start the services (daemons) without rebooting the machine.

⚠ Caution

Log in to the OS with administrator privileges and operate.

Windows Manager

1. Open the Control Panel window and search "Administrative Tools".
2. In the Administrative Tools window, open the **Services**.
3. Perform the following operations:
   - Stopping

     Select the following services from the list of services in the Services window and run **Stop Service** for each one.
     a. NvPRO Performance Manager
     b. NvPRO Topology Adapter
     c. NvPRO ResourceManagerAPI Service
     d. MasterScope UMF Operations Manager_*n* (*n* is a service number)
     e. NvPRO Base Manager
     f. FTBase service

g. NvPRO Performance Database

h. Wfdb_nvsflowdb*n* (*n* is a service number)

i. Wfdb_nvalertdb*n* (*n* is a service number)

j. Wfdb_wfdb*n* (*n* is a service number)

- Starting

  Confirm that all the services have stopped, select the following services from the list of services in the Services window and run **Start Service** for each one.

  a. Wfdb_wfdb*n* (*n* is a service number)

  b. Wfdb_nvalertdb*n* (*n* is a service number)

  c. Wfdb_nvsflowdb*n* (*n* is a service number)

  d. NvPRO Performance Database

  e. FTBase service

  f. NvPRO Base Manager

  g. MasterScope UMF Operations Manager_*n* (*n* is a service number)

  h. NvPRO ResourceManagerAPI Service

  i. NvPRO Topology Adapter

  j. NvPRO Performance Manager

⚠ Caution

"Wfdb_wfdb*n*", " Wfdb_nvalertdb*n*", and " Wfdb_nvsflowdb*n*" are only exist when using internal database.

Linux Manager

Depending on the OS version, execute different commands.

- Red Hat Enterprise Linux 6

  Use the following commands to control the manager daemons.

  /etc/init.d/UMFOperationsManager_*n* { stop | start } (*n* is a service number)

  /etc/init.d/Framework.FTB { stop | start }

  - Stopping

    To stop the manager daemons, enter the following commands from the command line.

    ```
    # /etc/init.d/UMFOperationsManager_n stop
    # /etc/init.d/Framework.FTB stop
    ```

  - Starting

    To start the manager daemons, enter the following commands from the command line.

    ```
    # /etc/init.d/Framework.FTB start
    # /etc/init.d/UMFOperationsManager_n start
    ```

- Red Hat Enterprise Linux 7

  Use the following commands to control the manager daemons.

  systemctl { stop | start } UMFOperationsManager_*n* (*n* is a service number)

/etc/init.d/Framework.FTB { stop | start }

- Stopping

  To stop the manager daemons, enter the following commands from the command line.

```
# systemctl stop UMFOperationsManager_n
# /etc/init.d/Framework.FTB stop
```

- Starting

  To start the manager daemons, enter the following commands from the command line.

```
# /etc/init.d/Framework.FTB start
# systemctl start UMFOperationsManager_n
```

10.3 Registering Licenses

In Network Manager, usage permissions are verified through the license manager feature.

When the software is installed, a trial version license (product code = NetMgr-Trial) is automatically registered and all Network Manager functions can be used for 3 months. After that time, a valid license must be registered to continue using the software.

The following is the procedure for registering a valid license.

⚠ Caution

When moving from the trial version license (NetMgr-Trial) to the registered license, be careful not to exceed the conditions of use established by the registered license. For details, refer to "10.3.2 Registering a license key (page 760)".

1. Register the license key and obtain a codeword request code.

   For details, refer to "10.3.2 Registering a license key (page 760)".

2. Fill the codeword request code and other necessary information in the codeword request form, and then send the form as directed in the codeword request form.

3. Register the acquired codeword.

   For details, refer to "10.3.3 Registering a codeword (page 762)".

4. After the codeword is registered, apply the license in one of the following ways.

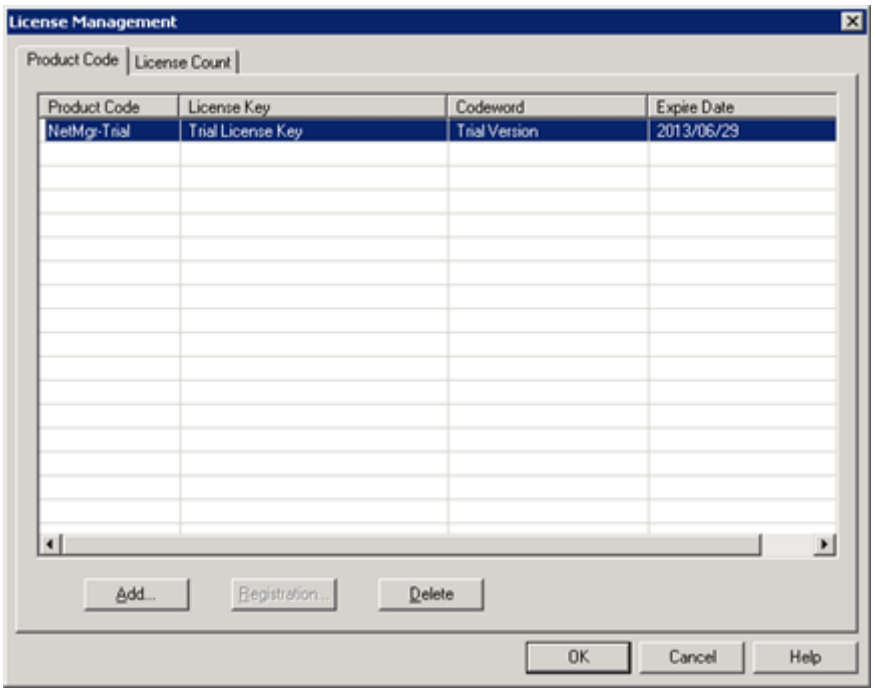
   - Restart the manager function.
   - Click **Reload** button in the "4.4.1.1 NetMgr License Manager dialog box (page 202)" to activate the license.

After registering the codeword for the registered license, delete the trial license key. If not deleting, the expiration warning box may appear each time a monitoring window is opened.

For how to delete licenses, refer to "10.3.4 Deleting a license (page 763)".

10.3.1 License Management window

License management is performed in the License Management window. To display the License Management window, in the main menu, select **Setting**>**License Management**.



- **Product Code** tab

  A list of currently issued license keys is displayed.

  - **Product Code**

    The product code is displayed.

  - **License Key**

    The license key is displayed.

  - **Codeword**

    The codeword status is displayed.

  - **Expire Date**

    The license expiry date is displayed.

- **Add** button

  Adds a new license key.

  For details, refer to "10.3.2 Registering a license key (page 760)".

- **Registration** button

  Registers a codeword for a license key for which a request has been submitted.

  For details, refer to "10.3.3 Registering a codeword (page 762)".

- **Delete** button

  Deletes the selected license.

  For details, refer to "10.3.4 Deleting a license (page 763)".

10.3.2 Registering a license key

Add a new license key. By following the procedure, the registered license key is recognized and the registered license will be valid.

Caution

1. When the license key for an authentic license is registered, the trial version license (NetMgr-Trial) becomes invalid. For this reason, registered configuration information that exceeds the conditions of use for the registered license must be deleted prior to registering the license key. Following are some precautions for each registered license type.

Registered license	Precautions
Basic license	• With the exception of the unlimited nodes basic license, there are a fixed number of devices that can be registered in Network Manager. If you exceed the registered number of devices permitted by the license, please delete device information (device icons) until you are no longer over the limit. • The NM license allows up to five devices. If you have assigned the NM license to six or more devices, you will need to change this so that the license is only assigned to five or fewer devices. • The RM license cannot be used. If these licenses have been assigned to any devices, they must be canceled for every device.
RM license	• The number of devices that can be allocated an RM license is fixed. If the number of devices assigned an RM license exceeds the fixed number, please cancel some of these RM Licenses until you are no longer over the limit.
NM unlimited license	(There are no precautions)
NP license	(There are no precautions)

   For how to delete the registered device, refer to "4.2.9.6 Deleting an icon (page 188)".

   For how to deallocate licenses, refer to "4.4.1.1 NetMgr License Manager dialog box (page 202)".

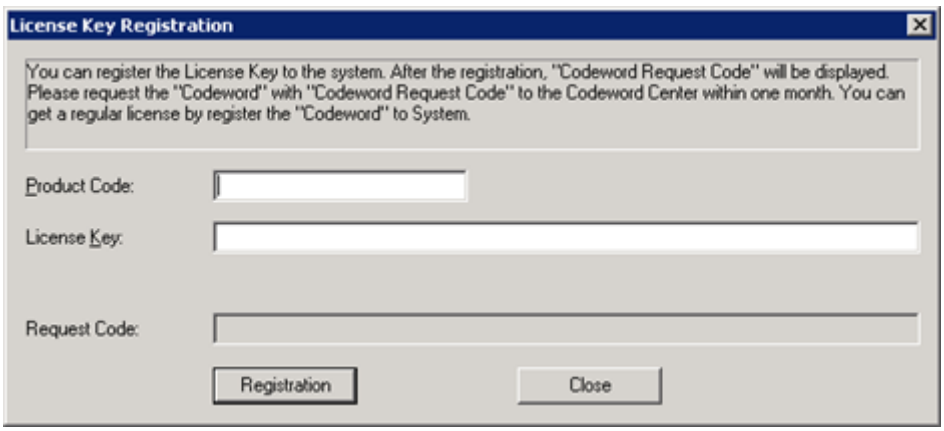
2. The precautions above also apply to deleting a registered license.
3. If the conditions set by the registered license are exceeded, the Network Manager functions will not be available for use and NetMgr License Manager dialog box cannot be displayed. To display the NetMgr License Manager dialog box, refer to "11.1.3 Displaying NetMgr License Manager dialog box under condition of license shortage (page 771)".

You must first change to the "configuration mode (page 27)".

1. Open the "10.3.1 License Management window (page 759)".

   In the main menu, select **Setting**>**License Management**.

2. Click **Add** button to open License Key Registration dialog box.



- **Product Code**

  Enter the product code.

- **License Key**

  Enter the license key.

- **Request Code**

  Displays the codeword request code.

- **Registration** button

  Click this button after entering the **Product Code** and **License Key** to display the **Request Code**.

- **Close** button

  Closes this dialog box.

