PureFlow

MonitoringManager2
NF7201A
Operation Manual

Eighth Edition

For safety and warning information, please read this manual before attempting to use the equipment.
Keep this manual with the equipment.

ANRITSU NETWORKS CO., LTD.

Document No.: NF7201-W001E-8.0

Safety Symbols

To prevent the risk of personal injury or loss related to equipment malfunction, Anritsu Corporation uses the following safety symbols to indicate safety-related information. Ensure that you clearly understand the meanings of the symbols BEFORE using the equipment. Some or all of the following symbols may be used on all Anritsu equipment. In addition, there may be other labels attached to products that are not shown in the diagrams in this manual.

Symbols used in manual

⚠ DANGER This indicates a very dangerous procedure that could result in serious injury or death if not performed properly.

⚠ WARNING This indicates a hazardous procedure that could result in serious injury or death if not performed properly.

⚠ CAUTION This indicates a hazardous procedure or danger that could result in light-to-severe injury, or loss related to equipment malfunction, if proper precautions are not taken.

Safety Symbols Used on Equipment and in Manual

The following safety symbols are used inside or on the equipment near operation locations to provide information about safety items and operation precautions. Ensure that you clearly understand the meanings of the symbols and take the necessary precautions BEFORE using the equipment.

This indicates a prohibited operation. The prohibited operation is indicated symbolically in or near the barred circle.

This indicates an obligatory safety precaution. The obligatory operation is indicated symbolically in or near the circle.

This indicates a warning or caution. The contents are indicated symbolically in or near the triangle.

This indicates a note. The contents are described in the box.

These indicate that the marked part should be recycled.

PureFlow
MonitoringManager2 NF7201A
Operation Manual

1 March 2013 (First Edition)
12 March 2018 (Eighth Edition)

System Software License Agreement

This license agreement (“the License”) constitutes a legally binding contract between you and Anritsu Networks Co., Ltd. (“Anritsu Networks”) concerning the use of Anritsu Networks system software (“the Software”). Once you start using the Software, it is deemed that you have agreed to be bound by the provisions in the License and that a contract based on these provisions has been entered into between you and Anritsu Networks.
The Software is protected by all relevant laws and treaties pertaining to copyrights and intellectual property rights, including but not limited to the Copyright Act. Anritsu Networks grants you the right to use the Software as per the License.

1. License Grant

Anritsu Networks grants you the following rights:

1. The Software includes server software and client software. The server software may only be installed on one computer. The client software may be installed on more than one computer.
2. You may use the Software only for the purposes of carrying out operations in your company.

2. Other Rights and Restrictions

1. The Software may not be used concurrently on more than one computer, regardless of whether the computers are owned by you or by a third party.
2. You may not make a copy of the Software for other than backup purposes, nor may you distribute, lend, rent, lease, use as collateral, or otherwise provide the Software to a third party. The license to use the Software cannot be transferred, sold, or otherwise passed to third party. You may under no circumstances transfer the license to use the Software to a worker or member of another company or group.
3. You may not modify, translate, reverse-engineer, decompile, disassemble, or create a product derived from the Software or related documents. You are granted the license to use one copy of the Software, in its entirety. The component parts of the Software may not be used separately.
4. The Software may not be used via a time-sharing, outsourcing, service bureau, or application service provider arrangement, nor may it be used to provide time-sharing, outsourcing, service bureau, or application service provider facilities or support the operations of an application service provider managing these facilities.
5. You may by no means provide access to or give the Software or any part of the Software to any third party or allow any third party to use the Software for business purposes.
6. The SQL Server bundled with the Software may only be used with the Software. It may not be used as a general SQL server, nor may it be used in combination with any other program.
7. You may not modify, correct, or otherwise change the ownership labels on the third-party software bundled with the Software. Source code supplied with third-party software is also subject to the restrictions specified in the License.
8. You may not transfer, gift, or otherwise provide the license or other rights to use the Software and/or related services to an individual or other company or group.

3. Right to Audit

1. Anritsu Networks and its suppliers may audit or use a designated auditor to audit your use of the Software to verify that you are using and managing the Software and

licensed programs in accordance with the terms set out in the License.

2. You agree to give Anritsu Networks and its suppliers or designated auditors reasonable access to your facilities and records for the purpose of conducting these audits. All costs incurred in providing assistance during these audits shall be borne by you; these costs may not be billed to the auditor.

4. License Cancelation and Termination

1. In the event that you violate any of the terms or provisions of the License, Anritsu Networks reserves the right to cancel the License immediately, without prior notice.
2. If the License is canceled, you must cease using the Software and dispose of the Software and all its component parts, all related documents, and all copies of the Software and its related documents, and erase the software completely from the storage media on your computer.
3. Anritsu Networks takes no responsibility for any incidental, consequential, or punitive damages incurred by you or a third party due to an inability to use the Software, in whole or in part, occasioned by the cancelation of the License.

5. Warranty

If the media on which the Software is provided (including the media on which the Software is recorded, the license key, and any other documentation) contains a physical defect, Anritsu Networks will replace the media, providing the defective media is returned within ninety (90) days of purchase. However, this warranty will be void under the following conditions:

- The defect or fault is due to mishandling, misuse, or unauthorized modification or repair of the equipment by the customer.
- The defect or fault is due to severe usage clearly exceeding normal usage.
- The defect or fault is due to improper or insufficient maintenance by the customer.
- The defect or fault is due to natural disaster including fire, flooding, and earthquake.

6. Limitations of Warranty

1. Anritsu Networks does not guarantee to fix any defects, including bugs and structural problems, that might exist in the Software. Each written information or advice given by Anritsu Networks shall require a new warranty, or in any way increase the scope of this warranty.
2. Anritsu Networks reserves the right to change or cease providing incidental services associated with the Software without your prior permission. Anritsu Networks does not guarantee that the usage environment of the Software when the License was concluded will remain the same in perpetuity.

7. Limitations of Liability

In no event will Anritsu Networks, the supplier and/or reseller of the Software, or the supplier of the third-party software be liable for (a) direct, indirect, incidental, special, punitive or consequential damages; or (b) damages from loss of earnings or sales, or loss of data or the opportunity to use data, or any other commercial damages or loss incurred by you or any third party arising from the use of the Software, including as a result of an illegal act or based on a contract or other legal grounds.

8. Confidentiality Obligations and Unauthorized Use of Software

You may not disclose or divulge to a third party, whether by intention or omission, any information obtained from licensing the Software, including but not limited to the Software's source code, construction, and mechanisms, regardless of whether the valid period of the License has expired or not. You may not use the Software in any way that violates the terms of the License.

9. Copyrights and Other Intellectual Property Rights

1. Anritsu Networks and its suppliers own all intellectual property rights, including

proprietary ownership rights and copyrights (hereafter known collectively as the Intellectual Property Rights), to the Software and all related documents, drawings, and other types of documentation.

2. The Intellectual Property Rights are protected by the Copyright Act and all relevant laws and treaties pertaining to copyrights and intellectual property rights, including laws related to intangible property rights.

10. Third-Party Software

1. The intellectual property rights of some of the components used by the Software and included on the delivery media are owned by third-party software vendors. The ownership of these components is described below.
   All copyrights and other intellectual property rights to MySQL, which is the operating environment of the Software, are owned by Oracle Corporation and are protected by the Copyright Act and other relevant laws in the United States and other countries.
2. Anritsu Networks may, for the purposes of redistributing third-party software, provide its suppliers with customer data such as your name and other documents exchanged between you and Anritsu Networks, including order forms and purchase agreements.

11. Export Restrictions

You may not use or otherwise export or re-export directly or indirectly this Software except as authorized by Japanese and United States law. In particular, this software may not be exported or re-exported (a) into any Japanese or US embargoed countries or (b) to anyone on the Japanese or US Treasury Department's list of Specially Designated Nationals or the US Department of Commerce Denied Persons List or Entity List. By using this Software, you warrant that you are not located in any such country or on any such list. You also agree that you will not use this Software for any purposes prohibited by Japanese and US law, including, without limitation, the development, design and manufacture or production of missiles or nuclear, chemical or biological weapons of mass destruction.

12. Reparations

If Anritsu Networks suffers any loss, financial or otherwise, due to your violation of the terms of this EULA, Anritsu Networks shall have the right to seek proportional damages from you.

13. Dispute Resolution

If matters of dispute or items not covered by this EULA arise, they shall be resolved by negotiations in good faith between you and Anritsu Networks.

14. Jurisdiction and Other Matters

The License is governed by the laws of Japan, without regard to conflicts of laws principles.

Anritsu Networks Co., Ltd. Contact

In the event of this equipment malfunctions, contact an Anritsu Networks Co., Ltd. Service and Sales office. Contact information can be found on the last page of the printed version of this manual, and is available in a separate file on the CD version.

Maintenance Agreement

Concluding a maintenance agreement provides you with access to a range of services. For details about our maintenance agreements, contact an Anritsu Networks sales representative or dealer.

Notes On Export Management

This product and its manuals may require an Export License/Approval by the Government of the product's country of origin for re-export from your country.

Before re-exporting the product or manuals, please contact us to confirm whether they are export-controlled items or not.

When you dispose of export-controlled items, the products/manuals need to be broken/shredded so as not to be unlawfully used for military purpose.

Trademark and Registered Trademark

Microsoft®, Windows®, Windows Server® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Core™ i3 is registered trademarks of Intel Corporation or its subsidiaries in the USA and other countries.

Oracle and Java are registered trademarks of Oracle Corporation and its affiliate or subsidiary companies in the United States and/or other countries. All the other company and product names included in this document are the registered trademarks or trademarks of their respective owners.

Acrobat® Reader® are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Reuse parts

Anritsu group promotes recycling activities in order to reuse available resources and save energy. This product may use recycled parts (mechanical components) that conform to Anritsu’s quality standards.

(Blank page)

About This Manual

This operation manual is intended for network administrators in charge of introducing, operating, and managing MonitoringManager2 (traffic-monitoring software for PureFlow GS1, GSX, WSX, and WS1). This manual is aimed at readers who have basic knowledge about the following aspects of internetworking:

- Local area networks (LAN)
- Ethernet
- Internet protocol (IP)

Table of Contents

(Blank page)

This chapter provides an overview of MonitoringManager2.

1.1 Overview of MonitoringManager2

MonitoringManager2 enables you to collect statistics on the traffic flowing in PureFlow GS1, GSX, WSX, and WS1 (also refered as "PureFlow node"), accumulate the statistics required for trend analysis, view the data in a graph, create a report, and edit data in Windows.

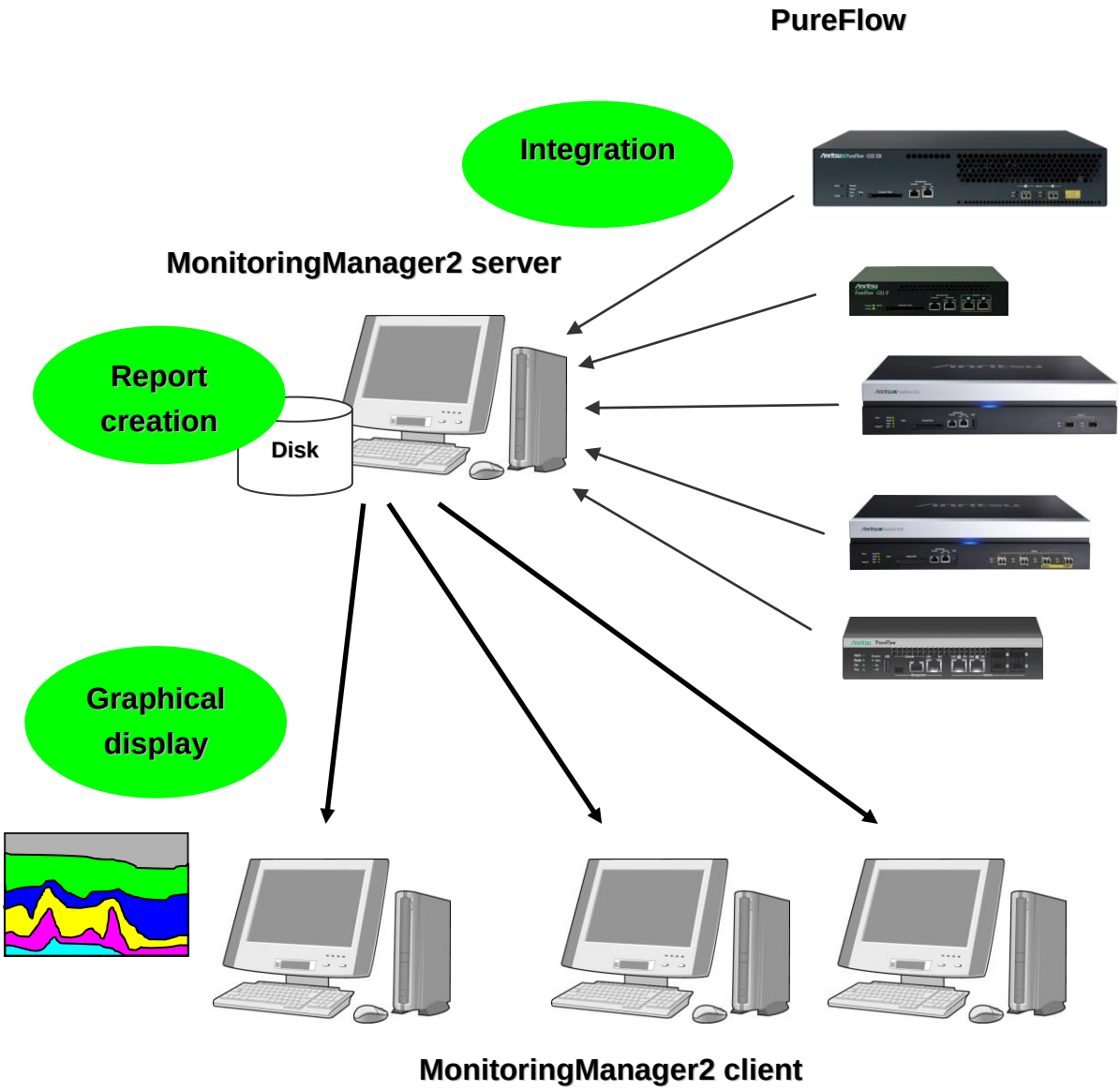


Figure 1.1-1 System configuration

By using the client software, you can manage the data collected by the server software of MonitoringManager2 from another PC via the network. The client software can be installed in multiple PCs.

Note:

Do not start up and configure (perform PureFlow registration, etc.) multiple copies of the client software at the same time. This might disable the graphical display and report creation features.

PureFlow node manage statistics by hierarchically shaping the traffic flowing on the network according to traffic attributes such as minimum/maximum bandwidth and buffer size.

The server software of MonitoringManager2 collects statistics periodically and stores them in the database. The client software of MonitoringManager2 allows you to view information such as traffic flow volume and network usage in real time by using GUI graphs or tables. Additionally, you can create a report that includes data stored in the database. There are two types of report formats: HTML and CSV.

The types of statistics that can be managed by using PureFlow node are described below.

- Monitor information
  The monitor information consists of the port counter and scenario counter. This information is the statistics of each port and scenario.
  In MonitoringManager2, the graph based on this monitor information is referred to as a scenario graph. The scenario graph allows you to easily check the volume of the traffic flowing in the scenarios of PureFlow node. Analyzing this graph allows you to determine whether the bandwidth divided and allocated by hierarchical shaping is correct or not.

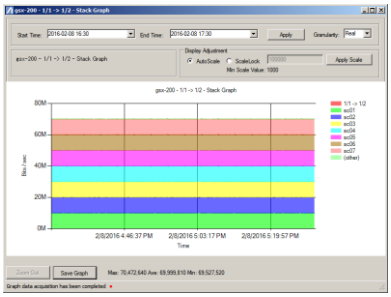


Figure 1.1-2 Scenario graph

By using MonitoringManager2, the threshold value of traffic flow volume can be set and a threshold value event issued if this threshold is reached. This enables network problems to be detected and resolved quickly and accurately.

- Top information
  The top information includes the top counter. This information helps you to ascertain network usage.
  In MonitoringManager2, the graph based on this top information is referred to as a top graph. The top graph allows you to check network usage in descending order of traffic flow volume for the top 25 users. Analyzing this graph allows you to determine the policy of allocating network bandwidth to users.

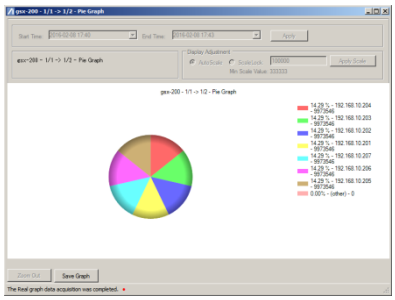


Figure 1.1-3 Top graph

The statistics (monitoring information) of PureFlow node that can be monitored from MonitoringManager2 are indicated below. For details about the monitoring information, see

PureFlowGS1 -
PureFlow GS1 Traffic Shaper PF7000C/PF7001C/PF7010C/PF7011C Operation Manual Configuration Guide

PureFlowGSX -
PureFlow GSX Traffic Shaper NF7101C Configuration Guide

PureFlowWSX -
PureFlow WSX Unified Network Controller NF7600 series Configuration Guide TCP Acceleration Edition
PureFlow WSX Unified Network Controller NF7600 series Configuration Guide Traffic Shaping Edition

PureFlowWS1 -
PureFlow WS1 Unified Network Controller NF7500 series Configuration Guide

Table 1.1-1 Monitoring information

Monitoring information			Minimum version of Monitoring Manager 2				
			GS1	GSX	WSX QoS	WSX TCP	WS1
Monitor information	Port counter	Traffic per port	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
	Scenario counter	Traffic per scenario	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
		Traffic per GS1 virtual channel (application queue mode) (Note 1)	×	–	–	–	–
		Scenario expansion option (Note 2)	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
		Discarded traffic	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
		Peak rate value for 1 minute	–	1.2.1	1.2.1	2.1.1	2.2.1
Top information	Top counter (up to top 25)	Source IP address	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
		Destination IP address	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
		Source IP address and destination IP address	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
		Application number (port number)	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
Display of properties (bandwidth) of port/scenario Content-aware shaping ● Bandwidth of virtual channel (application queue mode) 3-layer shaping ● Maximum transmission rate for network port ● Minimum bandwidth guarantee for virtual pipe			1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
Display of configuration of traffic acceleration function ● Primary peer, Secondary peer ● TCP-FEC function (enable, disable) ● compression function (enable, disable)			–	–	–	2.1.1	2.2.1

×: Monitoring disabled; –: The device is not equipped with the corresponding function.
WSX QoS: PureFlow WSX (Traffic shaping)
WSX TCP: PureFlow WSX (TCP acceleration)

Notes:

1. To monitor the content aware-shaping application in PureFlow GS1, License Key 1 of PureFlow GS1 must be enabled. Content-aware shaping is not available in PureFlow GSX, WSX, and WS1.

2. The number of scenarios for which statistics can be collected is limited according to the monitor information notification cycle. If the number of scenarios is set to 2,048 or more by using the scenario expansion option (License Key 3) of PureFlow GS1, or if PureFlow GSX, WSX, and WS1 is connected, set the monitor notification cycle and the number of scenarios to within the range shown in Table 1.3-1.

The formats in which graphs can be displayed and reports created in MonitoringManager2 are indicated below.

Table 1.1-2 Graph display and report creation formats

Graph display and report creation format				Minimum version of Monitoring Manager 2				
				GS1	GSX	WSX QoS	WSX TCP	WS1
Scenario graph	Real-time or stored data		Stacked bar graph	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
			Circle graph	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
			Bar graph	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
			Line graph	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
			Tables	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
	Report	Periodic	CSV	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
			HTML	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
		Manual	CSV	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
			HTML	1.1.1	1.1.1	1.2.1	2.1.1	2.2.1
Top graph	Real-time or stored data		Circle graph	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
			Tables	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
	Report	Periodic	CSV	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
			HTML	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
		Manual	CSV	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1
			HTML	1.2.1	1.2.1	1.2.1	2.1.1	2.2.1

WSX QoS: PureFlow WSX (Traffic shaping)
WSX TCP: PureFlow WSX (TCP acceleration)

Notes:

1. The peak can be monitored only when the monitor information notification cycle is set to 60 seconds.

2. Only a stacked bar graph or line graph can display the peak.

3. PureFlow WSX (TCP acceleration) and WS1 can display the Network port information in graph form.

4. A time mode setting feature is provided in MonitoringManager2 to support different time zones.
   The time modes are UTC mode and local time mode. In UTC mode, the monitor notification time stamp of PureFlow node is based on UTC (Coordinated Universal Time).
   In local time mode, the monitor notification time stamp of PureFlow node is based on the local time.
   Note that local time mode is provided to maintain compatibility with PureFlow GS1 v3.3.3 or earlier and PureFlow GSX (NF7101A) v1.1.1. Do not use this mode in the current version. Use UTC mode as the time mode. The time modes available in each version are listed in Tables 1.1-3 and 1.1-4.
   If local time mode is used and the time is set to a time zone that uses daylight saving time, the data when daylight saving time starts and ends might be duplicated or lost. For details, see Chapter 8.

Table 1.1-3 Correspondence table of PureFlow GS1(PF70XXC) version

MonitoringManager2	PureFlow GS1	
	v3.3.3 or earlier	v3.4.1 or later
Local time mode	Supported	Supported (Do not use this mode.)
UTC mode	Not supported	Supported

Table 1.1-4 Correspondence table of PureFlow GSX(NF7101C) version

MonitoringManager2	PureFlow GSX	
	v1.1.1	V1.2.1 or later
Local time mode	Supported	Supported (Do not use this mode.)
UTC mode	Not supported	Supported

1.2 Product configuration

1.2.1 List of part names

MonitoringManager2 is configured as described in the table below.

Table 1.2.1-1 List of part names

Model name	Part name	Overview
NF7201A	MonitoringManager2 basic license	Software: 1 copy on CD-R Basic license document: 1 copy

1.2.2 Product outline

MonitoringManager2 consists of server software, client software, and a basic license.

(1) Server software
Obtains the statistics collected from PureFlow node upon request from a client and sends the statistics to the client.

(2) Client software
Graphically displays the statistics sent from the server. The client software does not have to be installed in the same terminal as the one in which the server software is installed. Up to four clients can be connected to the server software at the same time.

(3) Basic license
This is the license key of the server software. This license allows up to five PureFlow node units to be used for monitoring. After installing the server software, issue the license key following the procedure described in the basic license key issuance guide stored on the CD-R. For how to install the issued license key, see "2.2 Installing the basic license file".

1.2.3 List of optional parts

Table 1.2.3-1 List of part names

Model name	Part name	Overview
NF7201-L001A	MonitoringManager2 additional license	Up to five PureFlow units can be added per license. Additional license document: 1 copy

1.2.4 Optional part outline

MonitoringManager2 additional license

This license is required to add PureFlow node units for monitoring. Up to five PureFlow node units can be added per license.

Up to 255 PureFlow node units can be added for monitoring by purchasing multiple licenses. For details of how to install additional licenses, see "2.3 Installing an additional license file".

Note:

One PureFlow node unit is counted as one unit for the purposes of this license, regardless of whether the unit is a management target or not.

1.3 Minimum operating environment

The minimum operating environment for MonitoringManager2 is described below.

Server software

- OS: Microsoft Windows Server 2016 Standard
  Microsoft Windows Server 2016 Datacenter
  Microsoft Windows Server 2012 Standard
  Microsoft Windows Server 2012 R2 Standard
  Microsoft Windows Server 2012 R2 Datacenter
  Microsoft Windows Server 2008 R2 Enterprise Edition (64-bit) SP1
  Microsoft Windows Server 2008 R2 Standard Edition (64-bit) SP1
- CPU: Core i3 2100 3.1 GHz
- Memory: 6 GB
- Hard disk: SAS RAID1 (500G) × 2

Note:

4.5 GB of free disk space for .NET framework 4.5.2 installation.

Client software

- OS: Microsoft Windows Server 2016 Standard
  Microsoft Windows Server 2016 Datacenter
  Microsoft Windows Server 2012 Standard
  Microsoft Windows Server 2012 R2 Standard
  Microsoft Windows Server 2012 R2 Datacenter
  Microsoft Windows Server 2008 R2 Enterprise Edition (64-bit) SP1
  Microsoft Windows Server 2008 R2 Standard Edition (64-bit) SP1
  Microsoft Windows 10 Professional (64-bit)
  Microsoft Windows 8.1 Professional (64-bit)
  Microsoft Windows 7 Professional (64-bit) SP1
- CPU: 1 GHz
- Memory: 2 GB
- Hard disk: 500 MB or more (size required for installation)

Note:

4.5 GB of free disk space for .NET framework 4.5.2 installation.

Supported PureFlow software version is described below.

PureFlow GS1(PF70XXC) software

- Version 3.3.3 or later

Note:

To monitor GS1, check that the software version of PureFlow GS1 is v3.3.3 or later.
Before connecting GS1 as a management target, execute the following command to set

the report mode.

PureFlow(A)> set probeagent reportmode all

If this setting is not enabled in the management target GS1, report data might be lost, and cause abnormal output in graph and report.

PureFlow GSX (NF7101C) software

- Version 1.1.1 or later

PureFlow WSX NF7600 series software
Traffic shaping software license applied

- Version 2.1.1 or later

Note:

If PureFlowWSX (traffic shaping software license applied) version is later than 2.1.1 and prior to 2.4.1, scenario tree display icon and pureflow device type displays as PureFlow GSX (NF7101C).

PureFlow WSX NF7600 series software
TCP acceleration software license applied

- Version 2.4.1 or later

PureFlow WS1 NF7500 series software

- Version 1.1.1 or later

Note:

When installing the server software and client software in a single computer, the required hard disk capacity is 500 GB or more.

In the operating environment of MonitoringManager2, use a script such as NTP startup to synchronize the time of PureFlow node to the time of the computers used for the server software and client software. Time gap between MonitoringManager2 and PureFlow node cause abnormal output in graph and report.

Note that even in the above environment, MonitoringManager2 may not operate, depending on the status of Windows Update or other applications.

Notes:

1. The number of scenarios that can be managed in this software varies depending on factors such as the hardware specifications of the server, the number of managed PureFlow units, and the number of reports output. The management and operation must be studied based on the server hardware disk I/O and amount of memory. The following table shows a guide to the number of scenarios (total number of scenarios regardless of the number of PureFlow units) that can be managed under the conditions of the server hardware specifications for each collection cycle.

   * "Can be managed" means that information collection and every-hour report output can be performed in the normal manner. The following table shows a guide to the number of scenario, when CSV report is output with 2048 scenarios. (If the number of maximum scenario is 800, the CSV report is output with 800 scenarios.)

   The number of scenarios that can be managed by MonitoringManager2 might be lower, depending on factors such as the hardware specifications of the server, the number of managed PureFlow units, and the number of reports output. How MonitoringManager2 is used must be decided based on the performance of the server hardware disk I/O and amount of memory installed.
   The following table shows a guide to the total number of scenarios that can be output in a CSV periodic report when one PureFlow node unit is being managed under the specified server hardware and monitoring collection cycle conditions.

Table 1.3-1 A guide to the number of scenarios that can be managed

Server hardware specifications	Collection cycle = 10 seconds	Collection cycle = 30 seconds	Collection cycle = 60 seconds
CPU: Core i3 2100 3.1 GHz Memory: 6 GB Hard disk: SAS RAID1 × 2	Up to 800 scenarios	Up to 2,048 scenarios	Up to 4,096 scenarios
CPU: Xeon X5470 3.33 GHz Memory: 6 GB Hard disk: SAS RAID5 × 3	Up to 2,048 scenarios	Up to 4,096 scenarios	Up to 40,000 scenarios
CPU: Xeon E5-2670 2.60 GHz Memory: 16 GB Hard disk: SAS RAID5+0 × 6	Up to 2,048 scenarios	Up to 4,096 scenarios	Up to 80,000 scenarios

2. If antivirus software is running at the same time as MonitoringManager2, the performance of MonitoringManager2 might drop significantly, correct data might not be able to be collected, or it may take a long time to output reports.

3. meet the minimum operating environments, "Server communication error occured. Restart MMClient." may be displayed on the output of MMClient. If the message is displayed, please review the server specifications and the scenario configuration.

4. Secure sufficient traffic between the server software of this software and PureFlow to receive and transmit the statistics information constantly. Traffic for about 10 Mbps is required when 80,000 scenarios are collected in the 60-second cycle.

A fee-based service is available to verify operation of MonitoringManager2 in your operating environment before purchase.

This chapter describes how to install MonitoringManager2.

2.1 Installation procedure

2.1.1 Installing the server software of PureFlow MonitoringManager2

* Execute MM2ServerSetup.exe on the CD-R.
* The language used for setup is selected based on the language specified in the OS.

Note:

The **User Account Control** screen will be displayed depending on the permissions of the user to install and the environment setting of the installation destination, so click the "**Yes**" button. The following is an example of the screen of Windows Server 2016. (The screen displayed by the OS may be different.)

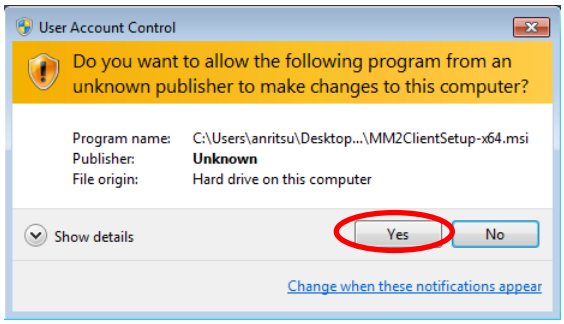


Figure 2.1.1-1 User Account Control dialog box

Installing the server software

1. If .NET Framework 4.5.2 is not installed, agree to the terms of the license agreement and then install it. If .NET Framework 4.5.2 or later have been already installed, this operation is skipped automatically and advances to the next clause.
2. The **Welcome to the MonitoringManager2 Server Software Setup Wizard** dialog box appears. Click **Next**.

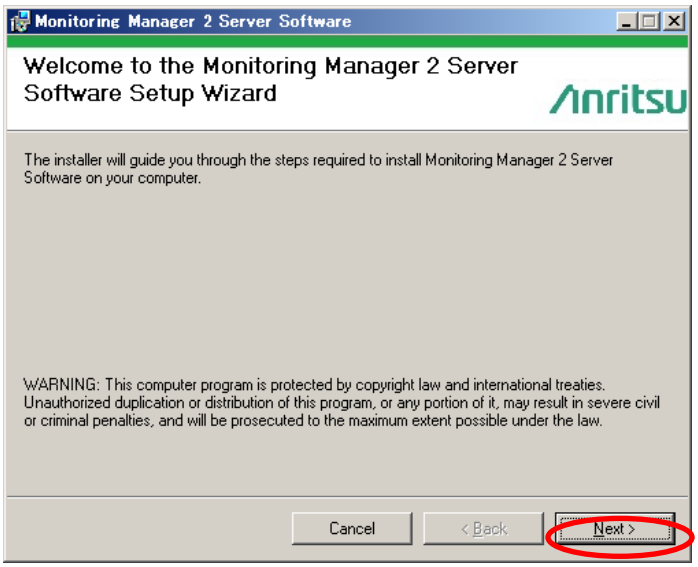


Figure 2.1.1-2 Welcome to the MonitoringManager2 Setup Wizard dialog box

3. The **License Agreement** dialog box appears. Select **I Agree** and click **Next**.

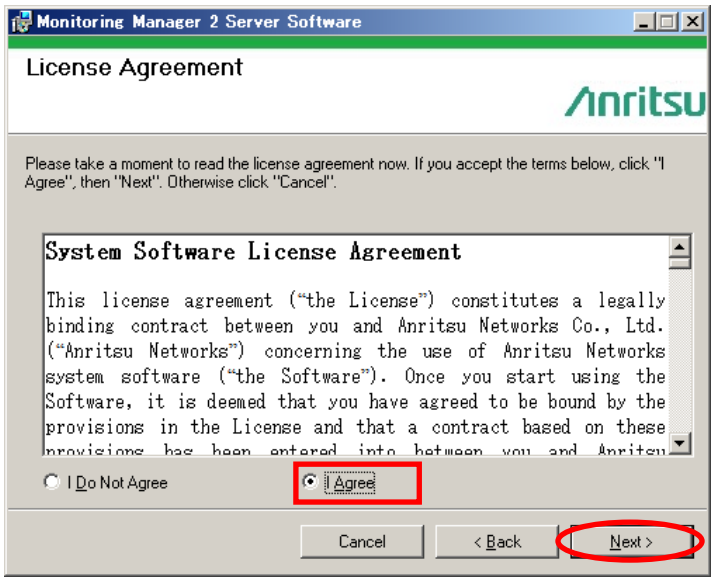


Figure 2.1.1-3 License Agreement dialog box

4. The **Select Installation Folder** dialog box appears. Select a user to be installed according to the security policy, and click **Next**.

