NEC

MasterScope Network Manager 9.0
Release Notes

Copyrights

Trademark

Introduction

Thank you for choosing MasterScope Network Manager.

This document describes the release contents of MasterScope Network Manager 9.0

- To return to the former page after jumping from the hyper link in the PDF manual, press ALT + Left keys. (In the case of using Adobe Reader)
- 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

Contents

1.1 Overview

MasterScope Network Manager (hereafter referred to as "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 concerning the characteristics of network elements
  - Visualization of the network device front panel
- Fault Management
  - Network status monitoring
  - Receipt of fault notifications from devices
  - Reporting of faults to the administrator
- Performance Management
  - Reports and graphical display of the network performance
  - Network traffic information based on sFlow protocol

Advanced functions of management operations:

- Resource Manager function

  Management of device configuration information and software
- Network Provisioning function

  Settings for devices linked with NEC Sigma System Center

Chapter 2. Operating Environment

Contents

2.1 System Configuration

Shows the system configuration of Network Manager.

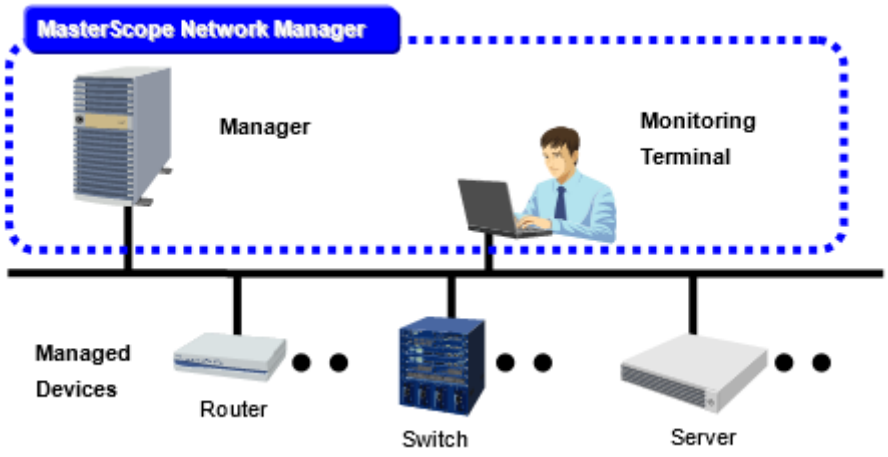


Figure 2-1 System Configuration

Network Manager consists of two functions: the manager function and the monitoring terminal function. The role of each function is shown in Table.

Table 2-1 Manager function and Monitoring Terminal function

Function	Description
Manager function	Manages and monitors target devices.
Monitoring Terminal function	Provides viewer functions such as operating and configuring the manager function and network status display.

Tip

The monitoring terminal function can be installed in multiple machines and they can connect simultaneously to a single manager function.

Network Manager uses the bundled databases (internal databases) to store various information such as configurations, failure events, and performance data (sFlow). Network Manager can also use the databases installed in the manager server (external databases) to store the information.

Pay attention to the following points when selecting databases.

1. Internal databases and external databases cannot be used concurrently. If using external databases, configurations, failure events, and performance data (sFlow) information is stored in the external databases. Internal databases are not used.
2. You cannot change the databases in midstream. For example, if external databases were used before upgrading, you cannot switch to the internal databases.

2.2 System Requirements

Network Manager operates on the following Operating Systems.

Table 2-2 List of supported Operating Systems

Operating System	Manager function	Monitoring Terminal function
Windows Server 2019 (x64)	Y 1) 2)	Y 1) 2)
Windows Server 2016 (x64)	Y 1) 2)	Y 1) 2)
Windows Server 2012 R2 (x64)	Y 1)	Y 1)
Windows Server 2012 (x64)	Y 1)	Y 1)
Windows 10 Pro, Enterprise (32bit / x64)	N	Y 3)
Windows 8.1 Pro, Enterprise (32bit / x64)	N	Y
Windows 7 Professional/Enterprise/Ultimate (32bit / x64)	N	Y

Note

1. Windows Server Core is not supported.
2. Nano Server is not supported.
3. Tablet mode is not supported.

System Requirements (for the Windows manager function)

Table shows the system requirements for the manager function.

Table 2-3 System requirements for the manager function

Item	Description
CPU	Intel Dual-Core Xeon or higher, or equivalent compatible processor recommended
System memory	1 GB or more
Disk (free space)	2 GB or more (20GB or more is recommended)
Network	100 Mbps LAN or faster recommended
Required software	• Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) 1) • Microsoft Visual C++ 2017 Redistributable Package (x86) 2)
Supported cluster	EXPRESSCLUSTER X 3.0 or later
External database software (Optional)	• Microsoft SQL Server 2014 3) • Microsoft SQL Server 2012 3)

Note

1. Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) is required when using internal databases. It will be installed automatically in the manager function installation.
2. Microsoft Visual C++ 2017 Redistributable Package (x86) will be installed automatically in the manager function installation.

   For the following Operating Systems, the Windows KB2999226 update program must have been applied.

   - Windows Server 2012 R2 (x64)
   - Windows Server 2012 (x64)

   If it has not been applied, perform a Windows Update or refer to the following information published by Microsoft to apply KB2999226.

https://support.microsoft.com/en-us/help/2999226/ *1

3. The following editions are not supported in the cluster environment.
   - Microsoft SQL Server 2014 Express
   - Microsoft SQL Server 2012 Express

System Requirements (for the monitoring terminal function)

Table 2-4 System requirements for the monitoring terminal function

Item	Description
CPU	Intel Core i3 or higher, or equivalent compatible processor recommended
System memory	512 MB minimum (1 GB or more is recommended)
Disk (free space)	400 MB
Network	100 Mbps LAN or faster recommended 1)
Required software	Telnet client 2)

Note

1. If the manager and monitoring terminal are connected with the network which has large communication latency like WAN, it may take a few minutes to start the monitoring terminal function.
2. The Remote Login function requires the telnet client. By default, the telnet client in Windows Operating Systems is disabled, so change it to enabled.

*1 This URL is current as of January 2019.

Chapter 3. Documents

The following lists the documents supplied with this version.