3. In the **Product Code** box, type the product code for the Network Manager software you have purchased.
4. In the **License Key** box, type the license key for the Network Manager software you have purchased.
5. Click the **Registration** button.
6. The codeword request code is displayed in the **Request Code** box.

Caution

A codeword should be registered within 1 month of registering the license key. Registering the codeword in the system authenticates the license. For details, refer to "10.3.3 Registering a codeword (page 762)".

7. Open the "4.4.1.1 NetMgr License Manager dialog box (page 202)".

   Right-click the **NetworkView** icon and select **NetMgr License Management** menu.

8. Click **Reload** button and check that the number of remains does not exceed the total number.

   If the remains of license count exceeds the total number, deallocate unnecessary advanced functions licenses in the NetMgr License Manager dialog box or delete unnecessary icons until you are no longer over the limit.

10.3.3 Registering a codeword

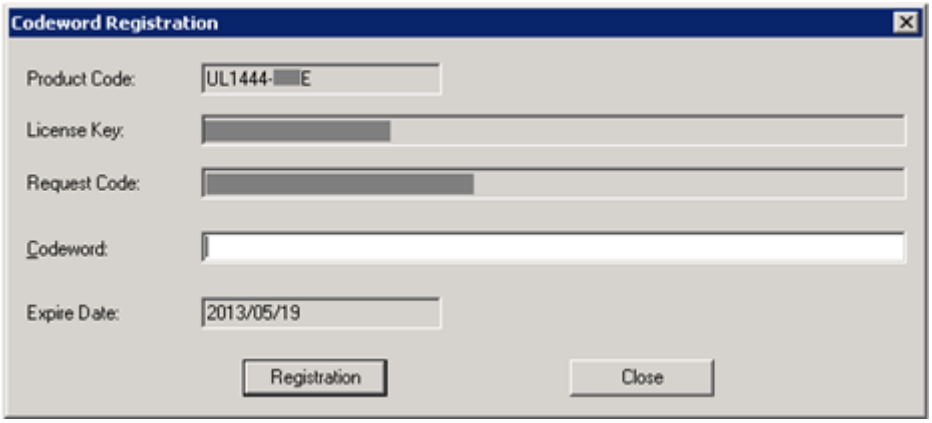
Register a codeword.

You must first change to the "configuration mode (page 27)".

1. Open the "10.3.1 License Management window (page 759)".

   In the main menu, select **Setting**>**License Management**.

2. Click **Registration** button to open Codeword Registration dialog box.



- **Product Code**

  The product code is displayed.
- **License Key**

  The license key is displayed.
- **Request Code**

  The request code is displayed.
- **Codeword**

  Enter the obtained codeword.
- **Expire Date**

  The license expiry date is displayed.
- **Registration** button

  To register the codeword, click this button after entering the codeword.
- **Close** button

  This closes the Codeword Registration window.

3. Type the obtained codeword in the **Codeword** box and click **Registration** button.
4. Reflect the license registration information to the system in one of the following ways.
   - Restart the manager function.
   - Click **Reload** button in the "4.4.1.1 NetMgr License Manager dialog box (page 202)".

After registering the codeword for the registered license, delete the trial license key (NetMgr-Trial) if it still remains. If not deleting, the expiration warning box may appear each time a monitoring window is opened.

For how to delete licenses, refer to "10.3.4 Deleting a license (page 763)".

10.3.4 Deleting a license

Delete a license.

You must first change to the "configuration mode (page 27)".

1. Open the "10.3.1 License Management window (page 759)".

   In the main menu, select **Setting**>**License Management**.
2. Select the license that you want to delete, and click **Delete** button.

3. In the confirmation dialog box, click **OK** button to delete the license.

10.3.5 Checking the number of license

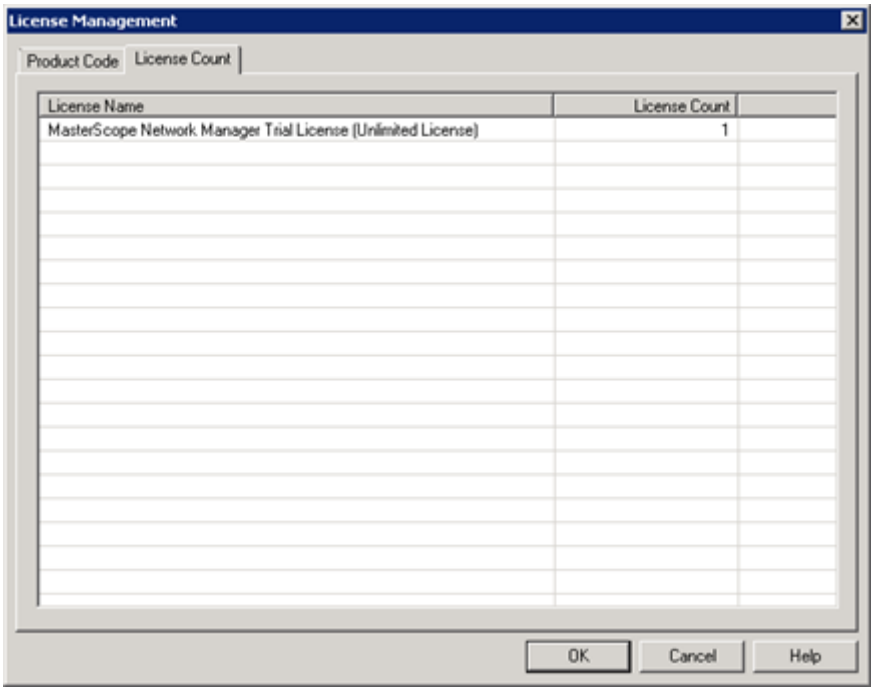
You must first change to the "configuration mode (page 27)".

1. Open the "10.3.1 License Management window (page 759)".

   In the main menu, select **Setting**>**License Management**.

2. Select **License Count** tab.

   The name of the available licenses will be displayed along with the number of licenses available for use.



10.4 Changing System Environment

10.4.1 Changing the IP address for the manager

When changing the IP address of the host installed with the manager function, be sure to perform the operation after stopping the manager and the connected monitoring terminal.

After the IP address has been changed on the manager host, start the manager services (daemons) starting and then start the monitoring terminal.

For details regarding stopping and starting the manager function, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

Changing the IP address of the manager has the following three effects.

1. Connection from the monitoring terminal

   Based on the **Manager hostname** that was set at the installation, the monitoring terminal performs name resolution processing (IP address discovery) and communicate with the manager. If the monitoring terminal can no longer connect to the manager after the IP address change, check for problems in the environment settings used for name resolution, such as the DNS and hosts file.

When the monitoring terminal function was installed, if you specified the manager IP address as the value of **Manager hostname**, follow the procedures of "10.4.3 Changing the destination of a monitoring terminal (page 766)".

When the manager function was installed, if you specified the IP address as the value of **Self hostname**, follow the procedures of "10.4.2 Changing the host name for the manager (page 765)".

2. Connection from IMS component

   When using the Web Console, it is necessary to update the configuration file (ims-conf.ini) of IMS component.

   - Configuration file

     On IMS *<%Data path%>*\conf\ims-conf.ini

   - Specification format

     ```
     noms.nvp.managers.<manager id>.ip-address = <IP address>
     ```

     For details, refer to the section *"Configuring to connect the products"* in *"MasterScope Network Management Web Console Getting Started Guide"*.

3. SNMP traps, system logs, and sFlow packet destinations on the monitored device side

   On the monitored device side, the manager IP address is specified as a configuration parameter used for sending SNMP traps, system logs, and sFlow packets.

   If the manager IP address was changed, you must change all the manager IP address values included in the settings used on the managed device side.

4. Source IP address for sending monitoring packets

   It is possible to explicitly specify the source IP address for sending monitoring packets from the manager.

   If the manager IP address has changed, check if this setting should be changed.

   For information regarding source IP address settings, refer to "10.4.5 Specifying a source IP address for monitoring packets (page 768)".

10.4.2 Changing the host name for the manager

Change the manager host name information that appears in the following Network Manager definition files.

When changing the host name of a manager host, be sure to stop the manager and the connected monitoring terminals before performing the operation. For details regarding stopping and starting the manager function, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

1. Stop the manager function.
2. Change the host name in SysMonMgr.ini to the new host name.

   Using the text editor, open *<On the manager, %installfolder%>*\Manager\sg\SysMonMgr.ini.

   ```
   [SelfNode]
   HostName=ManagerA
   ```

   Example: Changing the host name from Manager A to Manager B

```
[SelfNode]
HostName=ManagerA
```

->

```
[SelfNode]
HostName=ManagerB
```

Specify the host name up to 64 characters.

3. Change the host name in SysMonSvc.ini to the new host name.

   Using the text editor, open *<On the manager, %installfolder%>*\Manager\Svc\Common\sg\SysMonSvc.ini.

```
[UpperNode]
HostName=ManagerA
ServerPort=12530

[SelfNode]
HostName=ManagerA
```

Example: Changing the host name from Manager A to Manager B

```
[UpperNode]
HostName=ManagerA
ServerPort=12530

[SelfNode]
HostName=ManagerA
```

->

```
[UpperNode]
HostName=ManagerB
ServerPort=12530

[SelfNode]
HostName=ManagerB
```

Specify the host name up to 64 characters.

4. Change the host name in FwDlSvc.html to the new host name.

   Using the text editor, open *<On the manager, %installfolder%>*\Manager\sg\HttpServer\Root\FwDlSvc.html.

```
<PARAM NAME="UpperNode_HostName"      VALUE="ManagerA">
```

Example: Changing the host name from Manager A to Manager B

```
<PARAM NAME="UpperNode_HostName"
    VALUE="ManagerA">
```

->

```
<PARAM NAME="UpperNode_HostName"
    VALUE="ManagerB">
```

Specify the host name up to 64 characters.

5. Start the manager function.

Based on the **Manager hostname** that was set at the installation, the monitoring terminal performs name resolution processing (IP address discovery) and communicate with the manager.

Check for problems in the environment settings used for name resolution, such as the DNS and hosts file, and change the setting on the monitoring terminal side if necessary. For how to change the setting on the monitoring terminal side, refer to "10.4.3 Changing the destination of a monitoring terminal (page 766)".

10.4.3 Changing the destination of a monitoring terminal

Use the following procedure to change the destination manager of an installed monitoring window.