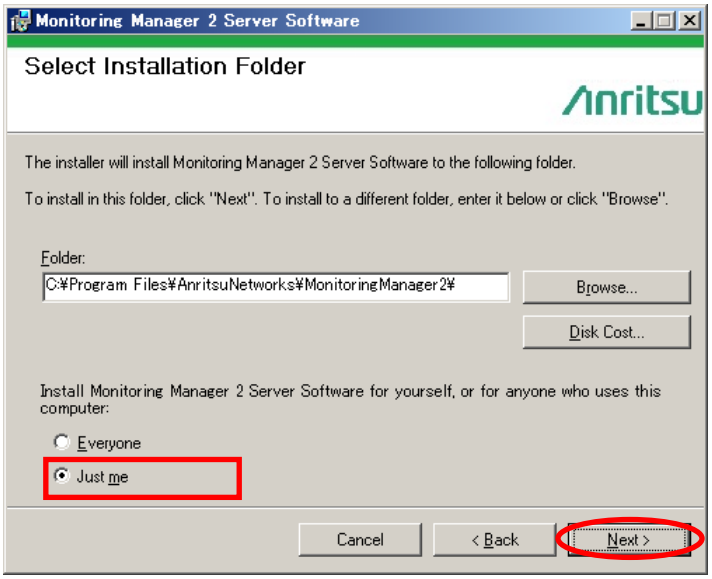


Figure 2.1.1-4 Select Installation Folder dialog box

5. The **Confirm Installation** dialog box appears. Click **Next**.

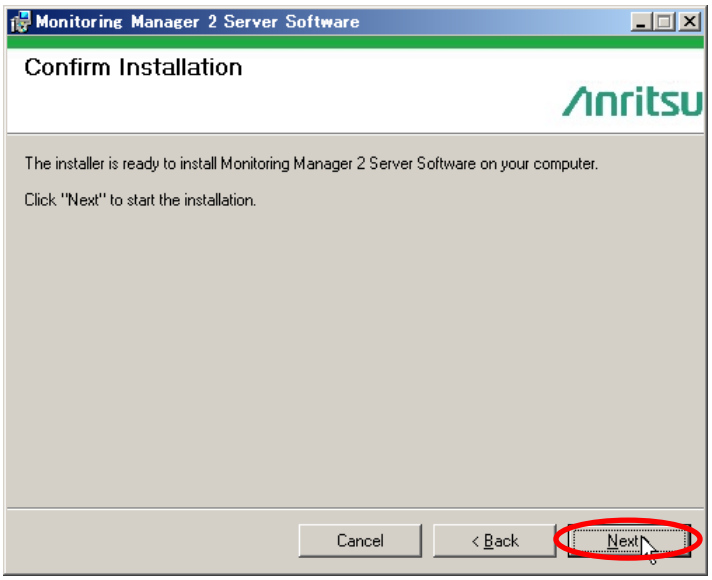


Figure 2.1.1-5 Confirm Installation dialog box

6. The **Select Database Folder**, **Setting Time Mode** dialog box appears. Select **UTC Mode** and click **Next**.

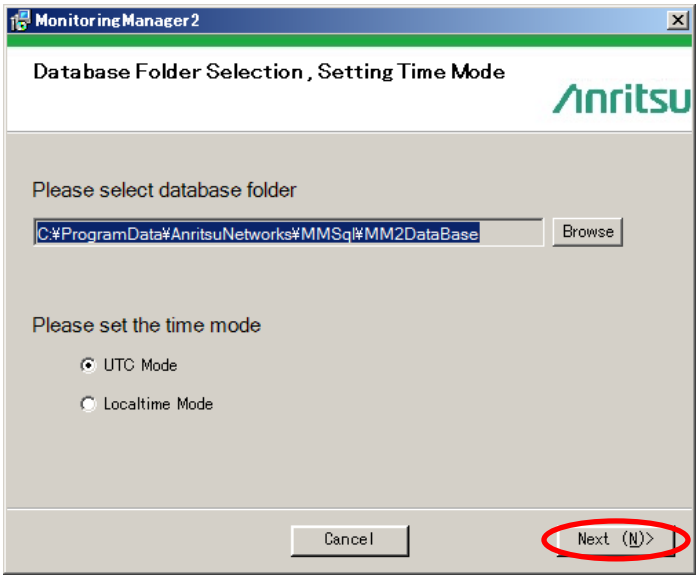


Figure 2.1.1-6 Select Database Folder dialog box

Note:

If local time mode is selected as the time mode of MonitoringManager2, select **Local Time Mode** here. Note that local time mode is provided to maintain compatibility with PureFlow GS1 v3.3.3 or earlier and PureFlow GSX (NF7101A) v1.1.1. Refer to Chapter 8 Time Modes to confirm the time mode that should be selected here.

7. The **Confirm Initialization** dialog box appears when the statistic information and setting information already exists. If you want to initialize current settings of MonitoringManager2, click **Yes** to initialize current settings. When reinstalling the software, if you want to keep the original database and report settings, click **No**. Dialog is not displayed at initial installation.

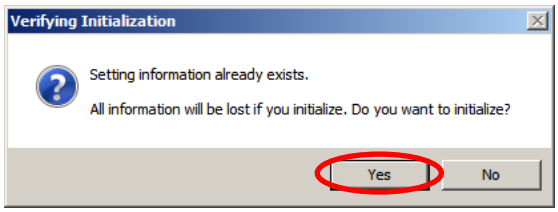


Figure 2.1.1-7 Confirm Initialization dialog box

8. The **Confirm Service Start** dialog box appears. Click **Yes**. Starting MonitoringManager2 server software.

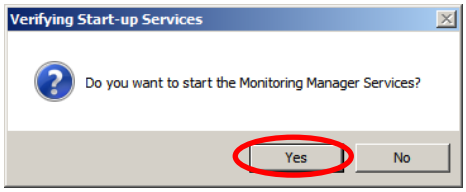


Figure 2.1.1-8 Confirm Service Start dialog box

Note:

Check that the server physical port that activates the server software is linked before starting Monitoring Manager Service. In versions v1.2.3 and earlier, if the server physical port links and is connected to the network after starting the server software while the server physical port is not linked, collection of statistics information does not start.

9. The **Installation Complete** dialog box appears. Click **Close**.

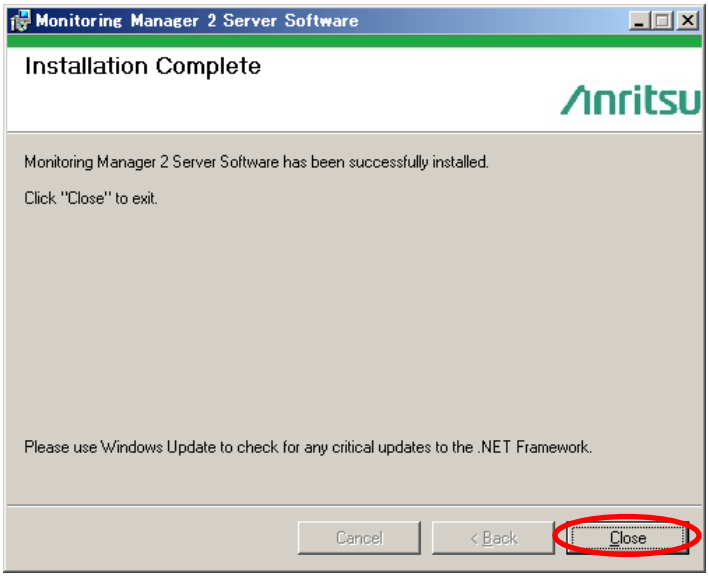


Figure 2.1.1-9 Installation Complete dialog box

Note:

Please do not change the folder name when you copy the folder of the CD-R. The installation of folder that you copied may not be carried out correctly.

2.1.2 Installing the client software of PureFlow MonitoringManager2

* Execute MM2ClientSetup.exe on the CD-R.
* The language used for setup is selected based on the language specified in the OS.

Note:

The **User Account Control** screen will be displayed depending on the permissions of the user to install and the environment setting of the installation destination, so click the "**Yes**" button. The following is an example of the screen of Windows Server 2016. (The screen displayed by the OS may be different.)

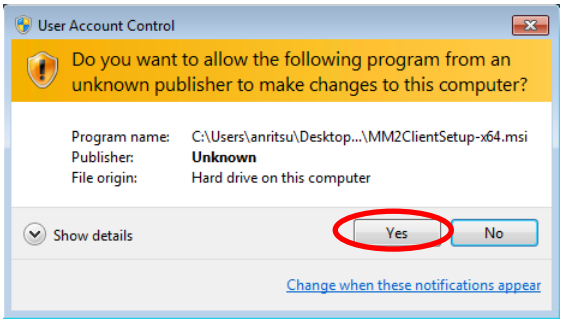


Figure 2.1.2-1 User Account Control dialog box

Installing the client software

1. If .NET Framework 4.5.2 is not installed, agree to the terms of the license agreement and then install it. If .NET Framework 4.5.2 or later have been already installed, this operation is skipped automatically and advances to the next clause.
2. The **Welcome to the MonitoringManager2 Client Software Setup Wizard** dialog box appears. Click **Next**.

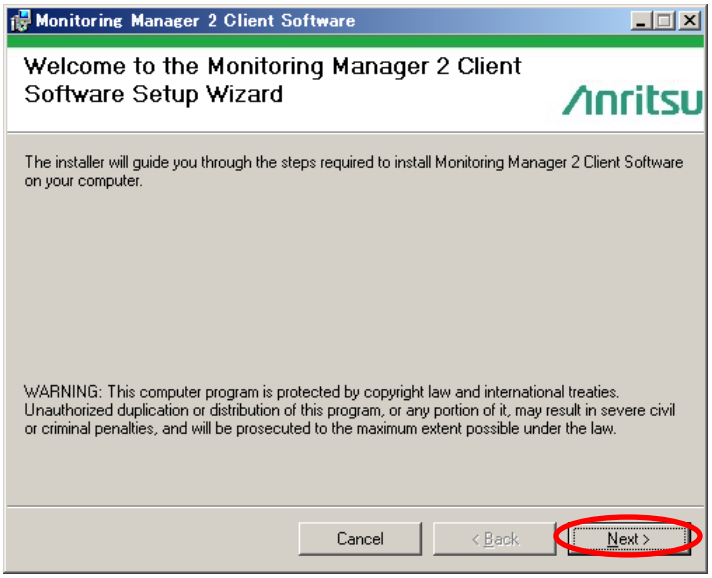


Figure 2.1.2-2 Welcome to the MonitoringManager2 Setup Wizard dialog box

3. The **License Agreement** dialog box appears. Select **I Agree** and click **Next**.

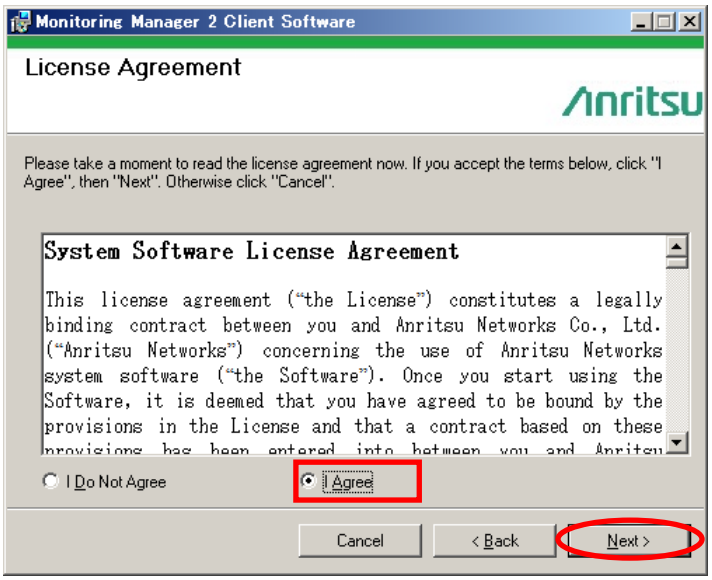


Figure 2.1.2-3 License Agreement dialog box

4. The **Select Installation Folder** dialog box appears. Select a user to be installed according to the security policy, and click **Next**.

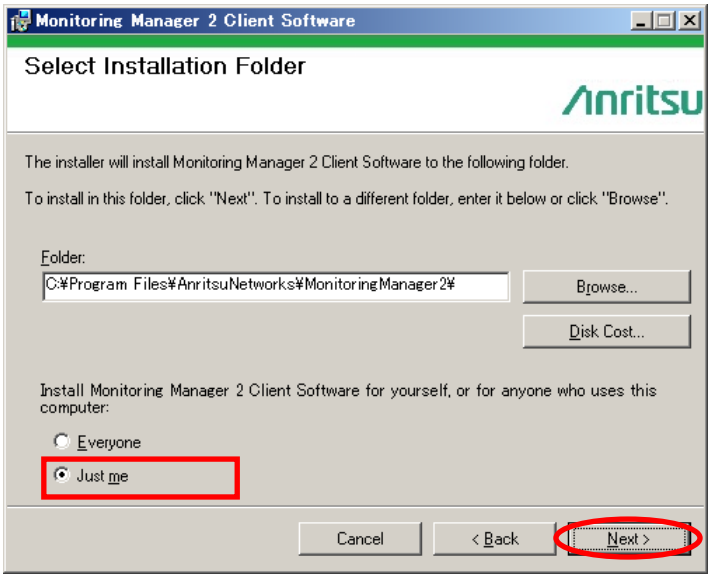


Figure 2.1.2-4 Select Installation Folder dialog box

5. The **Confirm Installation** dialog box appears. Click **Next**.

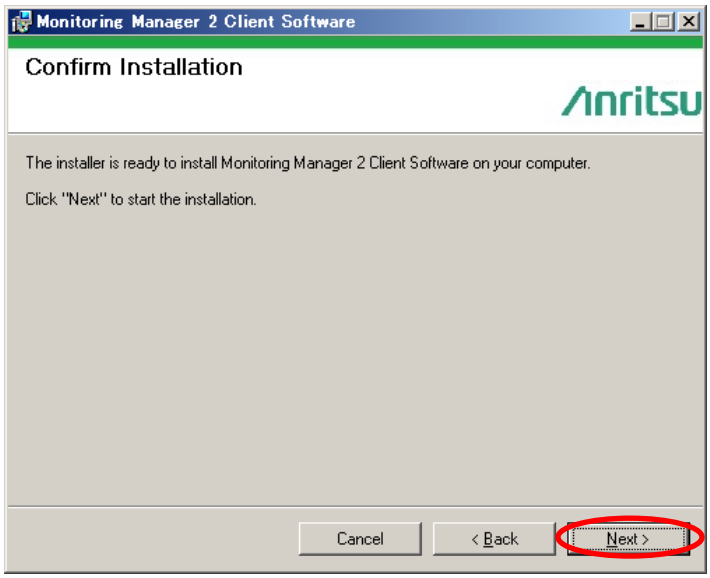


Figure 2.1.2-5 Confirm Installation dialog box

6. The **Installation Complete** dialog box appears. Click **Close**.

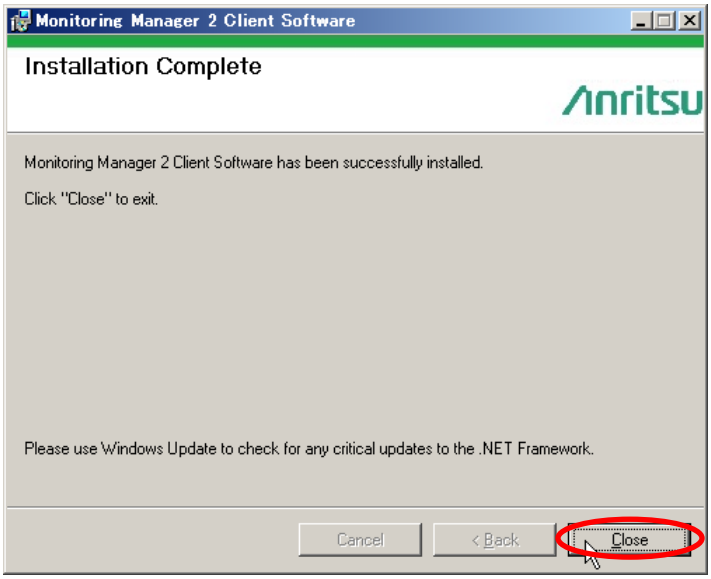


Figure 2.1.2-6 Installation Complete dialog box

Note:

Please do not change the folder name when you copy the folder of the CD-R. The installation of folder that you copied may not be carried out correctly.

2.2 Installing the basic license file

After installing the server software, issue the license key following the procedure described in the basic license key issuance guide stored on the CD-R.

After issuing the license key, store the received `license_mm.txt` file in the following location:
`Installation directory of MonitoringManager2/MMCollector` directory

When installing the server software in the default location, store it in:

```
C:\Program Files\AnritsuNetworks\MonitoringManager2\MMCollector\
```

After the license file is installed, it becomes valid when MMCollector service is next started. If MMCollector service is already running, restart it.
For details of how to start MMCollector service, see 7.3 Service management.

Notes:

1. If the basic license is not installed, you cannot register the devices to be monitored in this software.

2. The MAC address of the terminal in which MonitoringManager2 is installed is required when issuing the basic license.

2.3 Installing an additional license file

To add devices to be monitored, a PureFlow MonitoringManager2 additional license (NF7201-L001A) must be purchased. After purchasing this license, issue the license following the additional license key issuance procedure supplied by Anritsu. License files equivalent to the number of added units will be sent.

Store the received `license_mm.txt` file in the following location:
`Installation directory of MonitoringManager2/MMCollector` directory

When installing the server software in the default location, store it in:

```
C:\Program Files\AnritsuNetworks\MonitoringManager2\MMCollector\
```

If the `license_mm.txt` file already exists in the installation location, move it to another directory or delete it, and then copy the new `license_mm.txt` file to the installation location.

After the license file is installed, it becomes valid when MMCollector serviceis next started. If MMCollector service is already running, restart it.
For details of how to start MMCollector service, see 7.3 Service management.

Notes:

1. You can add up to five units per additional license.

2. To issue additional licenses after purchasing MonitoringManager2, you will need the serial number of the basic license, the serial number described in the additional license document, and the MAC address of the terminal in which the basic license is installed.

2.4 Installing the MonitoringManager2 instruction manual

After installing the client software, install the instruction manual PDF file. By installing this file, you can display the instruction manual from MMClient help menu.

Copy the instruction manual PDF file from CD-R in to the following location, and then change the file name to the specified name.

1) Make a local copy of instruction manual PDF file.
   Location of instruction manual PDF file in CD-R:
   NF7201-W001E-x.x_PureFlowMM2_operation_manual.pdf
   Where x.x is the version number of the operation manual. File name in the case of the sixth edition are as follows.
   NF7201-W001E-6.0_PureFlowMM2_operation_manual.pdf
2) Move a copy of instruction manual PDF file to specified MMClient folder
   Folder to which to copy instruction manual PDF file (installation folder of MMClient):
   `Installation directory of MonitoringManager2\MMClient\DOC\`
3) Change the file name as follows:
   MM2OperationManual.pdf

The following is an example for when MonitoringManager2 is installed in the default location:

```
C:\Program Files\AnritsuNetworks\MonitoringManager2\
  MMClient\DOC\MM2OperationManual.pdf
```

Note:

The instruction manual cannot be displayed in an environment in which PDF files cannot be viewed. Make sure that Adobe Acrobat Reader (10.0 or later) is installed before installing the instruction manual PDF file.

2.5 Cautions

2.5.1 Files in installation folder

Do not change, delete, move, overwrite, or add files in the installation folder by using methods other than those described in the instruction manual. Otherwise, MonitoringManager2 might not operate correctly, or might not be able to be uninstalled or recovered in the event of a failure.

MonitoringManager2 is located in the following folder by default:

```
C:\Program Files\AnritsuNetworks\MonitoringManager2\
```

2.5.2 Reflection of report settings at re-installing and upgrading the version

If the server software is re-installed or the version is upgraded without initialization, or if the backup data of the database is restored after re-installing the server software or upgrading the version following initialization, the periodic report setting is reflected as report execution is disabled.

This chapter describes how to uninstall MonitoringManager2.

3.1 Uninstallation procedure

Uninstall the client software and server software of MonitoringManager2 according to the procedures described below. After uninstallation is complete, restart Windows.

3.1.1 Uninstalling the client software of PureFlow MonitoringManager2

1. Close the graph window displayed by the client software.
2. Be sure to close the client software window.
3. Select **Uninstall a program** under **Programs** in **Control Panel**.

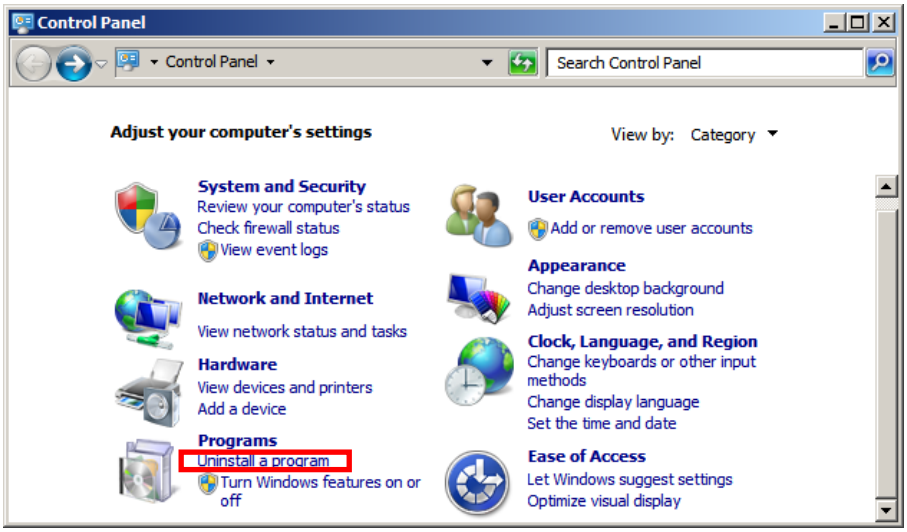


Figure 3.1.1-1 Control Panel

4. Select **MonitoringManager2 Client Software** and then click **Uninstall**.

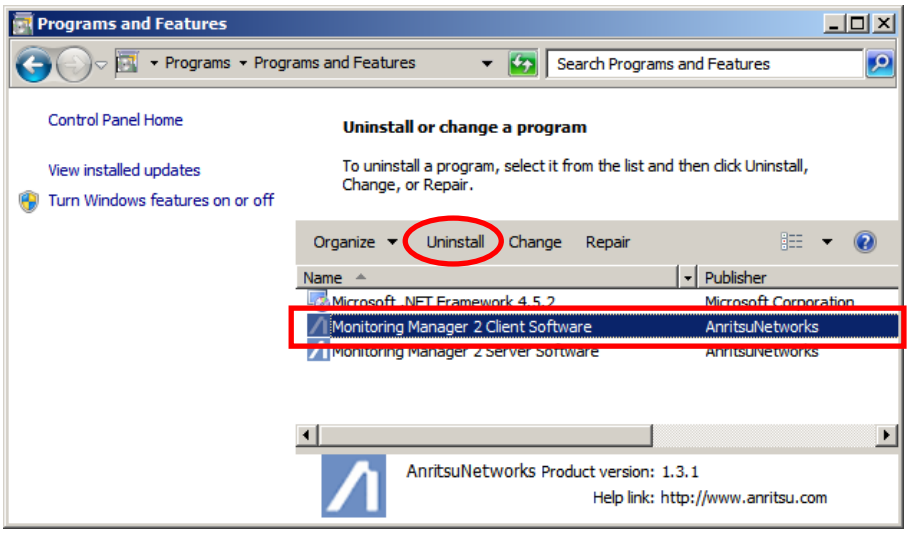


Figure 3.1.1-2 Programs and Features

Note:

In Windows 7, the **User Account Control** dialog box might appear. If this dialog box appears, click **Yes**.

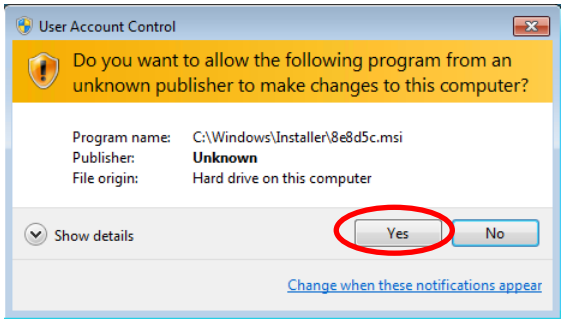


Figure 3.1.1-3 User Account Control dialog box

5. When the uninstallation confirmation dialog box appears, click **Yes**.

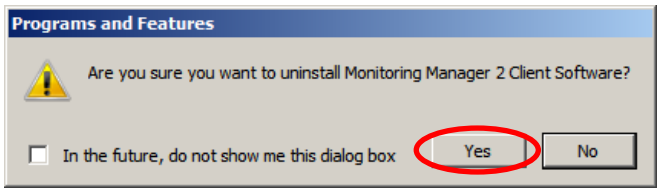


Figure 3.1.1-4 Uninstallation confirmation dialog box

* If the restart confirmation dialog box appears, select **Automatically close applications and attempt to restart them after setup is complete** and click **OK**.

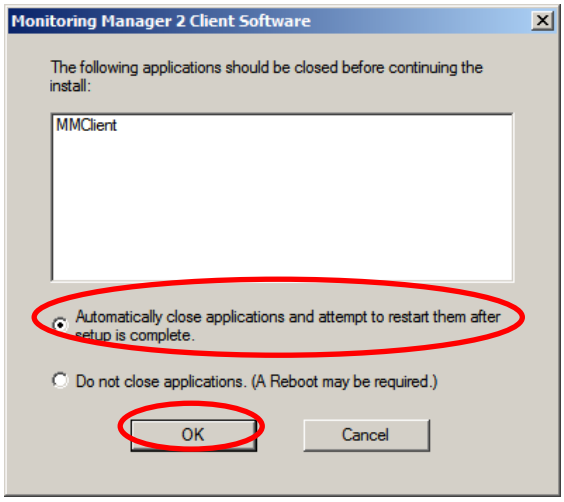


Figure 3.1.1-5 Restart confirmation dialog box

3.1.2 Uninstalling the server software of PureFlow MonitoringManager2

1. Be sure to close the client software and server software windows.
2. Select **Uninstall a program** under **Programs** in **Control Panel**.

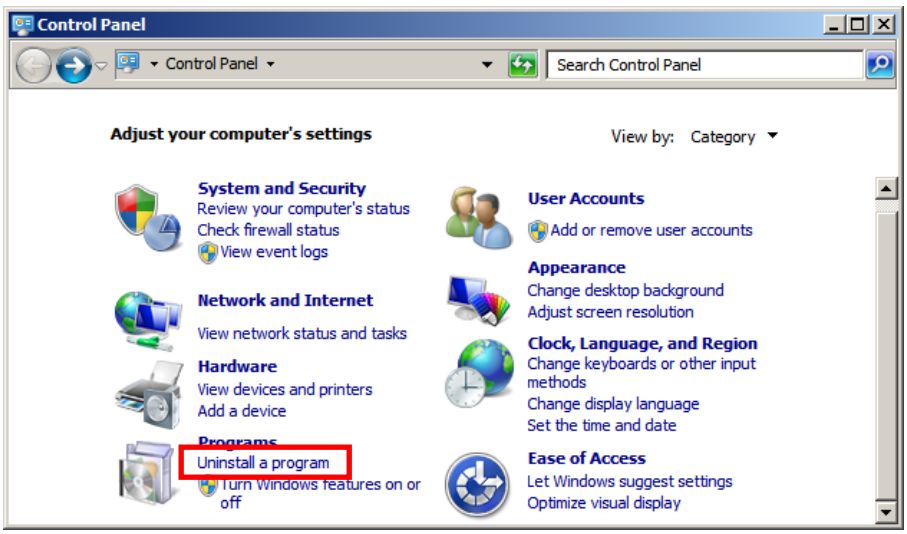


Figure 3.1.2-1 Control Panel

3. Select **MonitoringManager2 Server Software** and then click **Uninstall**.

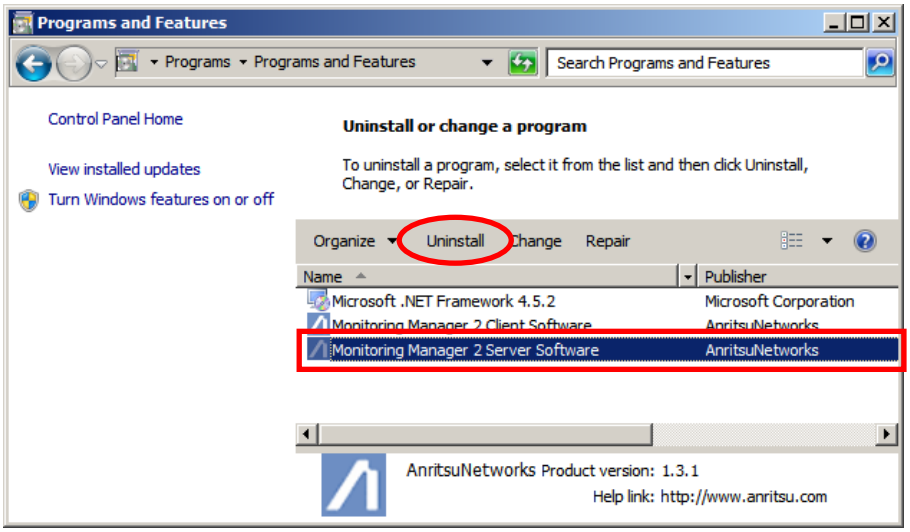


Figure 3.1.2-2 Programs and Features

4. When the uninstallation confirmation dialog box appears, click **Yes**.

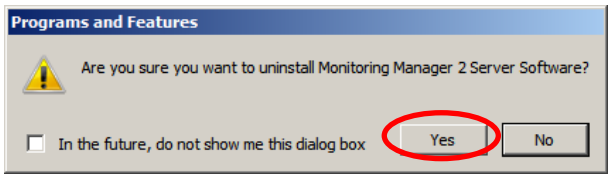


Figure 3.1.2-4 Uninstallation confirmation dialog box

* If the restart confirmation dialog box appears, select **Automatically close applications and attempt to restart them after setup is complete** and click **OK**.

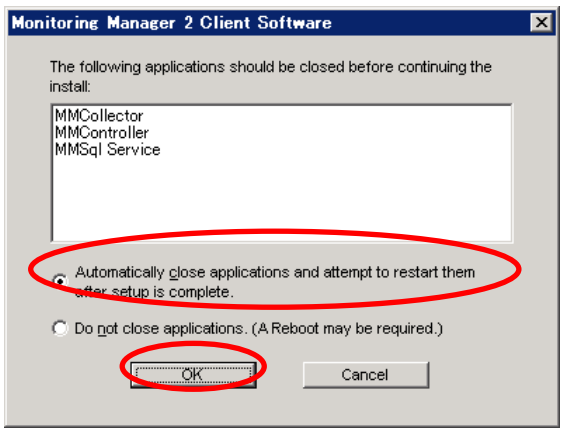


Figure 3.1.2-5 Restart confirmation dialog box

Note:

If uninstallation is cancelled at this point, an error occurs and the server software might not be able to be recovered or uninstalled. Do not cancel uninstallation.

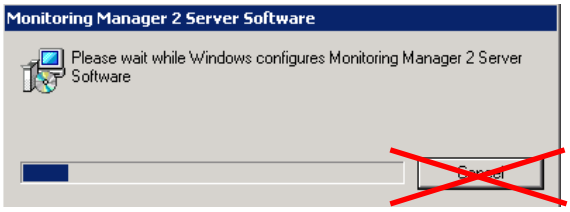


Figure 3.1.2-6 Do not cancel uninstallation

5. You cannot delete database and report setting data during uninstallation. To delete the setting data, delete the directory below.

   If the data is in the default location, delete the following directory:

   Database folder: `C:\ProgramData\AnritsuNetworks\MMSql\MM2DataBase`

   Report output folder: `C:\reports`

   You can keep the original database and report settings when reinstalling the software if you wish.

Notes:

1. Performing uninstallation causes periodic report output to stop. If you want to continue outputting a periodic report when reinstalling the software with the original settings, you must register the periodic report again.
   For details about how to register the report again, see 5.2.5 Reregistering report tasks excluded from the periodic report.

   Alternatively, to restore the original setting, you can export the report settings before uninstallation, and import the settings again after reinstallation to maintain the original periodic report settings.
   For details about how to export and import the report settings, see 5.4 Exporting and importing report settings.

2. When server software version v1.2.4 or earlier is used in Windows Server 2012 or Windows Server 2012 R2, import of the report settings (task.zip) after uninstalling the server software and re-installing it does not allow you to correctly register the report task in the Windows task scheduler and create the periodic report until the server is restarted. If you want not to restart server, delete all the report tasks before uninstalling the server software.

This chapter describes how to operate MonitoringManager2.

4.1 Workflow

Click **Start - All Programs - AnritsuNetworks - MMClient** to start the client software. After starting the client software, set the items below according to the relevant procedure:

4.2	Logging in	Start the client software and log in.
	↓	
4.3.1	Registering PureFlow nodes	Register the PureFlow node whose traffic is to be monitored.
	↓	
4.4.1	Creating a graph	Display the real-time monitor and past monitor graphs.
	↓	
4.13	Exiting the client software	

The following operations should also be performed if required:

4.7 Displaying the scenario status and specifying scenario settings
Monitor threshold value alarms from other servers such as the SYSLOG server.

4.5.5 Saving a graph
Save the graphical display.

4.5 Manipulating the graph window
Change the information displayed in the graph window.

4.11 Sorting the graph windows
Sort and display multiple graphs.

4.12 Help
Display the version information and data storage period.

4.14 Cautions
Specify the compatibility during execution of MonitoringManager2 and check the port number.

5. Reports Feature
Create a traffic report.
For details about reports, see Chapter 5 Reports.

4.2 Logging in

To specify the settings in MonitoringManager2 and display graphs by using MonitoringManager2, start the client software and log into the server software.

Click **Start - All Programs - AnritsuNetworks - MMClient**. If the **User Account Control** dialog box appears, click **Yes**.

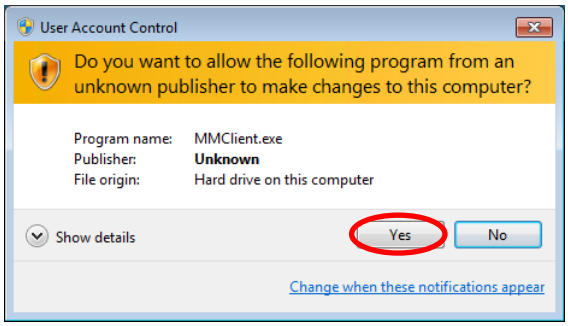


Figure 4.2-1 User Account Control dialog box

The client software starts and the **Login** dialog box appears. Enter the server name (server IP address), user name, and password.

The server name is set to "127.0.0.1", the user name to "administrator" and the password to "admin" (all paramters are 1-byte, alphanumeric, and lower-case characters only) by default.

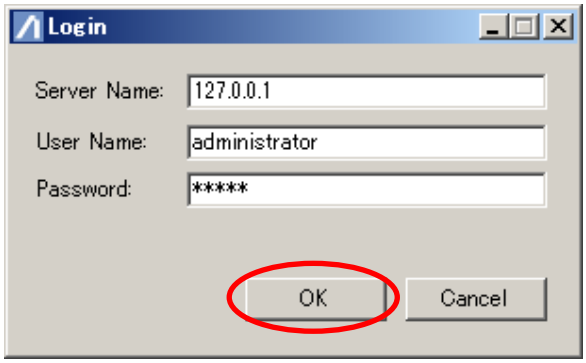


Figure 4.2-2 Login dialog box

Click **OK**.

If a user name or password that differs from the one registered is entered, an error message appears and the **Login** dialog box appears again. If you select **Cancel**, the **Login** dialog box closes and application is exited.

For details about the login authentication settings, see 7.5.1 Switching authentication mode.

Notes:

1. User can not login unless MMController Service, MMCollector Service and MM Sql Service are all activated. Please refer to the "7.3 Service Management" for how to start up the services.

2. When launching the client software by user except for the built-in administrator, start with administrator's privilege. Please refer to the operation manual of the OS for the method of starting with administrator's privilege.

4.3 Registering, setting, and deleting PureFlow nodes

4.3.1 Registering PureFlow nodes

Register the PureFlow node whose traffic is to be monitored by using MonitoringManager2.

Select **MMCollector** on the scenario tree pane. On the **Operation** menu, select **Register PureFlow**, or select the PureFlow registration icon. The new node registration pane appears. Or right-click the registered node on the scenario tree and select **Register PureFlow** on the pop-up menu. The maximum number of nodes that can be registered is 255.