Table 3-1 documents

Title (File name)	Description
MasterScope Network Manager 9.0 Release Notes (NVPRO_release.pdf)	This describes the release contents of Network Manager.
MasterScope Network Manager 9.0 Setup Guide For Windows environment (NvPRO_setup_win.pdf)	This describes the procedure to set up Network Manager (For Windows).
MasterScope Network Manager 9.0 Setup Guide For Windows / EXPRESSCLUSTER X environment (NvPRO_CS_setup_win.pdf)	This describes the procedure to set up Network Manager (For Windows) in the cluster system.
MasterScope Network Manager Setup Guide (Rolling Update) Windows / EXPRESSCLUSTER X Environment (NvPRO_update_win.pdf)	This describes how to update Network Manager (Windows version) using Rolling Update method in a cluster system.
MasterScope Network Manager 9.0 User's Manual (NvPRO.pdf)	This describes the procedures to use and operate Network Manager.
MasterScope Network Manager Web API 1.1 Reference Manual (NvPRO_webapi.pdf)	This is the reference manual of Network Manager Web API version 1.1.

Chapter 4.
New and Improved Functions

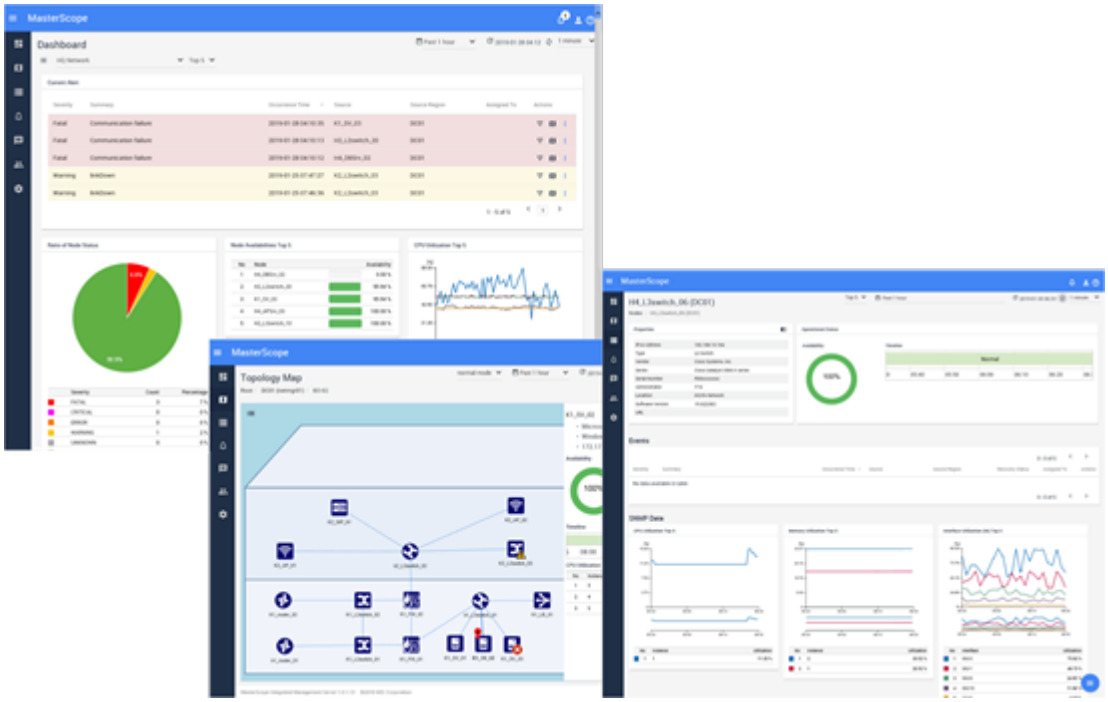
Contents

4.1 Support for Web Console

New Web Console functions, previously not available on the conventional web monitoring screen, are now provided.

New Web Console functions can be used on various web browsers. You can also perform the following operations by directly accessing this product via a web browser.

- Dashboard View
- Displaying a Network Configuration Map (Topology Map)
- Displaying Alert (Event) Information
- Displaying the Property Information of nodes and interfaces
- Alert Notification Settings (E-mail sending and action execution)



Tip

To use Web Console, the MasterScope Integrated Management Server component needs to be installed.

Furthermore, the following system integration is possible by connecting multiple products to the MasterScope Integrated Management Server component that is required to use Web Console.

- Integrating multiple Network Manager instances
- Integrating Network Manager and NFA

For the detailed system configuration and provided functions, refer to *"MasterScope Integrated Management Server 1.0 Release Notes."*

4.2 Improvements to Monitoring Rules

Rules have been added to the data collection function.

4.2.1 Providing built-in rules for MIB expression

For the Built-in MIB Expression rules of the data collection function, some rules are now provided to monitor items related to interfaces and to monitor the CPU and memory utilization.

The following rules are now supported.

- Rules applicable to all devices supporting IF-MIB
  - Bandwidth utilization for input and output interfaces

    Collects MIBs of the specified interfaces of the specified device and calculates the bandwidth utilization for interfaces.

    builtin:ifInUtil, builtin:ifInUtil64bit

    builtin:ifOutUtil, builtin:ifOutUtil64bit
  - Packet loss rate for inbound and outbound packets

    Collects MIBs of the specified interfaces of the specified device and calculates the percentage of packets discarded.

    builtin:ifInDiscards, builtin:ifOutDiscards
  - Packet error rate for inbound and outbound packets

    Collects MIBs of the specified interfaces of the specified device and calculates the percentage of error packets.

    builtin:ifInErrors, builtin:ifOutErrors
- Rules for the QX series
  - CPU utilization

    Collects MIBs related to the CPUs provided by the QX series and calculates the CPU utilization.

    builtin:QxSystemCpu, builtin:QxSlotCpu
  - Memory utilization

    Collects MIBs related to the memory provided by the QX series and calculates the memory utilization.

    builtin:QxMemory
- Rules for the IX series
  - CPU utilization

    Collects MIBs related to the CPUs provided by the IX series and calculates the CPU utilization.