Caution

If the monitoring terminal is installed on the same machine that the manager is being run on, you cannot connect to managers on other machines.

1. Close the monitoring terminal.
2. Change the following location to the new manager name.

   <On the monitoring terminal, %installfolder%>\Svc\sg\SysMonSvc.ini

```
[UpperNode]
HostName=ManagerA
```

   Example: To change the destination node from Manager A to Manager B:

```
[UpperNode]
HostName=ManagerA
```

   ->

```
[UpperNode]
HostName=ManagerB
```

   Specify a manager name within 64 characters.
3. Open the monitoring terminal.

10.4.4 Changing a port

Use the following procedure to change a port number after installation.

To change the port number for the manager

1. Stop the manager function.
2. Using the text editor, *<On the manager, %installfolder%>*\Manager\sg\SysMonMgr.ini, and change the following location to the new manager name.

```
[SelfNode]
HostName=ManagerA
ServerPort=12520
SvcServerPort=12521
```

   Example: I you change the communication port with the monitoring terminal from 12521 to 12522.

```
[SelfNode]
HostName=ManagerA
ServerPort=12520
SvcServerPort=12521
```

   ->

```
[SelfNode]
HostName=ManagerA
ServerPort=12520
SvcServerPort=12522
```

3. Start the manager function.

⚠ Caution

If the communications port for the manager was changed, you must also change the port number for the monitoring terminal.

To change the port number for the monitoring terminal

1. Close the monitoring window.
2. Using the text editor, open *<On the monitoring terminal, %installfolder%>*\Svc\sg\SysMonSvc.ini and change the following location to the new manager name.

```
[UpperNode]
HostName=ManagerA
ServerPort=12521
```

Example: If you change the port number used for communication with the monitoring terminal from 12521 to 12522.

```
[UpperNode]
HostName=ManagerA
ServerPort=12521
```

->

```
[UpperNode]
HostName=ManagerA
ServerPort=12522
```

3. Open the monitoring terminal.

10.4.5 Specifying a source IP address for monitoring packets

If Network Manager is installed on a machine with more than one NIC, fix the source IP address (IPv4 and IPv6) to be used for SNMP (both IPv4 and IPv6), ICMPv4, and ICMPv6 communication by configuring the source IP address (IPv4 and IPv6) information in the `nvisord.cf` file.

Use this when instructing monitored devices to only respond to communication from a specific IP address.

1. Stop Manager.
2. Open the following file and specify the IPv4 address or IPv6 address that you want to fix.

   <On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\local\nvisord.cf

   ```
   SrcIpAddress: <IPv4 address>
   SrcIpv6Address: <IPv6 address>
   ```

   If SrcIpAddress or SrcIpv6Address key does not exist, create one.

   Tip

   If SrcIpAddress and SrcIpv6Address are omitted (as they are by default), the source IP address will be set according to the routing control method used by the OS.

3. Start Manager.

Chapter 11. Troubleshooting

Contents

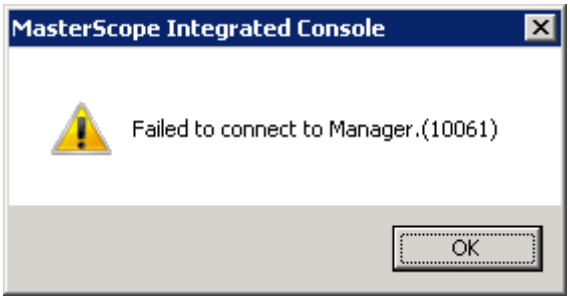
11.1 Errors in Starting the Monitoring Window 770
11.2 Errors in Operations 772
11.3 Errors and Precautions for Alert Management 774
11.4 Coexisting with Other Software 776

11.1 Errors in Starting the Monitoring Window

11.1.1 The error dialog box is displayed when starting the monitoring window

This section describes the error dialog boxes that are displayed when the monitoring window is launched.

11.1.1.1 Failed to connect to Manager.(10061)



Cause

- The manager is not running. Start the manager.

  For details, refer to "10.2 Starting and Stopping the Manager Function (page 757)".
- The specified connection destination manager for the monitoring window is incorrect. Set the correct connection destination.

  For details, refer to "10.4.3 Changing the destination of a monitoring terminal (page 766)".
- The port numbers for the manager and the monitoring window do not match. Enter matching port numbers.

  For details, refer to "10.4.4 Changing a port (page 767)".

11.1.1.2 MasterScope Network Manager is not available. Necessary license is insufficient.

Cause

- There is no valid license. Obtain and register a license key or codeword.

  For details, refer to "10.3 Registering Licenses (page 759)".
- The number of registered nodes exceeds the license upper limit. In order to resolve the excess of the node licenses, delete unnecessary nodes from the map.

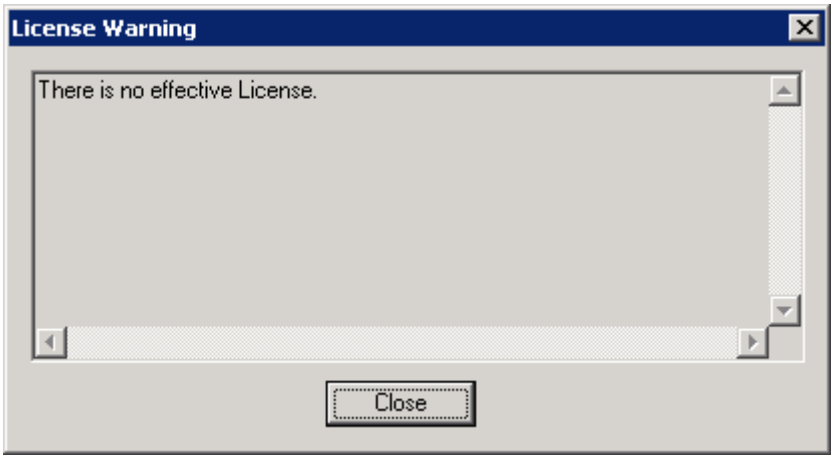
  For details regarding the number of allocatable node license, refer to "4.4 Managing the Advanced Functions License (page 201)". For details regarding deleting the nodes, refer to "4.2.9.6 Deleting an icon (page 188)".
- The number of allocated advanced function licenses exceeds the license upper limit. In order to resolve the excess of the advanced function licenses, deallocate unnecessary advanced licenses in the NetMgr License Manager dialog box.

For details regarding allocating advanced licenses, refer to "4.4 Managing the Advanced Functions License (page 201)".

Caution

If the **NetworkView** icon is not displayed and the NetMgr License Manager dialog box cannot be opened due to excess of the license, refer to "11.1.3 Displaying NetMgr License Manager dialog box under condition of license shortage (page 771)".

11.1.1.3 There is no effective License



Cause

- There is no valid license. Obtain and register a license key or codeword.

  For details, refer to "10.3 Registering Licenses (page 759)".

11.1.2 The tree view is not displayed hierarchically

If the tree view is not displayed hierarchically when the monitoring window is started, consider the following possible cause.

Cause

- There is no valid license. Obtain and register a license key or codeword.

  For details, refer to "10.3 Registering Licenses (page 759)".

11.1.3 Displaying NetMgr License Manager dialog box under condition of license shortage

If the upper limit of the registered license is exceeded, the Network Manager functions will not be available for use and the NetMgr License Manager dialog box cannot be displayed.

To operate NetMgr License Manager dialog box under the conditions that the upper limit of the registered license is exceeded, restart the manager function. After restarting the manager function, **NetworkView** icon is displayed only when the monitoring terminal is started up at the first time, and you can operate the NetMgr License Manager dialog box.

For details regarding restarting the manager function, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

⚠ Caution

To enable the monitoring terminal to start up just one time by restarting the manager, the valid license must be registered. If the there is no registered license other than a trial version license, the monitoring terminal cannot be started up even if the manager function was restarted.

11.2 Errors in Operations

11.2.1 The menu is not accessible (it is dimmed)

The various GUI controls in the Network Manager monitoring window, such as menus and buttons, become unavailable under the following conditions.

- Monitoring window operation mode

  There are some items in the Network Manager functions that cannot be used unless the system is in configuration mode. These items will appear grayed out when the operation mode for the monitoring window is set to monitoring mode.

  For details regarding the operation mode of the monitoring terminal, refer to "2.5 Operation Modes (page 27)".

- Logged-in user rights

  The three types of access rights recognized by Network Manager for the logged-in user are Reference Authority, Operation Authority and Configuration Authority. The order of strength of each of these rights are Configuration Authority>Operation Authority>Reference Authority.

  Some Network Manager functions require Operation Authority and Configuration Authority user rights.

  If you currently have Reference Authority and Operation Authority user rights, these functions (menus and buttons) will not be available.

  All functions that can only be operated in configuration mode require Configuration Authority.

  For details regarding user authority, refer to "4.1 Managing Users and Groups (page 101)".

- Network Manager Licenses

  Some Network Manager functions require extended function licenses. If the necessary extended function licenses are not applied to a device, these functions (menus) will not be available.

  For details regarding the advanced function license, refer to "1.2 Network Manager Licenses (page 12)".

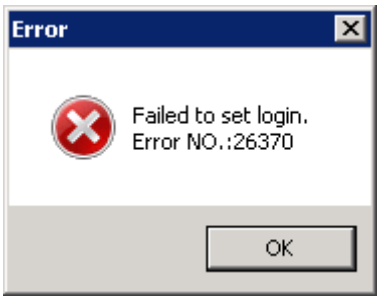
- Other conditions

  Menus and buttons may also be unavailable as a result of the status of the device at the time.

  For example, even if a user with Configuration Authority is operating in configuration mode and right-clicks a **device** icon selecting **Configuration Management**>**Monitoring-mode**>**ON** or **OFF** will be unavailable, depending on the current status of the monitoring mode for that device.

11.2.2 The error dialog box is displayed when setting device password

If the error dialog box below is displayed when setting a device password, consider the following potential causes.



Cause

- It is possible that icon properties are not set correctly. In particular, there is a high possibility that correct values are not set for the software version.

11.2.3 Monitoring terminal is disconnected from manager after leaving it without operation

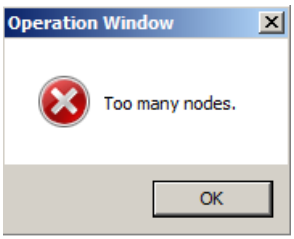
If the monitoring terminal is disconnected from the manager after leaving the terminal without operation, consider the following potential causes.