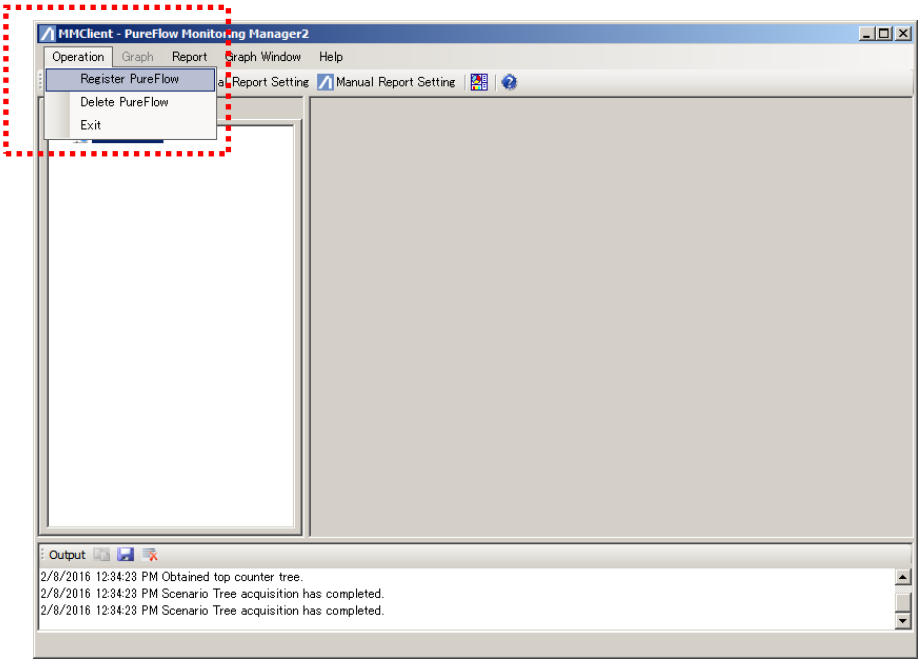


Figure 4.3.1-1 Registering a new node by using the menu

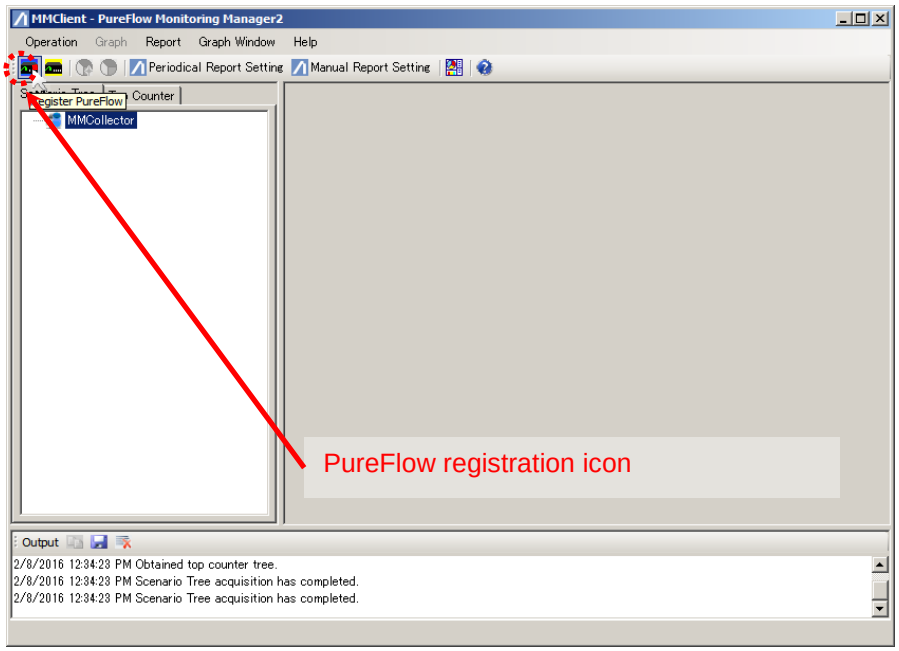


Figure 4.3.1-2 Registering a new node by using the PureFlow registration icon

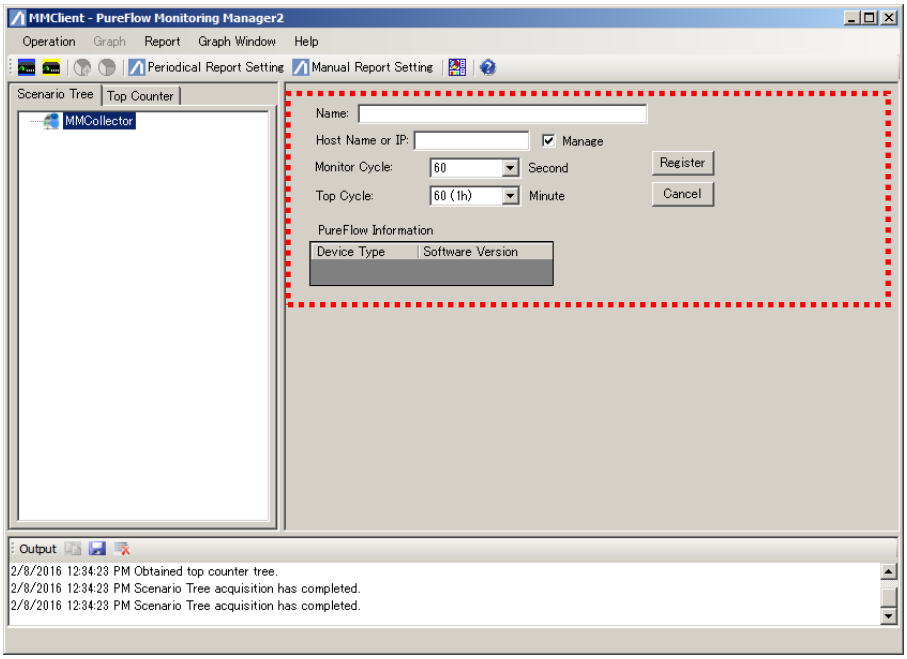


Figure 4.3.1-3 New node registration pane

Name

Enter the name of the PureFlow node to be registered.

A node with same name cannot be registered.

One-byte alphanumeric and two-byte characters can be used.

The symbols “"<>|:;*?¥/()[]{},$&' ([{〔〈《「『【 〝‘“ ,)]}, 〕〉》」』】’”〟 ” cannot be used.

One-byte or two-byte spaces cannot be used.

Up to 255 characters can be registered.

It is count one character regardless one-byte or two-byte.

IP or host name

Enter the IP address or host name of the node to be registered.

A node with same IP or host name cannot be registered.

For example, if the IP address of the node to be registered is "192.168.10.153", enter "192.168.10.153".

IP addresses ranging from 1.0.0.1 to 255.255.255.254 can be registered.

One-byte alphanumeric characters and period (.) can be entered for the host name.

Spaces cannot be used.

Up to 255 characters can be registered.

Monitor information notification interval

Select the interval at which to collect the scenario counter information of the node. Valid values are 60, 30, and 10 seconds. The default value is 60 seconds.

Top information notification interval

Select the interval at which to collect the top counter information of the node. Valid values are 10 minutes, 15 minutes, 20 minutes, 25 minutes, 30 minutes, 60 minutes (1h), 120 minutes (2h), 240 minutes (4h), 360 minutes (6h), 480 minutes (8h), 720 minutes (12h), and 1440 minutes (24h). The default value is 60 minutes (1h).

Specify as management target

Use this checkbox to specify whether the node is subject to management or not.

If the checkbox is selected, the registered node is connected and becomes subject to management.

If the checkbox is cleared, the node is registered but does not become subject to management.

Enter the above items, and click the **Register** button to register the node. Registered node appears on scenario tree window.
If there are any errors in the entered items, a message appears.

The icons displayed in the scenario tree vary depending on the node connection status and node model. Icons describes in Table 4.3.1-1.

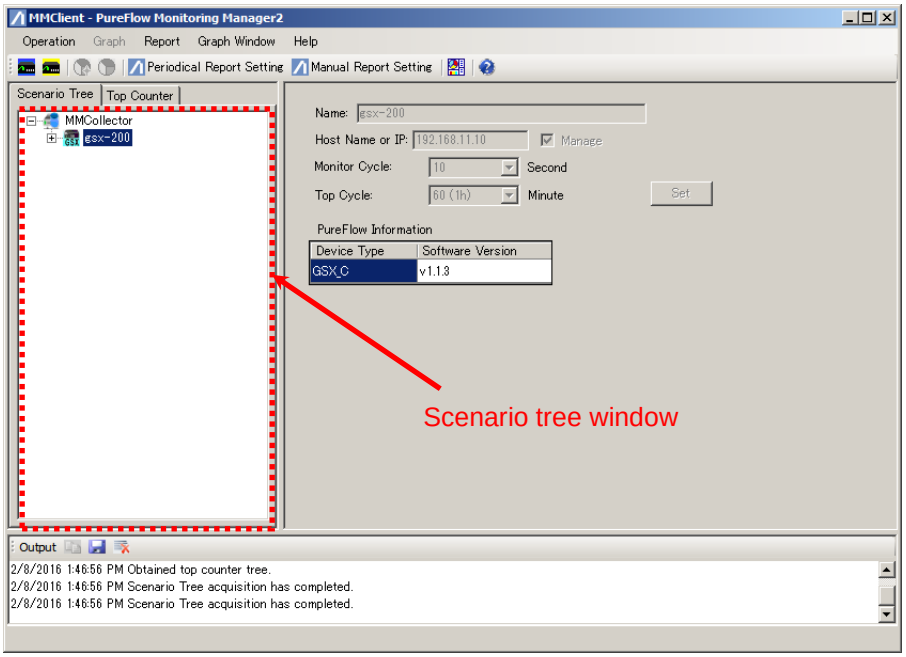


Figure 4.3.1-4 Window display after registering a new node

Table 4.3.1-1 PureFlow status icons

Model						Status
GS1	GSX	WSX-QoS	WSX-TCP	WS1	WS1-TCP	
						Blue: Node is connected.
						Yellow: Node is disconnected. (Reconnection processing is being executed at 1-minute intervals.)
						Gray: Node has been specified as not subject to management.
						White: Unknown model. (The node is either disconnected or not subject to management.) After a node is registered, the node is displayed as an unknown model until it is first connected.

WSX-QoS: PureFlowWSX (Traffic shaping),
WSX-TCP: PureFlowWSX (TCP acceleration),
WS1-TCP: PureFlowWS1 (TCP acceleration)

Notes:

1. Do not register device other than PureFlow. If a device other than a PureFlow is registered, incorrect values might be displayed on the graph of that node.

2. If the message, “The maximum limit of registered PureFlow nodes has been reached” appears even though the number of the registered nodes is less than the number of license units, it means that installation of the basic or an additional MonitoringManager2 license is not enabled. To enable the license(s), see 2.2 Installing the basic license file and 2.3 Installing an additional license file.

3. The scenarios are displayed in the scenario name order (ASCII code order) for GSX, WSX and WS1, and in the scenario ID order for GS1. For versions v1.2.3 or earlier, the scenarios are displayed in the scenario ID order.

4. Do not use "”", "¥", or "," for the scenario name of PureFlow node to be registered. Otherwise, a failure occurs when this software operates.

5. If replace PureFlow device to another PureFlow device that has the same IP address after registering PureFlow node, it may not be able to refer statistic information from former PureFlow device. To refer statistic information from former PureFlow device, To generate csv reports, html reports to save statistic informations.

6. If replace PureFlow device to another PureFlow device that has the same IP address after registering PureFlow node, the first statistic information from replaced PureFlow device may show a rate value different from the original rate.

7. Nodes cannot be connected to a PureFlow that is using NAT conversion.

4.3.2 Editing the PureFlow settings

You can edit some of the previously registered PureFlow node settings. The following settings can be edited:

- **Name**
- **Monitor information notification interval**
- **Top information notification interval**
- **Specify as management target**

IP or host name cannot be edited.

To edit the settings, select the node whose settings are to be edited in the tree on the left, right-click the pane showing the PureFlow node settings on the right, and select **Edit PureFlow** from the pop-up menu.

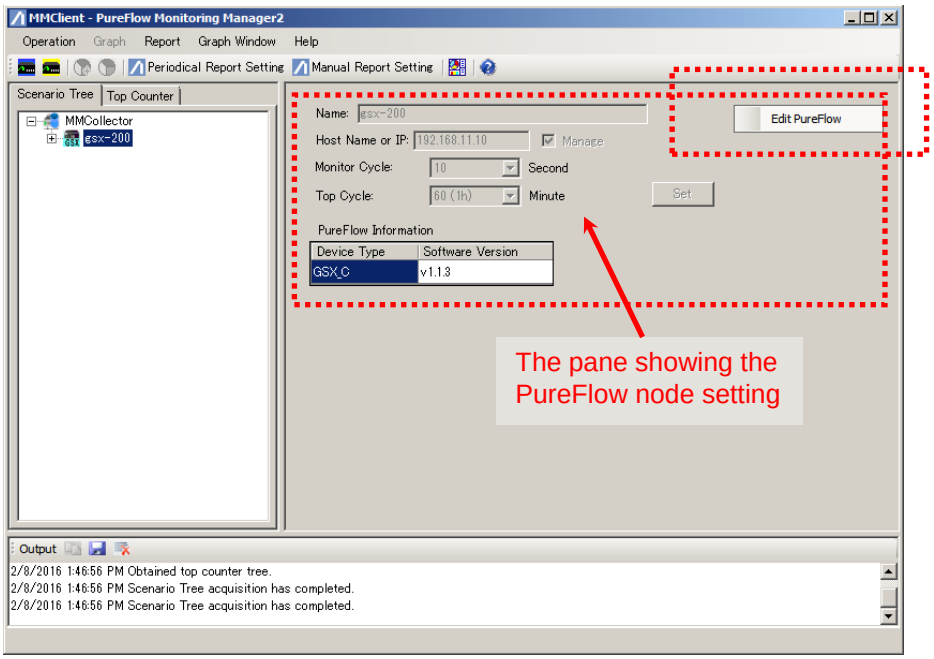


Figure 4.3.2-1 Editing the PureFlow settings by using the pop-up menu

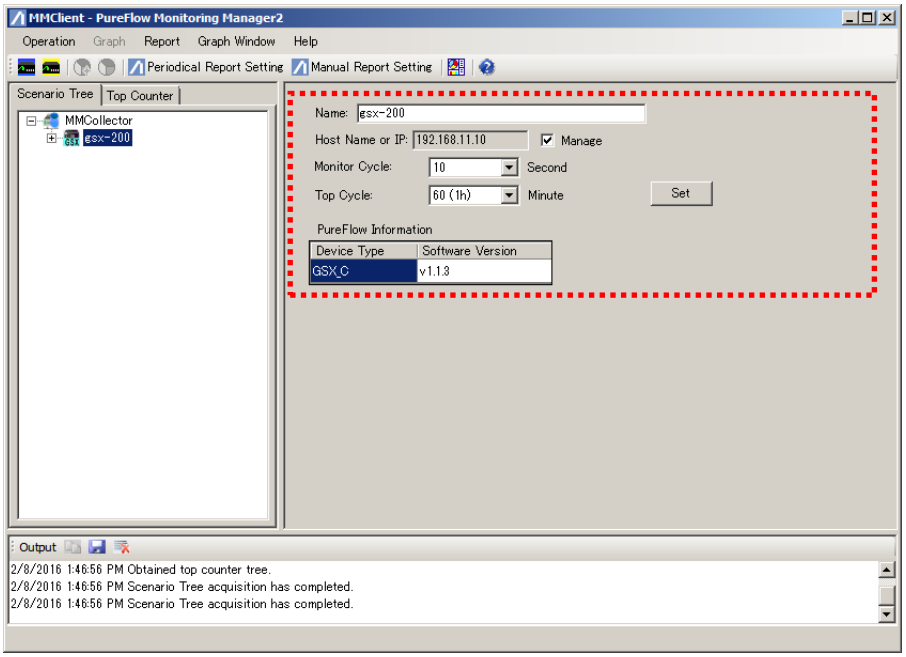


Figure 4.3.2-2 Pane on which to edit the PureFlow settings

After editing the relevant items, click the **Set** button. Cancel the changes by right-clicking and clicking **Cancel** on the pop-up menu.
A node with the same name as a previously registered node cannot be registered.

4.3.3 Deleting a PureFlow node

To delete a PureFlow node, select the node to be deleted in the scenario tree and click **Operation** then **Delete PureFlow**. Or right-click the node on the scenario tree and select **Delete PureFlow** on the pop-up menu. PureFlow nodes can also be deleted by clicking the PureFlow deletion icon.

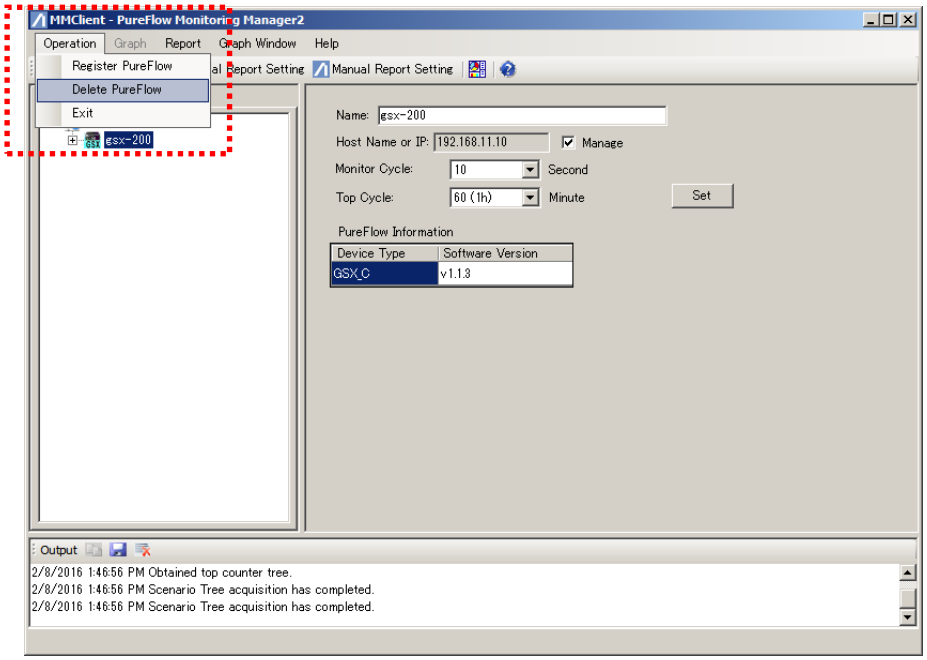


Figure 4.3.3-1 Deleting a PureFlow node by using the menu

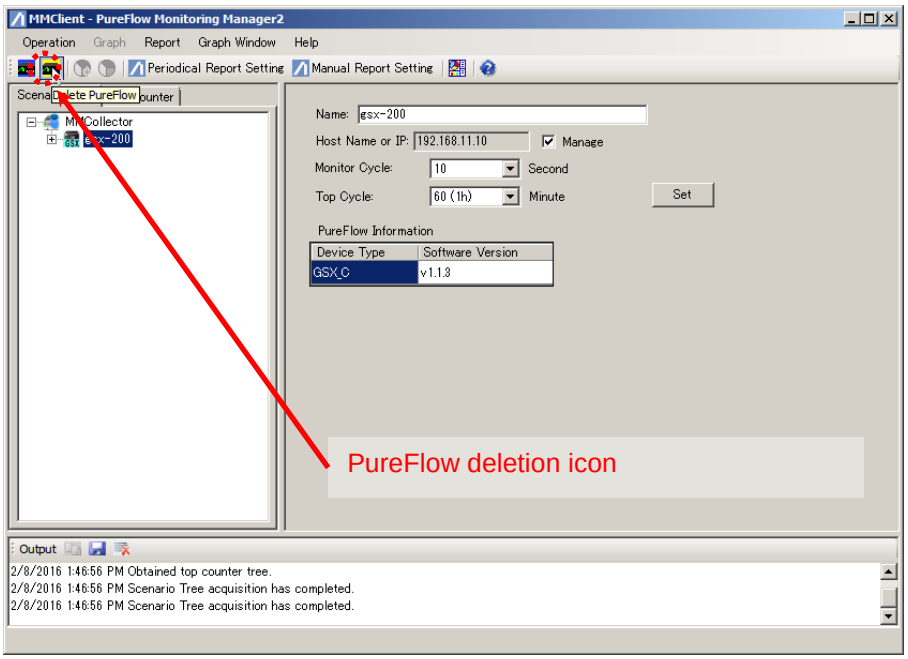


Figure 4.3.3-2 Deleting a PureFlow node by using the PureFlow deletion icon

A confirmation dialog box appears. If you click **Yes**, the PureFlow node is deleted. If you click **No**, deletion of the PureFlow node is canceled.

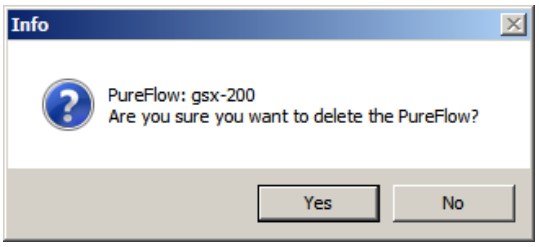


Figure 4.3.3-3 PureFlow deletion confirmation dialog box

Even when a node is deleted, the related graph and report settings are not deleted.

Note:

If the PureFlow node is deleted, the statistics information before deleting is not taken over even though PureFlow of the same IP or host name is registered.

4.3.4 PureFlow information display

The information of the registered PureFlow node can be displayed.

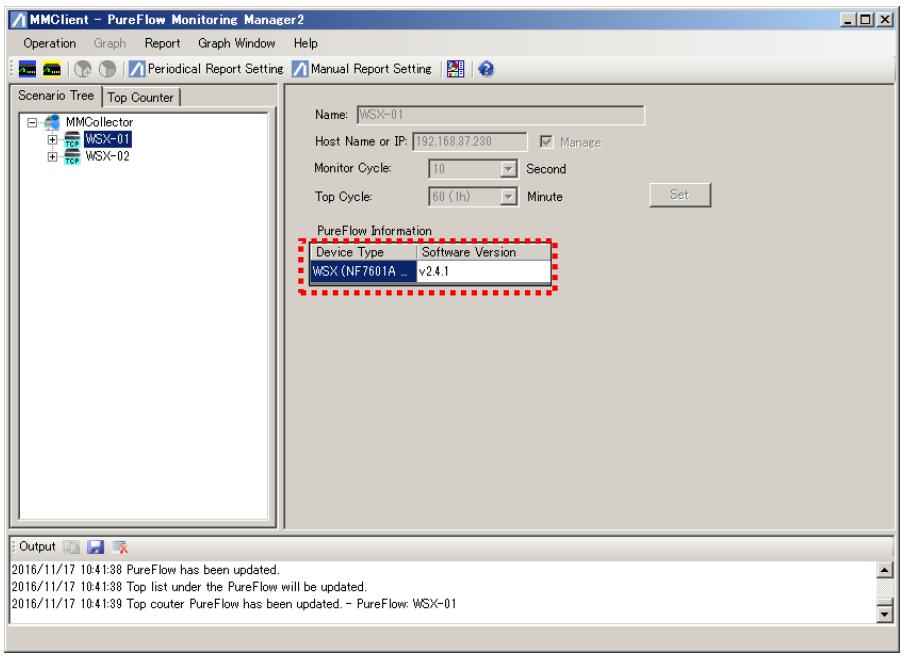


Figure 4.3.4-1 PureFlow information display

- Device Type
  Displays the information on the model of the already-connected PureFlow. Table 4.3.4-1 shows the displayed contents and corresponding device models.
- Software Versio
  Displays the control software version of PureFlow.

Table 4.3.4-1 Information on models

Device Type Displayed contents	Model (Model name)
GS1F_A	PureFlow GS1-F (PF7000A)
GS1FB_A	PureFlow GS1-FB (PF7001A)
GS1G_A	PureFlow GS1-G (PF7010A) PureFlow GS1-GR (NF7010A)
GS1GB_A	PureFlow GS1-GB (PF7011A) PureFlow GS1-GBR (NF7011A)
GS1F_C	PureFlow GS1-F (PF7000C)
GS1FB_C	PureFlow GS1-FB (PF7001C)
GS1G_C	PureFlow GS1-G (PF7010C)
GS1GB_C	PureFlow GS1-GB (PF7011C)
GSX_A	PureFlow GS-X (NF7101A)
GSX_C	PureFlow GS-X (NF7101C)
WSX (NF7601A, TCP)	PureFlow WSX (NF7601A) TCP acceleration software license applied
WSX (NF7602A, TCP)	PureFlow WSX Lite (NF7602A)
WSX (NF7603A, TCP)	PureFlow WSX (NF7603A) TCP acceleration software license applied
WSX (NF7604A, TCP)	PureFlow WSX (NF7604A) TCP acceleration software license applied
WSX (NF7605A, TCP)	PureFlow WSX Lite (NF7605A)
WSX (NF7601A, QoS)	PureFlow WSX (NF7601A) Traffic shaping software license applied
WSX (NF7603A, QoS)	PureFlow WSX (NF7602A) Traffic shaping software license applied
WSX (NF7604A, QoS)	PureFlow WSX (NF7603A) Traffic shaping software license applied
WS1 (NF7501A, QoS)	PureFlow WS1 (NF7501A)
WS1 (NF7501A, TCP)	PureFlow WS1 (NF7501A) TCP acceleration function license applied

4.4 Creating and deleting a graph

4.4.1 Creating a graph

MonitoringManager2 allows you to view real-time monitor*1 and past monitor*2 graphs showing the scenario counter information*3 and top counter information*4 during a specific time period. Hereafter, a graph that shows scenario counter information is called a scenario graph, and a graph that shows top counter information is called a top graph.

Up to 32 graphs can be displayed at the same time. When a lot of graphs are opened at the same time, command execution might slow down or the graph might not be rendered correctly, depending on factors such as the OS version, graphical performance of the hardware, and installed software.

*1: The real-time monitor is a graph that shows the current scenario counter information and top counter information. The created graph is referred to as a "real graph".

*2: The past monitor is a graph that shows stored scenario counter information and top counter information of a specific date and time. The created graph is referred to as a "past graph".

*3: The scenario counter information indicates the volume of traffic flowing on each port and scenario, as well as the number of discarded packets, and the peak volume (available only in PureFlow GSX, WSX, and WS1). A scenario graph can be displayed in units of bits per second ("bps"), bytes per second ("Bps"), or packets per second ("pps").

*4: The top counter information indicates the volume of traffic flowing for each IP address or application (port number). The traffic volumes are ranked and sorted in descending order from 1 to 25. A top graph can be displayed in units of bits per second ("bps"), bytes per second ("Bps"), or packets per second ("pps").

To create a scenario graph, select the port or scenario for which a graph is to be created from the scenario tree. On the **Graph** menu select **Create real graph** or **Create past graph**, or right-click the scenario tree and select **Graph - Create real graph** or **Create past graph** on the pop-up menu. The scenario graph creation pane appears. A scenario graph can also be created by clicking the real graph creation icon or past graph creation icon.

To create a top graph, select the port or scenario for which a graph is to be created on the top counter pane. On the **Graph** menu select **Create real graph** or **Create past graph**, or right-click the top counter pane and select **Graph** then **Create real graph** or **Create past graph** on the pop-up menu. The top graph creation pane appears. A top graph can also be created by clicking the real graph creation icon or past graph creation icon.

Note that top graphs can only be created for ports and scenarios for which the traffic counter has been set from the command line interface (CLI) of PureFlow node.

Note:

If a scenario is deleted in PureFlow node and if the scenario ID is changed after re-registration of the same scenario name, the statistics information before deleting is not taken over.

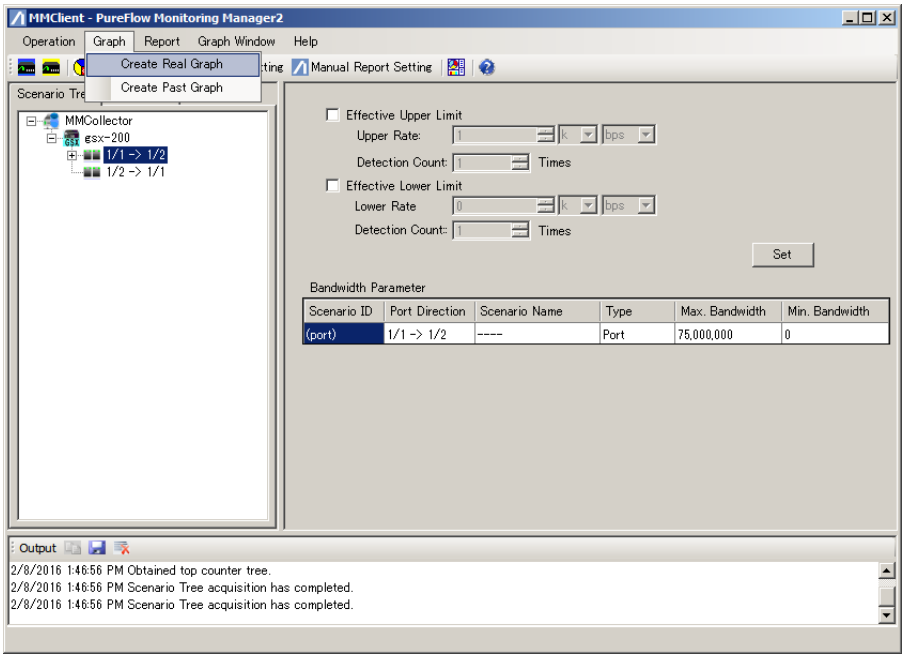


Figure 4.4.1-1 Creating a scenario graph by using the menu

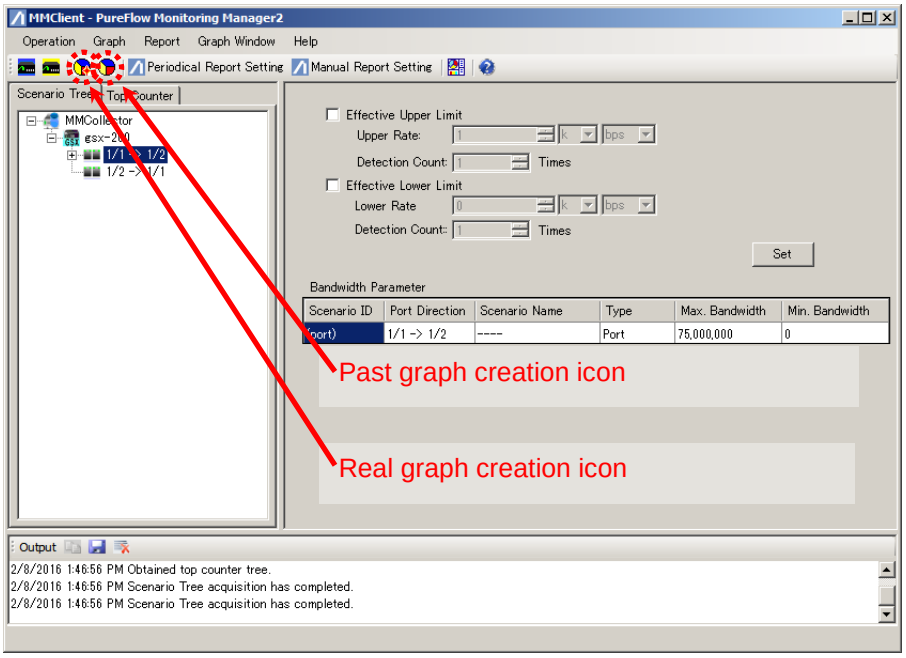


Figure 4.4.1-2 Creating a scenario graph by using the graph creation icons

4.4.2 Creating a scenario graph

The procedure for creating a scenario graph is described below.

Right-click the port or scenario for which a scenario graph is to be created on the scenario tree. Select **Graph** then **Create real graph** or **Create past graph** from the pop-up menu. The scenario graph creation pane then appears.

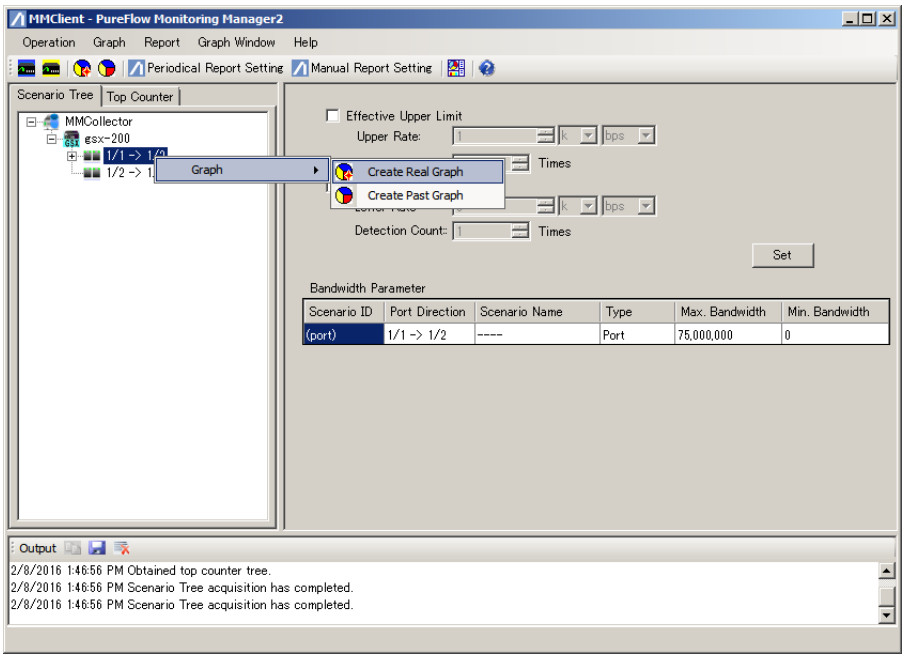


Figure 4.4.2-1 Creating a scenario graph by using the pop-up menu

Creating a real-time graph

Select **Create real graph**. The following dialog box appears.