    builtin:Ix1000Ix2000Ix3000Cpu
  - Memory utilization

    Collects MIBs related to the memory provided by the IX series and calculates the memory utilization.

    builtin:Ix1000Ix2000Ix3000Memory
- Rules for the IP8800 series and ALAXALA Networks devices
  - CPU utilization

Collects MIBs related to the CPUs provided by the IP8800 series and ALAXALA Networks devices, and calculates the CPU utilization.

builtin:Ip8800S8kR8kBcuCpu,

builtin:Ip8800R8kPruCpu, builtin:Ip8800S8kPsuCpu,

builtin:Ip8800S6700Cpu, builtin:Ip8800S6600Cpu,

builtin:Ip8800S6300Cpu, builtin:Ip8800S4600Cpu,

builtin:Ip8800S3800Cpu, builtin:Ip8800S3660Cpu,

builtin:Ip8800S3650Cpu, builtin:Ip8800S3640Cpu,

builtin:Ip8800S2500Cpu, builtin:Ip8800S2200Cpu,

builtin:Ip8800S2100Cpu, builtin:Ip8800S1250Cpu,

builtin:Ip8800S1240Cpu, builtin:Ip8800A260Cpu

- Memory utilization

  Collects MIBs related to the memory provided by the IP8800 series and ALAXALA Networks devices, and calculates the memory utilization.

  builtin:Ip8800S8kR8kBcuMemory,

  builtin:Ip8800R8kPruMemory, builtin:Ip8800S8kPsuMemory,

  builtin:Ip8800S6700Memory, builtin:Ip8800S6600Memory,

  builtin:Ip8800S6300Memory, builtin:Ip8800S4600Memory,

  builtin:Ip8800S3800Memory, builtin:Ip8800S3660Memory,

  builtin:Ip8800S3650Memory, builtin:Ip8800S3640Memory,

  builtin:Ip8800S2500Memory, builtin:Ip8800S2200Memory,

  builtin:Ip8800S2100Memory, builtin:Ip8800S1250Memory,

  builtin:Ip8800S1240Memory, builtin:Ip8800A260Memory

- Rules for the PF series
  - CPU utilization

    Collects MIBs related to the CPUs provided by the PF series and calculates the CPU utilization.

    builtin:Pf6800Cpu, builtin:Pf6800NetworkCoordinatorCpu,

    builtin:Pf5200Cpu, builtin:Pf5300Cpu

  - Memory utilization

    Collects MIBs related to the memory provided by the PF series and calculates the memory utilization.

    builtin:Pf6800Memory, builtin:Pf6800NetworkCoordinatorMemory,

    builtin:Pf5200Memory, builtin:Pf5300Memory

- Rules for the SV series (7000, 8500, 9500)
  - CPU utilization

    Collects MIBs related to the CPUs provided by the SV series and calculates the CPU utilization.

builtin:Sv7000Sv8500Sv9500Cpu

- Rules for the BX series and AudioCodes Mediant series
  - CPU utilization

    Collects MIBs related to the CPUs provided by the BX series and AudioCodes Mediant series, and calculates the CPU utilization.

    builtin:BxDataCpu, builtin:BxVoIpCpu
  - Memory utilization

    Collects MIBs related to the memory provided by the BX series and AudioCodes Mediant series, and calculates the memory utilization.

    builtin:BxDataMemory, builtin:BxVoIpMemory
- Rules for the Cisco Systems devices
  - CPU utilization

    Collects MIBs related to the CPUs provided by the Cisco wireless LAN controller and calculates the CPU utilization..

    builtin:CiscoWirelessLanControllerCpu

    Tip

    Use the conventional **Device CPU busy rate for Catalyst series** rule of the data collection function to monitor the CPU utilization of the Cisco Systems devices (Cisco Catalyst series, Nexus series, Router series, ASA5500 series) other than the Cisco wireless LAN controller.
  - Memory utilization

    Collects MIBs related to the memory provided by the Cisco Systems devices and calculates the memory utilization.

    builtin:CatalystMemory, builtin:NexusMemory,

    builtin: CiscoWirelessLanControllerMemory
- Rules for the Fortinet devices
  - CPU utilization

    Collects MIBs related to the CPUs provided by the Fortinet devices and calculates the CPU utilization.

    builtin:FortiGateSystemCpu, builtin:FortiGateProcessorCpu,

    builtin:FortiGateHaCpu, builtin:FortiManagerCpu
  - Memory utilization

    Collects MIBs related to the memory provided by the Fortinet devices and calculates the memory utilization.

    builtin:FortiGateSystemMemory, builtin:FortiGateLowMemMemory,

    builtin:FortiGateHaMemory, builtin:FortiManagerMemory
- Rules for the A10 Networks devices
  - CPU utilization

    Collects MIBs related to the CPUs provided by the A10 Networks devices and calculates the CPU utilization.

builtin:A10ControlCpu, builtin:A10DataCpu

- Memory utilization

  Collects MIBs related to the memory provided by the A10 Networks devices and calculates the memory utilization.

  builtin:A10Memory

4.3 Newly Supported Device Types

This section describes the functions for which the supported device types have been expanded in the current version, as well as providing information on those device types.

4.3.1 Adding the MIB definition and trap definition

The MIB definition files and trap definitions have been added for various models.

MIB definition file

The MIB definition (AMIB definition file and AMIB numeration file) has been added and updated for the following devices.

- QX series (Version: 19.00)
- IP8800 series (ALAXALA Networks products)
- PF series
- Cisco Systems products
- A10 Networks AX, Thunder series
- Fortinet products
- AudioCodes products

Trap definition

The trap definition (definition of the contents of the SNMP trap notification) has been added and updated for the following devices.

- ESMPRO Manager
- SV9500, SV8500, SV7000

⚠ Caution

The SNMP traps corresponding to the SV9500, SV8500, and SV7000 system messages have a different OID because of the settings of the device.

This version provides the two trap definitions according to the following settings of the device.

- ASYDL SYS1 INDEX963 Bit6=0, Bit7=0

  A trap is notified according to the alarm grade of a system message.

- ASYDL SYS1 INDEX963 Bit6=1, Bit7=1

  A trap is notified according to the error code of a system message.