Cause

In the Power Options of Windows control panel, confirm **System standby** and **System hibernates** are set to "Never".

11.2.4 The error dialog box is displayed when executing menu with many icons selected

The error dialog box below might be displayed when selecting a lot of icons and executing the menu item (for example, **Configuration Management**>**Update Property**). Consider the following potential causes.



Cause

- Cannot execute the process because too many icons are selected.

Solution

- Reduce the number of selected icons and try again.

11.3 Errors and Precautions for Alert Management

11.3.1 No alert display for SNMP traps

If no alerts are displayed for any SNMP traps

If another application receiving SNMP traps is installed on the same machine as Network Manager manager function, trap receipt failures may occur.

This is due to the fact that when the applications attempt to obtain access to the UDP port used to receive the traps, only one of the applications can get access, and the other application trying to obtain access fails to obtain access to the port used for receiving traps.

In the manager function of Network Manager for Windows, SNMP trap receipt in both applications is set up to use the Windows SNMP Trap Service, which makes it possible to receive SNMP traps in both applications.

When using the SNMP Trap Service in Network Manager, refer to "11.4.1 Using the Windows SNMP Trap service (page 776)" to configure the settings.

⚠ Caution

The SNMP Trap Service does not support SNMPv3 and IPv6 protocol. For this reason, using the SNMP Trap Service makes it impossible to receive SNMPv3 traps and SNMPv1/v2c traps over the IPv6 Protocol.

If alerts are not displayed for SNMPv3 traps only

1. If alerts issued by devices with authentication and encryption enabled, are not displayed for SNMPv3 traps only, check the following.
   - The settings for the node SNMPv3 properties may have been configured incorrectly. In the icon properties, check items such as the "User Name", "Engine ID", "Security Level", "Authentication Protocol", "Privacy Protocol", "Authentication Password", and "Privacy Password".
   - If the IP address of the device was changed, the Engine ID may have been changed. If the Engine ID of the received traps and the Engine ID configured in the node properties are different, traps are not received. In this case, use device icon properties to configure an appropriate IP address and then run the **Update Property** menu to get the most current Engine ID. For more information about updating device information, refer to "4.2.7 Updating device information via a network (page 179)".
2. It may be that device icons with the same IP addresses have been registered and the Engine IDs configured for the respective nodes are different. You can use the following procedures to fix this problem.
   a. In the icon properties, look for devices configured with the same IP address.
   b. Use device icon properties to check the settings under the SNMPv3 tab and make sure the settings of all the device icons are the same.
   c. Run a **Update Required Property** menu to update the Engine IDs.

If alerts are not displayed only for SNMPv3 informs

1. If alerts are not displayed for SNMPv3 informs, check the following.

- If the engine ID of the SNMP inform differs from the **EngineID(v3)** setting of **SNMP Trap Parameter** in the Environment Setting dialog box, the inform will not be received. In this case, make the **EngineID(v3)** setting of the Environment Setting dialog box consistent with the remote engine ID specified in the monitored device. For details about the Environment Setting dialog box, refer to "4.8 Configuring the Operating Environment for the Fault Management (page 233)".

2. If alerts are not displayed for the SNMPv3 inform issued by a device that enabled either authentication or encryption, check the following.
   - Settings regarding SNMPv3 might not be correctly specified in the node properties. Check the user name, security level, authentication protocol, encryption protocol, authentication password, and encryption password of the device properties.
3. If alerts are not displayed for the SNMPv3 inform issued by a specific device, check the following.
   - SNMPv3 has a mechanism to establish the validity period of a message to enhance security by synchronizing the time between the sender and receiver of the packet transmission. If this time synchronization cannot properly be executed due to any device specification, you cannot receive an SNMPv3 inform from the device. For details, check with the device vendor.

11.3.2 The system logs are not displayed as alerts

In Network Manager, when syslogs with a severity of WARNING or higher are received an alert is displayed.

Syslogs that are at the NOTICE level or lower are discarded.

11.3.3 Garbled character strings in SNMP traps

When an SNMP trap is received, the message content may be garbled.

Follow the steps below to resolve this issue.

Cause

Possible causes are as follows:

- The data type definition for the garbled MIB (AMIB definition file) has not been incorporated into this product, or the data types for varBindList values have not been defined correctly in the trap definition.
- The node's **SNMP Character Code** icon property has not been set properly.

Solution

- Incorporate the MIB file (AMIB definition file) that defines the data type of the garbled MIB to Network Manager, or specify an appropriate type for varBindList of the trap definition on the Trap Definition Management window.

  For how to incorporate the MIB file, refer to "7.4 Adding MIBs (page 648)".

  For how to specify the data type, refer to "4.11.5.1 Add/Edit/Properties of Trap Definition dialog box (page 282)".
- If no value is specified for the node's **SNMP Character Code** icon property, specify **Unicode (UTF-8)** for **SNMP Character Code** and check to see that the characters are not garbled.

Tip

The OctetString type MIB cannot be displayed in hexadecimal correctly even if the MIB file (AMIB definition file) defining this MIB type is incorporated in Network Manager.

From the Trap Definition Management window, specify OctetString for the varBindList type that defines the relevant trap, or set up the relevant MIB so that it can be displayed in hexadecimal.

For instructions on how to display the MIB definition in hexadecimal, refer to "7.4.1.4 MIB Definition hexadecimal notation setting procedure (page 655)".

11.3.4 Precautions when a large number of alerts are received

Depending on the settings of the state monitoring or the threshold monitoring of performance data, a large number of alerts may be issued at the same time. For example, the manager is monitoring all ports of the entire monitored devices with an extremely low threshold value.

The maximum number of alerts that Network Manager can store is one hundred thousand. If Network Manager receives about one million alerts at a time, the entire function of Network Manager may not work properly. This is because the amount of information to be received is limited to a certain amount in order to avoid infinite increase of consuming memory in the program when storing the information in the NvPRO Base Manager service.

Method to confirm occurrence of the symptom

If the following symptoms are confirmed after alerts exceeding a million occur at the same time, the problem will occur.

- New alert information is not displayed in the Alert Management window.
- A new icon can not be registered.

Solution

Restart the manager function.

11.4 Coexisting with Other Software

11.4.1 Using the Windows SNMP Trap service

Two methods are available for receiving SNMP traps in the manager in the Windows version of Network Manager.

- The SNMP module within Network Manager receives the SNMP trap.
- SNMP traps are received through the "SNMP Trap Service" in Windows.

The default setting in Network Manager uses the Network Manager SNMP module.

This section describes how to change the settings to use the "SNMP Trap Service".

The benefits of using the SNMP Trap Service

- It can coexist with other APs receiving SNMP traps.

Benefits of using the Network Manager SNMP module:

- Even if SNMP traps are continuously received, there are few that are left unfinished.

Caution

When using SNMP Trap Service, The SNMPv3 traps and traps on IPv6 cannot be received because SNMP Trap Service does not support these protocol.

1. Open the following file on the manager machine.

   The storage location:

   <On the manager, %sharedfolder%>\Manager\sg\NvPRO\NVWORK\local\nvisord.cf

   If nvisord.cf does not exist, create a new one.

2. Write the following in the nvisord.cf file.

   - When using the SNMP Trap Service:

     ```
     UseMgmtApi:True
     ```

   - When using the Network Manager module:

     ```
     UseMgmtApi:False
     ```

     (You can also delete the "UseMgmeApi" line.)

3. Add the dependency on SNMP Trap Service.

   a. Open the command prompt (terminal).

   b. Change directory to *<On the manager, %installfolder%>*\Manager\bin, and then execute a command to set the dependence relation of SNMP Trap Service (NvPRODependSnmpService.exe) as follows.

      - When using the SNMP Trap Service:

        ```
        > NvPRODependSnmpService.exe add
        ```

      - When using the Network Manager module:

        ```
        > NvPRODependSnmpService.exe del
        ```

      Specify add or del to an argument. Arguments are not case-sensitive.

   Caution

   a. In the cluster system, execute this command on both the active host and the standby host.

   b. Execute this command as an administrator.

   c. After executing the command, a success or failure message is displayed. The contents of messages are as follows.

	Message	Details
1	SUCCESS : Set dependence SNMP Trap Service.	Succeeded in adding the dependency on SNMP Trap Service.
2	FAILED : Not exist NvPRO Base Manager Service.	NvPRO Base Manager service does not exist. Network Manager might not be installed. Install Network Manager manager function.
3	FAILED : Not exist SNMP Trap Service.	SNMP Trap Service does not exist. SNMP Trap Service might not be installed. Install

	Message	Details
		SNMP Trap Service included with Windows.
4	FAILED : Set dependence SNMP Trap Service.[error code]	Failed to add the dependency on SNMP Trap Service.
5	SUCCESS : Deleted dependence SNMP Trap Service.	Succeeded in deleting the dependency on SNMP Trap Service.
6	FAILED : Deleted dependence SNMP Trap Service.[error code]	Failed to delete the dependency on SNMP Trap Service.
7	ERROR : arguments error.	Illegal argument is specified. You can specify only `add` or `del`.

4. Restart "NvPRO Base Manager" service and the services depending on this service.
5. Restart "MasterScope UMF Operations Manager_*n*" service for Network Manager and the services depending on this service.

11.4.2 Sharing the SYSLOG port with other software

This software uses a SYSLOG port (514/udp) to receive system logs from devices. If you need to share the port with other devices that receive system logs, or a Linux syslogd, it will be necessary to perform one of the following procedures.

- Change the port used to receive system logs in this software to something other than 514/udp. (The syslog monitoring function port for these products cannot be closed.)
- Change the port used to receive system logs by other products to something other than 514/udp, or close the port for receiving system logs.

⚠ Caution

If you change the syslog port to a setting other than 514, you must also change the setting on the syslog sender side.

The 514/udp port is not the default port used by Linux syslogd for monitoring. As long as you do not change the syslogd settings, this system will not create a conflict with the system log monitoring function in Network Manager.

- When changing Network Manager settings:

  To change the syslog reception port used by the Network Manager to something other than 514/udp, perform the following steps.

  1. Change the following setting file name. Delete the end of ".org".

     `<On the manager, %installfolder%>\Manager\sg\NvPRO\SyslogManager\NvPROSyslogManagerMgr.ini.org`

  2. Change the value of socketBindPort to something other than 514.

     ⚠ Caution

     Changing the settings to a setting other than socketBindPort is not supported.