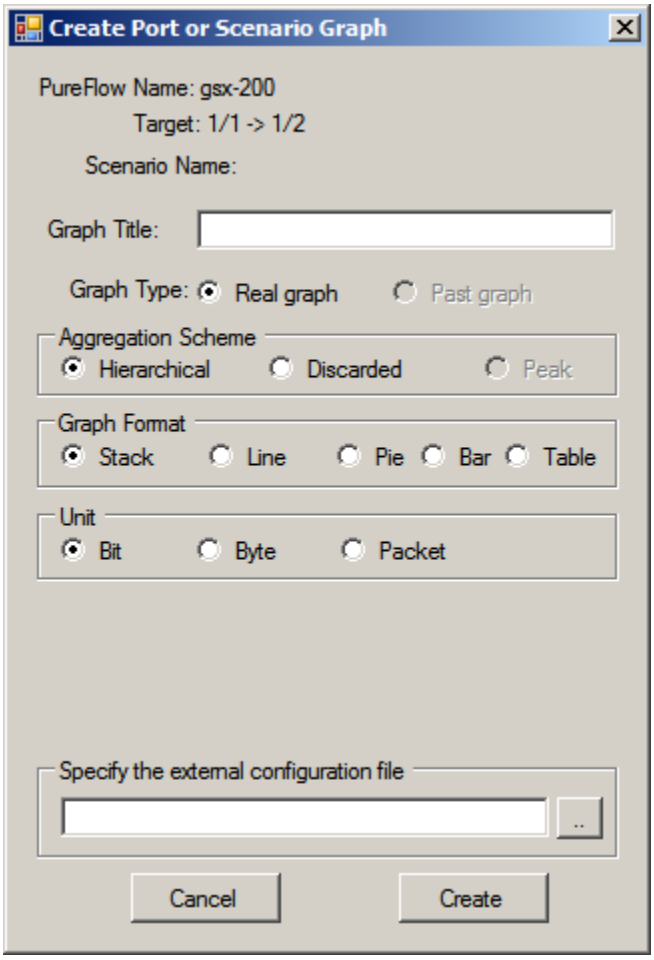


Figure 4.4.2-2 Real-time graph setting dialog box

Graph title

Enter the graph title.

One-byte alphanumeric and two-byte characters can be used.

The symbols “"<>|:;*?¥/()[]{},$&' ([{〔〈《「『【〝‘“ ,)]}, 〕〉》」』】’”〟 ” cannot be used.

Up to 255 characters can be registered.

It is count one character regardless one-byte or two-byte.

When the graph title is blank, the name indicated by **PureFlow name** and character string indicated by **Target** are combined to create the title.

Counting target

Select from **Hierarchical traffic**, **Discarded traffic**, and **Peak**.

Graph format

Select from **Stacked bar**, **Circle**, **Bar**, and **Line**.

Unit

Select from **Bits**, **Bytes**, and **Packets**.

Note:

When selecting **Peak** as the counting target, the connected device must be PureFlow GSX, WSX, or WS1 and the notification interval must be set to 60 seconds. Also, when selecting **Peak**, only **Stacked bar** and **Line** can be selected for the graph format, and only **Bits** and **Bytes** can be selected for the unit.

External configuration file

If an external configuration file is not specified, the color of the traffic data in the graph is determined automatically.

An external configuration file is a CSV file that includes scenario names and colors (RGB format) separated by a comma " , ".
The colors are indicated as numbers from 0 to 255 for each of R, G, and B. The smaller the number is, the brighter the color is. The larger the number is, the darker the color is. For the displayed color, see "Appendix E RGB Chart".

Table 4.4.2-1 Example external configuration file

Scenario name	R (red)	G (green)	B (blue)
sc001	0	0	255
sc002	0	255	0
sc003	255	0	0

Example CSV file (sample.csv)

sc001,0,0,255

sc002,0,255,0

sc003,255,0,0

If a match is detected with a scenario name or scenario comment in the external configuration file, the graph is displayed according to the detected scenario name and color settings.

An external configuration file can be specified for each graph to be created.

Click the **Create** button to create a scenario graph for the selected port or scenario.

Creating a past graph

Select **Create past graph**. The following dialog box appears.

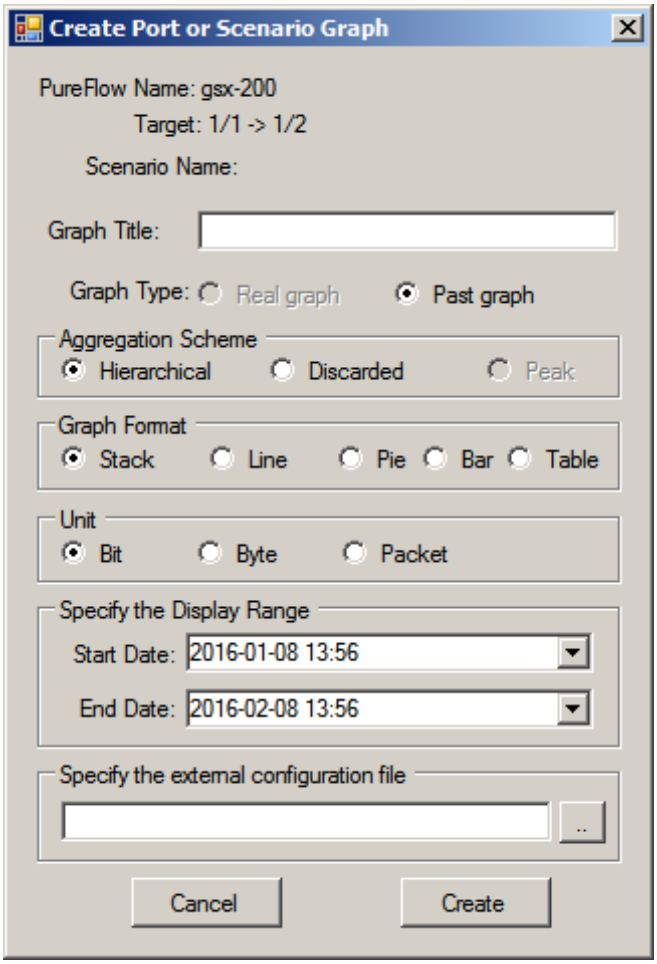


Figure 4.4.2-3 Past graph setting dialog box

The counting target, graph format, unit, and external configuration file can be specified in the same way as when creating a real-time graph.

Display period

Start date..... Specify the start date of the past period (year, month, day, hour, and minute). The default value is 1 month before the graph setting dialog box was opened.

End date..... Specify the end date of the past period (year, month, day, hour, and minute). The default value is when the graph setting dialog box was opened.

Click the **Create** button to create a scenario graph for the selected port or scenario based on a past period.

Creating a Network port graph

When selecting a real graph or past graph for the Network port of PureFlow WSX (TCP acceleration) or WS1, the following screen appears.

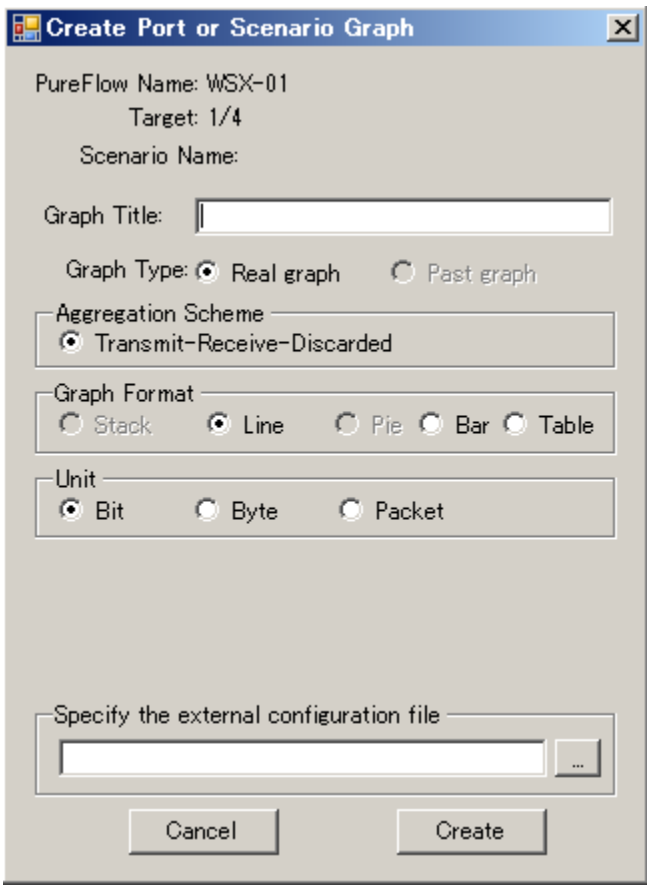


Figure 4.4.2-4 Network port graph setting dialog box

Only the Transmit-Receive-Discard counter is settable as Aggregation Scheme.

Graph Format is selectable from Line, Bar, or Table.

How to specify Graph Title, Unit, Start Date, End Date, and Specify the external configuration file is the same as that for a real graph or past graph.

Click the **Create** button to create a real graph or past graph for the selected Network port.

Note:

When Bit or Byte is selected for the Transmit-Receive-Discard counter graph for the Network port, the Discard counter for Bit or Byte does not appear.

4.4.3 Creating a top graph

The procedure for creating a top graph is described below.

Right-click the port or scenario for which a top graph is to be created on the top counter pane. Select **Graph** then **Create real graph** or **Create past graph** from the pop-up menu. The top graph creation pane then appears.

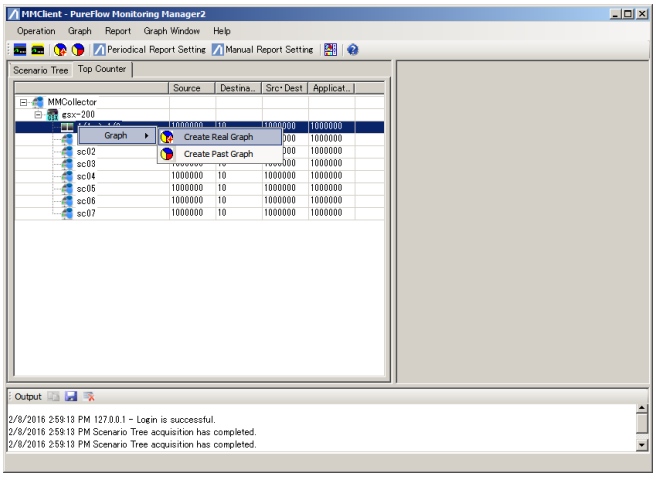


Figure 4.4.3-1 Creating a top graph by using the pop-up menu

Note:

The top counter tree in the top counter pane shows only the scenario name without displaying hierarchically. Accordingly, it may be difficult to distinguish between scenarios with the same names. Set different scenario names to distinguish the scenario names in PureFlow node.

Creating a real-time graph

Select **Create real graph**. The following dialog box appears.

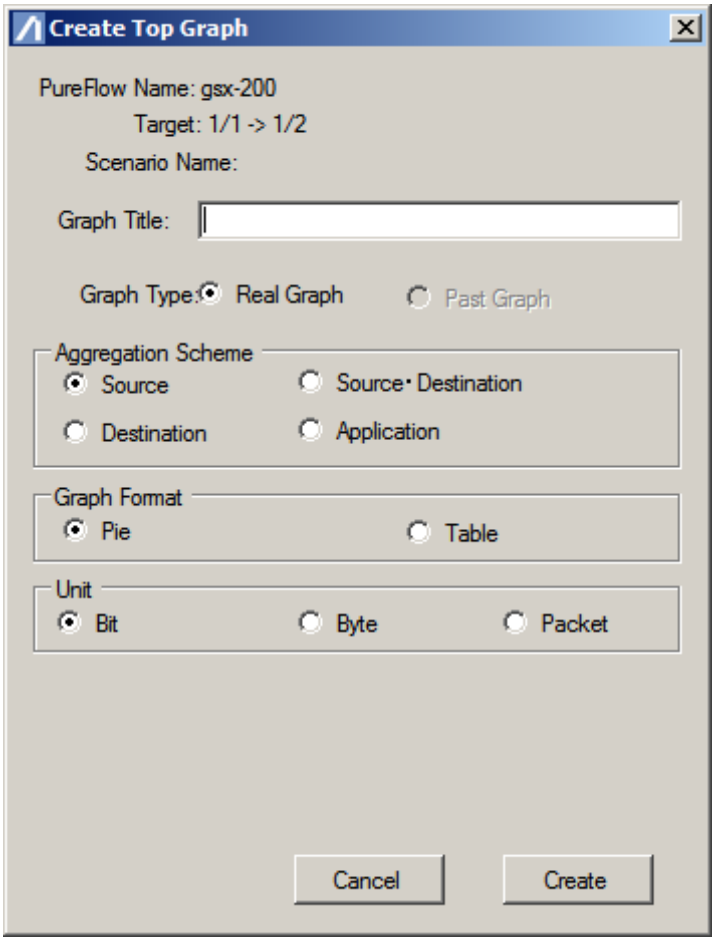


Figure 4.4.3-2 Real-time graph setting dialog box

Graph title

Enter the graph title.

One-byte alphanumeric and two-byte characters can be used.

The symbols “"<>|:;*?¥/()[]{},$&' ([{〔〈《「『【 〝‘“ ,)]}, 〕〉》」』】’”〟 ” cannot be used.

Up to 255 characters can be registered.

It is count one character regardless one-byte or two-byte.

When the graph title is blank, the name indicated by **PureFlow name** and character string indicated by **Target** are combined to create the title.

Counting target

Select how to identify which flow of traffic from an upstream device to display from the following:

Source.....Source IP address

Destination .....Destination IP address

Source and destination.....Combination of source and destination IP addresses

Application.....TCP/UDP port number

Graph format

Select from **Circle** or **Table**.

Unit

Select from **Bits**, **Bytes**, and **Packets**.

Click the **Create** button to create a top graph for the selected port or scenario.

Creating a past graph

Select **Create past graph**. The following dialog box appears.

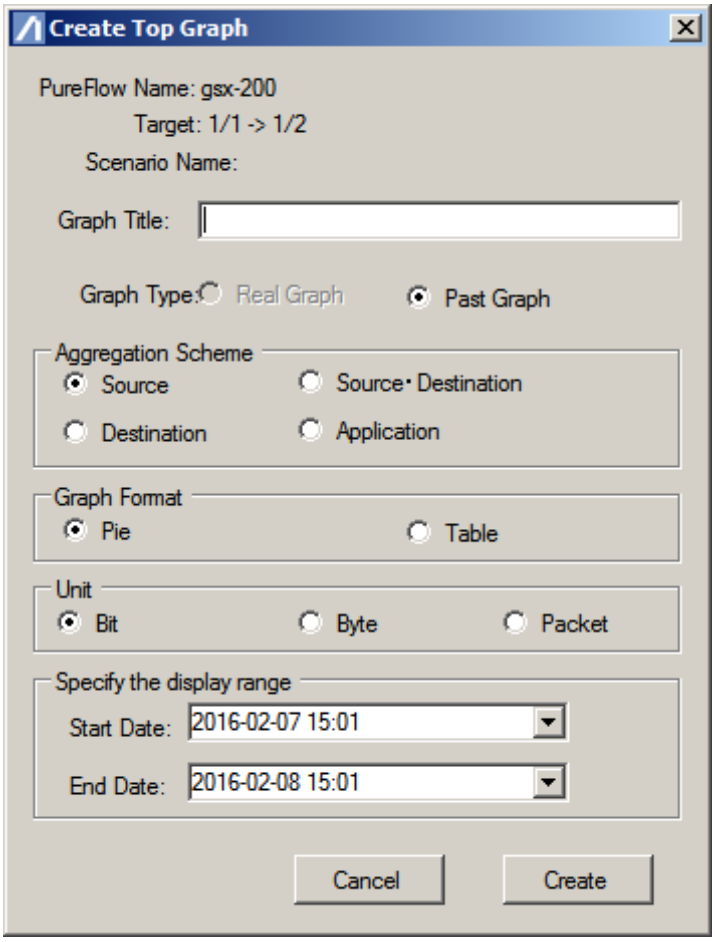


Figure 4.4.3-3 Past graph setting dialog box

The counting target, graph format, and unit can be specified in the same way as when creating a real-time graph.

Display period

Start date.....Specify the start date of the past period (year, month, day, hour, and minute). The default value is 1 day before the graph setting screen was opened.

End date.....Specify the end date of the past period (year, month, day, hour, and minute). The default value is when the graph setting screen was opened.

Click the **Create** button to create a top graph for the selected port or scenario based on a past period.

4.4.4 Deleting a graph

To delete a created graph, click the Close (×) button on the top right of the graph window.

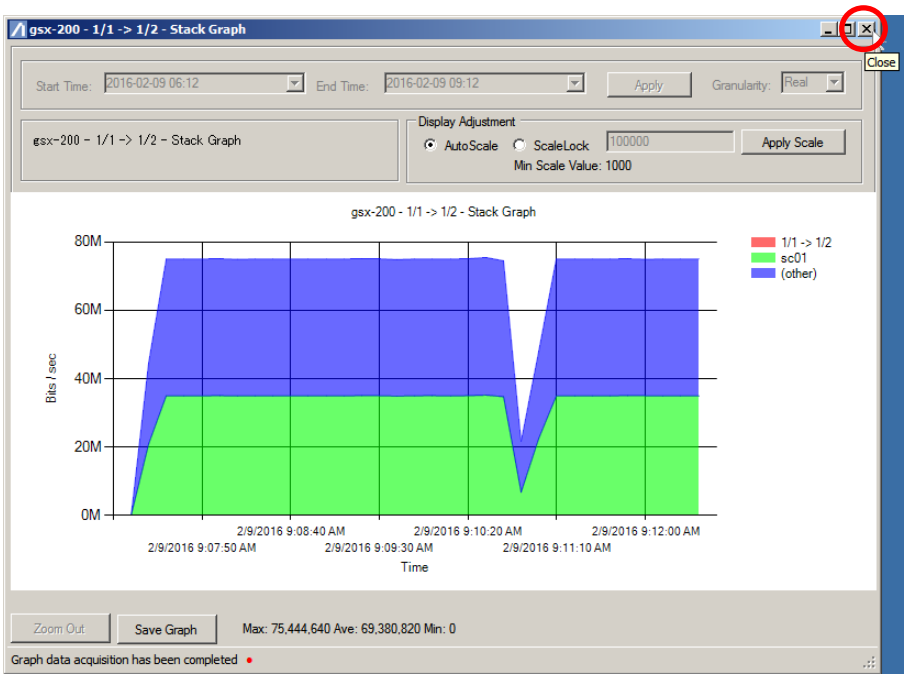


Figure 4.4.4-1 Deleting a graph by using the Close button

Even when a graph is deleted, the related report settings are not deleted.

4.4.5 Cautions when creating a graph

1. In the hierarchical traffic graph that shows the scenario counter information, the counter information of the selected scenario and the counter information of the scenarios under the selected scenario are combined and displayed. Up to 255 scenarios under the selected scenario can be combined and displayed at the same time. Scenarios are selected from scenario tree display order upper side. This limit applies for both real-time and past graphs.
   The scenarios to be displayed can be limited by using the external configuration file. The scenarios specified to not be displayed in the external configuration file can be also displayed on the graph by not specifying an external configuration file. Note that when the number of the individually-specified scenarios exceeds 255, only data for 255 scenarios is displayed on the graph.
2. Because no scenario exists under the port or scenario in the lowest layer, only **Line** can be specified as the graph format in this case.
3. The discarded traffic of a port can be displayed only when **Packets** is selected as the unit. If discarded traffic is displayed in bit or byte units, the discarded traffic is always displayed as 0 bps (Bps).

4.5 Manipulating the graph window

When a graph is created, it appears in the graph window. In this window, you can change the display scale and data display period, zoom the graph display, and save the graph.

For details about how to create or delete a graph, see 4.4 Creating and deleting a graph.

4.5.1 Types of graphs and operations

The following operations can be executed in the graph window. Note that the operations that can be executed in the graph window vary depending on the graph type.

- Change the data display period (past graphs only)
- Change the display scale (stacked bar, line, and bar graphs only)
- Zoom the graph display (stacked bar, line, and bar graphs only)
- Save the graph (all types of graphs)

If the operation is not available, the corresponding area is grayed out.

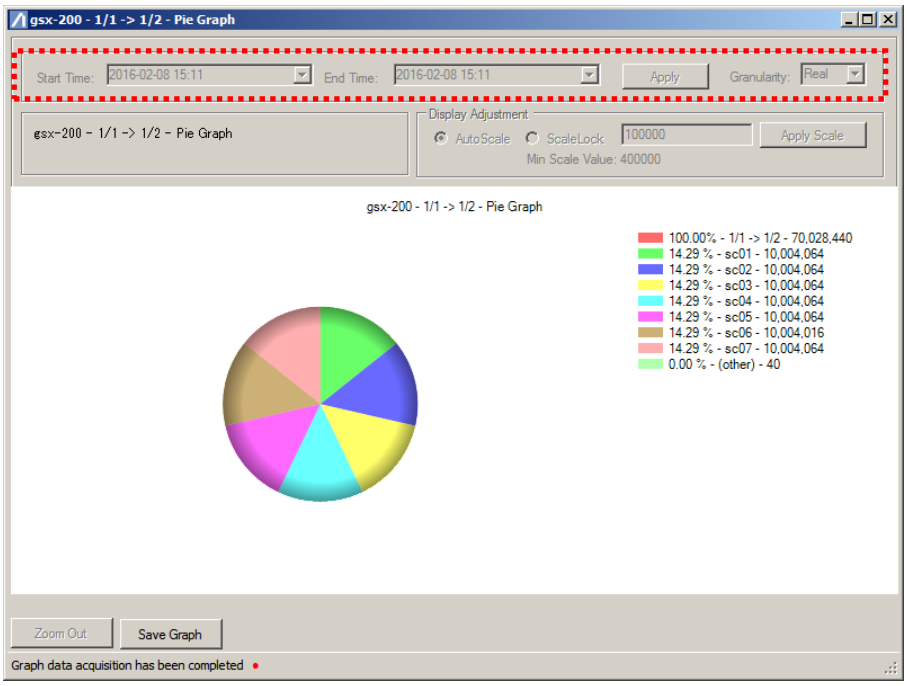


Figure 4.5.1-1 Real-time graph window (changing the data display period is unavailable)

4.5.2 Changing the data display period

You can change the horizontal axis (time) scale of the graph and set the start and end of the display data period.

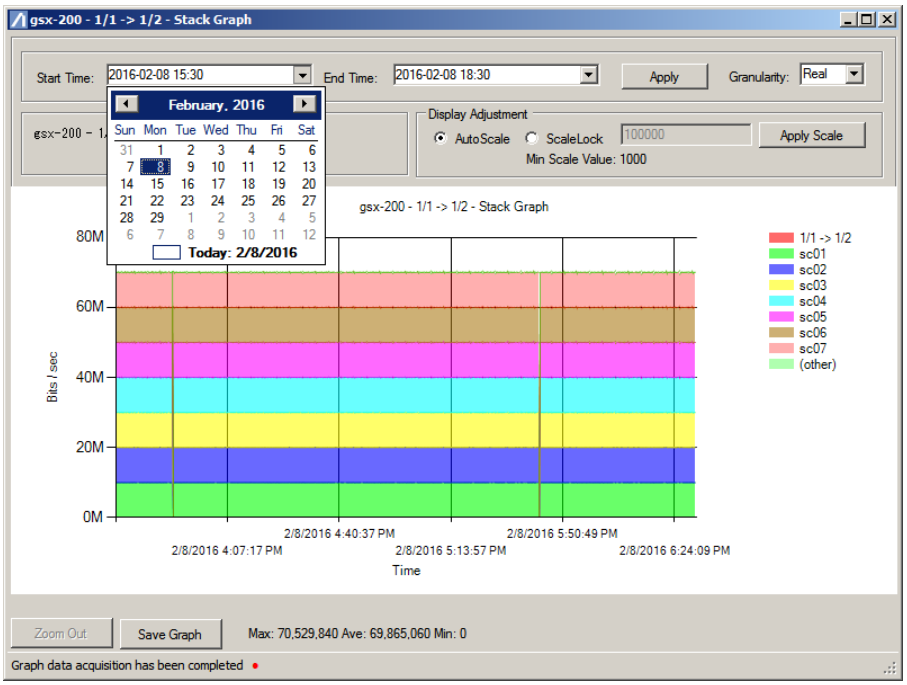


Figure 4.5.2-1 Setting the start and end times

When the time granularity is changed, the end time is changed as follows.

Table 4.5.2-1 Change of end time due to change in time granularity

Time granularity	End time
Real	3 hours after start time
5 minutes	1 day after start time
1 hour	1 week after start time
3 hours	1 month after start time
1 day	1 year after start time

If you click the **Update display** button, the graph of the specified data display period appears.

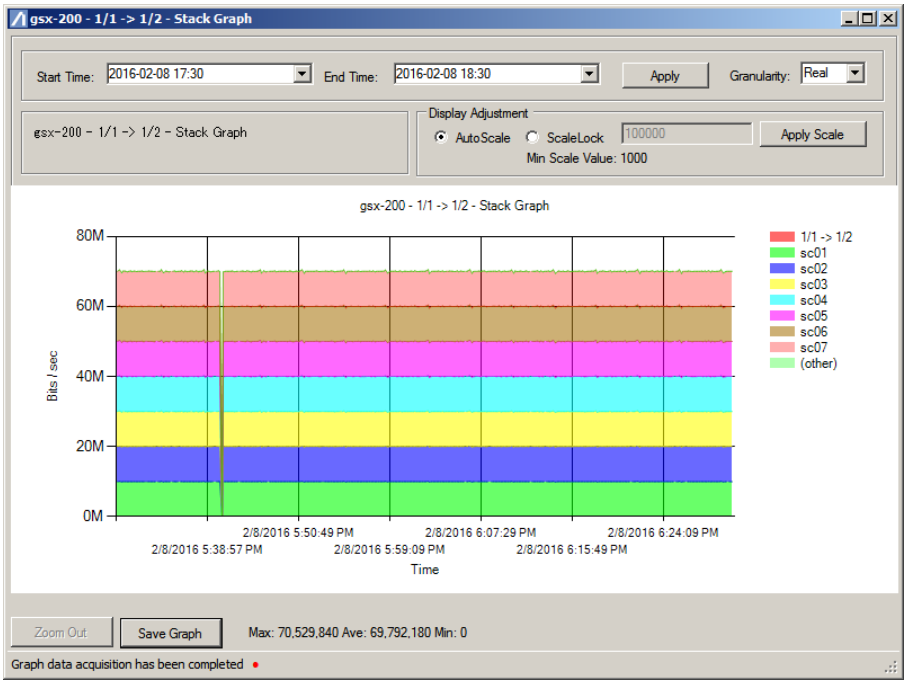


Figure 4.5.2-2 Changing the data display period

4.5.3 Changing the display scale

You can change the vertical axis (bits per second) scale of the graph.

If **AutoScale** is selected in the **Display adjustment** field, a graph appears in the default display scale when the **Confirm scale** button is clicked.

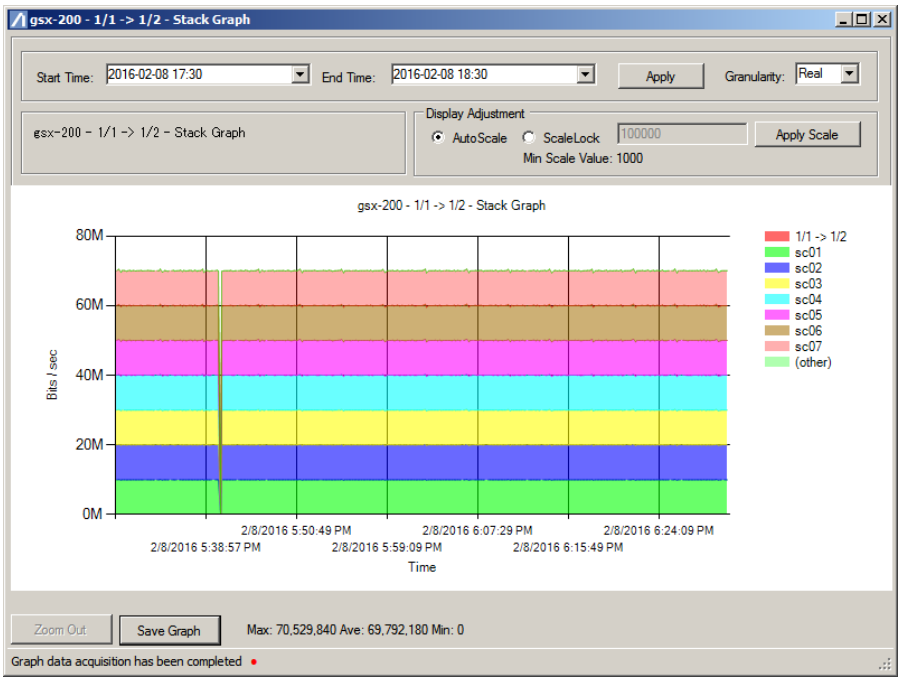


Figure 4.5.3-1 Changing the data display scale (AutoScale)

If **ScaleLock** is selected in the **Display adjustment** field, by specifying the maximum value of the vertical axis and clicking the **Confirm scale** button, the graph can be displayed in the specified display scale.
The minimum scale value is fixed depending on a unit of the vertical axis displayed in AutoScale.

Table 4.5.3-1 Minimum scale value depending on the vertical axis display unit

Vertical axis display unit	Minimum scale value
None	10
K	10
M	1000
G	1000
P	1000000 (Only for bar graphs)
T	1000000 (Only for bar graphs)

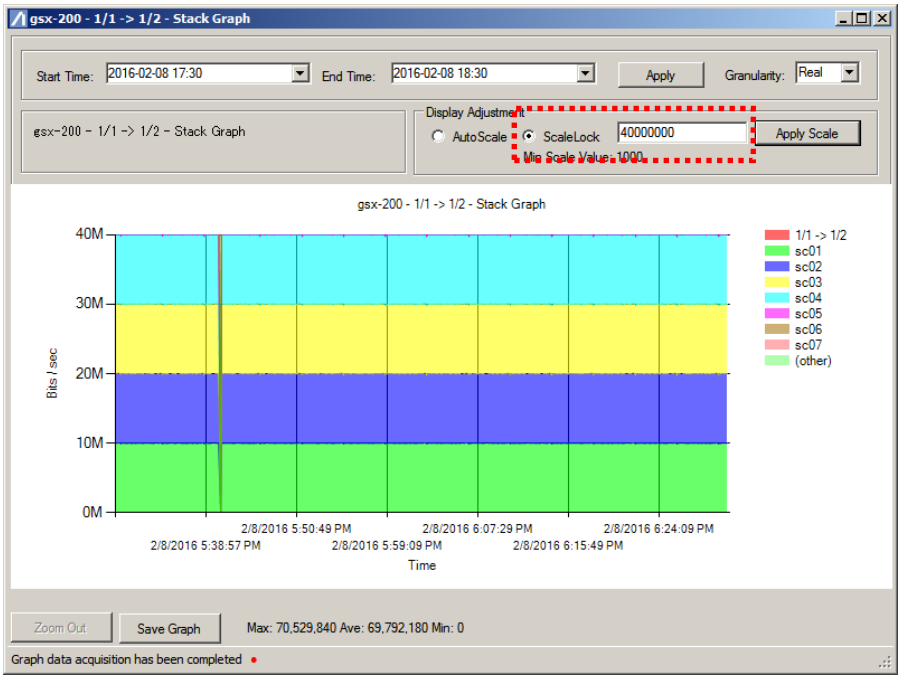


Figure 4.5.3-2 Changing the data display scale (ScaleLock)

Note:

If the display unit is disabled, the minimum scale value is 1/30 of the maximum value of the vertical axis in the default display. For how to disable the display unit, see 4.5.6 Graph display setting.

4.5.4 Zooming the graph display

If **AutoScale** is selected in the **Display adjustment** field, an area of the graph can be zoomed until the display area width is 1/100th the maximum value of the vertical axis in the default graph display.
If **ScaleLock** is selected in the **Display adjustment** field, an area of the graph can be zoomed until the display area width is 1/100th the specified maximum value of the vertical axis.

Drag the area to be zoomed.

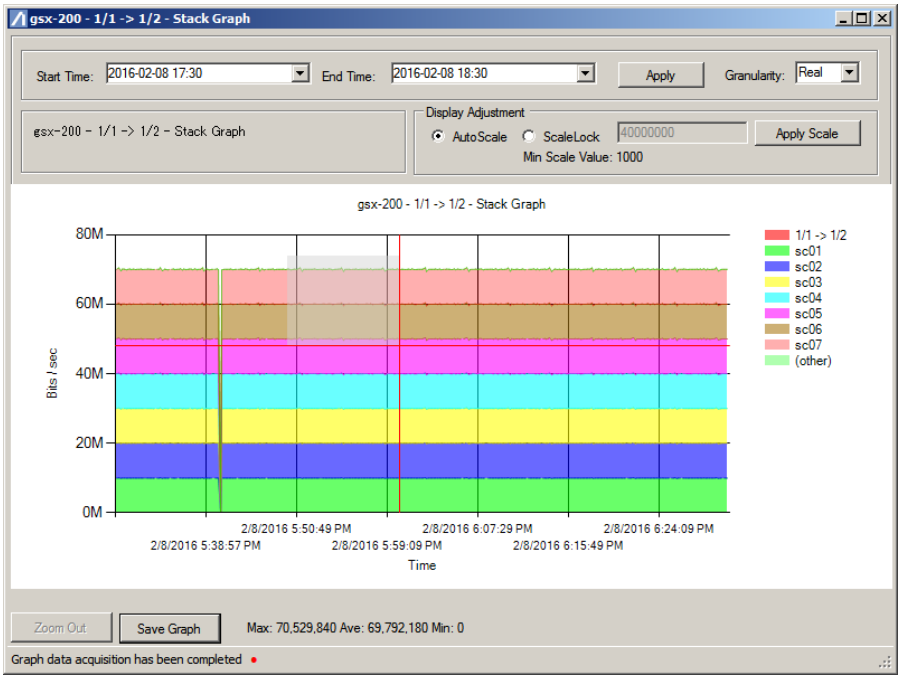


Figure 4.5.4-1 Selecting the area to be zoomed

A graph of the dragged area appears.

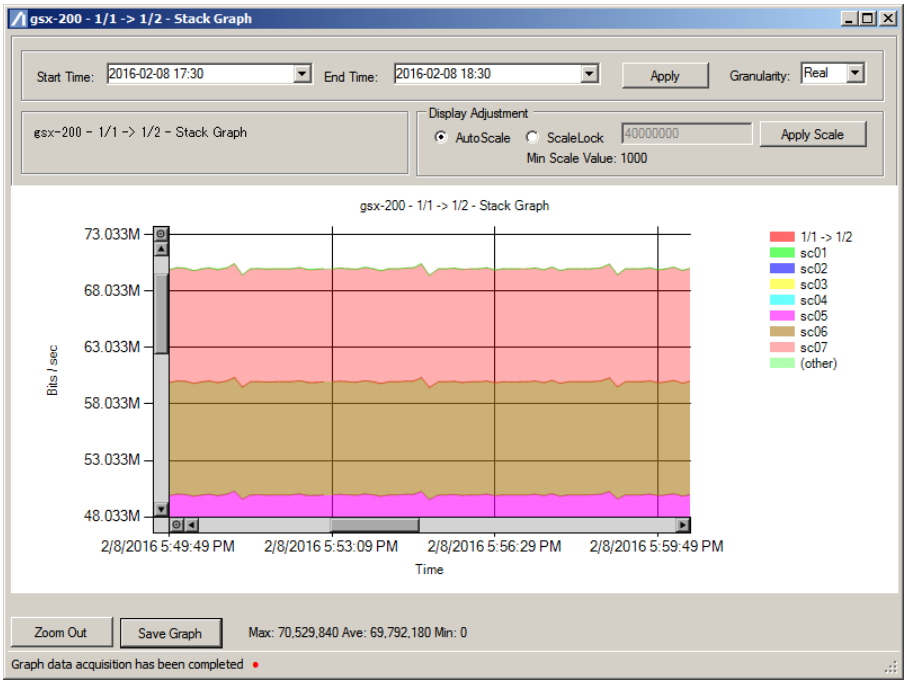


Figure 4.5.4-2 Display of zoomed area as a graph

Click the following buttons on each axis to zoom out the graph.