Set either of the above settings on the device.

4.3.2 Configuration and software management (Resource Manager function)

Devices newly supported by the Resource Manager function are shown below, along with their scope of support under the function.

⚠ Caution

Scope of support depends on individual device specifications.

QX-S3400F series

The following describes the status of the support of the QX-S3400F series.

- Supported version: 7.2.8 or higher
- The scope of supported function is shown in Table.

Table 4-1 Scope of support for QX-S3400F Series

Resource Manager Function Details	Supported
Collect running-config [1)]	Y
Deploy running-config	N
Collect startup-config	Y
Deploy startup-config	Y
Manage configuration changes	Y
Backup software	Y
Deploy software	Y
Reboot	Y

Note

1. The use of an external FTP/TFTP server is not supported.

QX-S6600 series

The following describes the status of the support of the QX-S6600 series.

- Supported version: 7.1.3 or higher
- The scope of supported function is shown in Table.

Table 4-2 Scope of support for QX-S6600 Series

Resource Manager Function Details	Supported
Collect running-config [1)]	Y
Deploy running-config	N
Collect startup-config	Y
Deploy startup-config	Y
Manage configuration changes	Y
Backup software	Y
Deploy software	Y

Resource Manager Function Details	Supported
Reboot	Y

Note

1. The use of an external FTP/TFTP server is not supported.

IP8800/S8600 series

The following describes the status of support for the IP8800/S8600 series.

- Supported version: 12.7.C or higher
- The scope of supported function is shown in Table.

Table 4-3 Scope of support for IP8800/S8600 Series

Resource Manager Function Details	Supported
Collect running-config	Y
Deploy running-config	N
Collect startup-config	Y
Deploy startup-config	Y
Manage configuration changes	Y
Backup software	Y
Deploy software	Y 1)
Reboot	Y

Note

1. The device manages the software with a fixed file name, so current software cannot be remained when deploying new software. The software is always overwritten.

Caution

For the 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.

IP8800/S3660 series

The following describes the status of the support of the IP8800/S3660 series.

- Supported version: 12.1.A or higher
- The following table shows the support status of each function.

Table 4-4 Scope of support for IP8800/S3660 Series

Resource Manager Function Details	Supported
Collect running-config	Y
Deploy running-config	Y 1)
Collect startup-config	Y

Resource Manager Function Details	Supported
Deploy startup-config	Y
Manage configuration changes	Y
Backup software	Y
Deploy software	Y 2)
Reboot	Y

Note

1. In the stack configuration, uploading running-config is not supported due to the device specification.
2. 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.

IX2000 series

The following models of the IX2000 series have undergone verification and evaluation to confirm that they are operable without a problem.

- IX2106 (Version: 9.6.12)

Cisco Catalyst (IOS-XE) series

The following describes the status of support for the Cisco Catalyst (IOS-XE) series.

- Supported version: 3.2.2SE (15.1(1)SE2) or higher
- The scope of supported function is shown in Table.

Table 4-5 Scope of support for Cisco Catalyst (IOS-XE) Series

Resource Manager Function Details	Supported
Collect running-config	Y
Deploy running-config	Y
Collect startup-config	Y
Deploy startup-config	Y
Manage configuration changes	Y
Backup software	Y 1)
Deploy software	Y 2)
Reboot	Y

Note

1. When the IOS-XE software version is 3.8 (15.3(1)) or higher and lower than 16, software backup is supported.
2. For the Catalyst 4500 series, the IOS-XE software of version 3.8 (15.3(1)) or higher can be deployed.

Cisco ASR 920 series

The following describes the status of support for the Cisco ASR 920 series.

- Supported version: 3.14.1S (15.5(1)S1) or higher
- The following table shows the support status of each function.

Table 4-6 Scope of support for Cisco ASR 920 Series

Resource Manager Function Details	Supported
Collect running-config	Y
Deploy running-config	Y
Collect startup-config	Y
Deploy startup-config	Y
Manage configuration changes	Y
Backup software	Y 1)
Deploy software	Y 1)
Reboot	Y

Note

1. Version 16.x or higher is not supported.

Caution

Set **OS Type** for the icon properties of the target node to **ASR1000**.

Devices in the Cisco ASR 920 series 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.

The Resource Manager function can deploy only the IOS-XE software. Therefore, when deploying the IOS-XE software by using the Resource Manager function, 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.

Cisco Nexus 3000 and 9000 series

The following describes the status of support for the Cisco Nexus 3000 and 9000 series.

- Supported version: 7.0(3) or higher
- The scope of supported function is shown in Table.

Table 4-7 Scope of support for Cisco Nexus 3000 and 9000 Series

Resource Manager Function Details	Supported
Collect running-config	Y
Deploy running-config	Y
Collect startup-config	Y
Deploy startup-config	N
Manage configuration changes	Y
Backup software	N
Deploy software	N
Reboot	Y

Caution

Set **OS Type** for the icon properties of the target node to **NX-OS**.

For Cisco Nexus 9000, only the standalone model running on NX-OS is supported.

F5 BIG-IP series

The following describes the status of support for the F5 BIG-IP series (v12 and v13).

- Supported version: 12.x, 13.x
- The scope of supported function is shown in Table.

Table 4-8 Scope of support for F5 BIG-IP v12 and v13

Resource Manager Function Details	Supported
Collect running-config	Y
Deploy running-config	Y
Collect startup-config	N
Deploy startup-config	N
Manage configuration changes	Y
Backup software	N
Deploy software	N
Reboot	Y

Caution

Set **OS Type** for the icon properties of the target node **BIG-IP_TMOS**.

4.3.3 Linking with NEC SigmaSystemCenter (Network Provisioning function)

Devices newly supported by the Network Provisioning function are shown in Table.

Caution

Scope of support depends on individual device specifications.

Table 4-9 Devices supported by the Network Provisioning function

Device Name	Version	Supported
IP8800/S3660 series	12.1.A or higher	VLAN Settings
IP8800/S8600 series	12.7.C or higher	VLAN Settings

4.4 Other Improvements

This section describes other improvements.

4.4.1 Improvements in the simple script to run device commands

Files in the managed device can now be transferred to the internal FTP server of Network Manager by scheduling command execution or by using the `nvpdevcmdexe` command.