  3. Restart the manager function.

- When changing settings in other software programs:

For information on changing the port used to receive system logs in other software program to something other than 514/udp, or closing the actual syslog receiving port, refer to the user manual for that software.

Tip

Changing syslogd settings in Linux:

Closing the syslog port	Changing the syslog port to something other than 514
Change `/etc/sysconfig/syslog` to `before: SYSLOGD_OPTIONS="-m 0 -r"` `after : SYSLOGD_OPTIONS="-m 0"` and then restart syslogd (execute `/etc/init.d/syslog restart`).	Change "syslog 514/udp" of `/etc/services` to something other than514, and restart syslogd (`/etc/init.d/syslog restart`).

11.4.3 TFTP server competition with other software

If the TFTP server built into Network Manager and the TFTP server of other software compete, and the external software TFTP server cannot be used through Network Manager, it is possible to use the TFTP server built into Network Manager through external software.

The following is the method for using the TFTP server built

- In the following file, *<On the manager, %sharedfolder%>*`\Manager\sg\NvPRO\RMAPI\nvrmapi.ini` change "tftpResident=0" to "tftpResident=1" and save.
- Restart the NvPRO ResourceManagerAPI Service.
- At this point, the TFTP server built into Network Manager will be running at all times, and may be used by external software.
- tftproot is *<On the manager, %sharedfolder%>*`\Manager\sg\NvPRO\RMAPI\dat\tftp\`. It is possible to get or put a file, and to create a new file.
- Because a file with one of the following names is used by Network Manager, a file with one of these names cannot be used by external software: tftpxxxx.tmp/ tftpdxxxx.tmp (x: 12 digits, numerals 0-9)
- Because it is possible that use by external software could have effects on Network Manager operations, it is necessary to thoroughly test the entire system before such use.

Appendix A. Linking with MasterScope SystemManager G

Network Manager can send alert messages to coexisting MasterScope SystemManager G (hereafter referred to as SystemManager G) when SystemManagerG is installed in the same directory.

To display Network Manager alert messages in the Business view provided by SystemManager G, configure the filter definition settings for Network Manager alert messages. For detailed settings, refer to the documentations for SystemManager G.

Tip

The filter definition files below are provided by default. Import additional files as required.

<On the monitoring terminal, %installfolder%>\Svc\knowledge\NetworkManager.txt

A.1 Alert Message Format

The following is the format of messages reported in SystemManager G by Network Manager.

Category	Network	
Application	Network Manager	
Object	Value	Description
	NvPro System	Indicates a message issued by the Network Manager system.
	NvPro SNMP Trap	Indicates a SNMP trap message.
	NvPro Syslog	Indicates a syslog message.
	NvPro Alert	Indicates a state monitoring alert message, or aggregated alert.
Message ID	The ID of an event managed in Network Manager.	
Severity	The severity level specified in the Network Manager monitoring settings.	
Node	The name of the node for which an alert was detected in Network Manager.	
Message Text	Detailed contents are explained below.	

The format of message text depends on the alert type (Object value). The format details for different alert types are below.

The message format can be customized. For details, refer to "A.3 Customizing the Message Text Format (page 782)".

The values managed in the Network Manager Alert Management window fill the parameters (character strings enclosed by a $) listed in the format.

1. Messages indicating an SNMP trap (NvPro SNMP Trap)

```
[ID=$ID$]$Summary$(D=$Detail$)(IP=$IP$)(Enterprise=$Enterprise$)
(Gen=$Gen$)(Spec=$Spec$)
```

Parameter	Description	Comments
ID	The ID number managed in alert management of Network Manager.	
$Summary$	Alert summary.	Only the first 32 characters are reported. If null value, "none" is reported. 1)

Parameter	Description	Comments
$Detail$	Alert details.	Only the first 128 characters are reported. If null value, "none" is reported. 1)
IP	The IP address of the corresponding node.	Only the IPv4 address is reported.
$Enterprise$	The Enterprise value for received SNMP traps.	
Gen	The Generic-Trap value for received SNMP traps.	
$Spec$	The Specific-Trap value for received SNMP traps.	

1) When customizing the message format, the character limit for each parameter is not applied.

Message text example:

```
[ID=9]linkUp(D=Interface 0 was link-up.)(IP=10.1.1.1)
(Enterprise=1.3.6.1.4.1.119.2.2.4.4.18.3)(Gen=6)(Spec=1)
```

2. Messages indicating a syslog (NvPro Syslog)

[ID=ID]$Summary$(D=$Detail$)(IP=IP)(A=$Action$)(F=$Facility$)(Sev=$Severity$)(K=KID)

Parameter	Description	Comments
ID	The ID number managed in alert management of Network Manager.	
$Summary$	Alert summary.	Only the first 32 characters are reported. If null value, "none" is reported. 1)
$Detail$	Alert details.	Only the first 128 characters are reported. If null value, "none" is reported.
IP	The IP address of the corresponding node.	Only the IPv4 address is reported. 1)
$Action$	Always filled with "none."	
$Facility$	The syslog Facility value (decimal notation)	
$Severity$	The syslog Severity value	
KID	Always filled with "0."	

1) When customizing the message format, the character limit for each parameter is not applied.

Message text example:

```
[ID=1114]The syslog (Error) occurred.
(D=<3> PPOE[008]: Received packet with bad PacketLen 999,
FastEthernet)(IP=10.1.1.1)(A=none)(F=23)(Sev=Error)(K=0)
```

3. Other messages (NvPro System, NvPro Alert)

```
[ID=$ID$]$Summary$(D=$Detail$)(IP=$IP$)(Snd=$Snd$)(M=$MID$)
```

Parameter	Description	Comments
ID	The ID number managed in alert management of Network Manager.	

Parameter	Description	Comments
$Summary$	Alert summary.	Only the first 32 characters are reported. If null value, "none" is reported. 1)
$Detail$	Alert details.	Only the first 128 characters are reported. If null value, "none" is reported. 1)
IP	The IP address of the corresponding node.	Only the IPv4 address is reported.
Snd	Alert publisher information.	
MID	Alert message definition ID.	

1) When customizing the message format, the character limit for each parameter is not applied.

Message text example:

```
[ID=9]Communication failure(D=Failed to communicate with the node)
(IP=10.1.1.1)(Snd=IcmpUpDown)(M=198)
```

A.2 Character Limit for Messages

There is an upper limit on the number of characters that can be handled by SystemManager G in a single message. If the length of text in alert overview or details information in Network Manager is too long, there is notification that the excess characters have been discarded.

For example, if the SNMP trap definition is set to display all varBind list information in the alert details (specified as "%all"), then the contents of the notification message will be cut off depending on the length of the varBind list information. In such a case, customize the format of message text. When customizing the message format, the character limit for each parameter is not applied, and each parameter can be sorted in any order. For these reasons, you can include necessary information in the message text reliably. However, note that the character limit for whole message text is still limited to 1,024 characters and part of the message exceeds the maximum length is truncated.

For details regarding message format customization, refer to "A.3 Customizing the Message Text Format (page 782)".

A.3 Customizing the Message Text Format

By customizing the message format, the character limit for each parameter is not applied, and each parameter can be hidden or sorted flexibly.

1. Copy the following file and rename the file as `AlertActionMsgFormat.ini`.

   <On the manager, %installfolder%>`\Manager\sg\NvPRO\AlertActionMsg\AlertActionMsgFormat.ini.org`

2. Edit this file as follows according to an alert type.

   - SNMP TRAP

     Delete "#" at the beginning of the following lines. To change output order or output contents, edit "ORDER=" parameter value.

     ```
     #[SNMP TRAP]
     #ORDER=Summary,D,IP,Enterprise,Gen,Spec
     ```

   - SYSLOG

Delete "#" at the beginning of the following lines. To change output order or output contents, edit "ORDER=" parameter value.

```
#[SYSLOG]
#ORDER=Summary,D,IP,A,F,Sev,K
```

- OTHER

  Delete "#" at the beginning of the following lines. To change output order or output contents, edit "ORDER=" parameter value.

```
# [OTHER]
#ORDER=Summary,D,IP,Snd,M
```

3. Save the edited file and restart the manager.

   For how to restart the manager, refer to "10.2 Starting and Stopping the Manager Function (page 757)".

A.4 Sending a Message as an SNMP Trap

Transfer messages reported in the SystemManager G Business view to other SNMP managers using the `NvPROTrapSend` command provided in Network Manager.

SNMP trap send settings are configured in the report settings (action report) for the category filter definitions registered in Business view. For information regarding the report settings in Business view, refer to the documentations for SystemManager G.

This section shows the report settings (action report) parameters in Business view. For information regarding each of the `NvPROTrapSend` command parameters, refer to "9.8 Command for Sending SNMP Traps (page 717)".

- Configuring action report settings for sending SNMP traps

Action Report Parameter Name	Setting Information
Command	*<On the manager, %installfolder%>*\bin\NvPROTrapSend
Work Directory	*<On the manager, %installfolder%>*\bin
Option	-ip *ipaddress* -c "MasterScope" -o1 "$GENERATEDDATE$ $GENERATEDTIME$" -o3 "$SEVERITY$" -o4 "$NODE$ message" -o5 "< $APPLICATION$> $MESSAGETEXT$" (enter on one line without line breaks)

- Option specification details

  -ip *ipaddress*

  Specifies an SNMP Manager IPv4 address for the SNMP trap destination in decimal notation.

  -c "MasterScope"

  Specifies an SNMP trap community name in a maximum of 16 single-byte alphanumeric characters. Specify "MasterScope" here.

  -o1 "$GENERATEDDATE$ $GENERATEDTIME$" :

  Specifies the date and time when an alert is received using the replacement strings below.

  $GENERATEDDATE$: Replaced with the date of the message.

$GENERATEDTIME$: Replaced with the time of the message.

-o3 "$SEVERITY$"

Specifies the severity level of an alert using the replacement string below.

$SEVERITY$: Replaced with the message severity level.

-o4 "$NODE$ *message*"

Specifies the message overview text using the replacement string below to specify node name information.

$NODE$: Replaced with the message node name.

-o5 "<$APPLICATION$> $MESSAGETEXT$"

Specifies the message details using the replacement strings below to specify the message application information and message text.