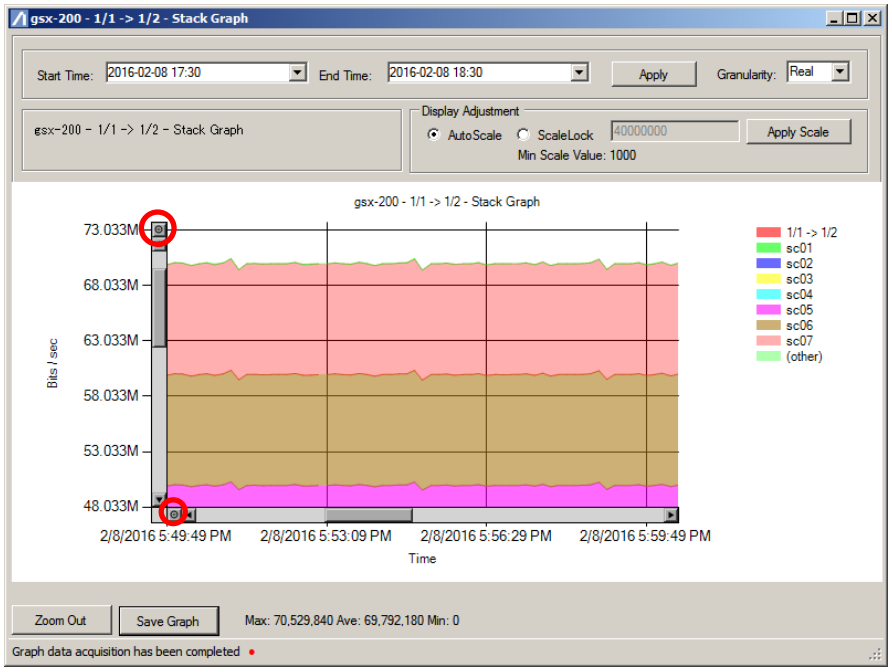


Figure 4.5.4-3 Zooming out the graph

By clicking the **Back to previous** button, the last graph before zooming appears.

4.5.5 Saving a graph

You can save a traffic monitoring graph in JPEG format. If the graph format is the table, it can be saved in CSV format.

Click the **Save graph** button while the graph to be saved is displayed.

Specify the folder in which to save the graph and the file name in the file save window, and click the **Save** button.

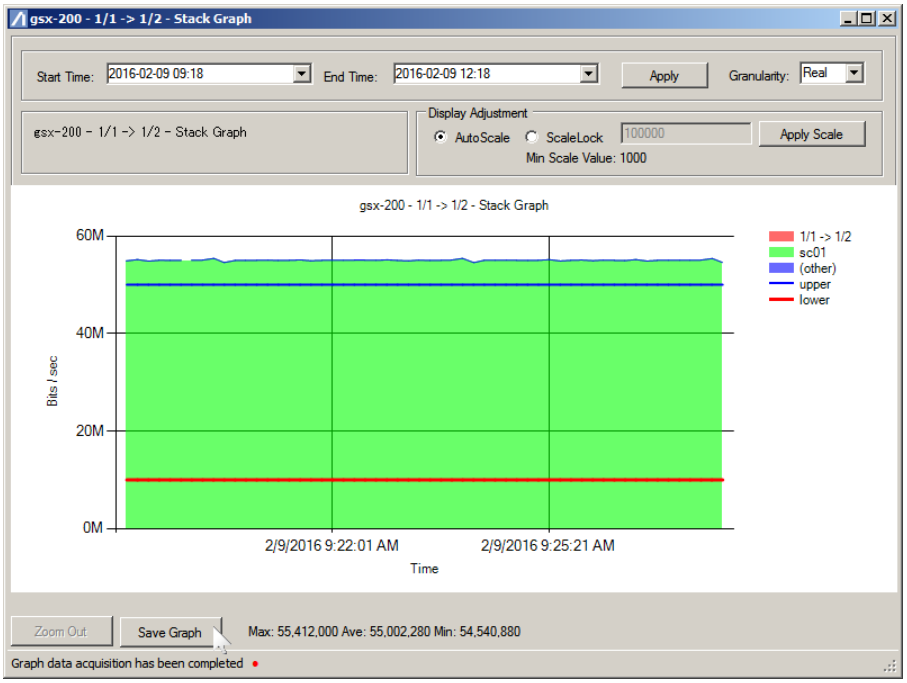


Figure 4.5.5-1 Saving a graph

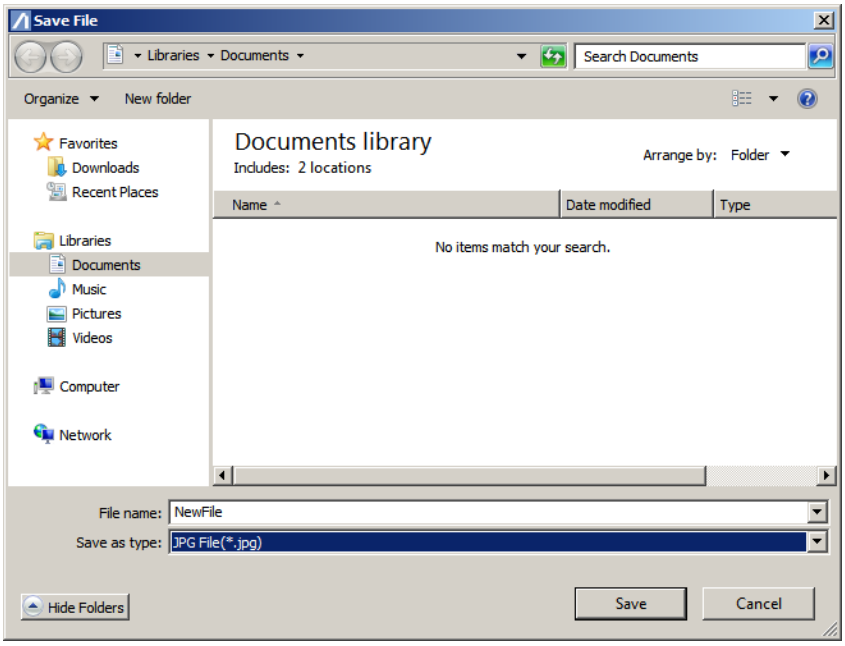


Figure 4.5.5-2 File save window

Note:

The design and layout of the file save window varies depending on the OS.

4.5.6 Graph display setting

In version v1.3.1 or later, the following graph display settings can be selected.

- Setting for displaying leader lines of a circle graph
- Setting for displaying data labels of a bar graph
- Setting of background line color saturation of a bar graph
- Setting of transmission rate of colors specified for the external configuration file
- Setting of unit display for stacked bar, line, and bar graphs

Select the setting according to the following procedure.

1. Exit MMClient.
2. Open MMClient.config using the text editor.
   The location of MMClient.config is given below.
   C:¥ProgramData¥AnritsuNetworks¥MMClient¥MMClient.config
3. Change the value of each setting tag.
4. Overwrite MMClient.config and save it.
5. Start MMClient.

The tag names and set values are listed below.

Table 4.5.6-1 Tag name and set value

Displayed contents	Tag name	Set value
Setting for displaying leader lines of a circle graph Setting for displaying data labels of a bar graph	PieBarDisableLabel AndExtendLegend	true: No leader line appears. No data label appears. false: Leader lines appear. Data labels appear. (compatible display for versions v1.2.4 or earlier). Default value: true
Setting of background line color saturation of a bar graph	BarHorizontalLine LookBehind	true: Displays in darker color. false: Display in lighter color (compatible display for versions v1.2.4 or earlier) Default value: true
Setting of transmission rate of colors specified for the external configuration file	GraphCSVAlpha	0 to 100: Color darkness/lightness 0: Transparent, 100: Opaque Default value: 50 (compatible display for versions v1.2.4 or earlier)
Setting of unit display for stacked bar, line, and bar graphs (K/M/G display)	EnableGraphUnit	true: Displays a unit false: Does not display a unit (compatible display for versions v1.2.4 or earlier) Default value: true

4.6 Counter data type

This software collects "Monitor information and "Top information" of the statistics information managed by PureFlow node. This software displays a real-time graph or previous graph and creates a report according to the collected data.

The statistics information of PureFlow node is classified into the following counter types according to targets from which the data is collected.

- Network port counter
- Scenario counter (including a port scenario)
- Top counter

The information is classified into the following counter types according to the purpose of the graph or report.

- Scenario and port counter information (monitor information)
  - Hierarchical counter information
  - Discard counter information
  - Peak counter information (only for GSX, WSX, or WS1)
  - Network port counter information (Transmit-Receive-Discard counter information) (only for WSX (TCP acceleration) or WS1)
- Top counter information (top information, flow counter for PureFlowGS1)

This software manages the port information of PureFlow WSX (TCP acceleration) and WS1 divided into the Network port and port scenario. The port scenario is handled in the same way as the normal scenario. The ports of PureFlow GS1, GSX, and WSX (Traffic shaping are handled in the same way as the port scenario.

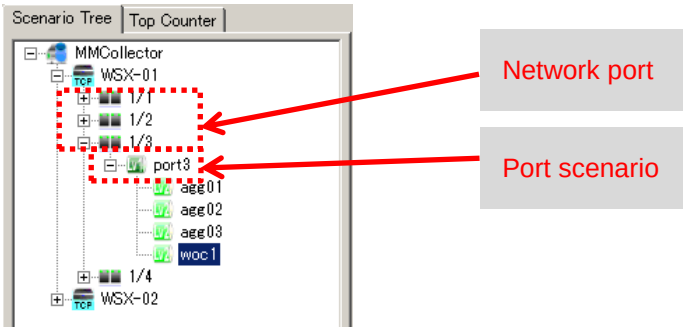


Figure 4.6-1 Network port and port scenario

Table 4.6-1 shows the relationship between the counter information for each data collection target and the counter type for each purpose.

Table 4.6-1 Relationship between the counter type for each data collection target and the counter type for each purpose

For each purpose / For each target	Scenario and port counter information (monitor information)			Top counter information (Top information)
	Hierarchical counter	Discard counter	Peak counter	
Network port counter	○	○	-	-
Scenario counter	○	○	○	-
Top counter	-	-	-	○

○: Used for the counter for each purpose; -: Not used for the counter for each purpose.

4.6.1 Network port counter and scenario counter

The Network port counter and scenario counter show the counted number of bytes and packets of the flow that passed the Network port and scenario of PureFlow node. The hierarchical counter uses the total transmission byte/bit/packet, transmission byte/bit/packet rate value, and data aggregation time.
The discard counter uses the total transmission byte/bit/packet, total discard byte/bit/packet, transmission byte/bit/packet rate value, discard byte/bit/packet rate value, and data aggregation time.

The Network port counter and scenario counter collects the information listed below.

- Total reception byte
- Total transmission byte
- Total discard byte (only for scenarios)
- Total reception packet
- Total transmission packet
- Total discard packet
- Scenario status (only for WSX (TCP acceleration) or WS1)
- Data aggregation time

This software calculates the following values based on the collected information.

This software calculates the following bit value based on the counter values for each byte.

- Total reception bit
- Total transmission bit
- Total discard bit (only for scenarios)

The difference between the current counter value and previous counter value is divided by the number of seconds elapsed during notification of the counter value every time notification is made to calculate each rate value. For example, the reception byte rate is calculated as described below.

> Number of elapsed seconds = Data aggregation time of the current counter value - Data aggregation time of the previous counter value
> Reception byte rate = (Total reception byte (current value) − Total reception byte (previous value)) / Number of elapsed time

- Reception byte rate
- Transmission byte rate
- Discard byte rate (only for scenarios)
- Reception bit rate
- Transmission bit rate
- Discard bit rate (only for scenarios)
- Reception packet rate
- Transmission packet rate
- Discard packet rate

The scenario status, which is the statistics information of PureFlow WSX (TCP acceleration) and WS1, is output only to the CSV report. Output of this report in the initial status is disabled. The report output setting enables output of this information to the CSV report. For details of the setting, refer to "5.5.3 Monitor information CSV reports".

4.6.2 Top counter

The top counter lists the use status of the flow that passed the scenario and port scenario. The list contains up to the top 25 for each transmission source, destination, and application (port number). This counter is used when collecting the information for each top information notification cycle that was configured. To collect the value indicated by the top counter, the traffic counter must be set from CLI of PureFlow node in advance. The traffic counter for the port and scenario can be set.
The following information is obtained as the top counter information for the target scenario or port scenario.

- Top counter aggregation start time
- Top counter aggregation end time
- Number of transmission packets
- Number of transmission bytes

The following information is obtained as the detailed top counter information.

- Transmission source top
  - Transmission source address
  - Number of transmission bytes
  - Number of transmission packets
- Reception destination top
  - Reception destination address
  - Number of transmission bytes
  - Number of transmission packets
- Transmission source, reception destination top
  - Transmission source address
  - Reception destination address
  - Number of transmission bytes
  - Number of transmission packets
- Application top
  - Protocol number
  - Number of transmission bytes
  - Number of transmission packets

4.6.3 Peak counter

The peak counter information shows the maximum rate value in one minute of the flow that passed the scenario. Monitoring is enabled only when the registered node is PureFlow GSX, WSX, or WS1 and when the monitor information notification cycle is 60 seconds.

The following information is collected as the peak counter information.

- Byte peak rate value (Maximum rate (Bps) value for one minute)
- Average byte rate value (Average rate (Bps) value for one minute)

4.7 Statistics information output

Graph display (real graph, past graph, and HTML report) of the statistics information collected by this software and output of this information in a CSV file (CSV report) can visualize the communication information and clarify the communication status of PureFlow node. This section describes the counter type of statistics information collected by this software and the relationship between the graph display and report output.

This software can display the following types of graphs.

- Monitor information
  - Stacked bar graph
  - Line graph
  - Circle graph
  - Bar graph
  - Table
- Top information
  - Circle graph
  - Table

A unit of data must be specified for displaying the data in graph form.

- Bit unit
- Byte unit
- Packet unit

Regarding the bit unit, one byte is equal to and can be replaced by eight bits. Some counter types show the statistics only in a packet unit or in a bit-and-byte unit.

This software can output four types of statistics information formats as listed below, and these format types are roughly divided into two types: graph output and CSV output.

- Graph output
  - Real graph
  - Past graph
  - HTML report*
- CSV output
  - CSV report*

* For details of the HTML report and CSV report, refer to "Chapter 5 Report Feature".

If the graph type is the same but the graph output format is different in three format types to output graphs, the period determination method of data to be output varies. Items other than this method do not vary.

The values shown in each type of Monitor information graph are listed in the table below.

Table 4.7-1 Value displayed in a Monitor information graph

Graph format / Graph type	Stacked bar graph	Line graph	Circle graph	Bar graph	Table
Real graph	A	A	A	A	A
Past graph	A	A	B	B	B

A: Rate value per minute, B: Increment for the selected period

4.7.1 Hierarchical counter in a stacked bar graph and line graph

For the transmission rate value of the specified scenario or port (parent scenario and port), the transmission rate value for the specified period in addition to the transmission rate value of the lower scenario (child scenario) for the same period is displayed in one graph.

The series shown as Other is the value obtained by the following calculation.

Other = Rate value of the parent scenario/port − sum (Rate value of each child scenario)

The stacked bar graph shows the stacked rate values of the child scenarios and last-stacked Other. Although the legend shows the parent scenario/port, the rate value of the parent scenario/port is not displayed in graph format.

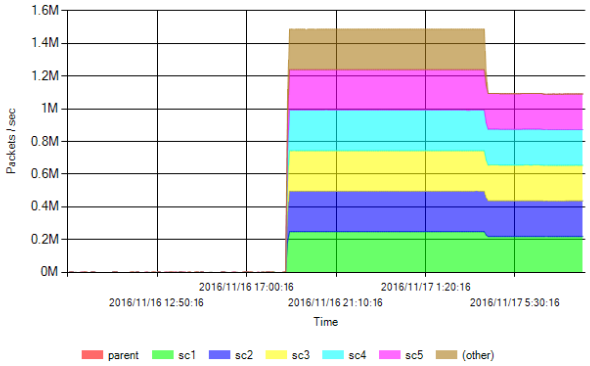


Figure 4.7.1-1 Hierarchical counter in a stacked bar graph

The line graph shows the rate values of the parent scenario/port, child scenario, and Other.

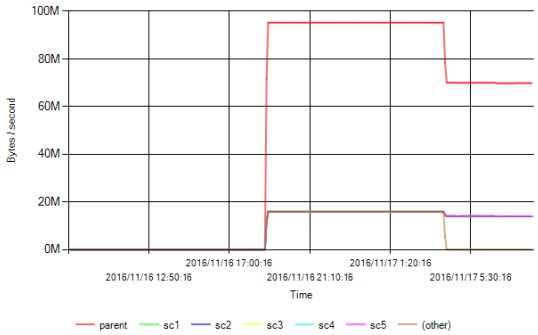


Figure 4.7.1-2 Hierarchical counter in a line graph

Up to 255 child scenarios can be displayed in graph format. See “4.4.5 Cautions when creating a graph”

4.7.2 Hierarchical counter in a circle graph, bar graph, and table

For the transmission counter of the specified scenario or port (parent scenario and port), the increment of the transmission counter value for the specified period in addition to the increment of the transmission counter value of the lower scenario (child scenario) is displayed in one graph or table.
The transmission counter value to be used refers to the data at the oldest time and latest time within the specified range.

Increment of transmission counter = Transmission counter value at the latest time − Transmission counter value at the oldest time

A real graph refers to the two latest items of data within 10 minutes after the latest time. The rate value between the two latest items of data is displayed.

Number of elapsed seconds = Data aggregation time of the latest counter value − Data aggregation time of the next latest counter value Rate value of a real graph = (Latest counter value − Next latest counter value) / Number of elapsed seconds

(Other) is obtained by subtracting the increment of the transmission counter value of the child scenario from the increment of the transmission counter value of the parent scenario/port.

Other = Increment of the transmission counter value of the parent scenario/port − sum (increment of the counter value of each child scenario)

A circle graph shows the percentages of the child scenario and Other value based on 100% of the counter value of the parent scenario/port. The legend shows the rate value or increment value for each counter.

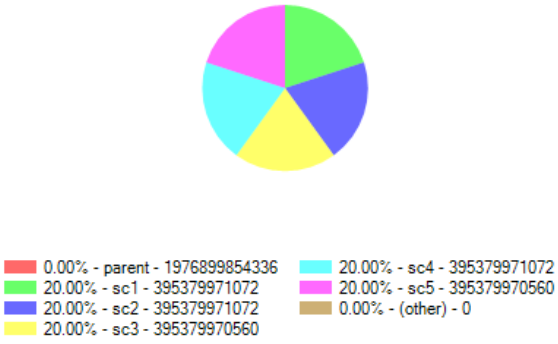


Figure 4.7.2-1 Hierarchical counter in a circle graph

Bar graphs show all of the parent scenario/port, child scenario, and Other of the obtained transmission counter value.

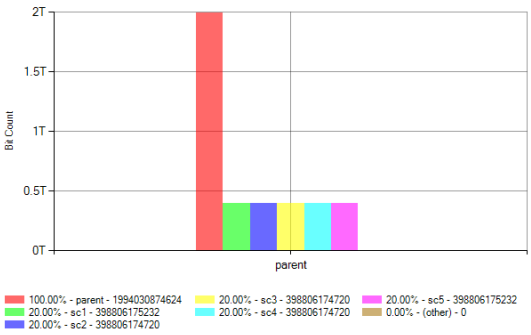


Figure 4.7.2-2 Hierarchical counter in a bar graph

Table shows the numerical values of the parent scenario/port, child scenario, and Other of the obtained transmission counter value.

Scenario	Transmit
parent	558,593,288
sc1	111,718,656
sc2	111,718,656
sc3	111,718,656
sc4	111,718,656
sc5	111,718,664
(other)	0

Figure 4.7.2-3 Hierarchical counter in a table of a real graph or past graph

The HTML report table shows the transmission counter information of the parent scenario/port.

Scenario Name	Transmitted Packet Count	(Other)
parent	67,577,367,675	8,275,885,355

Figure 4.7.2-4 Hierarchical counter in an HTML report table

Up to 255 child scenarios can be displayed. The subsequent child scenarios cannot be displayed. See “4.4.5 Cautions when creating a graph”.

Note:

The rate value per second is used as the displayed transmission counter value for a real graph in circle graph, bar graph, and table formats. In a past graph and HTML report, the increment of the transmission counter value for the selected time is used as the displayed transmission counter value.
The purpose of using a real graph in the formats of circle graph, bar graph, and table is to show the percentage of the flow that sequentially changes in combination with line and stacked bar graphs based on the parent scenario.

The purpose of using a past graph and HTML report in a circle graph, bar graph, and table is to display the percentage of total transmission amount for the specified period.

4.7.3 Discard counter in a stacked bar graph and line graph

The transmission counter rate value and discard counter rate value of the specified scenario or port for the specified period are displayed.

A stacked bar graph shows the transmission counter by stacking on the discard counter.

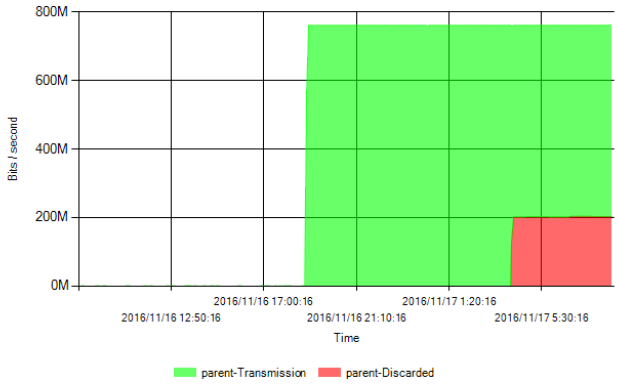


Figure 4.7.3-1 Discard counter in a stacked bar graph

A line graph shows the discard counter and transmission counter.

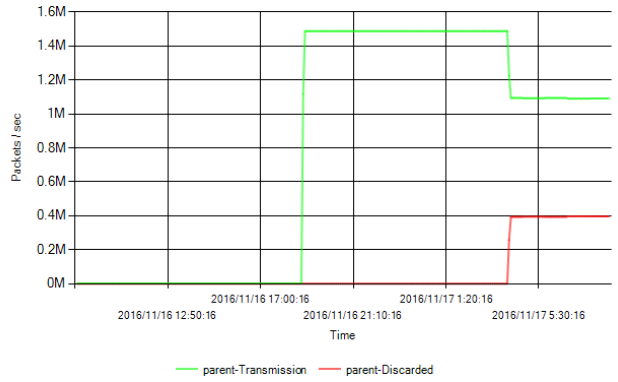


Figure 4.7.3-2 Discard counter in a line graph

4.7.4 Discard counter in a circle graph, bar graph, and table

The increment of the transmission counter value and that of the discard counter value of the specified scenario or port for the specified period are displayed.

The transmission counter value to be used refers to the data at the oldest time and latest time within the specified range.

Increment of transmission counter = Transmission counter value at the latest time − Transmission counter value at the oldest time Increment of discard counter = Discard counter value at the latest time − Discard counter value at the oldest time

A real graph refers to the two latest items of data within 10 minutes after the latest time. The rate value between the two latest items of data is displayed.

Number of elapsed seconds = Data aggregation time of the latest counter value − Data aggregation time of the next latest counter value Rate value of a real graph = (Latest counter value − Next latest counter value) / Number of elapsed seconds

A circle graph shows the percentage of the discard counter and transmission counter values.

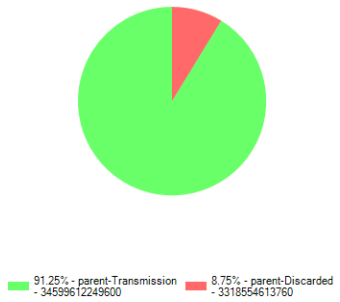


Figure 4.7.4-1 Discard counter in a circle graph

A bar graph shows the discard counter and transmission counter values.

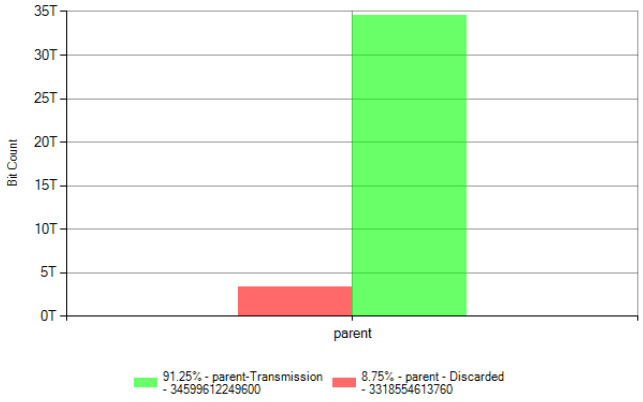


Figure 4.7.4-2 Discard counter in a bar graph

A table shows the transmission counter and discard counter values.

Transmitted Byte Count	Discarded Byte Count
4,324,951,531,200	414,819,326,720

Figure 4.7.4-3 Discard counter in a table

Note:

A real graph in circle graph, bar graph, and table formats shows the rate values per second of the transmission counter and discard counter. A past graph and HTML report show increments of the transmission counter and discard counter for the selected time. The purpose of using a real graph in the formats of circle graph, bar graph, and table is to show the ratio of the transmission counter and discard counter that sequentially changes in combination with line and stacked bar graphs.

The purpose of using a past graph and HTML report in a circle graph, bar graph, and table is to display the percentages of the total transmission and discard amounts for the specified period.

4.7.5 Peak counter in a stacked bar graph and line graph

The byte peak rate counter value and transmission byte rate counter rate value of the specified scenario or port for the specified period are displayed.
The peak graph does not show the rate value calculated inside this software but shows the byte rate value transmitted together with the peak counter.

The stacked bar graph shows the peak counter value as the filled background and the transmission counter value at the front.

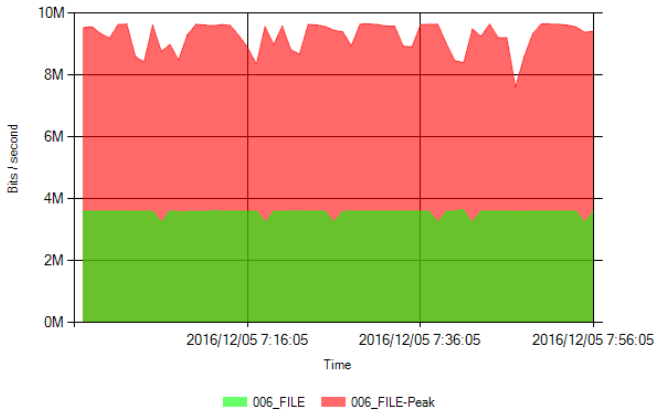


Figure 4.7.5-1 Peak counter in a stacked bar graph

A line graph shows the peak counter and transmission counter values.

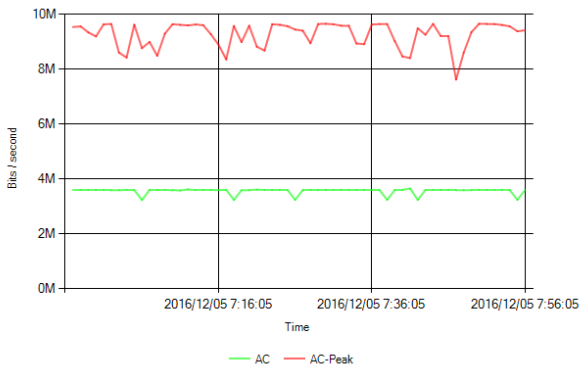


Figure 4.7.5-2 Peak counter in a line graph

4.7.6 Network port counter in a line graph

The transmission counter rate value, reception counter rate value, and discard counter rate value of the Network port of PureFlow WSX (TCP acceleration) and WS1 are displayed in line graph format.

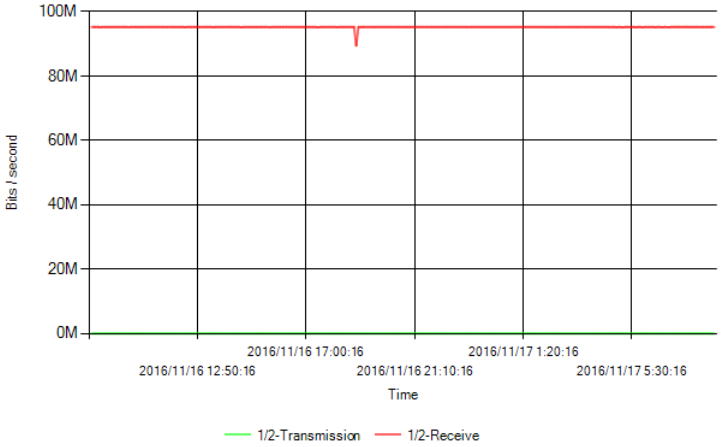


Figure 4.7.6-1 Network port counter in a line graph

The discard counter rate value only in a packet unit is displayed.

4.7.7 Network port counter in a bar graph and table

For the transmission counter value, reception counter value, and discard counter value of the Network port of PureFlow WSX (TCP acceleration) and WS1, the increment of the counter value within the specified range is displayed in bar graph and table formats.

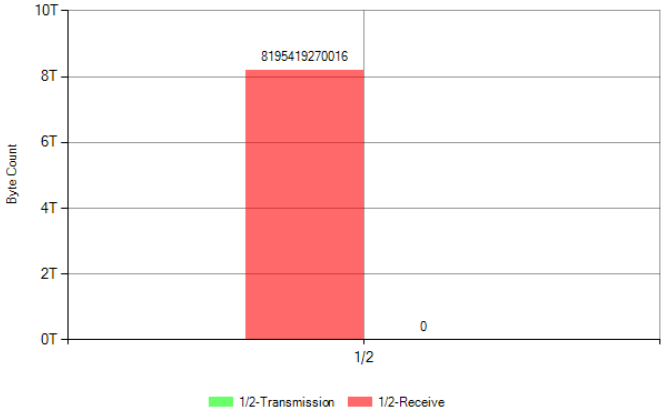


Figure 4.7.7-1 Network port counter in a bar graph

Increments of the reception counter, transmission counter, and discard counter are displayed in bar graph format.
The table shows increments of the reception counter, transmission counter, and discard counter in numerical values.

Port Direction	Transmitted Packet Count	Receive Packet Count	Discarded Packet Count
1/2	0	128,053,426,093	0

Figure 4.7.7-2 Network port counter in a bar graph

Note:

A real graph in bar graph and table formats show the rate values per second of the transmission counter, reception counter, and discard counter. A past graph and HTML report show increments of the transmission counter, reception counter, and discard counter for the selected time.

The purpose of using a real graph in the formats of bar graph and table is to show the rate values of the transmission counter, reception counter, and discard counter that sequentially change in combination with line and stacked bar graphs.

The purpose of using a past graph and HTML report in a bar graph and table is to display the total amounts of transmission, reception, and discard for the specified period.

4.7.8 CSV report (transmission and discard counter)

A CSV report is the information of the Network port counter and scenario counter output in CSV format.
The time reference range of a CSV report is the same as the past graph range of the hierarchical counter.

The start time and end time mean the time at which two counters that were used for calculation of the delta value are obtained respectively. The data displayed in the same line is the statistics information aggregated at the end time.

The total reception counter value, total transmission counter value, and total discard counter value that were notified from Pureflow are output directly.

The delta reception value, delta transmission value, and delta discarded value are calculated by obtaining the difference between the data at the end time and the data at the start time, and are then output.

Delta counter value = Total counter value at the end time − Total counter value at the start time

The reception average value, transmission average value, and discard average value are calculated by dividing the delta value by the number of elapsed seconds from the end time and start time, and are output.

Number of elapsed seconds = End time − Start time Average value = Delta counter value/Number of elapsed seconds

For the peak rate value, the peak rate value of the time corresponding to the end time is used.

For items output as a CSV report, refer to "5.5.3 Monitor information CSV reports".

4.7.9 Top counter in a circle graph and table

For the scenario or port to be the top counter aggregation target specified in the device main unit, the top counter graph aggregates and shows the data that was calculated by the four aggregation methods (transmission source address, transmission destination address, transmission source/destination address, and port number) for each scenario port.

The information of the top 25 is displayed, and the other transmission counter values are added to Other and displayed.
For the data of the top 25 in the aggregated period, the rate calculated from the data having same transmission source address, transmission destination address, transmission source/destination address, and port number (same aggregation target) are displayed.

Number of elapsed seconds = The latest time in data aggregation range
− The oldest time in data aggregation range
Total value of the counter value of each top 25
= sum (The counter value of same aggregated target)
Rate value of each top 25 = Total value of the counter value of each top 25 /
Number of elapsed seconds

Other is the rate value obtained by subtracting the total value of the counter values of the top 25 from the total counter value of the top counter aggregation targets, and divided by number of elapsed seconds.

Number of elapsed seconds = The latest time in data aggregation range
− The oldest time in data aggregation range
(Other) = {Total counter value of the top counter aggregation targets − sum (counter values up to the top 25)} / Number of elapsed seconds

The top circle graph shows the values and the ratio.

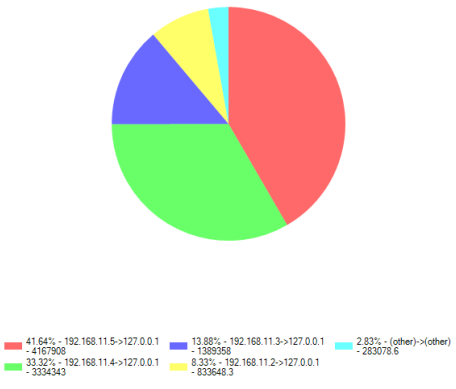


Figure 4.7.9-1 Top counter in a circle graph

The top table shows the aggregation values.