The newly supported simple script can control the starting and stopping of the internal FTP server of Network Manager. By using replacement strings related to FTP, you can perform authentication for the FTP sever.

4.4.2 Increasing the node property information

Serial Number has been added to **Properties** of a node.

This item is available to record information that will be used for maintenance of the managed node and so on.

Along with this, WebAPI can also handle information associated with **Serial Number**.

4.4.3 Providing the MIB tree configuration check tool

If the MIB definition for an object in the MIB object index is incorporated to Network Manager as in the example below, the MIB value for the MIB object index cannot be obtained correctly.

Example:

```
sysUpTimeInstance OBJECT IDENTIFIER ::= { sysUpTime 0 }
```

In the above example, an object named *"sysUpTimeInstance"* is defined for *"0"* associated with *"sysUpTime"*.

If the above 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.

The `nvpamibcheck` command is now provided as the check tool to check whether a MIB definition affecting acquisition of a MIB value is incorporated into Network Manager.

Before incorporating the MIB definition file (AMIB definition file) to Network Manager, be sure to run the `nvpamibcheck` command to confirm that there are no MIB definitions affecting the operations.

Chapter 5. Functions with Specification Changes

Contents

5.1 Specification Changes in Version 9.0

This section describes functions for which specifications have changed under MasterScope Network Manager 9.0

5.1.1 Addition of services (processes)

Since Web Console is now supported, services (processes) related Network Manager have been added.

When monitoring Network Manager related services (processes) in a cluster environment, change the configuration.

Table 5-1 Added Services and Processes

OS	Added services and processes
Windows	• NvPRO Performance Database (NvPROPerfDB) • NvPRO Topology Adapter (NvPROTopologyAdapter) • NvPRO Performance Manager (NvPROPerfMgr)
Linux	• *$NVP_INSTALL_PATH*/Manager/bin/NvPRO/pgsql10/bin/postgres -D *$NVP_SHARE_PATH*/Manager/sg/database/NvPROPerfDB • *$NVP_INSTALL_PATH*/Manager/bin/NvPROTopologyAdapter • *$NVP_INSTALL_PATH*/Manager/bin/NvPROPerfMgr

Tip

- *$NVP_INSTALL_PATH* indicates the install path of the manager function of Network Manager. The default install path is `/opt/NetvisorPro`.

  (When this product is installed by using the MasterScope Media, the default install path is `/opt/UMF/Operations`.)
- *$NVP_SHARE_PATH* indicates the shared data path of the manager function of Network Manager. In an environment in which the install path and shared data path are not separated, the same path as used for the install path is used.

5.1.2 Changes to the MIB definition incorporation procedure

In this version, the `nvpamibcheck` command has been provided, changing the procedure for incorporating the MIB definition (AMIB definition file) to Network Manager.

Specifically, after the MIB definition file is converted to the AMIB definition file by the `NvPROMib2Amib -amib` command, the `nvpamibcheck` command always checks the contents of the AMIB definition file to be read. Then, the `NvPROReloadDefFileMgr` command reads the AMIB definition file.

For details, see *"Incorporating an AMIB definition file and type definition file"* in the MasterScope Network Manager User's Manual.

5.2 Specification Changes in Version 8.0

This section describes functions for which specifications have changed under MasterScope Network Manager 8.0

5.2.1 Changes to specification of Trap Definition Management

Along with the enhancement of the trap definition operation, the specification of the trap definition management has been changed

5.2.1.1 Changes to the Trap definition operation

In MasterScope Network Manager 8.0, the specification of the trap definition operation has been changed as follows:

- The operation for the trap definition with conventional files is now abolished.
- The following commands can no longer operate trap definitions.
  - `NvPROMib2Amib -trap`
  - `NvPROReloadDllMgr`
  - `NvPROReloadDefFileMgr`
- The operation after version 8.0 can be performed on the trap definition management window or by newly added commands (`nvptrapdefconf`, `nvpmib2trapdef`).

Tip

The operation of AMIB definition files is performed by `NvPROMib2Amib` and `NvPROReloadDefFileMgr` commands as in the past.

Caution

If you store the trap definition files in the conventional storage location of trap definition files, `NvPROReloadDllMgr` and `NvPROReloadDefFileMgr` commands do not reload these files, however, these files are reloaded after restarting the manager.

- Conventional storage location of trap definition files

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

  For a non-cluster configuration, read *<on the manager, %sharedfolder%>* as *<on the manager, %installfolder%>*.

For this reason, if trap definition files are stored in above location, existing trap definitions will be overwritten unintentionally.

After version 8.0, it is recommended not to store trap definition files in the conventional storage location.

5.2.1.2 Trap definition file migration process

If you upgrade an earlier version to MasterScope Network Manager 8.0, convert the contents of all existing trap definition files into the definition format that makes them operable in the trap definition management window and perform a migration process when starting services for the first time.

Caution

Operations with the former trap definition files will no longer be possible.

The following lists the migration targets.

- Standard trap definition files supplied with the product

  In the trap definition management window, they are managed in the category of "System definition".

- Trap definition files automatically generated from an MIB file

In the trap definition management window, they are managed in the category of "MIB original definition."

- User-created trap definitions (user.def)

  In the trap definition management window, they are managed in the category of "User definition". Any trap definitions that are clearly judged to have been created by users although their file names do not contain user.def are processed as migration targets in the "User definition" category.

The specifications of the trap definition management window are such that multiple definitions in the same category, for which the combinations of settings are the same for the Enterprise ID, Specific Trap Code, Generic Trap Code, and Node, cannot be retained. For this reason, if there are duplicate trap definitions in a category, only the definition that has the highest priority for processing Network Manager is regarded as a migration target.

If there are duplicate trap definitions, the priority is determined as below.