$APPLICATION$: Replaced with message application name.

$MESSAGETEXT$: Replaced with message text.

Appendix B. Icons

List available icons when creating a network map.

B.1 Map

The following icons belong to the map group:

Icon Type	Image	Description
map		General map
city		City
factory		Factory
building		Building
floor		Floor in the building
wlan_map		Wireless LAN environment
corsmap		Submap

B.2 Node

The following icons belong to the node group:

1. Router/Switch

Icon Type	Image	Description
IP8800_S2200		IP8800/S2200 series
IP8800_S2400		IP8800/S2400 series
IP8800_S2430-24T		
IP8800_S2430-24T2X		
IP8800_S2430-48T		
IP8800_S2430-48T2X		

Icon Type	Image	Description
IP8800_S2500		IP8800/S2500 series
IP8800_S2530-48P2X		
IP8800_S3600		IP8800/S3600 series
IP8800_S3630-24P		
IP8800_S3630-24S2XW		
IP8800_S3630-24T		
IP8800_S3630-24T2X		
IP8800_S3630-48T2XW		
IP8800_S3630-48TW		
IP8800_S3640-24S2XW		
IP8800_S3640-24SW		
IP8800_S3640-24T		
IP8800_S3640-24T2XW		
IP8800_S3640-24TW		
IP8800_S3640-48T2XW		
IP8800_S3640-48TW		
IP8800_S3650-24T6XW		
IP8800_S3650-20S6XW		
IP8800_S3650-48T4XW		
IP8800_S3660-24T4XW		

Icon Type	Image	Description
IP8800_S3660-48T4XW		
IP8800_S3660-48X4QW		
IP8800_S3660-48XT4QW		
IP8800_S3800		IP8800/S3800 series
IP8800_S3830-44XW		
IP8800_S3830-44X4QW		
IP8800_S4630-4M		IP8800/S4600 series
IP8800_S6300		IP8800/S6300 series
IP8800_S6304		
IP8800_S6308		
IP8800_S6600		IP8800/S6600 series
IP8800_S6604		
IP8800_S6608		
IP8800_S6700		IP8800/S6700 series
IP8800_S6708		
IP8800_S8308		IP8800/S8300 series
IP8800_S8600		IP8800/S8600 series
IP8800_S8608		
IP8800_S8616		
IP8800_S8632		

Icon Type	Image	Description
IP8800_SS1200		IP8800/SS1200 series
IP8800_SS1230-24P2C		
IP8800_SS1230-24T2C		
IP8800_SS1230-48T2C		
IP8800_SS1240-24P2C		
IP8800_SS1240-24T2C		
IP8800_SS1240-48T2C		
IP8800_S_ALAXDefault		IP8800 (ALAXALA)
IP8800_S		IP8800/S300, S400 series
IP8800_S301		
IP8800_S302		
IP8800_S401		
IP8800_S402		
IP8800_S403		
IP8800_R		IP8800/R series
IP8800_R401		
IP8800_R402		
IP8800_R403		
QX-R		QX series

Icon Type	Image	Description
QX-S		
QX-S_IEEE8021X		
QXS808E		QX-S800E series
QXS810EP-PW		
QXS816EP		
QXS816EP-PW		
QXS824EP		
QXS1008GT-2G		QX-S1000G series
QXS1008GT-2G-PW		
QXS1016GT-4G		
QXS1016GT-4G-PW		
QXS1024GT-4G		
QXS1024GT-4G-PW		
QXS1048GT-4G		
QXS2008		QX-S2000 series
QXS2017		
QXS2026		
QXS2108		QX-S2100 series
QXS2110P-I		
QXS3020TP		QX-S3000 series

Icon Type	Image	Description
QXS3026		
QXS3026C		
QXS3026E		
QXS3026T		
QXS3050		
QXS3109T		QX-S3100 series
QXS3109TP		
QXS3117T		
QXS3126C		
QXS3126T		
QXS3209TP		QX-S3200 series
QXS3218TP		
QXS3226TP		
QXS3526		QX-S3500 series
QXS3528P		
QXS3552P		
QXS3628P		QX-S3600 series
QXS3628TP		
QXS3652P		

Icon Type	Image	Description
QXS3710P		QX-S3700 series
QXS3828TP-BS		QX-S3800 series
QXS3852TP-BS		
QXS4052P		QX-S4050 series
QXS5012G		QX-S5000 series
QXS5012T		
QXS5024G		
QXS5116P		QX-S5100 series
QXS5124P		
QXS5126P-PW		
QXS5148P		
QXS5224GP-4X		QX-S5200G series
QXS5224GT-4X		
QXS5224GT-4X-PW		
QXS5248GT-4X		
QXS5248GT-4X-PW		
QXS5516		QX-S5500 series
QXS5526P		
QXS5526P-D		
QXS5526T		

Icon Type	Image	Description
QXS5550P		
QXS5524GT-4X1C		QX-S5500G series
QXS5524GT-4X2Q		
QXS5524GP-4X1C		
QXS5548GT-4X1C		
QXS5548GT-4X2Q		
QXS5625P		QX-S5600 series
QXS5625T		
QXS5649P		
QXS5732P		QX-S5700 series
QXS5756P		
QXS5828T		QX-S5800 series
QXS5948GT-4X2Q		QX-S5900 series
QXS5948XP-4Q		
QXS5948XT-4Q		
QXS6503		QX-S6500 series
QXS6506		
QXS6502XG		QX-S6500-XG series
QXS6503XG		
QXS6506XG		

Icon Type	Image	Description
IX		IX series
IX1000		IX1000 series
IX2003		IX2000 series
IX2004		
IX2005		
IX2010		
IX2015		
IX2025		
IX2105		
IX2106		
IX2207		
IX2215		
IX3010		IX3000 series
IX3015		
IX3110		
IX3315		IX5000 series
IX5000		
IX5005		
IX5010		
IX5500		IX5500 series

Icon Type	Image	Description
IX5503		
IX5504		
PF5200		PF series
PF5220		
PF5240F-48T4XW		
PF5240R-48T4XW		
PF5248		
PF5459-48GT-4X2Q		
PF5459-48XP-4Q		
PF5459-48XT-4Q		
PF5820		
PF6800		
vRouter		
N8406-005A		Blade server internal switch
swblade		
BF210_24		BF series
SV7000_TP		SV7000 series
SV8300		SV8000 series
SV8500		
SV9100		SV9000 series

Icon Type	Image	Description
SV9300		
SV9500		
WA1020		WA series
WA1500		
WA1510		
WA1511		
WA2020		
WA2021		
WA2600		
WA2610-AP		
WA2611-AP		
WL_Controller		WL series
WL2012		
WL2024		
WL3006-B		
WL3012		
WL3025		
WL3036		
WL3036r		
WL3050		
MW0521		MW0500 series

Icon Type	Image	Description
MW0522		
CX		CX series
CX_2600		
CX2610-FE		
CX2690-AE		
CX-Hammernet		CX series
CX-uH24		
IP8800_620		IP8800/620
IP8800_710		IP8800/700 series
IP8800_710_S		
IP8800_710A		
IP8800_710A_S		
IP8800_710B		
IP8800_720		
IP8800_720_S		
IP8800_730		
IP8800_730_S		
IP8800_735		
IP8800_735_S		

Icon Type	Image	Description
IP8800_740		
IP8800_740_S		
IP8800_750		
IP8800_750_S		
IP8800_ES8800_700Default		IP8800/700, ES8800/1700
ES8800_1711		ES8800/1700 series
ES8800_1712		
ES8800_1720		
ES8800_1730		
ES1000_12G		ES1000 series
ES1000_6		
ES1000_8G		
ES100X_16G		ES100X series
ES100X_16GA		
ES100X_24GA		
ES100X_24GC		
ES100X_24GF		
ES100X_48GB		
ES100X_48GF		

Icon Type	Image	Description
ES100X_72GA		
ES100X_72GB		
ES100X_72GC		
SS8000_200		SS8000/200 series
SS8000_210		
SS8000_220		
SS8000_230		
SS8000_250		
IP8000_200		IP8000/200 series
IP8000_205		
IP8000_206		
IP8000_210		
IP8000_212		
IP8000_220		
IP8000_230		
IP8000_232		
IP8000_235		
IP8000_240		
IP8000_250		

Icon Type	Image	Description
IP8000_260		
MAR		MegaAccess Router series
IP38X_103		IP38X series
IP38X_107e		
IP38X_1100		
IP38X_140e		
IP38X_140f		
IP38X_140i		
IP38X_140p		
IP38X_1500		
IP38X_2000		
IP38X_300		IP38X series
IP38X_3000		
ip48		IP48 series
NEChub		NEC Hub
IP45_025AT-G		IP45/025AT series
IP45_025AT2-G		
ip45		IP45 series
IP45_C2611XM		

Icon Type	Image	Description
IP45_C3725		
ASR920		Cisco Systems ASR920 series
ASR1000		Cisco Systems ASR1000 series
C2940-8TT		Cisco Systems Catalyst2940 series
C2950-12		Cisco Systems Catalyst2950 series
C2950-24		
C2950G-24		
C2950G-48		
C2950T-24		
C2960-24TC		Cisco Systems Catalyst2960 series
C2960-24TT		
C2960-48TC		
C2960-48TT		
C2960-8TC		
C2960G-24TC		
C2960G-48TC		
C2970G-24T		Cisco Systems Catalyst2970 series
C2970G-24TS		
C3550-12G		Cisco Systems Catalyst3550 series

Icon Type	Image	Description
C3550-12T		
C3550-24		
C3560-24PS		Cisco Systems Catalyst3560 series
C3560-24TS		
C3560-8PC		
C3750-24PS		Cisco Systems Catalyst3750 series
C3750-24TS		
C3750G-12S		
C3750G-16TD		
C3750G-24T		
C3750G-24TS		
C3750G-24TS1U		
C3850		Cisco Systems Catalyst3850 series
C4503		Cisco Systems Catalyst4500 series
C4506		
C4507R		
C4948		Cisco Systems Catalyst4900 series
C4948-10GE		
C6506_L2		Cisco Systems Catalyst6500 series