Order	Source-Destination: Top(TOP25)	pps	%
1	192.168.11.1 -> 127.0.0.1	19,176.32	16.283
2	192.168.11.2 -> 127.0.0.1	19,176.32	16.283
3	192.168.11.4 -> 127.0.0.1	19,176.30	16.283
4	192.168.11.3 -> 127.0.0.1	19,176.30	16.283
5	192.168.11.5 -> 127.0.0.1	19,176.29	16.283
6	192.168.11.6 -> 127.0.0.1	14,093.45	11.967
7	192.168.11.7 -> 127.0.0.1	0.05	0.00004
(Other)	-----	7,794.34	6.618

Figure 4.7.9-2 Top counter in a table

4.7.10 CSV report (top counter)

For a CSV report of the top counter, the top counter information within the time reference range is combined and information up to the top 25 and the counter values are output. For the items to be collected, refer to "4.6.2 Top counter". For the items of the top CSV, refer to "5.5.4 Top information CSV reports".

4.7.11 Relationship between the counter type and graph/report output

The relationship between the monitor information output type and counter value type is shown in Table 4.7.11-1.

Table 4.7.11-1 Relationship between the monitor information output type and counter value type

Output type / Counter value	CSV report	Real graph, past graph, HTML report			
		Network port	Hierarchy	Discard	Peak
Counter values of total reception byte, bit, and packet	○	○	○	○	-
Counter values of total transmission byte, bit, and packet	○	○	-	-	-
Counter values of total discard byte, bit, and packet	○	○	-	○	-
Rate values of reception byte, bit, and packet	-	○	○	○	-
Rate values of transmission byte, bit, and packet	-	○	-	-	-
Rate values of discard byte, bit, and packet	-	○	-	○	-
Counter values of delta reception byte, bit, and packet	○	-	-	-	-
Counter values of delta transmission byte, bit, and packet	○	-	-	-	-
Counter value of delta discard byte, bit, and packet	○	-	-	-	-
Average values of reception byte, bit, and packet	○	-	-	-	-
Average values of transmission byte, bit, and packet	○	-	-	-	-
Average values of discard byte, bit, and packet	○	-	-	-	-
Peak rate value	○	-	-	-	○
Average rate value corresponding to the peak rate	-	-	-	-	○
Data aggregation time	○	○	○	○	○

○: Uses the counter value; -: Does not use the counter value.

The relationship between the top information output type and counter value type is shown in Table 4.7.11-2.

Table 4.7.11-2 Relationship between the top information output type and counter value type

Counter value \ Output type	CSV report	Real graph, past graph, HTML report			
		Transmission destination	Reception source	Transmission destination Reception source	Application (Port number)
Top counter aggregation start time	○	○	○	○	○
Top counter aggregation end time	○	○	○	○	○
Number of transmission packets	○	○	○	○	○
Number of transmission bytes	○	○	○	○	○
Transmission source top, transmission source address	○	○	-	-	-
Transmission destination top, number of transmission bytes, bits, and packets	○	○	-	-	-
Reception source top, reception source address	○	-	○	-	-
Reception source top, number of reception bytes, bits, and packets	○	-	○	-	-
Transmission destination, reception source top, transmission source address	○	-	-	○	-
Transmission destination, reception source top, reception source address	○	-	-	○	-
Transmission destination, reception source top Number of reception bytes, bits, packets	○	-	-	○	-
Application top, reception source address	○	-	-	-	○
Application top, number of reception bytes, bits, and packets	○	-	-	-	○

○: Uses the counter value; -: Does not use the counter value.

4.7.12 Correspondence between the counter type and graph output

Table 4.7.12-1 shows the correspondence between the counter types and graph types.

Table 4.7.12-1 Correspondence between the counter types and graph types

	Stacked bar graph	Line graph	Circle graph	Bar graph	Table
Hierarchical counter*1	○	○	○	○	○
Discard counter*2	○	○	○	○	○
Peak counter*3	○	○	—	—	—
Network port counter*4	—	○	—	○	○
Top counter*5	—	—	○	—	○

*1 For a scenario or port that does not have scenarios under it, only a line graph can be displayed.

*2 For a port (excluding the port scenario), values in units of bits or bytes are not displayed or 0 is always displayed even if it can be displayed.
For the discard counter of the port, only the packets are collected.

*3 The peak counter can be selected only when the device is GSX, WSX, or WS1 and the notification cycle is set to 60 seconds.
The peak counter of the Network port cannot be displayed.
Only bit or byte can be selected as the data unit.

*4 The Network port counter is the graph format that can be selected only for the Network port of PureFlow WSX (TCP acceleration) and WS1.

*5 The top counter can be selected when the top counter (flow counter for GS1) is set on the device side.

4.7.13 Cautions regarding graph types

The selectable counter type varies according to the selected port and scenario.

- Port of PureFlow GS1, GSX, and WSX (Traffic shaping): Transmission, discard, peak
- Network port of PureFlow WSX (TCP acceleration) and WS1: Network port
- Scenario (including the port scenario of PureFlow WSX (TCP acceleration) and WS1): Transmission, discard, peak

Additionally, the graph types are restricted according to the settings of the scenarios and device.

- Port or scenario without scenarios under it: Line graph only
- PureFlowGS1: A peak graph cannot be selected.
- The notification cycle is not 60 seconds: A peak graph cannot be selected.

For the top counter, the top counter or flow counter must be set in the device.

4.8 Data decimation and granularity

MonitoringManager2 collects monitor information and top information from the statistics managed by PureFlow node. MonitoringManager2 displays graphs that show real-time or past information and creates reports based on the collected data.

To effectively collect and maintain long-term monitor information, MonitoringManager2 filters the monitor information as it is collected. The data is filtered and saved according to the following five types of time granularity:

- Real granularity: One item of data per notification (the interval varies depending on the monitor notification interval)
- 5-minute granularity: One item of data per notification received every five minutes
- 1-hour granularity: One item of data per notification received every hour
- 3-hour granularity: One item of data per notification received every three hours
- 1-day granularity: One item of data per notification received once a day

When creating a graph and report, the granularity is determined according to the settings of the display time range and notification interval. When displaying short-term information, collected data whose intervals are short (granularity is fine) is referenced. When displaying long-term information, collected data whose intervals are long (granularity is rough) is referenced.

The storage period can be set for each granularity. When the time granularity is fine, data can be displayed in a graph with a fine granularity. However, this consumes a large amount of hard disk capacity. A longer storage period equates to more hard disk capacity consumption. For details about how to set the storage period, see 7.4.1 Specifying the data storage period.

Granularity cannot be specified for top information; it can only be specified for real-time data.

4.8.1 Determining the granularity for past scenario graphs

When displaying a past scenario graph, the granularity of the data is determined according to the specified display time range. How to determine the granularity is described below.

1. Calculate the time length of the display period.
   Time length = (End time of range) – (Start time of range)
2. Determine the granularity according to the time length as follows:

Less than 24 hours:	Real granularity
24 hours or more but less than 7 days:	5-minute granularity
7 days or more but less than 1 month:	1-hour granularity (1 month is calculated based on the start time)
1 month or more but less than 1 year:	3-hour granularity
1 year or more:	1-day granularity

4.8.2 Determining the display range and granularity for real-time scenario graphs

Real-time scenario graphs show data in a 3-hour range from the current time. The display data is updated automatically at the time interval specified for the notification interval.

The granularity of the data is real granularity.

4.8.3 Determining the granularity for periodic reports

The granularity of the data used for periodic reports is determined according to the creation interval specified when setting the report task.

- Hourly: Real granularity
- Daily: 5-minute granularity
- Weekly: 1-hour granularity
- Monthly: 3-hour granularity
- Yearly: 1-day granularity

4.8.4 Determining the granularity for manual reports

The granularity of the data used for manual reports is determined according to the cycle specified when setting the report task. The range of the report to be output is from the end time to the time one cycle earlier than the end time.

- 1 hour: Real granularity
- 1 day: 5-minute granularity
- 1 week: 1-hour granularity
- 1 month: 3-hour granularity
- 1 year: 1-day granularity
- 10 minutes: Real granularity

4.9 Time reference range when creating a graph and HTML report

Use of the data for displaying the graph is determined after comparing the data aggregation time with the time reference range. The time reference ranges that vary according to the graph type are described here.

4.9.1 Time reference range for monitor information in a real graph

Stacked bar and line graphs show the data within the time range between the display time and three hours before the display time.

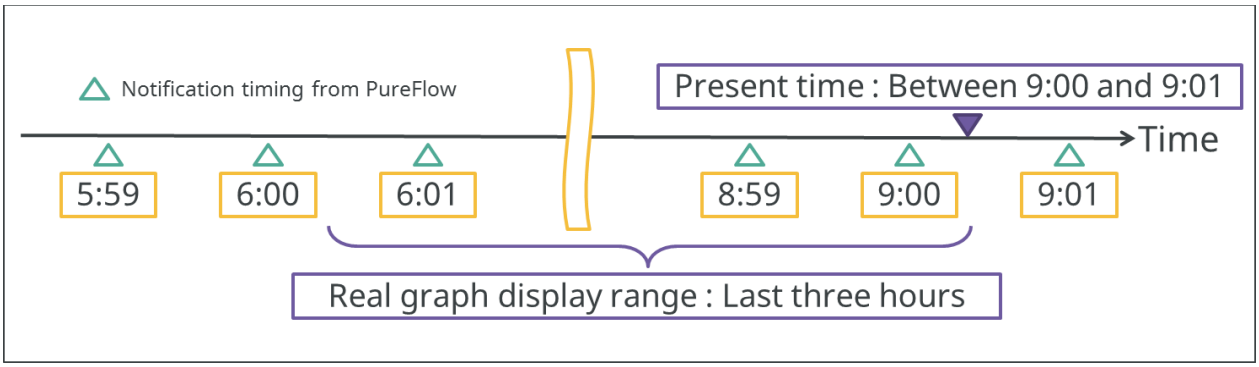


Figure 4.9.1-1 Time reference range of monitor information in a stacked bar graph, line graph, and real graph

A circle graph, bar graph, and table show the data determined based on the two latest items of data obtained from the range between the display time and 10 minutes before the display time. If either or both of the two latest items of data are lost, the two latest items of obtained data are used.

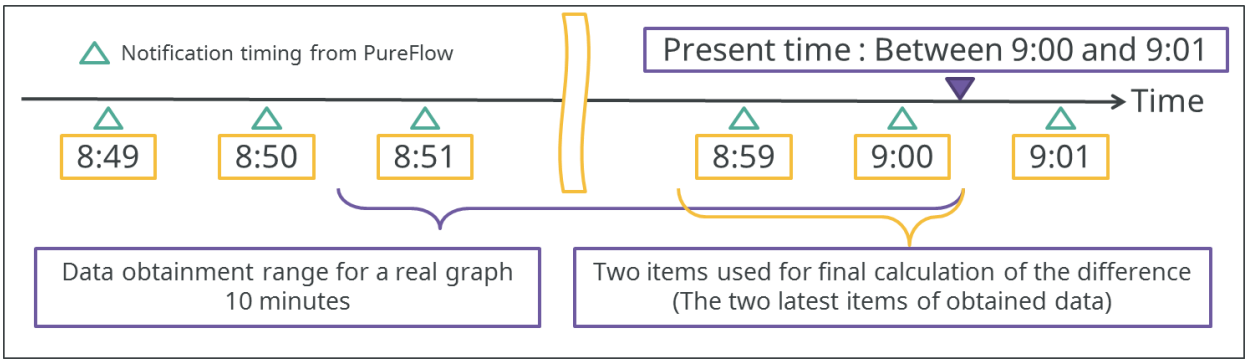


Figure 4.9.1-2 Time reference range of monitor information in a circle graph, bar graph, table, and real graph

4.9.2 Time reference range for monitor information in a past graph

For a past graph, users can specify the time range as required. The granularity is determined automatically according to the time range. Refer to "4.8 Data decimation and granularity".

Stacked bar and line graphs show the data within the specified time range.

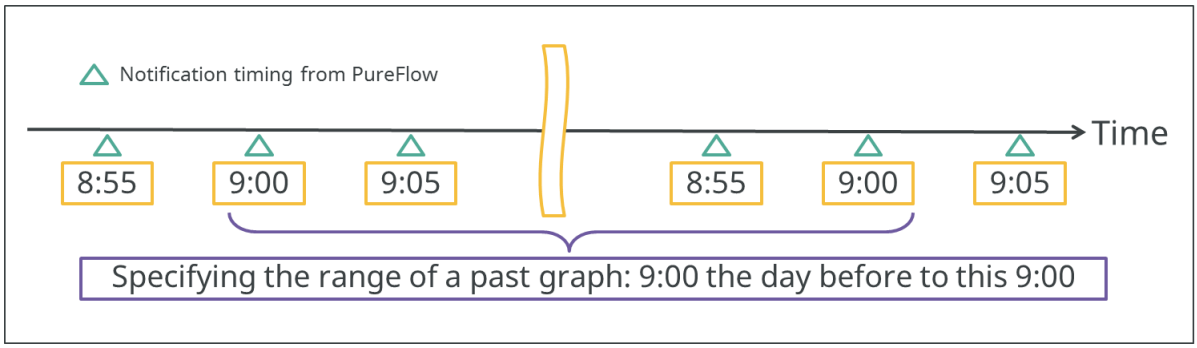


Figure 4.9.2-1 Time reference range of monitor information in a stacked bar graph, line graph, and past graph

For a circle graph, bar graph, and table, the data at the oldest time and latest time within the specified time range is obtained and used.

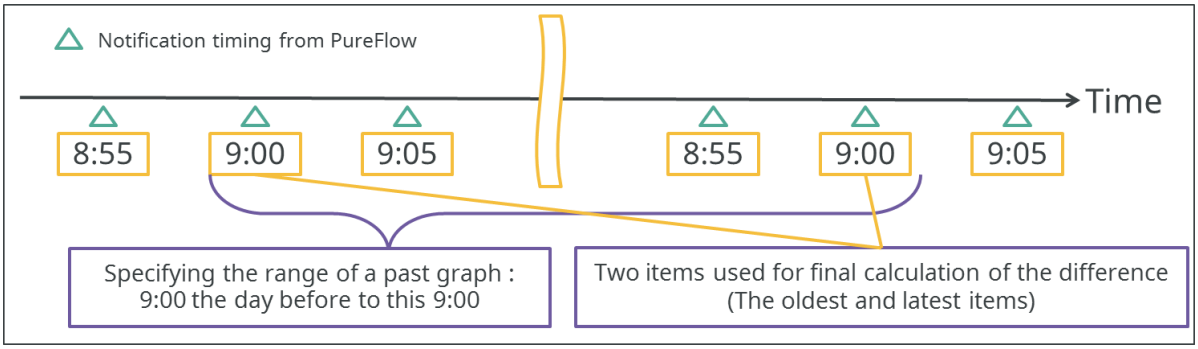


Figure 4.9.2-2 Time reference range of monitor information in a circle graph, bar graph, table, and past graph

4.9.3 Time reference range for monitor information in an HTML report

The data in the period of one cycle is used. The time reference range for a periodic report is between one cycle before the report creation start time and the report creation start time. The time reference range for a manual report is between one cycle before the report end time and the report end time.

For periodic report

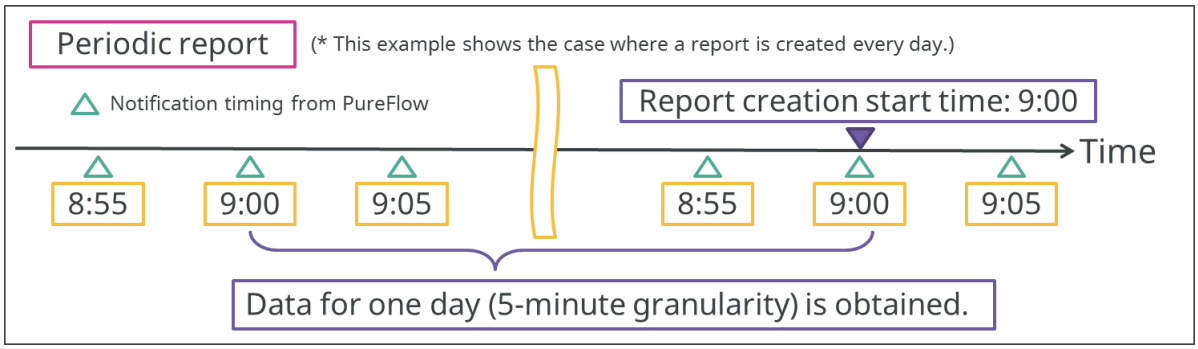


Figure 4.9.3-1 Time reference range of monitor information in a periodic report or HTML report

For a manual report

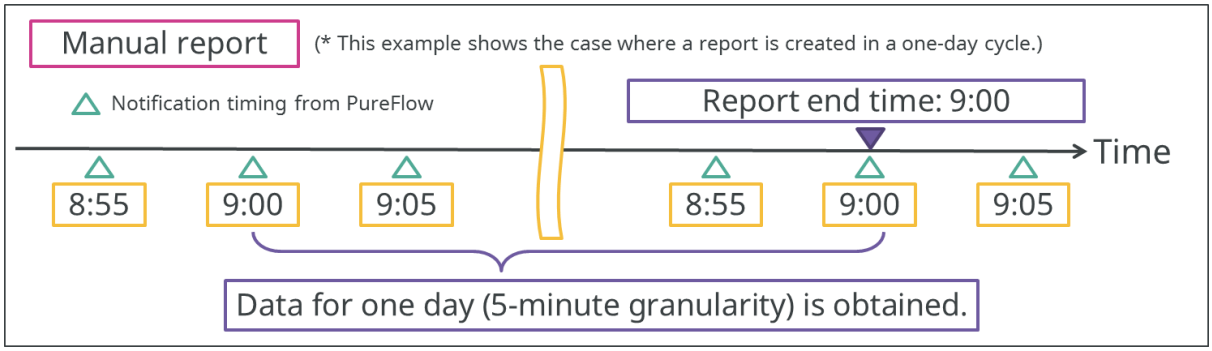


Figure 4.9.3-2 Time reference range of monitor information in a manual report or HTML report

For outputting the report, the same data as a past graph is obtained and displayed. (The period determination method is excluded.)

Stacked bar and line graphs show the data within the specified time range.
For a circle graph, bar graph, and table, the data at the oldest time and latest time within the specified time range is obtained and used.

4.9.4 Aggregation start time and end time of top information

There is the aggregation start time and end time for notification of the top information.
This means the time at which the top counter inside the device aggregates the top information.

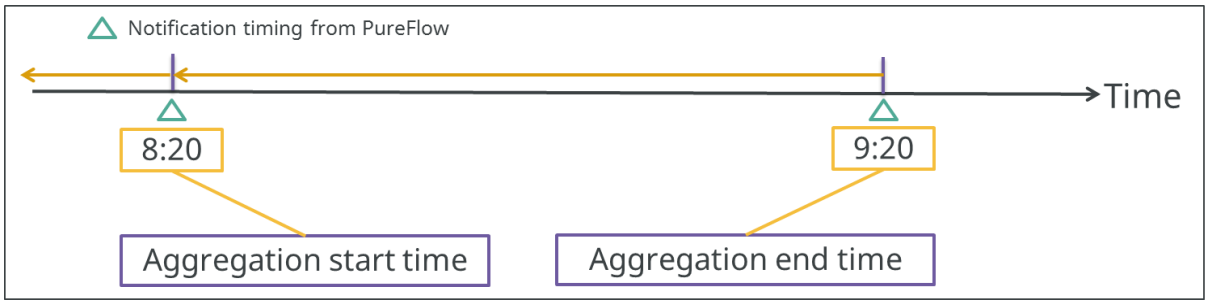


Figure 4.9.4-1 Aggregation start time and end time of top information

4.9.5 Time reference range for top information in a real graph

A real graph for the top information shows the top counter information for the last one time.

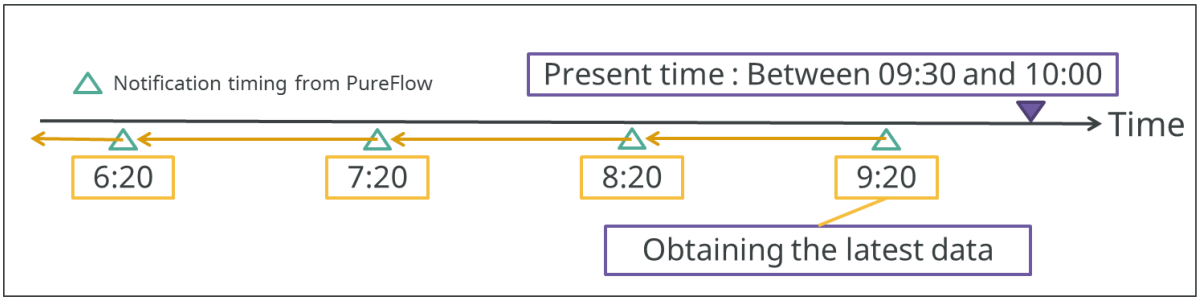


Figure 4.9.5-1 Time reference range for top information in a real graph

4.9.6 Time reference range for top information in a past graph

In a past graph for the top information, all the top counter information is combined while the specified period includes the aggregation period, and the top 25 of the total counter values of this information is output.

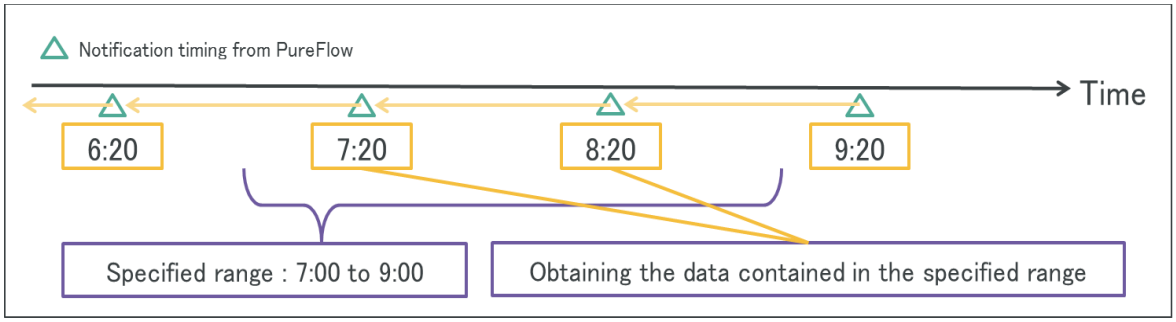


Figure 4.9.6-1 Time reference range for top information in a past graph

4.9.7 Time reference range for top information in an HTML report

The method of determining the time reference range of the top counter in an HTML report is the same as the time reference range determination method of the monitor information in an HTML report. For details, refer to "4.9.3 Time reference range for monitor information in an HTML report".

All of the top counter information within the time reference range is combined, and the top 25 of the total counter values of this information is output.

4.10 Displaying the scenario status and specifying scenario settings

If the volume of traffic exceeds or falls below the specified threshold value, an over- or under-threshold event can be issued.

This feature enables MonitoringManager2 to detect and report when the volume of traffic is too high or too low, allowing network problems to be detected and resolved quickly and accurately.

MonitoringManager2 reports over- or under-threshold events in the following three ways:

- By sending an SNMP trap
- By sending a syslog message
- By displaying the event on the client software console

By using the scenario comment feature, you can specify an alias (scenario comment) for a scenario set in PureFlow node. This alias is used when displaying the scenario on MonitoringManager2. Scenario comments are displayed in the scenario tree. They are also displayed when creating a graph or report.

4.10.1 Over- or under-threshold event detection

The over- or under-threshold event detection includes the following two types each totaling four types.

1) When “Rate upper limit” is enabled
   - Higher than “Rate upper limit”
   - Lower than “Rate upper limit”

2) When “Rate lower limit” is enabled
   - Higher than “Rate lower limit”
   - Lower than “Rate lower limit”

The over- or under-threshold event detection takes effect when the rate value of the scenario or the port exceeds the rate upper limit and the rate lower limit set for the scenario or the port.

A decision of over- or under-threshold event detection is given every time the monitor information is noticed. The over- or under-threshold event detection takes effect when the rate value stays higher than the value for more than the number of consecutively detected events. The number of consecutively detected events is reset when the state of over- or under-threshold is canceled before the value reaching the number of consecutively detected events.

Figure 4.10.1-1 and Figure 4.10.1-2 show the timing to detect the over- or under-threshold event when it exceeds the upper limit with the number of consecutively detected events set to one and three.

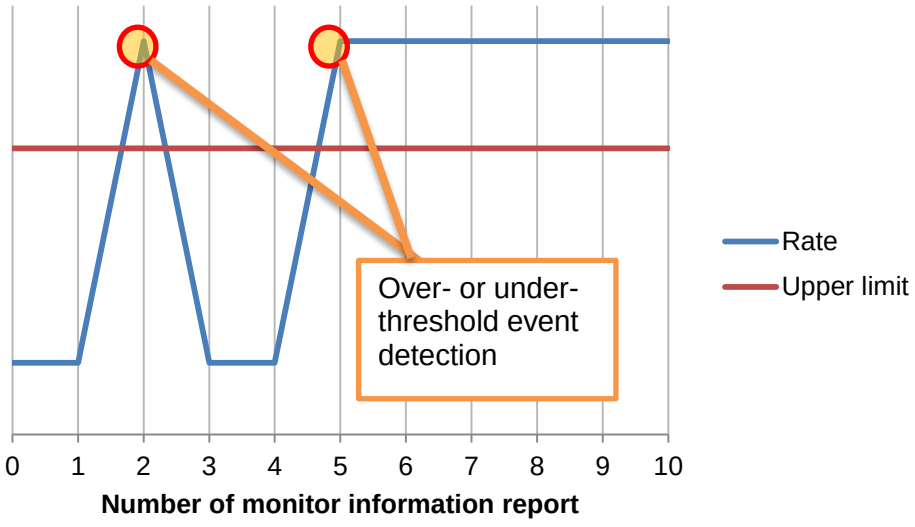


Figure 4.10.1-1 Timing to detect the over- or under-threshold event when the number of consecutively detected events is set to one

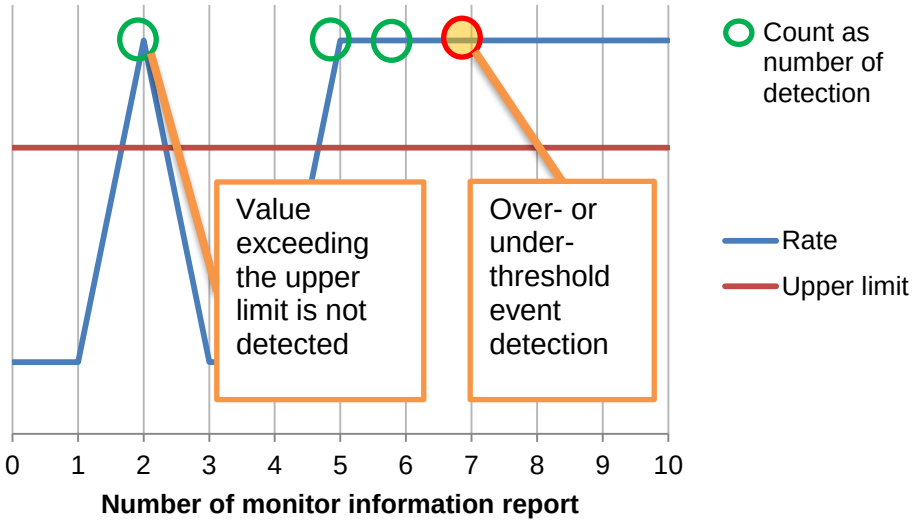


Figure 4.10.1-2 Timing to detect the over- or under-threshold event when the number of consecutively detected events is set to three

When the value stays higher than the upper limit or lower than the lower limit, detecting an over- or under-threshold event does not take effect until the value becomes lower than the upper limit or higher than the lower limit.

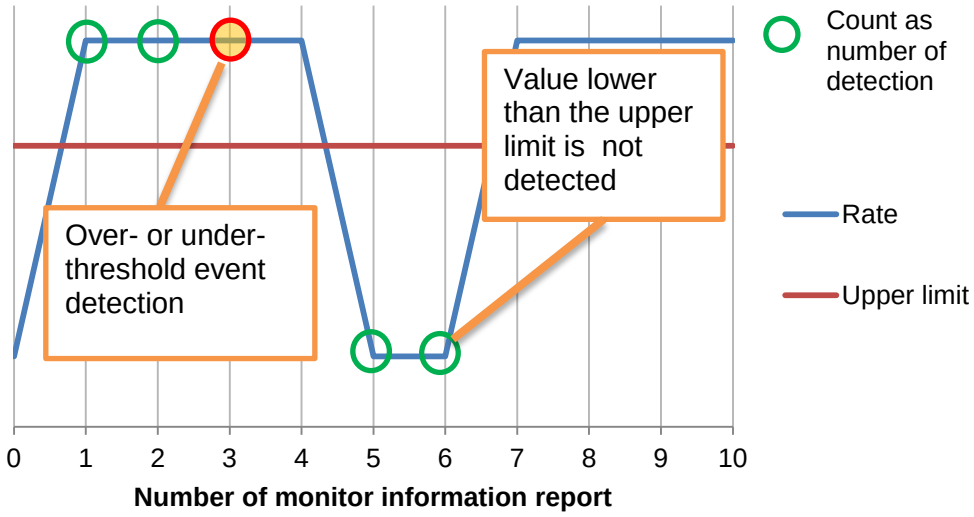


Figure 4.10.1-3 The case when the value lower than the upper limit is not detected when the number of consecutively detected events is set to three

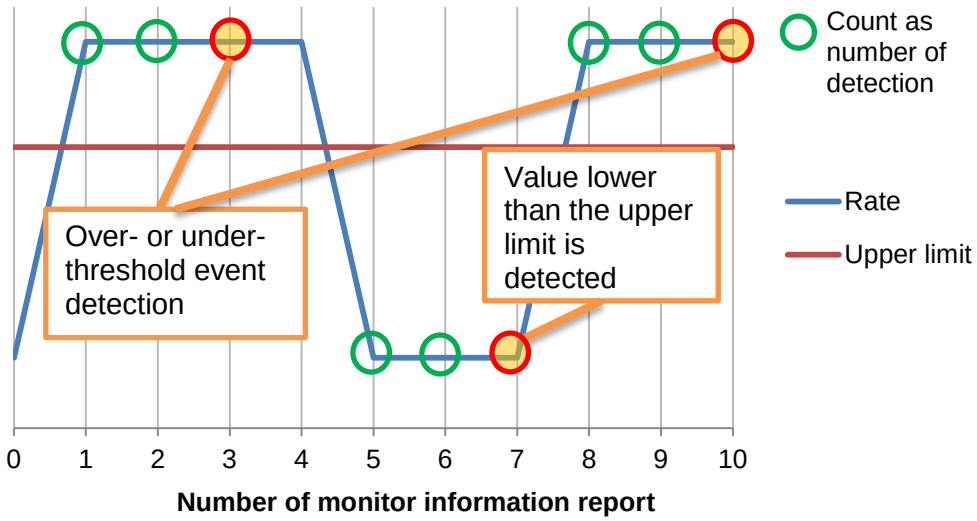


Figure 4.10.1-4 The case when the value lower than the upper limit is detected when the number of consecutively detected events is set to three

The upper limit value and the lower limit value of the threshold are determined separately. When the status changes from that exceeding the upper limit to that falling below the lower limit, it activates detecting the over- or under-threshold event for both the value lower than the upper limit and the lower limit.

MonitoringManager2 reports over- or under-threshold events in the following three ways:

- By sending an SNMP trap
- By sending a syslog message
- By displaying the event on the client software console

Be sure to specify the following settings when enabling the over- or under-threshold report feature.
For details about how to set the report feature, see 7.5.6 Specifying detection event settings.

To report an over- or under-threshold event by using an SNMP trap or syslog message, information about the host that will receive the trap or message must be registered in advance.
For details about how to specify the destination of an SNMP trap, see 7.5.4 Specifying SNMP settings.
For details about how to specify the destination of a syslog message, see 7.5.5 Specifying SYSLOG server settings.

If over- or under-threshold events are specified to not be reported, over- or under-threshold event detection results are not reported at all.

You can change the timing to report over- or under-threshold event detection by changing the notification interval setting.

- **real**: Over- or under-threshold events are reported when detected
- **Every 5 minutes**: All events that occur within a five-minute period are compiled and sent at five-minute intervals
- **Hourly**: All events that occur within a one-hour period are compiled and sent at hourly intervals
- **3-hourly**: All events that occur within a three-hour period are compiled and sent at three hourly intervals
- **Daily**: All events that occur within a one-day period are compiled and sent daily

When the cycle of the over- or under-threshold report is set to real-time, the over- or under-threshold event detected is reported every time the event is detected. When the cycle is set to other values, the information of the over- or under-threshold event detected during the set report cycle is accumulated and collectively reported after the report cycle has passed.

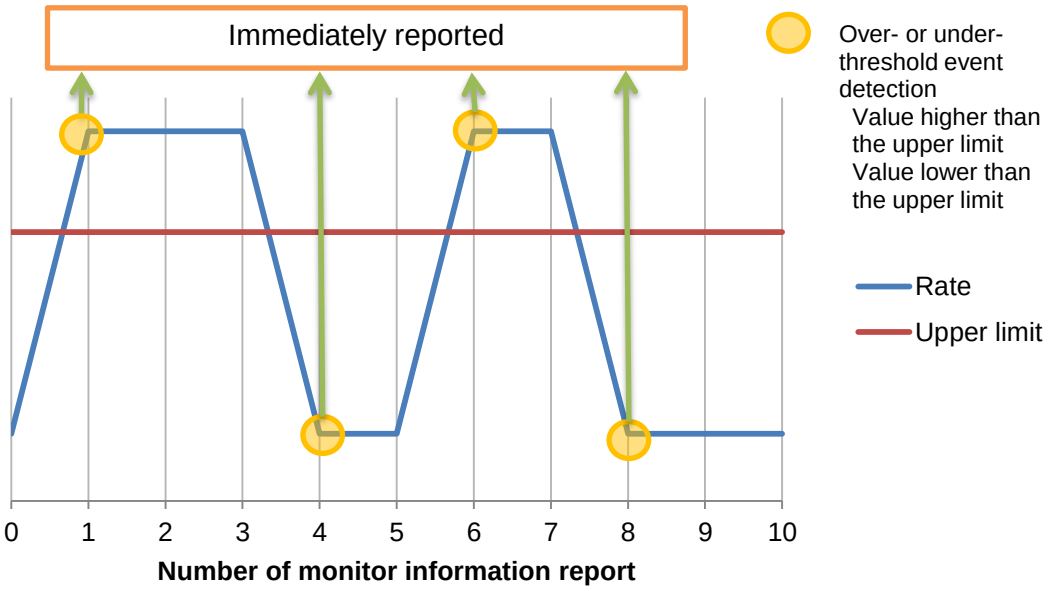


Figure 4.10.1-5 The case when the report cycle is 60 seconds, the number of consecutively detected events is one and the report cycle of the over- or under-threshold is real-time

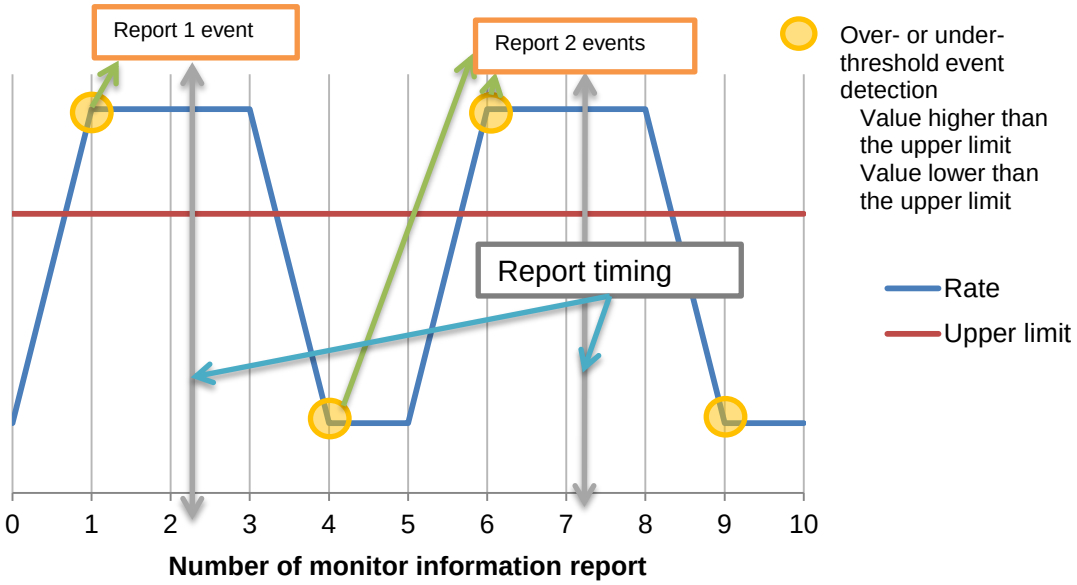


Figure 4.10.1-6 The case when the report cycle is 60 seconds, the number of consecutively detected events is one and the report cycle of the over- or under-threshold is 5 minutes

You can change SYSLOG severity of an over- or under-threshold event by changing the notification log type. Default of the notification log type is Notice.
An over- or under-threshold notification event reports only if a SYSLOG server notification level is higher or equal then the notification log type. For details about SYSLOG severity level, see 7.5.5 Specifying SYSLOG server settings.