- If there are duplicate trap definitions among multiple trap definition files, the priority is judged from the names of the files containing the trap definitions. Specifically, the definition with the highest priority is the one contained in the `user.def` file. For all other definitions, a trap definition whose file name comes later in the character code order is judged to have higher priority.
- The specifications of the processing of MasterScope Network Manager are such that if, in the Enterprise in a trap definition and an SNMP trap, the end of the OID is ".0", the alert notification process is performed by excluding the ".0". For this reason, in the Enterprise in a trap definition, a definition with a ".0" at the end of the OID and a definition without a ".0" at the end of the OID are handled as the same OID definition. For trap definitions that are regarded as duplicate regardless of the presence and absence of a ".0" at the end of the OID in the Enterprise, the definition with a ".0" added is judged to have higher priority.

In the migration process, the following process is performed on the trap definition with higher priority.

- Enterprise definition conversion

  If, in the trap definition to be migrated, the end of the vendor identifier (Enterprise) is ".0", it is migrated by deleting the ".0".

- Node definition division

  If the trap definitions to be migrated include a trap definition in which multiple components are registered delimited by a comma (,) for the Node, the trap definition is migrated as multiple trap definitions by dividing the components for the Node.

After the completion of the migration process, the former trap definition files are moved to the following folder.

Destination of former trap definition files

<On the manager, %sharefolder%>`\Manager\sg\NvPRO\NVWORK\public\trap_backup\`*<YYYYMMDDHHmmSS>*

- For a non-cluster configuration, read *<On the manager, %sharefolder%>* as *<On the manager, %installfolder%>*.
- *<YYYYMMDDHHmmSS>* is the folder name representing the date and time the migration process was performed.

If you want to incorporate any trap definitions judged to have low priority, register them using the trap definition management window or the trap definition batch registration command (`nvptrapdefconf`), based on the contents of the former trap definition file.

5.2.2 Changes to menu names

In MasterScope Network Manager 8.0, the names of the following two menus have been changed.

Before changes (version 6.1 or earlier)		After changes (version 8.0 or later)
Programmable Flow Authentication Setting	->	**ProgrammableFlow Authentication Setting**
Programmable Flow Topology Discovery	->	**ProgrammableFlow Topology Discovery**

ProgrammableFlow Topology Discovery There are no changes to the functions on each menu.

5.2.3 Changes to the specifications of the state monitoring/ data collection setting commands

In MasterScope Network Manager 8.0, the specifications related to the operation of entries in the start state with the state monitoring setting command (nvpstsmonconf) and the data collection setting command (nvpdatacolconf) have been changed.

In MasterScope Network Manager 6.1 or earlier, if the -silent argument was specified with each setting command, the target entry could be stopped to change or delete the entry even if the entry was in the start state. For this reason, if the target entry was specified incorrectly, this could result in the unintended stoppage of entry operation or the deletion of the entry, possibly affecting the operation of the system.

In MasterScope Network Manager 8.0, from the viewpoint of preventing erroneous operations, the specifications have been changed so that if the -silent argument is specified, any entries in the start state cannot be operated. If wanting to operate an entry in the start state, stop the entry operation explicitly first and then change or delete the entry.

5.2.4 Changes to the management method of Cisco ASA 5500 startup-config in multiple context mode

In the Resource Manager function, the management method of startup-configs of Cisco ASA 5500 series under the multiple context mode has been improved.

In version MasterScope Network Manager 5.1, the management method of startup-configs of general contexts has been changed as follows to enable more intuitive management.

The changes are as below.

- Displayed nodes in the startup-config management window
  - Before change

    Only admin context nodes are displayed.
  - After change

    Both admin context nodes and general context nodes are displayed.
- Acquiring, displaying, and detecting differences of startup-configs
  - Before change

Startup-configs of both an admin context and general contexts are merged in one image when acquiring and displaying them. Detecting differences of startup-configs is also performed for the merged image, therefore it is difficult to find a context where a startup-config has been changed.

- After change

  Startup-configs of an admin context and general contexts are acquired and displayed separatedly for each context. Detecting differences is also performed for each context.

- Deploying startup-configs
  - Before change

    It is necessary to deploy them after deleting the sharp (#) at the start of "#~context~" on the start line of the general context image, located in the startup-config image of the Admin context node.

  - After change No special editing operations such as those before the change are necessary. You can execute the deploy operation directly on the general context node. For details of how to make settings for management, refer to "Managing Cisco ASA 5500 redundant/ multiple context mode configuration" in the MasterScope Network Manager User's Manual.

5.3 Specification Changes in Version 6.1

This section describes functions for which specifications have changed under MasterScope Network Manager 6.1

5.3.1 Changes to the target data of the setting backup

In the setting backup function (SysMonMgr -backup), the backup target data has been changed.

MasterScope Network Manager 5.1 and earlier, if configuring the performance management by sFlow with CSV file output option, the following CSV files that contain flow data were also backed up.

- Path of flow data CSV files:

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

These files are used for analyzing flow data by other applications. They are not necessary for restoring the settings.

MasterScope Network Manager 6.1, these files have been excluded from the backup targets to reduce backup data size.

⚠ Caution

If you want to backup the flow data CSV files, copy them to another folder by hand.

5.3.2 Changes to the processing method of Counter-type and Counter64-type MIBs

In the data collecting function, the method of difference calculation for Counter-type and Counter64-type MIBs has been changed.

For details of Counter-type and Counter64-type MIBs, refer to "About Counter-type and Counter64-type MIBs" described later.

MasterScope Network Manager 5.1 and earlier, if the acquired Counter-type or Counter64-type MIB value was less than the previous value (the counter had exceeded the maximum value, and returned to 0), the acquired value was treated as an invalid value. For this reason, when the accumulated value returned to 0, the acquired data was not displayed in the graph.

MasterScope Network Manager 6.1, this specification has been changed to calculate the difference as the accumulated value has returned to 0 only once, if the Counter-type or Counter64-type value is less than the previous value.

This specification change makes it possible to calculate the differences correctly and display graphs without data missing even if the accumulated values have returned to 0 once within the interval.

⚠ Caution

When collecting the Counter-type MIBs, you should specify the appropriate time interval so that the accumulated value does not return to 0 multiple times.

For example, when collecting the traffic (ifInOctets or ifOutOctets) from the interface where 100 Mbps communication always occurs, the accumulated value returns to 0 in about less than 6 minutes (232 * 8 / 100,000,000 (bps) = 343.6 (sec)). If the interval is set to 12 minutes, the accumulated value may return to 0 twice within the interval and the traffic may not be calculated correctly.