Icon Type	Image	Description
C6509-E		
C7204VXR		Cisco Systems Cisco 7200 series
Catalyst		Cisco Systems Catalyst series
CiscoDevice		Cisco Systems device
Aironet1100		Cisco Systems Aironet series
Aironet1200		
Aironet350		
PIX515		Cisco Systems PixFirewall series
PixFirewall		
ASA5500		Cisco Systems ASA5500 series
ASA5500-ADMIN-CONTEXT		Cisco Systems ASA5500 series Multi context (ADMIN-CONTEXT)
ASA5500-CONTEXT		Cisco Systems ASA5500 series Multi context (GENERAL-CONTEXT)
Nexus2000		Cisco Systems Nexus2000 series
Nexus2200		
Nexus5000		Cisco Systems Nexus5000 series
Nexus5500		
Nexus5600		
Nexus7000		Cisco Systems Nexus7000 series (Default VDC)
Nexus7700		

Icon Type	Image	Description
Nexus7000-VDC		Cisco Systems Nexus7000 series VDC
Nexus7700-VDC		
CiscoAPIC		Cisco Systems Application Policy Infrastructure Controller
AX1230S-24P2C		ALAXALA Networks AX1200S series
AX1230S-24T2C		
AX1230S-48T2C		
AX2430S-24T		ALAXALA Networks AX2430S series
AX2430S-24T2X		
AX2430S-48T		
AX2430S-48T2X		
AX2530S-48P2X		ALAXALA Networks AX2530S series
AX3630S-24P		ALAXALA Networks AX3630S series
AX3630S-24S2XW		
AX3630S-24T		
AX3630S-24T2X		
AX3630S-48T2XW		
AX3630S-48TW		
AX3640S-24S2XW		ALAXALA Networks AX3640S series
AX3640S-24SW		

Icon Type	Image	Description
AX3640S-24T		
AX3640S-24T2XW		
AX3640S-24TW		
AX3640S-48T2XW		
AX3640S-48TW		
AX3650S-20S6XW		ALAXALA Networks AX3650S series
AX3650S-24T6XW		
AX3650S-48T4XW		
AX3660S-24T4XW		ALAXALA Networks AX3660S series
AX3660S-48T4XW		
AX3660S-48X4QW		
AX3660S-48XT4QW		
AX3830S-44XW		ALAXALA Networks AX3800S series
AX3830S-44X4QW		
AX4630S-4M		ALAXALA Networks AX4600S series
AX6304S		ALAXALA Networks AX6300S series
AX6308S		
AX6708S		ALAXALA Networks AX6700S series
AX8308S		ALAXALA Networks AX8300S series
AX8600S		ALAXALA Networks AX8600S series

Icon Type	Image	Description
AX8608S		
AX8616S		
AX8632S		
BIG-IP		F5 Networks BIG-IP series
BIG-IP_V9		
BIG-IP_TMOS		
BIG-IP1600		
BIG-IP3600		
BIG-IP3900		
BIG-IP6900		
BIG-IP8900		
BIG-IP8950		
BIG-IP11050		
APRESIA		Hitachi Cable APRESIA series
A10_AX		A10 Networks AX series
A10_Thunder		A10 Networks Thunder series
ServerIron		Brocade Communications Systems (former Foundry Networks) device
Brocade		
Foundry		
NetIron400		

Icon Type	Image	Description
NetIronCER2000		
NetIronCES2000		
NetIronXMR		
BIMG8		
FastIron		
FastIronEdge		
FESX424-PREM		
FESX448-PREM		
VDX-6700		
VDX-6720		
ICX-6000		
ICX-6450		
MLX		
MLXe		
FCX		
TurboIron		
Extreme		Extreme Networks device
YAMAHA		YAMAHA device
Allied		Allied Telesis device
CC8216XL2		

Icon Type	Image	Description
CC8224SL		
CC8324XL		
CC8724SL		
CC8948XL		
CCGS908M		
CCGS916M		
CCGS924M		
SII		Seiko Instruments device
Lucent_MAX		Lucent Technologies MAX series
Inkra		Inkra Networks device
AP_2000		Proxim Wireless AP series
AP_4000		
FX_DS540AP		CONTEC device
FX_FD540APL		
FX_FD540APW		
FX_FD540APD		
Aruba61		Aruba Networks device
Aruba70		
Aruba800		

Icon Type	Image	Description
BL10e		Hewlett-Packard device
BL20p		
ProCurve		
ProCurve-2510		
HP_A3100-8_v2_EI		
HP_A3100-16_v2_SI		
HP_A5120-24G_SI		
Fortinet		Fortinet device
FortiGate		Fortinet FortiGate series
FortiAnalyzer		Fortinet FortiAnalyzer
FortiManager		Fortinet FortiManager
PaloAlto		Palo Alto Networks device
EX2200		Juniper EX series
EX3200		
EX3300		
EX4200		
EX4500		
EX6200		
EX8200		
NetScalerMPX		Citrix NetScaler series

Icon Type	Image	Description
ODN-803		Oi Electric device
router		Router
hub		Hub
bridge		Bridge
L2Switch		Layer 2 switch
L3Switch		Layer 3 switch
accesspoint		Access point
NDEVICE		Network device
ibSwitch		Blade Switch
OtherSwitch		Other switch
OtherRouter		Other router

2. Server/PC

Icon Type	Image	Description
host		Host
pcserv		PC server
ex58full		Express 58800 server
ex58mini		
ex58desk		
ex58rack		
ex58mid		

Icon Type	Image	Description
ex58tfull		
ex58tmid		
ex58blade		
ex58other		
ex58wfull		
ex58wmini		
ex58wdesk		
ex58wmid		
ex58wother		
ex58svb		
sv98		SV98 server
sv98full		
sv98mini		SV98 server
sv98desk		
sv98other		
ws		Workstation
ews4800		EWS4800
up4800		UP4800
nx7000		NX7000

Icon Type	Image	Description
hp9000s700		HP9000
rs6000		RS6000
pc		PC
pc98		
Win95		
WinNT		
Win2000		
WinXP		
WinVista		
Win7		
Win8		
Win10		
Win2003		
Win2008		
Win2008R2		
Win2012		
Win2012R2		
Win2016		
Windows		
notepc		

Icon Type	Image	Description
NetWare		NetWare server
x		X client
Linux		Linux server
azusa		AzusA
asama		AsAmA
cmmblade		Blade server / Internal Switch
cmm		
cpuModule		
sbSvb		
sbEm		
sbSwm		
sbSwm10g		Other server
OtherServer		
OtherHost		Other host

3. Other Network Device

Icon Type	Image	Description
monitor		RMON device
rmon2		
nvrmon		
Firewall		Firewall

Icon Type	Image	Description
WAF		Web Application Firewall
IDSIPS		IDS/IPS
LoadBalancer		Load Balancer
DHCP		DHCP Server
NWprinter		Printer
printer		
IP_TEL		IP phone
IP-BS		
MG		
commserver		Communication server
multiport		Multi-port transceiver
modem		Modem
repeater		Repeater
NWDevice		Network device
NVTP_UnKnown		Unknown device

Appendix C. Embedded MIB File List

The following is a list of embedded MIB files (AMIB Difinition File)

<On the manager, %installfolder%>\Manager\sg\NvPRO\NVWORK\local\amib

MIB File Name (AMIB Definition File Name)	Vendor / Model
NEC-BASE-MANAGEMENT-MIB.def	NEC device
necPOE.def	
NEC-PORT-MIB.def	
NEC-TRUNK-MIB.def	
NEC-VLAN-MIB2.def	
oadp-mib.def	
AX1230S.def	IP8800/SS1200, S2400, S2500, S3600, S6300, S6600, S6700, S8300, S8600, R8600, A260 series ALAXALA Networks AX1200S, 2400S, 2500S, 3600S, 6300S, 6600S, 6700S, 8300S, 8600S, 8600R, 260A series
AX1240S.def	
AX1250S.def	
AX2230S.def	
AX2430S.def	
AX2530S-MIB.def	
AX260A.def	
AX3630S.def	
AX3660S.def	
AX46S.def	
AX63S.def	
AX-AXRP-MIB.def	
AX-BFD-MIB.def	
AX-BFD-TC-MIB.def	
AX-BOOTMANAGEMENT-MIB.def	
AX-DEVICE-MIB.def	
AX-EFMOAM-MIB.def	
AX-FDB-MIB.def	
AX-FLOW-MIB.def	
AX-LOGIN-MIB.def	
AX-MANAGEMENT-MIB.def	
AX-MLD-MIB.def	
AX-NOTIFICATION.def	
AX-OSPF-MIB.def	
AX-OSPFV3-MIB.def	
AX-QUEUE-MIB.def	
AX-SHAPER-MIB.def	

MIB File Name (AMIB Definition File Name)	Vendor / Model
AX-SMC-MIB.def	
AX-SMCSERVICE-MIB.def	
AX-SMI-MIB.def	
AX-STATIC-MIB.def	
AX-STATS-MIB.def	
AX-STMCTL-MIB.def	
AX-SYSTEM-MIB.def	
AX-TRACK-MIB.def	
AX-VLAN-MIB.def	
AX-VRF-MIB.def	
a3com-huawei-entity-ext.def	QX series
a3com-huawei-ftm.def	
huawei_device_mib.def	
huawei_splat_rstp_mib.def	
necdlsw.def	
nec-h3c-common-system.def	
nec-h3c-config-man.def	
nec-h3c-dvpn.def	
nec-h3c-entity-ext.def	
nec-h3c-flash-man.def	
nec-h3c-ftm.def	
nec-h3c-ike-monitor.def	
nec-h3c-ipsec-monitor.def	
nec-h3c-radius.def	
nec-h3c-sys-man.def	
nec-hh3c-common-system.def	
nec-hh3c-config-man.def	
nec-hh3c-dvpn.def	
nec-hh3c-entity-ext.def	
nec-hh3c-flash-man.def	
nec-hh3c-ftm.def	
nec-hh3c-ike-monitor.def	
nec-hh3c-ipsec-monitor.def	
nec-hh3c-oid.def	
nec-hh3c-radius.def	
nec-hh3c-sys-man.def	
nec-hh3c-ui-man.def	
nec-huawei-3com-oid.def	