If the notification interval setting is changed, accumulated notifications will be sent at the next notification timing. If the notification interval setting is too short, all the accumulated notifications might be sent at once.

Note:

If a threshold value is specified for a lot of scenarios, the load on MonitoringManager2 increases due to the necessity of checking the threshold value when collecting data. When using MonitoringManager2 in the recommended operating environment, limit the total number of threshold value settings for the ports and scenarios of all nodes to be monitored to 4,000. When using MonitoringManager2 in the minimum operating environment, limit the total number of threshold value settings to 1,000.

If network failure occurs, the cause might be overloading of the software due to over- or under-threshold events being detected simultaneously at multiple nodes. When specifying the monitoring of over- or under-threshold events, focus only on the important scenarios, and limit the number of threshold settings to 100 for notifications that might occur concurrently.

4.10.2 Setting threshold values for ports and scenarios

You can set threshold values for each port and scenario.

Two types of detection settings can be made for over-threshold events and two for under-threshold events (four settings in total), as shown below.

1) When **Rate upper limit** is enabled:
   - Rate has exceeded upper limit
   - Rate has fallen below upper limit

2) When **Rate lower limit** is enabled:
   - Rate has risen above lower limit
   - Rate has fallen below lower limit

When a port or scenario is selected on the scenario tree, the currently-set threshold value of the selected port or scenario is displayed.

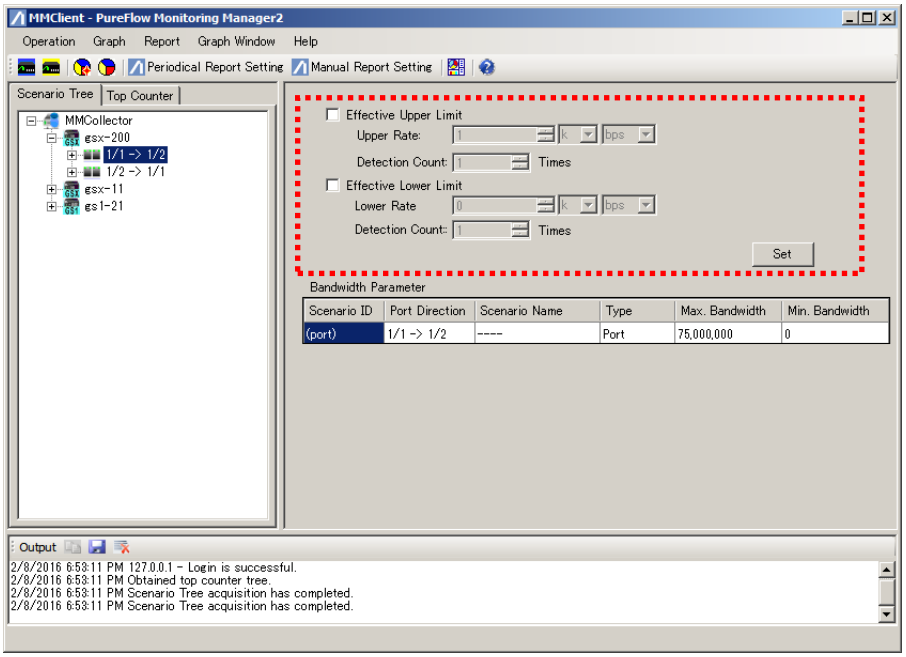


Figure 4.10.2-1 Threshold value setting field

Enable rate upper limit check box

Select this check box to enable detection of events when the rate has exceeded or fallen below the upper limit.

Enable rate lower limit check box

Select this check box to enable detection of events when the rate has risen above or fallen below the lower limit.

Rate upper limit

In PureFlow GS1 or WS1, select from a range of 1 k to 1 G [bps], 1 k to 125 M [Bps].
In PureFlow GSX or WSX, select from a range of 1 k to 10 G [bps], 1 k to 1.25 G [Bps].
The default value is 1 k [bps].
Integer number can be used in numeric part.
For example, Maximum rate upper limit value of PureFlow GSX, 1.25 GBps set as 1250 MBps.

Rate lower limit

In PureFlow GS1 or WS1, select from a range of 0 k to 1 G [bps], 0 k to 125 M [Bps].
In PureFlow GSX or WSX, select from a range of 0 k to 10 G [bps], 0 k to 1.25 G [Bps].
The default value is 1 k [bps].
Integer number can be used in numeric part.
For example, Maximum rate lower limit value of PureFlow GSX, 1.25 GBps set as 1250 MBps.

Number of consecutively detected events

Whether the flow volume exceeds the threshold value or not is checked every time monitor information is sent from PureFlow node to MonitoringManager2. This item is used to specify the number of times the rate has to consecutively exceed the threshold value in this check before an event is reported.
The maximum number that can be specified is 10 (times). The default value is 1 (time).
For example, if, for a particular node, **Monitor information notification interval** is set to 10 seconds and **Number of consecutively detected events** is 2, a notification is issued every 20 or 30 seconds when the flow volume continuously exceeds the threshold value.

When the threshold setting is enabled, lines indicating the rate upper and lower limits are added to the stacked bar and line graphs of the related port or scenario. This allows you to quickly compare the traffic volume with the threshold value.

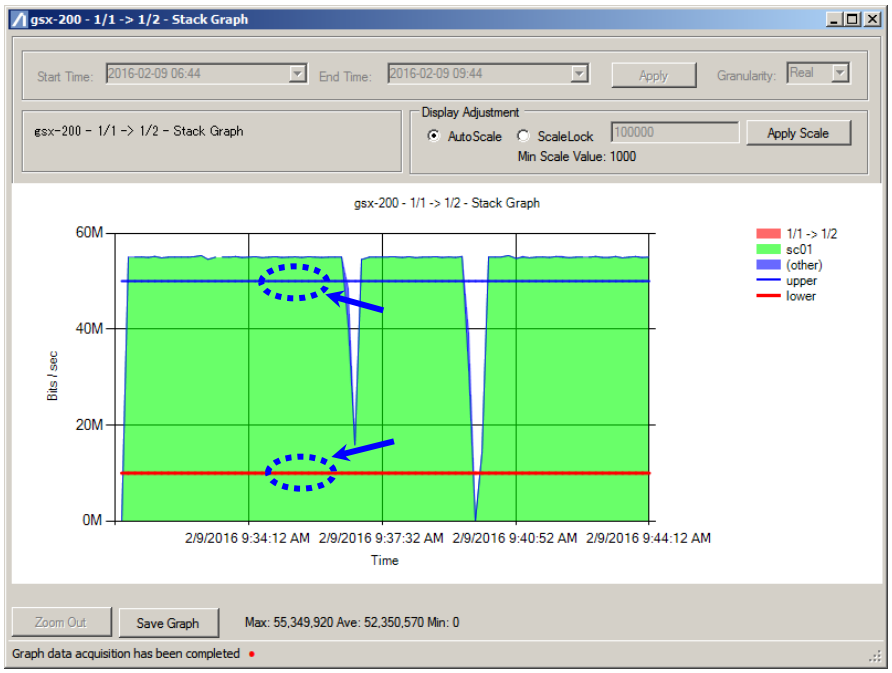
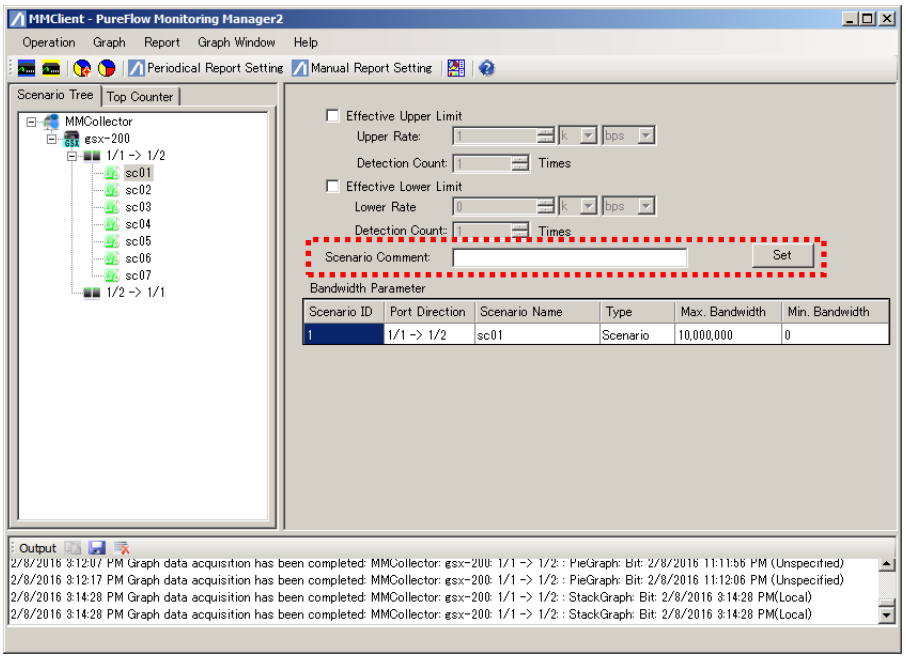


Figure 4.10.2-2 Console display of notification issued when the rate exceeds or falls below the threshold value

If the threshold setting is enabled and an over- or under-threshold event is detected, the detection result is reported.

4.10.3 Setting scenario comments

When a scenario is selected on the scenario tree, the scenario comment setting field is displayed. This field is not displayed when a port is selected.



4.10.3-1 Setting a scenario comment

Scenario comment text box

Enter the scenario comment.

One-byte alphanumeric and two-byte characters can be used.

The symbols ", ¥' cannot be used for the scenario comment.

Up to 255 characters can be registered.

If the scenario comment is left blank, any scenario comment already registered for that scenario is deleted.

The same scenario comment as an existing comment cannot be set.

The scenario comment is set by using the same setting button as the one used to set threshold value detection. Enter the scenario comment after specifying the settings for threshold event notification and then click the **Set** button to apply both settings at the same time.

4.10.4 Displaying the bandwidth settings

When a port or scenario is selected on the scenario tree, the current bandwidth settings specified for the selected port or scenario are displayed.

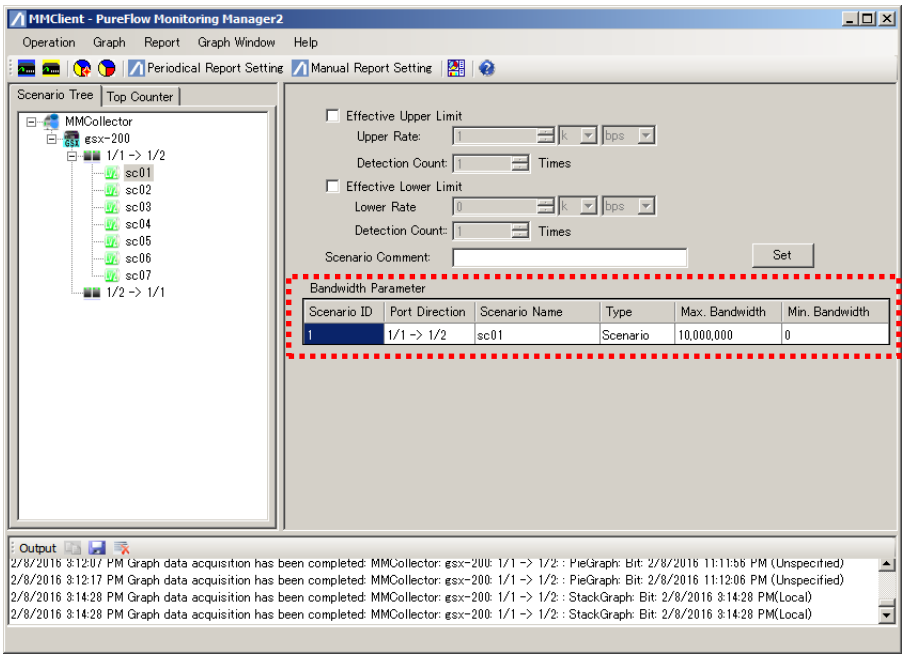


Figure 4.10.4-1 Bandwidth settings

Bandwidth settings

- Scenario ID

  (port) is displayed for the ports.

- Port Direction

  Displays the direction of the port to which the scenario belongs.

  For PureFlow WSX (TCP acceleration) or WS1, the Network port corresponding to the port scenario to which the scenario belongs is displayed. 1/1 is displayed for /port1, 1/2 for /port2, 1/3 for /port3, and 1/4 for /port4.

- Scenario Name

  Scenario name (up to 43 characters)

  or Scenario comment (up to 256 characters) is displayed. If the scenario comment is set, it is displayed.

- Type

  The scenario type is displayed. (port) is displayed for the ports.

  Table 4.10.4-1 shows the correspondence between the display and scenario types.

- Maximum (Max.) Bandwidth and Minimum (Min.) Bandwidth

  When scenario is selected, displays the maximum and minimum bandwidth of the scenario. If the maximum traffic of the scenario is not set, the maximum bandwidth is displayed with 0.

  When port is selected, minimum bandwidth is displayed with 0 and maximum bandwidth is displayed with below.

  - PureFlow GS1-F/FB : 100,000,000 (Fixed)
  - PureFlow GS1-G/GB/GR/GBR : 1,000,000,000 (Fixed)
  - PureFlow GSX : Maximum bandwidth value of level 1 scenario
  - PureFlow WSX/WS1 : 0 (Fixed)

Table 4.10.4-1 Scenario setting type and corresponding display

Display	WSX (TCP acceleration) and WS1	GSX and WSX (Traffic shaping)	GS1
Aggregate	aggregate scenario		
Individual	individual scenario		
Discard	discard scenario		-
Wan Accel	wan-accel scenario	-	-
Application	-	-	application scenario
Virtual Pipe	-	-	vpipe scenario
Aggregate (outbound)	aggregate scenario (in outbound tree mode)	-	-
Individual (outbound)	individual scenario (in outbound tree mode)	-	-
Discard (outbound)	discard scenario (in outbound tree mode)	-	-
Wan Accel (outbound)	wan-accel scenario (in outbound tree mode)	-	-

-: There are no settings of corresponding scenarios.

4.10.5 Displaying acceleration scenario setting information

When selecting the acceleration scenario from the scenario tree window, the acceleration scenario setting is displayed.

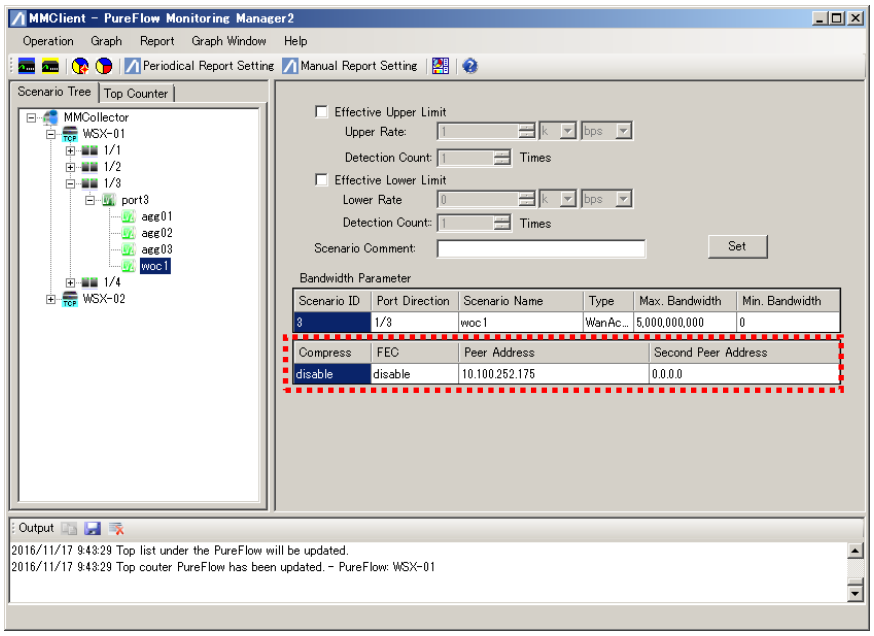


Figure 4.10.5-1 Traffic setting information

Acceleration scenario setting information

- Compression (enable, disable)
  Displays enabling (enable) or disabling (disable) of the compression function for the wan-accel scenario.
- FEC (enable, disable)
  Displays enabling (enable) or disabling (disable) of the FEC function for the wan-accel scenario.
- Peer address, Second Peer address
  Displays the Primary IP address and Secondary IP address of the wan-accel scenario.

4.10.6 Notes concerning scenario names

1. Scenario names are displayed in the scenario tree with scenarios for which comments have been entered displayed first.
2. If a scenario name in any layer of PureFlow node is more than 43 characters long, the name is cut off at the 43th character when managed in MonitoringManager2. If a scenario with a name of over 43 characters is specified, the scenario might not be able to be displayed on a graph or output in a report.
3. If a scenario for which a name has not been specified in PureFlow GS1 is specified in the hierarchy, the scenario ID is used as the scenario name when the scenario is managed in MonitoringManager2.
4. If scenarios with the same name are specified in the same layer of MonitoringManager2, the scenarios might not be able to be displayed on a graph or output in a report. Do not duplicate scenario names when specifying names in PureFlow node.
   Note, however, that scenarios with the same name can be handled as different scenarios by specifying a different scenario comment.

4.11 Sorting the graph windows

When multiple graphs have been created, the graph to display can be selected from a list of graph windows. The graph windows can also be sorted by selecting **Sort windows**.

To display a graph from a list of windows, click **Graph window** then **Window list** on the menu bar, and select the graph to display.

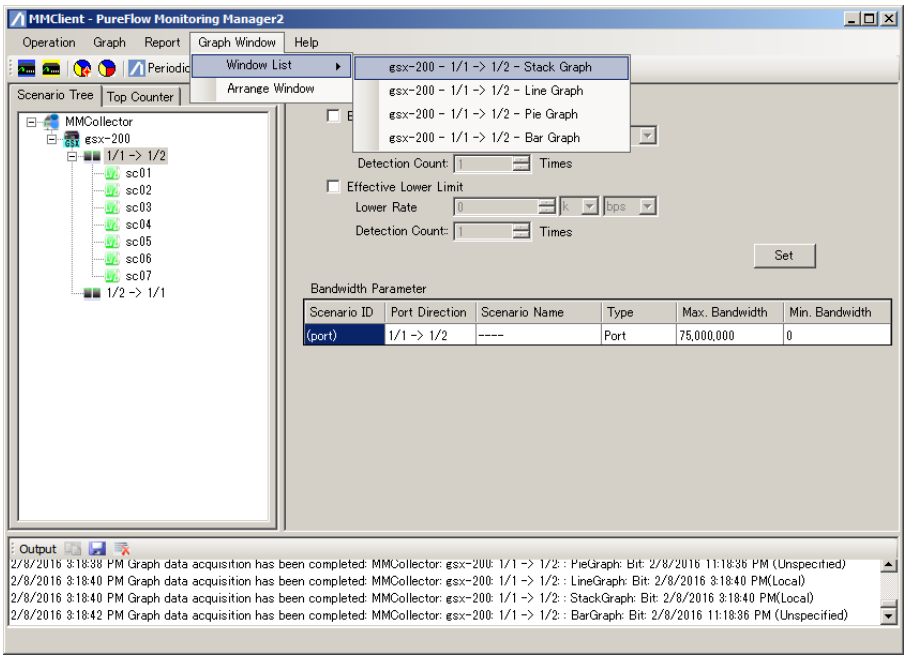


Figure 4.11-1 Displaying a graph from a list of graph windows

To sort the graph windows, click **Graph window** then **Sort windows** on the menu bar.

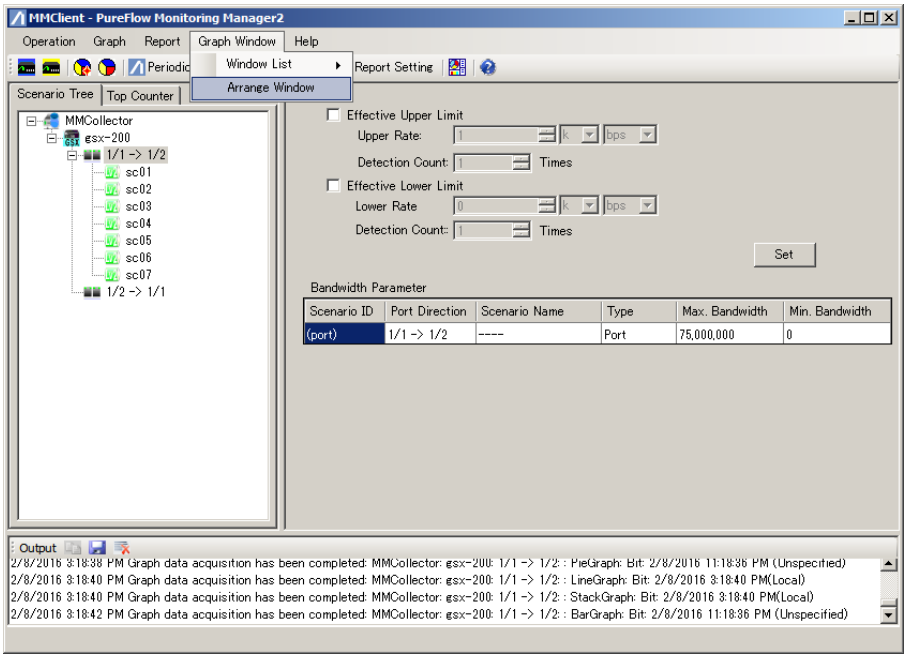


Figure 4.11-2 Sort windows menu item

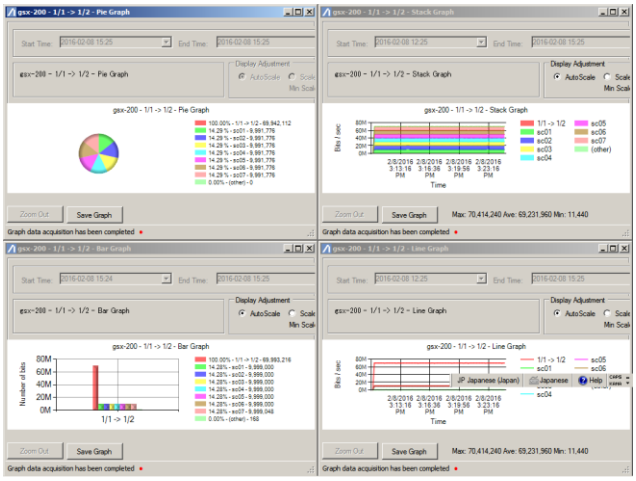


Figure 4.11-3 Window on which graph windows are sorted

4.12 Help

4.12.1 Displaying an overview of the software and its operation method

You can view an overview of MonitoringManager2 and its operation method by using the Help feature.

Select **Help** then **Help PDF link** on the menu bar.

Note:

The Help feature cannot be displayed if the Help PDF file and PDF viewer is not installed. See 2.4 Installing the MonitoringManager2 instruction manual for how to install the Help PDF file.

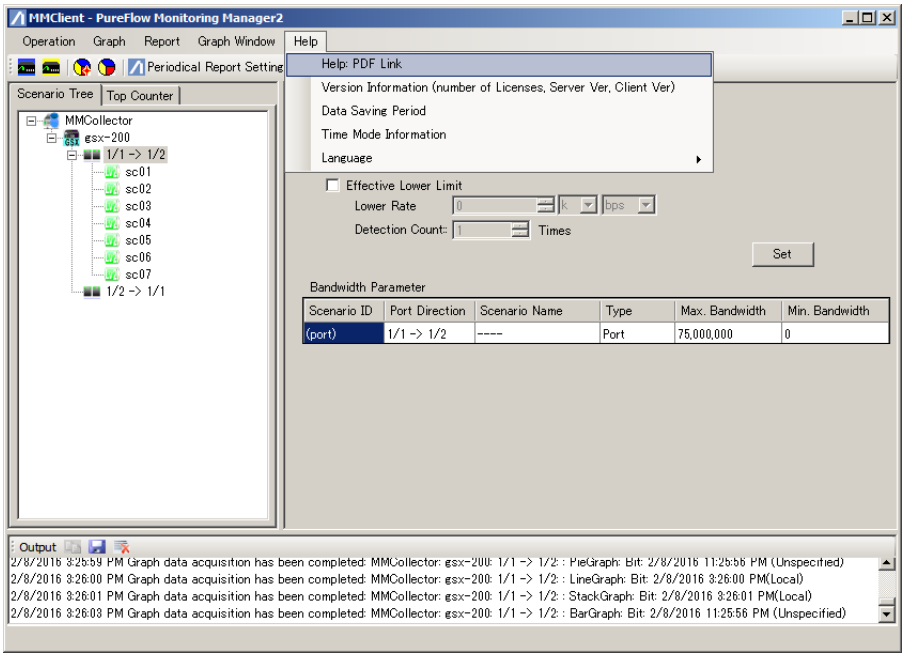


Figure 4.12.1-1 Help (selected from the menu bar)

To check the software version information, select **Help** then **Version information (number of licenses, server version, client version)** on the menu bar. The license information indicates the maximum number of PureFlow node units that can be registered by using the basic license and additional licenses installed together with MonitoringManager2.

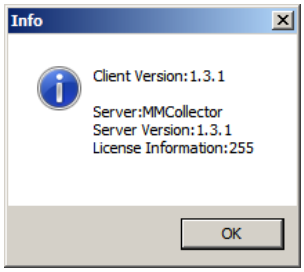


Figure 4.12.1-2 Checking the version information (number of licenses, server version, client version) from the Help menu

To check the data storage period, select **Help** then **Check data storage period** on the menu bar.

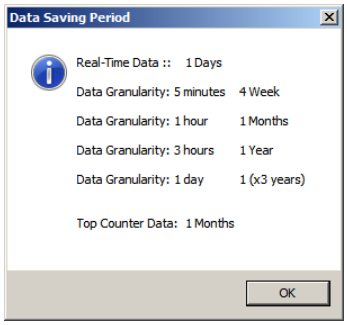


Figure 4.12.1-3 Checking the data storage period from the Help menu

4.12.2 Selecting the language

You can select the language to be used for the MonitoringManager2 GUI.

Select **Help**, **Language**, then **Japanese** or **English**.

The language used for the MonitoringManager2 GUI is switched as soon as this setting is made.

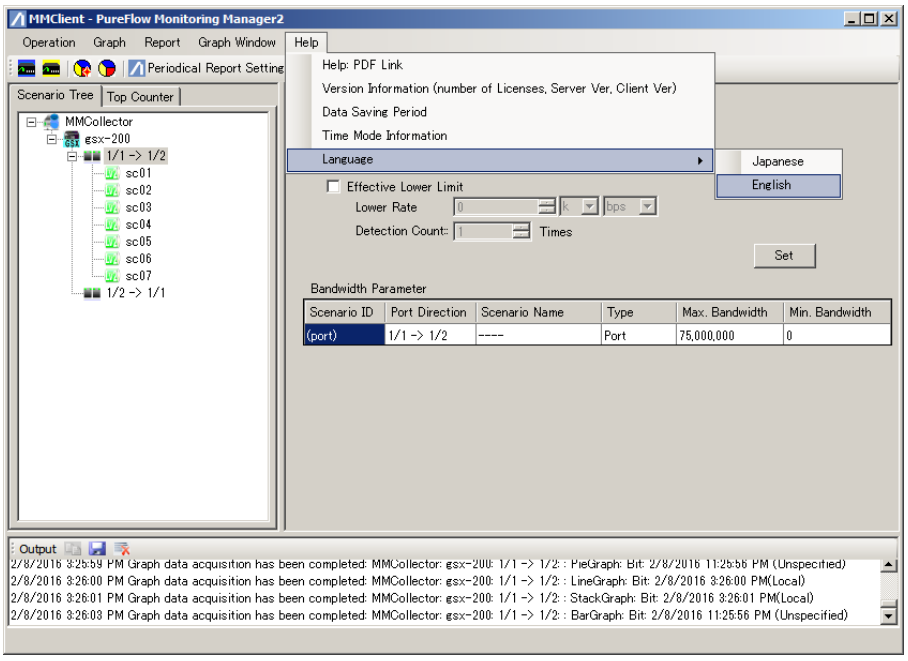


Figure 4.12.2-1 Selecting the language

4.13 Exiting the client software

To exit the client software, select **Operation** then **Exit** on the menu bar or click the Close (×) button on the active title bar.

4.14 Cautions

4.14.1 Monitor information

If there are a lot of scenarios whose traffic is to be monitored and monitoring information notifications are received by MonitoringManager2 at short intervals, MonitoringManager2 might not be able to process the received notifications due to an overload of server processing capacity. Specify as long a monitor information notification interval as possible in accordance with the total number of scenarios in all nodes. The monitor information notification interval can be set in a range from 10 seconds to 1 minute.

The total number of scenarios and the length of the notification interval vary depending on the system performance. Use the following value as a rough guide:

$$\frac{\text{Total numbers of scenario}}{\text{Notification cycle (seconds)}} < 1000$$

For example, if 300 scenarios are registered in each of 100 nodes whose traffic is to be monitored, set the monitor information notification interval to 30 seconds or more.

Set the number of scenarios in each node of PureFlow GS1 whose traffic is to be monitored by using MonitoringManager2 to 2,048 or lower. For PureFlow GSX, WSX, and WS1, see Table 1.3-1 A guide to the number of scenarios that can be managed. If the number of scenarios exceeds the limit and a node to which these scenarios are registered is connected, MonitoringManager2 might not operate correctly.

4.14.2 Top information

If there are a lot of top counters whose information is to be collected and top information notifications are received by MonitoringManager2 at short intervals, MonitoringManager2 might not be able to process the received notifications due to an overload of server processing capacity. Specify as long a top information notification interval as possible in accordance with the total number of top counters whose information is to be collected in all nodes. The top information notification interval can be set in a range from 10 seconds to 1,440 minutes (one day).

The following condition for the total number of top counters whose information is to be collected in all the nodes to be monitored by MonitoringManager2 must be satisfied:

Number of nodes × Number of top counters whose information is to be collected < 1000

The total number of top counters whose information is to be collected and the length of the notification interval vary depending on the system performance. Use the value below as a rough guide. This expression is based on the recommended operating environment.

$$\frac{\text{Total number of top counter measurement target in all nodes}}{\text{Notification cycle (seconds)}} < 1000$$

For example, if 32 top counters whose information is to be collected are registered in each of 30 nodes whose traffic is to be monitored, set the top information notification interval to 10 minutes or more. If the notification interval is not available as one of the setting items, select a value larger than the calculated value. In case above, a value larger than 10 minutes should be selected for the top information notification interval.

4.14.3 Port numbers used in MonitoringManager2

The following communication port numbers are used in MonitoringManager2. When MonitoringManager2 is used in an environment in which a firewall is used, permit communication with the following port numbers as required:

Port number used for communication between MonitoringManager2 server software and PureFlow: 51967

Port number used for communication between MonitoringManager2 server software and client software: 8002

(Blank page)

This chapter describes the report feature, which is used to create traffic reports.

5.1 Overview

The report feature is used to create traffic reports based on the statistics collected from PureFlow node. The report feature is used to create two kinds of reports: periodic reports, in which report data is created periodically and automatically at a specific interval, and manual reports, in which traffic reports for a specific period are created on demand.

- Periodic reports
  You can specify the report creation interval to create traffic reports periodically. Periodic reports are created automatically and periodically by MonitoringManager2.
- Manual reports
  You can specify a target period to create traffic reports on demand. Manual reports are created by executing the **Create Manual Report** command from the client software.

Periodic and manual reports are created in the following two formats: Graphical images showing changes in traffic are saved in HTML format. Numerical data showing changes in traffic is saved in CSV format. To check traffic changes on a graph, create a report in HTML format. To analyze traffic changes by using commercially-available spreadsheet software or graph drawing software, create a report in CSV format.

- HTML-format reports
  HTML-format reports are traffic reports that including multiple graphical images showing changes in the monitor and top information against time saved in HTML format. This report contains graphical images of the monitor and top information. By using an HTML-format report, you can view the traffic data on a web browser.
- CSV-format report
  There are two types of CSV-format reports: a CSV-format report containing the monitor information and a CSV-format report containing the top information. Numeric data that indicates the traffic flow for each port or scenario is saved in the CSV-format report containing the monitor information. The network usage listed in descending order of traffic flow volume for the top 25 users is saved for each top information collection interval in the CSV-format report containing the top information. By using these CSV-format reports, you can analyze traffic information by using commercially-available spreadsheet software or graph drawing software.

Notes:

1. If the free space of the report output destination disk is 1 GB or less, the report is not output. If the disk free space is too small during report output, the report output process is canceled.
   The log is recorded only if there is enough space to record the log when report output is canceled.