In this case, take measures such as shortening the collection interval.

About Counter-type and Counter64-type MIBs

Counter-type and Counter64-type MIBs hold the accumulated values from when the device has started. These accumulated values become useful by calculating the differences from current values and previous values.

The range of Counter-type values is 0 to 4,294,967,295, and the range of Counter64-type values is 0 to 18,446,744,073,709,551,615. These values return to 0 when they exceed the maximum value.

5.3.3 Changing behavior when collection processing is not completed within the interval

In the data collecting function, the data collection behavior has been changed when collection processing is not completed within the interval.

In MasterScope Network Manager 4.0 and 5.1, if the data collection processing was not completed within the interval, the collection processing was skipped at that time and the next interval was set.

- Example: When the collection processing at five minutes intervals is set to Switch A

  If acquisition of data is not completed within five minutes after the first collection request for Switch A, the first request is canceled without collecting data and the second collection request is issued. The second request is also monitored whether the data collection is completed within file minutes. If not, the data collection is skipped and the request is canceled.

In MasterScope Network Manager 6.1, this specification has been changed to wait until the data collection has completed even if the collection processing is not completed within the interval. The specification after changing is the same as MasterScope Network Manager 2.0.

5.3.4 Changes to the default display method for OctetString-type MIBs

The default display method for OctetString-type data in SNMP packes has been changed.

In MasterScope Network Manager 5.1 and earlier, OctetString-type data was displayed in hexadecimal by default. To display OctetString-type data as a character string, the data type defined in AMIB definition files should be changed to "DisplayString". InMasterScope Network Manager 6.1, this specification has been changed to display data in character strings by default.

To display OctetString-type data in hexadecimal, add the MIB object ID in the prescribed file. For details, refer to MasterScope Network Manager User's Manual "7.4.1.5. MIB Definition hexadecimal notation setting procedure".

5.4 Specification Changes in Version 5.1

This section describes functions for which specifications have changed under MasterScope Network Manager 5.1

5.4.1 Changes to the location of MIB definition files

Network Manager comes with the MIB file definition information (AMIB definition files) required to use each function. It is also possible to add new definition information (AMIB definition files) from MIB files published by RFC or device vendors.

In MasterScope Network Manager 4.0 and earlier, the built-in AMIB definition files and user-added AMIB definition files are stored in the same folder. InMasterScope Network Manager 5.1, the installation folder of built-in AMIB definition files has been changed in order to avoid confusion with user-incorporated AMIB definition files.

- Installation path of built-in AMIB definition files (changed) On the manager,

  <On the manager, %installfolder%>\Manager\sg\NvPRO\NVWORK\local\amib\

- Installation path of user-added AMIB definition files (not changed) On the manager,

  <On the manager, %sharefolder%>\Manager\sg\NvPRO\NVWORK\local\amib\

If same definitions exist, the definition in the user-added AMIB definition file is given high priority.

5.4.2 Changes to required software

5.4.2.1 Database software

Through MasterScope Network Manager 4.0, an external database was required, but this is no longer a requirement due to the built-in database included in MasterScope Network Manager 5.1.

If the internal database is used, separate database software is no longer required. However, separate database software is still required when using an external database.

5.4.3 Various changes to Alert Management specifications

5.4.3.1 Alert recovery processing when restarting the Manager

The previous specification, in which all unrecovered alerts were recovered when restarting the Manager, has been improved so that alerts that do not need to be recovered are not automatically recovered when restarting the Manager. Such alerts remain in the same state as before the restart.

Tip

Autorecover alerts detected by the State Monitoring function are automatically recovered when restarting the Manager, and monitoring is resumed the Manager restarts. If an error is still detected after this, the alert is reissued.

5.4.3.2 Changes to the severity level of undefined SNMP trap alerts

In MasterScope Network Manager 4.0 and earlier, the severity level of alerts for received SNMP traps not defined in the trap definition file (i.e., notifications with "Vendor-defined Trap" listed in the Summary field) was set to "Normal."

But in MasterScope Network Manager 5.1, this specification has been changed so that when an SNMP trap is received that is not defined in the trap definition file, the severity level for the notification is now reported as "Unknown."

5.4.3.3 More options in the [Update Property] menu

The icon properties updatable via the node icon right-click menu by clicking [Configuration Management] and selecting [Update Property] have been revised, and now more options are included in the [Update Property] menu.

- Specifications in Version 4.0 and earlier:

  When **pdate Property** was selected, all the properties that could be retrieved from the device were updated.

- Specifications in Version 5.1:

  Update Property>**Update Required Property**, only those properties retrieved from the device that are required for operation of the product are updated.

  Update Property>**Update All Property**, all the properties that can be retrieved from the device are updated, in the same way that they were updated in versions 4.0 and earlier.

Tip

For details regarding the updatable properties, refer to the MasterScope Network Manager User's Manual "4.2.7. Updating device information via a network".

As a result of these changes, even when device properties are updated it is still possible to retain manually input administrator information and default target ports for an interface during operation.

Chapter 6. Precautions and Limitations

In this version, there are following precautions and limitations.

Contents

6.1 Precautions on Upgrading

The following describes the precautions on upgrading an old version to the latest version.

6.1.1 Precautions to take when both new and old versions of the monitoring terminal function exist

Network Manager supplies an arrangement whereby it can support the temporary existence of both new and old versions of the monitoring terminal function, considering the possibility that not all monitoring terminals can be upgraded at once when the environment in which multiple monitoring terminals are deployed and operated is to be upgraded to the new version.

If you connect the new version of the manager function to an old version of the monitoring terminal function, you can perform operations such as map view and alert confirmation in the range of the old version of the function, but you must note the following when performing operations on the old version of the monitoring terminal.

Precautions on menu executions on the map view

If an attempt is made to perform the following menu executions and window operations from an old version (6.1 or earlier) of the monitoring terminal function, an error message is displayed, and they cannot be performed normally.

- **Manual Register** execution and operation
- Map or node

  Property execution and operation
- Connection-line Properties dialog box operation (newly adding)
- Connection-line Properties dialog box operation (editing)

They cannot be performed normally in the following, either.