MIB File Name (AMIB Definition File Name)	Vendor / Model
nec-huawei-ar46-dev-adm.def	
nec-huawei-hgmp.def	
nec-huawei-lag.def	
nec-huawei-mpls-ldp.def	
nec-huawei-mpls-lsr.def	
nec-huawei-ndec.def	
nec-huawei-rmon-ext.def	
nec-huawei-sna-dlsw.def	
nec-huawei-8021x-ext.def	
nec-huawei-flash-man.def	
nec-huawei-ifqos2.def	
nec-huawei-lsw-dev-adm.def	
nec-huawei-oid.def	
nec-huawei-rrpp.def	
nec-huawei-splat-devm.def	
nec-huawei-splat-igsp.def	
nec-huawei-splat-inf.def	
nec-huawei-splat-mam.def	
nec-huawei-splat-mstp.def	
nec-huawei-splat-qos.def	
nec-huawei-splat-trap.def	
nec-huawei-splat-vlan.def	
nec-huawei-trng.def	
necpfm.def	
PICO-IPSEC-FLOW-MONITOR-MIB.def	IX1000, 2000, 3000 series
PICO-SMI.def	
PICO-SMI-ID-MIB.def	
mmpfPMib.def	IX5000, 5500 series
mpCardInf.def	
mpCardTRAP.def	
mpRfileMib.def	
mpRfileTrap.def	
mpRPR.def	
mpRprTRAP.def	
10G-L3-NEC.def	SIGMABLADE internal switch
LL3-NEC.def	
PF5200.def	PF series
PF5300.def	

MIB File Name (AMIB Definition File Name)	Vendor / Model
GbTOR-PF5820.def	
PF6000.def	BF210 series
PF6000-UNC-MIB.def	
Commgmt.def	
L2mgmt.def	
necAuth.def	
NEC-SW-ID-REC-MIB.def	
necTime.def	
IPX-EXTENSION-MIB.def	SV7000 series
IPX-TRAFFIC-MIB.def	
WA-SMI.def	WA series
AIRESPACE-SWITCHING-MIB.def	WL series
AIRESPACE-WIRELESS-MIB.def	
BSN-REF-MIB.def	
aeic_V305.def	CX series
consoleConf.def	
cx2600_220_0401_R06.def	
cx26App.def	
cx26ExtendedVlan.def	
cx26Filter.def	
cx26FltInf.def	
cx26Mng.def	
cx26Port.def	
cx26PortConfig.def	
cx26ProcessesCpu.def	
NEC-BASE-MIB.def	
sysLog.def	
MW0500V300.def	MW0500 series
sh380_200.DEF	SH380 series
ip8000_120.DEF	IP8000/120
ip8800_410.DEF	IP8800/410 series
ip8800_600.DEF	IP8800/600 series
IP8800-600-32.def	
IP8800_700.def	IP8800/700 series
IP8800_R.def	IP8800/R400 series
IP8800_S.def	IP8800/S300, S400 series
POWERNET.DEF	APC device

MIB File Name (AMIB Definition File Name)	Vendor / Model
ATM-ACCOUNTING-INFORMATION-MIB-V1SMI.def	Cisco Systems device
ATM-ADDR-MIB-V1SMI.def	
C-2900.DEF	
C-CPU.DEF	
cisco-cdp.def	
CISCO-CONFIG-MAN-MIB.def	
CISCO-IMAGE-MIB.def	
CISCO-L2L3-INTERFACE-CONFIG-MIB.def	
CISCO-LAG-MIB.def	
CISCO-LWAPP-SYS-MIB.def	
CISCO-MEMORY-POOL-MIB.def	
cisco-pagp-mib.def	
CISCO-PORT-SECURITY-MIB.def	
CISCO-PRIVATE-VLAN-MIB-V1SMI.def	
CISCO-PROCESS-MIB.def	
CISCO-PRODUCTS-MIB.def	
CISCO-SMI.def	
CISCO-STACK-MIB.def	
CISCO-SYSLOG-MIB.def	
CISCO-SYSTEM-EXT-MIB.def	
CISCO-VLAN-MEMBERSHIP-MIB-V1SMI.def	
CISCO-VTP-MIB-V1SMI.def	
C-STACK.DEF	
OLD-CISCO-CHASSIS-MIB.def	
OLD-CISCO-FLASH-MIB.def	
OLD-CISCO-INTERFACES-MIB.def	
OLD-CISCO-IP-MIB.def	
OLD-CISCO-SYS-MIB.def	
OLD-CISCO-TS-MIB.def	
CISCO-ETHERNET-FABRIC-EXTENDER-MIB.def	Cisco Systems Nexus 5000, 7000 series
F5-BIGIP-APM-MIB.def	F5 Networks BIG-IP series
F5-BIGIP-COMMON-MIB.def	
F5-BIGIP-GLOBAL-MIB.def	
F5-BIGIP-LOCAL-MIB.def	

MIB File Name (AMIB Definition File Name)	Vendor / Model
F5-BIGIP-SYSTEM-MIB.def	
LOAD-BAL-SYSTEM-MIB.def	
A10-AX-MIB.def	A10 Networks AX, Thunder series
A10-COMMON-MIB.def	
AC-SYSTEM-MIB.def	AudioCodes device
AUDIOCODES-TYPES-MIB.def	
FORTINET-CORE-MIB.def	Fortinet device
FORTINET-FORTIGATE-MIB.def	
FORTINET-FORTIMANAGERFORTIANALYZER-MIB.def	
Apresia-mibs.def	Hitachi Cable APRESIA series
foundry.def	Brocade Communications Systems (former Foundry Networks) device
foundry_ip.DEF	
foundry_sw.DEF	
FOUNDRY-CAR-MIB.def	
FOUNDRY-SN-AGENT-MIB.def	
FOUNDRY-SN-APPLETALK-MIB.def	
FOUNDRY-SN-BGP4-GROUP-MIB.def	
FOUNDRY-SN-IGMP-MIB.def	
FOUNDRY-SN-IP-ACL-MIB.def	
FOUNDRY-SN-IP-MIB.def	
FOUNDRY-SN-IP-VRRP-MIB.def	
FOUNDRY-SN-IPX-MIB.def	
FOUNDRY-SN-MPLS-LSR-MIB.def	
FOUNDRY-SN-MPLS-TC-MIB.def	
FOUNDRY-SN-MPLS-TE-MIB.def	
FOUNDRY-SN-OSPF-GROUP-MIB.def	
FOUNDRY-SN-POS-GROUP-MIB.def	
FOUNDRY-SN-ROOT-MIB.def	
FOUNDRY-SN-SWITCH-GROUP-MIB.def	
FOUNDRY-SN-SW-L4-SWITCH-GROUP-MIB.def	
FOUNDRY-SN-VSRP-MIB.def	
FOUNDRY-VLAN-CAR-MIB.def	
hpEntMib.def	Hewlett-Packard device
hpicfOid.def	
hpNetSwitch.def	

MIB File Name (AMIB Definition File Name)	Vendor / Model
hpSwitchConfig.def	
hpSwitchStat.def	
hpVlan.def	
yamaha-product.def	YAMAHA device
yamaha-rt.def	
yamaha-rt-firmware.def	
yamaha-rt-hardware.def	
yamaha-rt-interfaces.def	
yamaha-smi.def	
atrouter.def	Allied Telesis device
fstswtch.def	
GS900M.def	
EVNTAGENT-MIB.DEF	Microsoft Windows (Event to Trap Translator)
NEC-CLUSTER-EVENT-MIB.def	EXPRESSCLUSTER X
NEC-CLUSTER-MANAGEMENT-MIB.def	
NEC-CLUSTER-SMI.def	
ESMABC.def	ESMPRO
ESMCPU.DEF	
ESMAGENT.def	
ESMAMI.def	
ESMARRAY.def	
ESMBIOS.def	
ESMBUS.def	
ESMMEM.DEF	
ESMDRV.def	
ESMELOG.def	
ESMEMCTL.def	
ESMENV.def	
ESMEXCHS.def	
ESMEXT.def	
ESMFRU.def	
ESMFTC.def	
ESMGINFO.def	
ESMLCD.def	
ESMLIQUD.def	
ESMMYLEX.def	

MIB File Name (AMIB Definition File Name)	Vendor / Model
ESMNET.def	
esmnic.def	
ESMOS.def	
ESMPRO_SM.def	
ESMPS.def	
ESMRES.def	
ESMSEC.def	
ESMSNMP.def	
ESMSR.def	
ESMSTAT.def	
ESMSTGEX.def	
ESMSTRG.def	
ESMSYSIO.def	
ESMTPGEN.DEF	
ESMTPOPT.def	
ESMVIDEO.def	
ESMVOL.def	
AlrtActMailMgr.def	Network Manager
netvisor.def	
NetvisorPro.def	
NVBASE.DEF	
nvpro.def	
nvproDC.def	
NvPRODataCollect.def	
NvPROLicense.def	
NvPROMapFilter.def	
NVRMON.DEF	
ATM-FORUM-ADDR-REG.def	RFC and others
ATM-FORUM-MIB.def	
ATM-FORUM-TC-MIB-V1SMI.def	
ATM-MIB.def	
ATM-MIB-V1SMI.def	
ATM-RMON-MIB-V1SMI.def	
BGP4-MIB.def	
BRIDGE.def	
ENTITY-MIB.def	
ETHER.DEF	
HOST-RESOURCES-MIB.DEF	

MIB File Name (AMIB Definition File Name)	Vendor / Model
HOST-RESOURCES-TYPES.DEF	
ieee8023-lag.def	
if-mib.def	
IPV6-MLD-MIB.def	
ISDN-MIB.def	
LAN-EMULATION-CLIENT-MIB-V1SMI.def	
LLDP-MIB.def	
MAU-MIB.def	
MIB-II.DEF	
MIP.def	
OSPF-MIB.def	
OSPF-TRAP-MIB.def	
P-BRIDGE-MIB.def	
PNNI-MIB-V1SMI.def	
Q-BRIDGE-V1SMI.def	
radius-acc-client-mib.def	
radius-auth-client-mib.def	
REPEATER.DEF	
rfc1155.def	
rfc2452.def	
rfc2454.def	
rfc2465.def	
rfc2466.def	
rfc3621.def	
rfc4293.def	
RIPv2-MIB.def	
SNMP-COMMUNITY-MIB.def	
SNMP-FRAMEWORK-MIB.def	
SNMP-MPD-MIB.def	
SNMP-USER-BASED-SM-MIB.def	
SNMPv2.def	
SNMPv2-SMI.def	
VRRP-MIB.def	

MasterScope Network Manager 9.0
User's Manual

NVP00ME0900-01

January, 2019 1 Edition

NEC Corporation