- Registration of **Simple Line** from the Line Type Selection dialog box
- **Port Name** display setting saving (The display is switched only with the executed monitoring terminal function.)

Precautions on using the device and network autodiscover function

If you register a device or a network by executing the following menu from an old version (6.1 or earlier) of the monitoring terminal function, it is recorded twice in the same audit log.

- Autodiscover of **TCP/IP Hosts**
- Autodiscover of **Network and Routers**
- Autodiscover of **Nexus**

Example of an audit log in which it is recorded twice (message text):

```
A node is added. (NODE=node:192.168.10.250)(METHOD=AUTO DISCOVER)
```

Precautions on using the setting of the network view management authority

With the new version of the monitoring terminal function, even a user who can view only limited maps and nodes can operate all maps and nodes if he or she logs in from an old version (5.1 or earlier) of the monitoring terminal function. In addition, in node copying and movement operations, the management authority set for the node after the operations differs depending on which of the new and old versions of the monitoring terminal functions is used to perform the operations.

For example, if you grant only the management authority for Map_A and Node_A to user management group A, and you paste a copy of Node_A to Map_B from the new version of the monitoring terminal function, the management authority for the pasted Node_A is the same as the original management authority. If, on the other hand, you perform the same operation from an old version of the management terminal function, the management authority for Node_A is the same as that for Map_B, the upper map to which it is pasted.

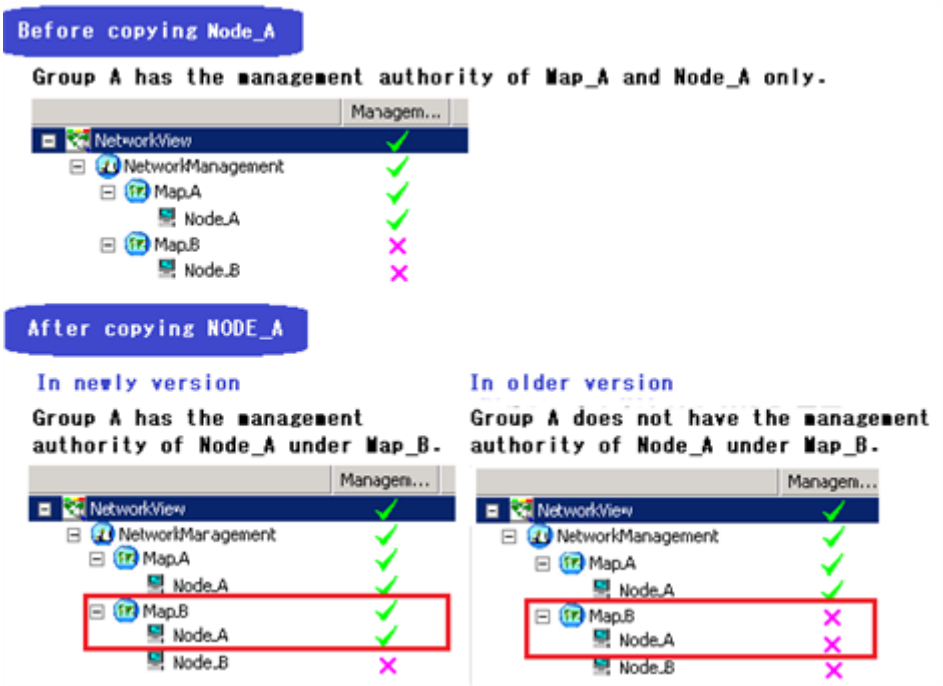


Figure 6-1 Difference in management authority after a node copy operation

⚠ Caution

The operation in which a connection is made to the new version of the manager function with an old version of the monitoring terminal function is a temporary avoidance method for continuing monitoring operation, and longtime operation in this state shall not be guaranteed. It is recommended to upgrade all monitoring terminal functions to the new version as soon as possible.

6.1.2 Precautions on incorporating an MIB for data collection

To make the collection settings for a vendor-extended MIB in the data collection MIB calculation formula, you must incorporate an MIB file containing the definition of the MIB to be collected in Network Manager.

In MasterScope Network Manager 6.1 or later, the processing method has been changed to confirm the definitions in the incorporated MIB file in all processes of the MIB calculation formula, so that the OIDs and instance numbers of the MIB can be determined and processed more accurately. For

this reason, even if MasterScope Network Manager operates normally in an environment of MasterScope Network Manager 5.1 or earlier but if any MIB file has failed to be incorporated, MasterScope Network Manager may not operate normally after upgrade to version 6.1 or later.

Before the upgrade, confirm the MIB file incorporation state to check that there is no MIB incorporation error.

6.2 Precautions on Topology Information Autodiscover

The following describes the precautions on topology information autodiscover.

Precautions on performing physical topology discovery

If you execute **physical topology discovery**, you may not be able to perform the following operations until the completion of the process due to exclusive control for ensuring configuration information consistency.

- Open the menu on the icon (map or node)
- Operation from the WebAPI (configuration information management API) on the icon (map or node)

If you select a map and execute autodiscover of **Physical Topology**, this has an influence on the operation on all maps and nodes under the map. If you select multiple nodes and execute autodiscover of **Physical Topology**, this has an influence on the operation on the selected nodes and the maps on which the nodes are registered.

Precautions on performing ProgrammableFlow Topology discovery

If you execute autodiscover of **ProgrammableFlow Topology**, you may not be able to perform the following operations until the completion of the process due to exclusive control for ensuring configuration information consistency.

- Open the menu on the map and the nodes under the map
- Operation from the WebAPI (configuration information management API) on the map and the nodes under the map

Precautions on operating the Topology Check tool

If you execute the **Check Topology** on a node, you may not be able to perform operations on the node from the WebAPI (configuration information management API) until the completion of the process due to exclusive control for ensuring configuration information consistency.

6.3 Limitation about Patlite reports

The Patlite report using RS-232C port, such as PHC-100A and PHE-3FB, is not supported.

MasterScope Network Manager 9.0
Release Notes

NVP00RE0900-01

January, 2019 1 Edition

NEC Corporation