2. In HTML-format transmission counter reports, the counter information of the selected scenario and the counter information of the scenarios under the selected scenario are combined and displayed on the graph. Up to 255 scenarios under the selected scenario can be combined and displayed at the same time.

3. If an error occurs during report creation, the OS event viewer shows a message. For the displayed message, see "Appendix F Event Viewer Message List".

5.2 Periodic reports

Periodic traffic reports start being created as soon as the periodic report setting is registered. To create a periodic report, execute the **Create Periodic Report** command from the client software. To stop the periodic report creation, execute **Delete Periodic Report Setting**.

Multiple periodic reports can be registered. For example, you can create a periodic report for each PureFlow node.

The maximum number of periodic report that can be registered is 250.

If a periodic report is specified that includes the same starting time (report creation time) as other reports and a specifies the output of a large number of HTML-format and CSV-format reports, the report might not be able to be created within the specified interval or the creation of the report might affect data collection from PureFlow. It is therefore important to adjust periodic report settings to ensure the smooth operation of the system, such as by specifying different starting times or reducing the number of reports to be output.

Since the number of periodic report settings that can be duplicated depends on the server performance, be sure to output the report once and use a performance monitor or resource monitor to check the load on the CPU or hard disk drive during the output process.

5.2.1 Creating a periodic report

Select **Report** then **Create Periodic Report** from the menu bar. Or, click the **Periodic report setting** icon from the icon bar. The **periodic report list** pane appears.

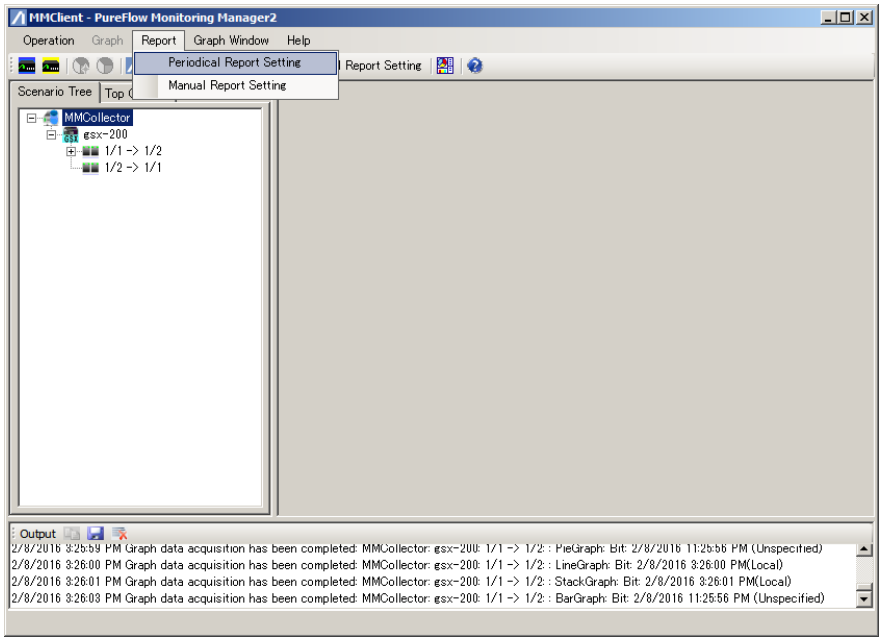


Figure 5.2.1-1 Creating a periodic report by using the menu bar

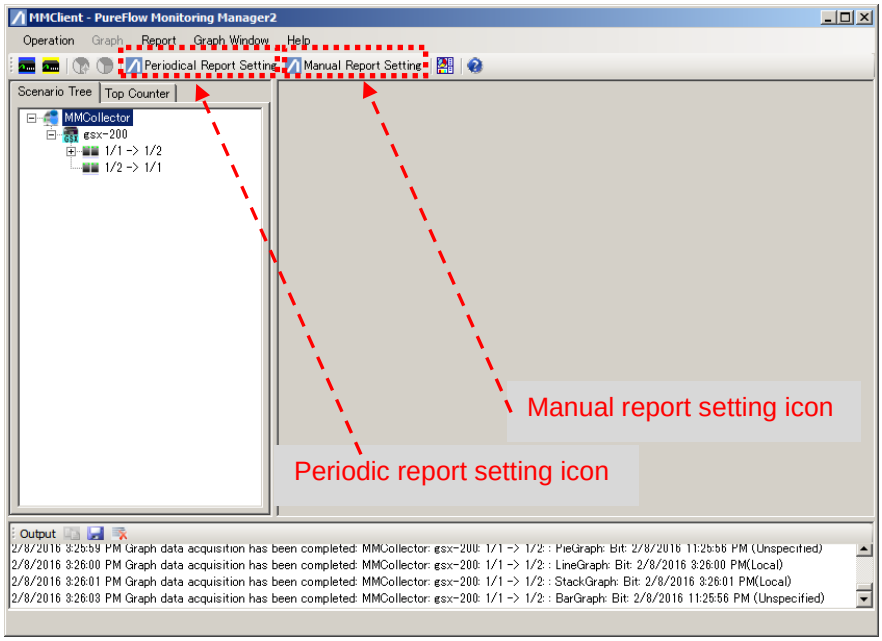


Figure 5.2.1-2 Creating a report by using the report creation icons

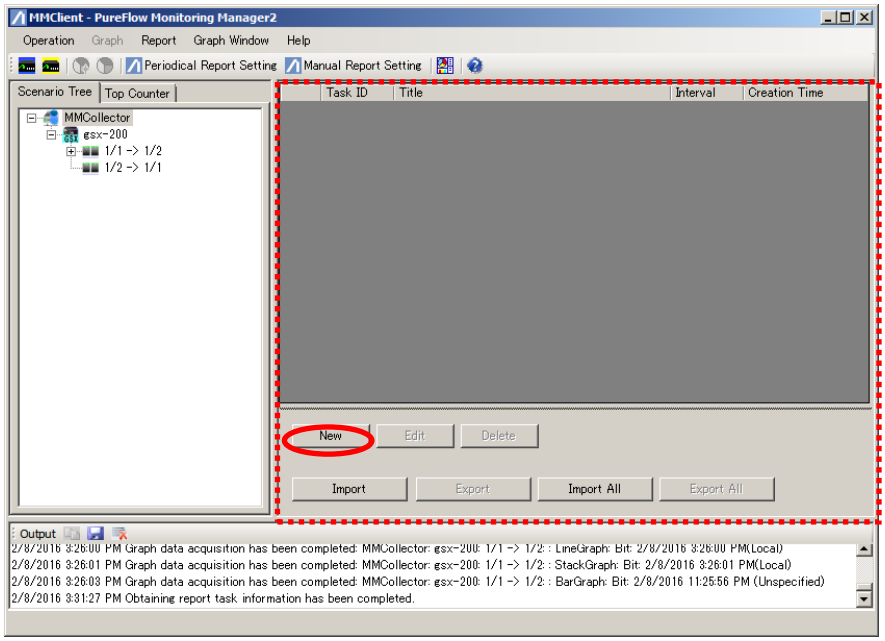


Figure 5.2.1-3 Periodic report list pane

Click the **New** button on the periodic report list pane. The **Create Periodic Report** dialog box appears.

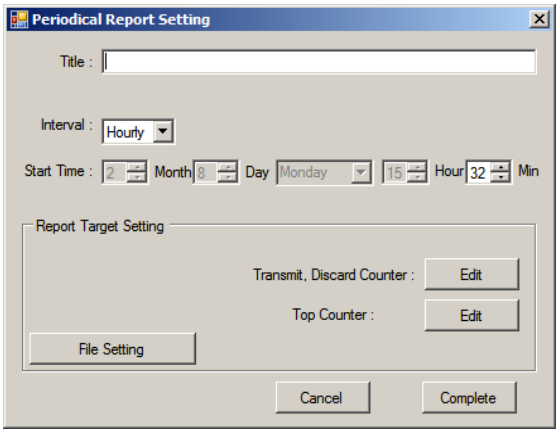


Figure 5.2.1-4 Create Periodic Report dialog box

Title

Enter the title of the periodic report.

One-byte alphanumeric and two-byte characters can be used.

The symbols “"<>|:;*?\/0[]{},$&' ([{〔〈《「『【 〝‘“ ,)]}, 〕〉》」』】’”〟 ” cannot be used.

Up to 255 characters can be registered.

Interval

Specify the interval at which a periodic report will be created.

Select from **Hourly**, **Daily**, **Weekly**, **Monthly**, and **Yearly**.

Starting time

The items to be set as the starting time vary depending on the specified interval.

Setting of report target

Specify the type of periodic report to create.

Transmission and discard counters

Top counter

Click the **Edit** button. The **Report target setting pane** appears.

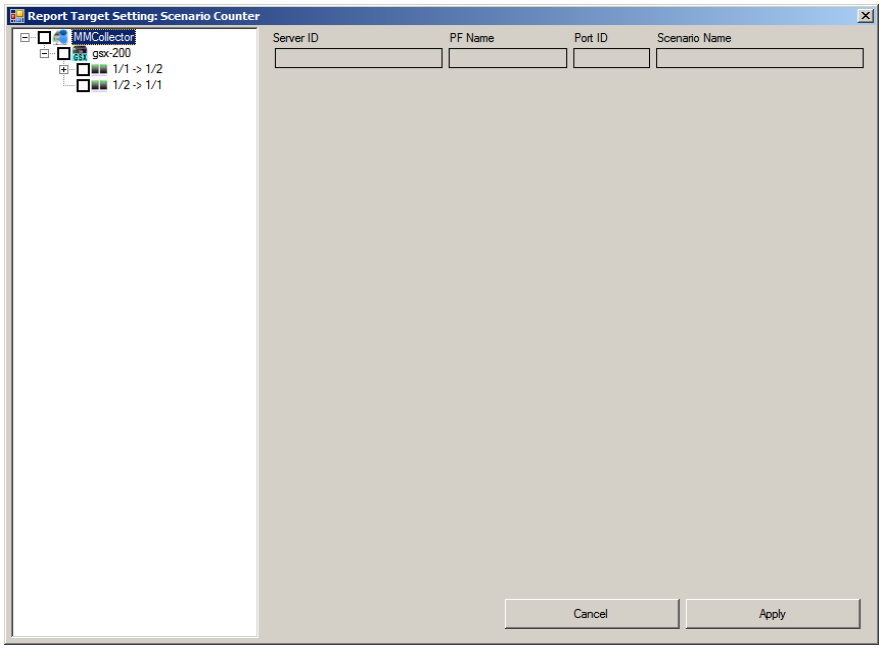


Figure 5.2.1-5 Report target setting pane

The registered nodes, ports and scenarios appear as a tree. The multiple ports or scenarios can be selected. Select the check box of the port or scenario for which the periodic report is to be created.

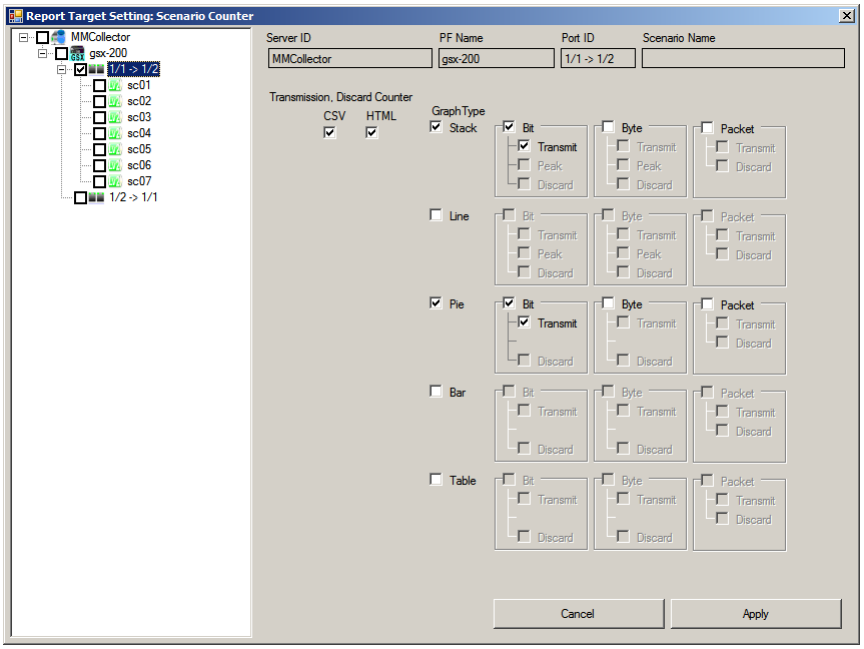


Figure 5.2.1-6 Selecting the report output format

Select the display format from **CSV**, **HTML** or both. If you select the HTML format, select the graph type, display unit, and counter information.

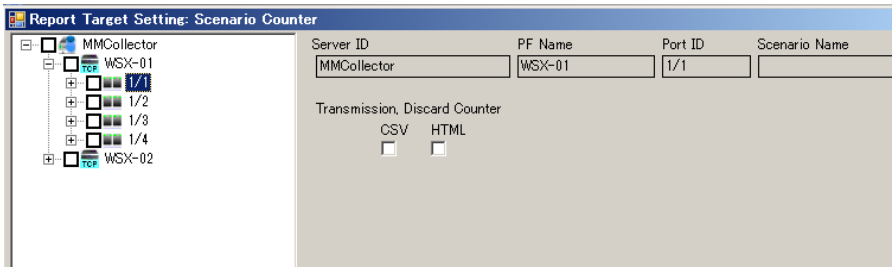


Figure 5.2.1-7 Selecting the report output format of the Network port

When selecting HTML format for an HTML report of the Network port, all the types of reports that can be output for the Network port are output.

Set the above items, and then click the **Apply** button. Cancel the report output format settings by clicking the **Cancel** button.

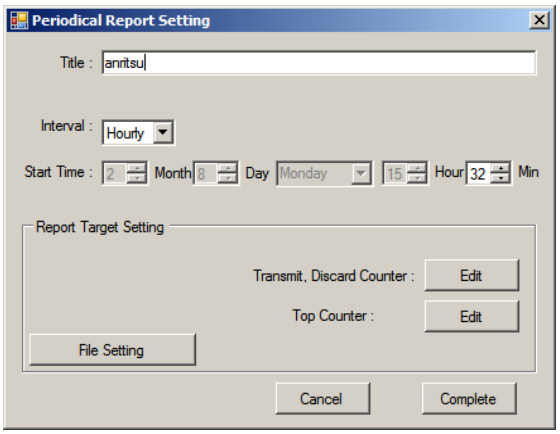


Figure 5.2.1-8 Create Periodic Report dialog box

Create a periodic report at the specified interval by clicking the **Complete** button. Cancel the periodic report settings by clicking the **Cancel** button.

For how to view the report data, see 5.2.7 Viewing periodic report data.

Notes:

1. If the periodic report output time is set to the same time as another report, multiple reports are loaded and written to the disk at the same time, which might exceed the server processing capacity. Stagger the periodic report output times in 1 hour intervals.

2. When the time zone is set to Local, the displayed time in the report may differ from the actual local time depending on the time zone of the area. For details, see Chapter 8.

3. If you want to specify the report creation period and report target period separately, change the execution time in the periodic report settings by using the Windows task scheduler. The execution time can only be changed to a value that is within the periodic report interval. For example, for an hourly report, the execution time must be within one hour, and for a daily report, it must be within one day. Note that if the execution time is changed again by using MM2Client after being changed by using the task scheduler, the time specified by using the task scheduler is overwritten. In this case, change the time again by using the task scheduler.

   Example: Daily report

   - Report creation time: 02:00 everyday
   - Report target period: 00:00 to 00:00 the next day

   [Procedure]

   1. Register the execution time as “00:00 everyday” in the periodic report settings on MM2Cient.
   2. Change the task execution time specified for reporting to “02:00 everyday” by using the task scheduler.

   If the task execution time is within five minutes of the end of the report target period, the task will actually be executed five minutes later to ensure that the previous data collection is complete.

4. Periodic report is started to create after 5 minutes from the time set.

5. Avoid exceeding 100 bytes as a guide when setting the report title. If the report title is lengthy and if the report cannot be created due to the Windows OS restrictions that stipulate that the name of a temporarily created or finally output file cannot exceed 255 bytes including the path name and file name, the report task may not be imported and exported.

5.2.2 Configuration file menu

Import or export the report target by clicking the **Configuration File Menu** button in the **Create Periodic Report** dialog box.

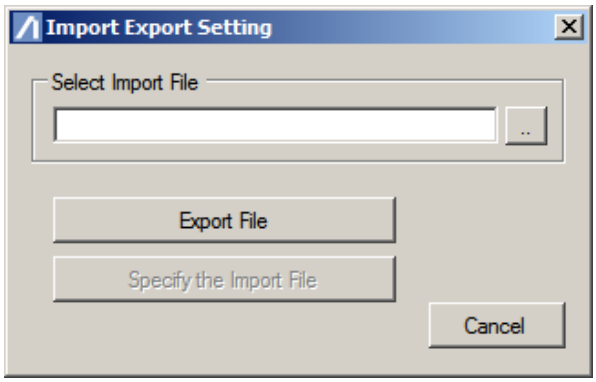


Figure 5.2.2-1 Import/Export Target Settings dialog box

You can import a target configuration file (CSV format) exported and saved by using this system.

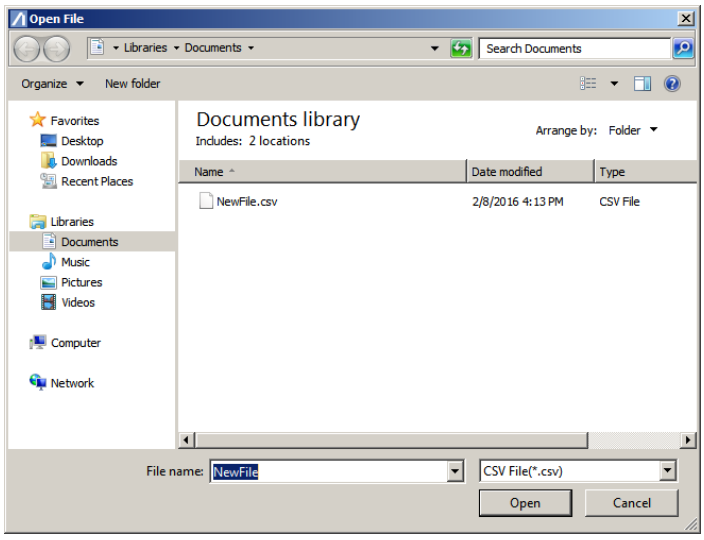


Figure 5.2.2-2 Import file selection dialog box

The file to be imported can be selected by clicking the browse button (…) in the **Import target configuration file** field.
The **Specify and Import File** button becomes available when a file is selected. The report target information can be read from the specified file by clicking this button.

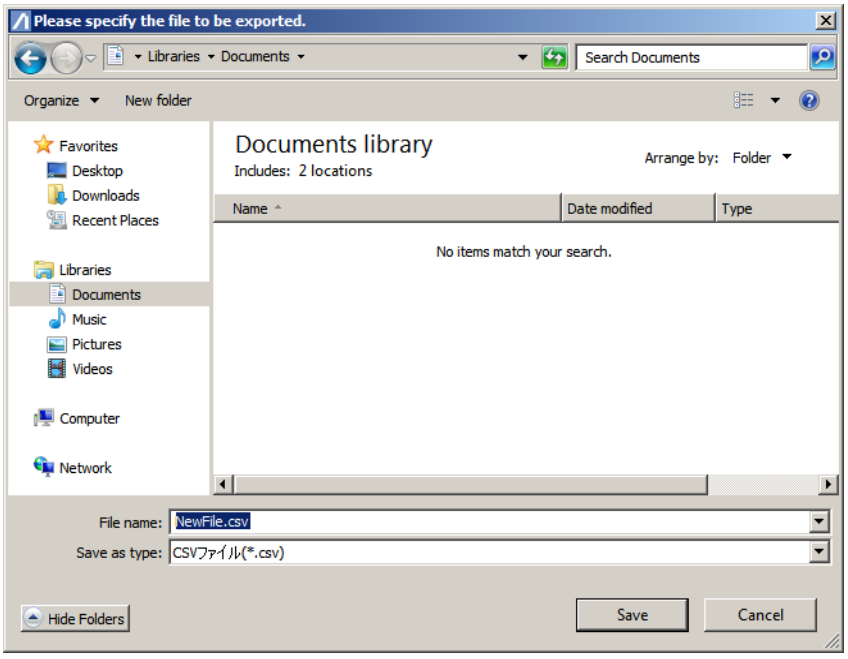


Figure 5.2.2-3 Export file selection dialog box

The file selection dialog box is displayed by clicking the **Export Target Configuration File** button.
The report target information is saved in the specified file by clicking the **Save** button.

Notes:

1. If the check boxes of the target settings of the selected report are not selected at all, all the ports and scenarios are output to the target configuration file. If the check boxes of the target settings are selected, the checked ports and scenarios are output to the target configuration file.

2. When saving the target setting file, determine the saving folder and file name so that the number of characters including the folder path and file name does not exceed 255 bytes. Otherwise, the information may not be obtained because Windows OS restrictions stipulate that the characters of the names of the paths and files cannot exceed 255 bytes.

5.2.3 Setting the report target

The tree on the report target setting pane can be edited and the output settings of the ports and scenarios applied to other ports and scenarios.

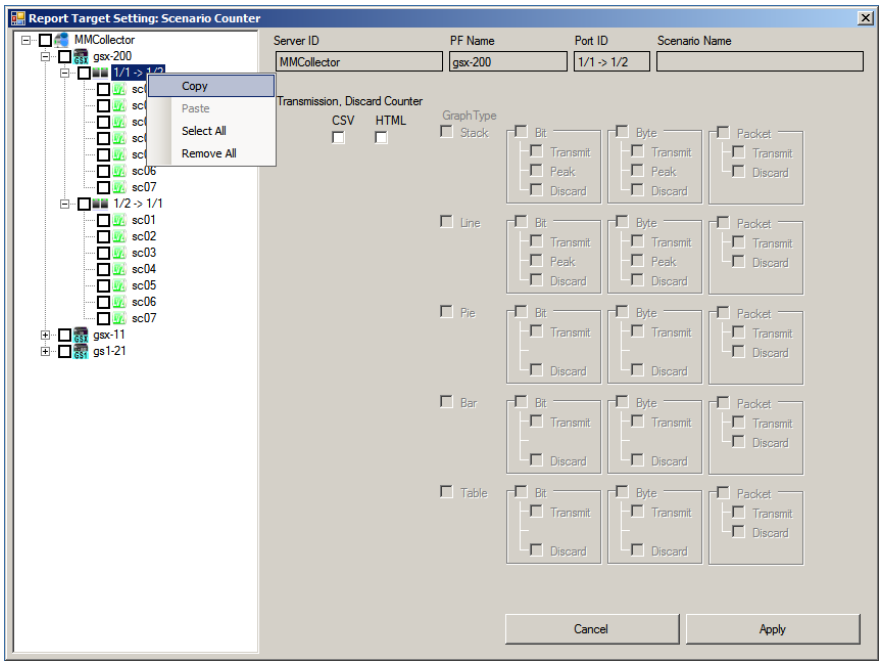


Figure 5.2.3-1 Report target setting pane (copy/paste)

The output information of the transmission and discard counters can be stored in the memory by right-clicking the scenario tree of the selected port or scenario and selecting **Copy**.
The output information of the transmission and discard counters of the copy source can be set by right-clicking the port or scenario of the copy destination and selecting **Paste**.

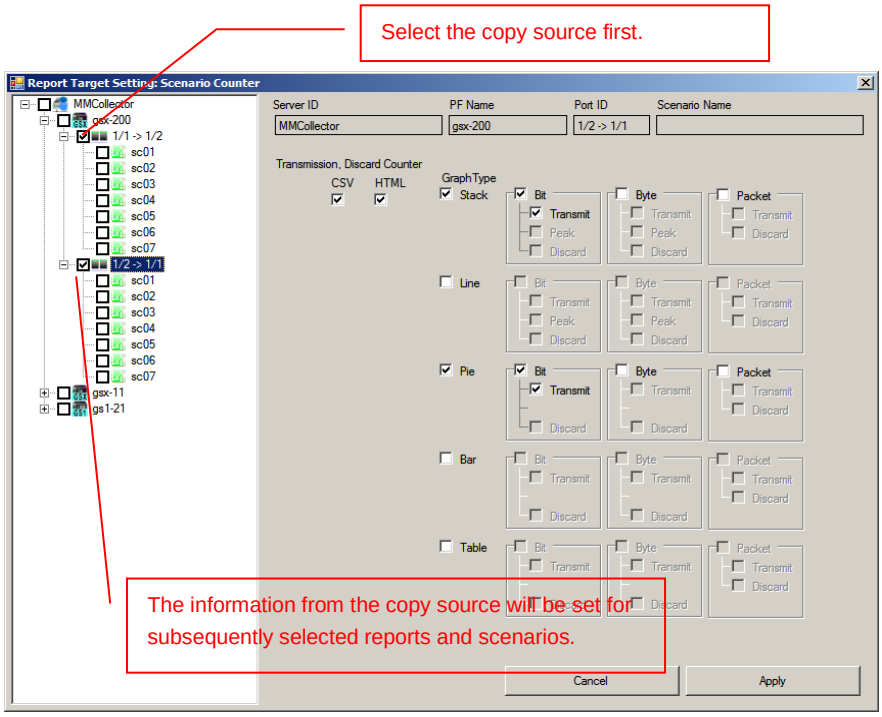


Figure 5.2.3-2 Report target setting pane (copying by selecting check boxes)

Select the check box on the left side of a port or scenario on the tree to allow copy-and-paste in the same way as the right-click operation described above.
The output information of the transmission and discard counters of the port or scenario whose check box was selected first is set by selecting the check box of the port or scenario of the copy source.

Note that the settings of the middle-layer ports and scenarios cannot be copied to the lowest-layer port and scenario by using the check box function.

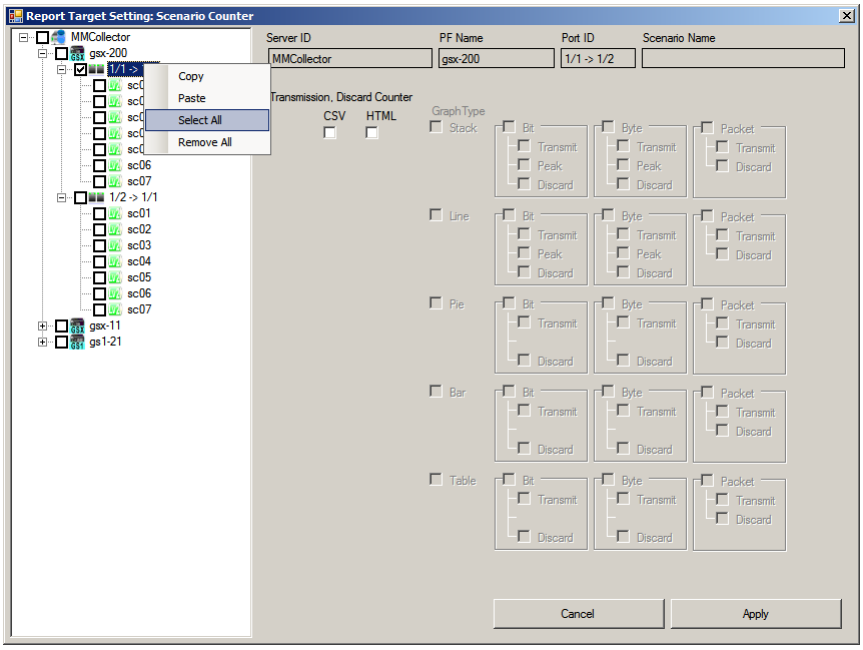


Figure 5.2.3-3 Report target setting pane (Select All and Clear All menu items)

The check boxes of all the output information of the transmission and discard counters are selected by right-clicking the scenario tree of the selected port or scenario and selecting **Select All**.

Select **Clear All** to clear the check boxes of all the output information of the transmission and discard counters.

Notes:

To check all ports and scenarios, edit the exported target configuration file (CSV file) and import it again with all items selected.

1. Exporting the target configuration file
   Select Report then Create Manual Report from the menu bar and export the target configuration file. For how to export the target configuration file, see "5.2.2 Configuration file menu".

2. Target configuration file
   The items of the target configuration file are listed below.

Table 5.2.3-1 Target configuration file items

Line position	Item name	Description
1	ReportID	Report task ID
2	ServerID	Fixed in "MMCollector"
3	ReportType	Report type 0 indicates the scenario report, and 1 indicates the top counter report.
4	PFName	PureFlow ID
5	PortID	ID for the Network port of PureFlow 1 indicates the traffic direction from 1/1 to 1/2, and 2 indicates the direction from 1/2 to 1/1.
6	ScenarioID	Scenario ID
7	PureFlow name	PureFlow name
8	Port direction	Port direction
9	Scenario name	Scenario name (without hierarchy) or scenario comment
10 or later	-	0 indicates the file for which a report is not created, and 1 indicates the file for which a report is created.

3. Editing the target configuration file
   Open the target configuration file exported in step 1, select the columns of the 10th to 97th lines, and replace the 0s with 1s. To check only CSV files, select the column of the 10th line, and to check only HTML files, select the columns of the 11th to 97th lines. Replace the 0s with 1s. Do not change the values of the 1st to 9th lines. The value of the Report ID is ignored at importing.
   Note that cells in the target configuration file that contain the notation "Spare" cannot be used. The file will be imported with the Spare cells skipped.

4. Importing the target configuration file
   Import the target configuration file edited in step 3.
   For how to import the target configuration file, see "5.2.2 Configuration file menu".
   The information in the imported target configuration file can be reviewed on the report target setting pane.

5.2.4 Checking and editing periodic report settings

Select **Report** then **Create Periodic Report** from the menu bar. The periodic report list pane appears. Select the periodic report to be checked and edited. Click the **Edit** button.

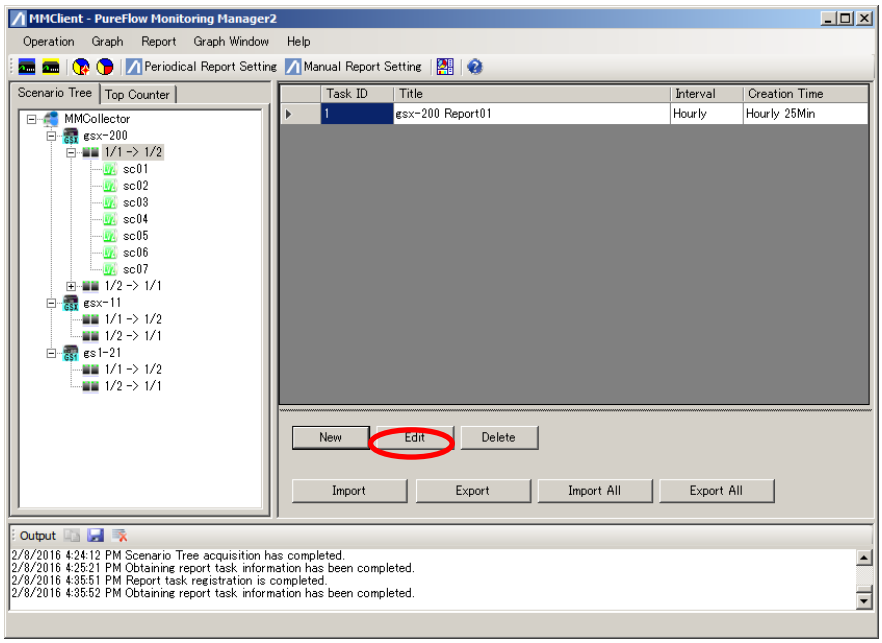


Figure 5.2.4-1 Periodic report list pane

You can check and edit registered periodic report settings. Specify settings in the same way as when creating a new report after displaying the periodic report setting pane. Click the **Complete** button to update the periodic report settings.

For how to set the report task parameters, see 5.2.1 Creating a periodic report. For how to set the report target, see 5.2.2 Configuration file menu and 5.2.3 Setting the report target.

5.2.5 Reregistering report tasks excluded from the periodic report

Some report tasks registered in the periodic report list might be grayed out. These report tasks have been excluded from periodic report management by MonitoringManager2 for some reason.

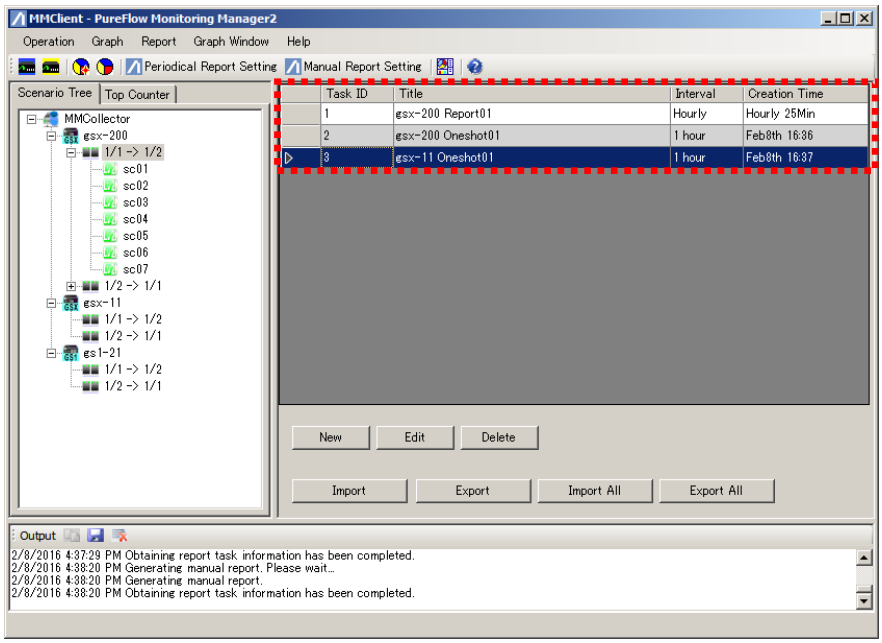


Figure 5.2.5-1 Report tasks excluded from periodic report management

The factors leading to the exclusion of the tasks from periodic report management are described below.

1. The report tasks are registered as manual reports.
2. The report tasks stopped being executed as periodic reports when MonitoringManager2 was uninstalled.
3. The task scheduler setting for periodic execution was changed or deleted.

Although the settings of the periodic reports excluded from management are saved in MonitoringManager2, the reports themselves might not be created.

Report tasks excluded from management can be registered again as periodic reports in MonitoringManager2 by performing the registration process again in the editing dialog box.

The valid periodic reports can be checked in the report list on the **MMController Service** tab of **MMAdminTool**. For how to check valid reports, see 7.5.9 Checking the connection status and report list of MMClient.

5.2.6 Deleting a periodic report

Select **Report** then **Create Periodic Report** from the menu bar. The periodic report list pane appears. Select the periodic report to be deleted. Click the **Delete** button.

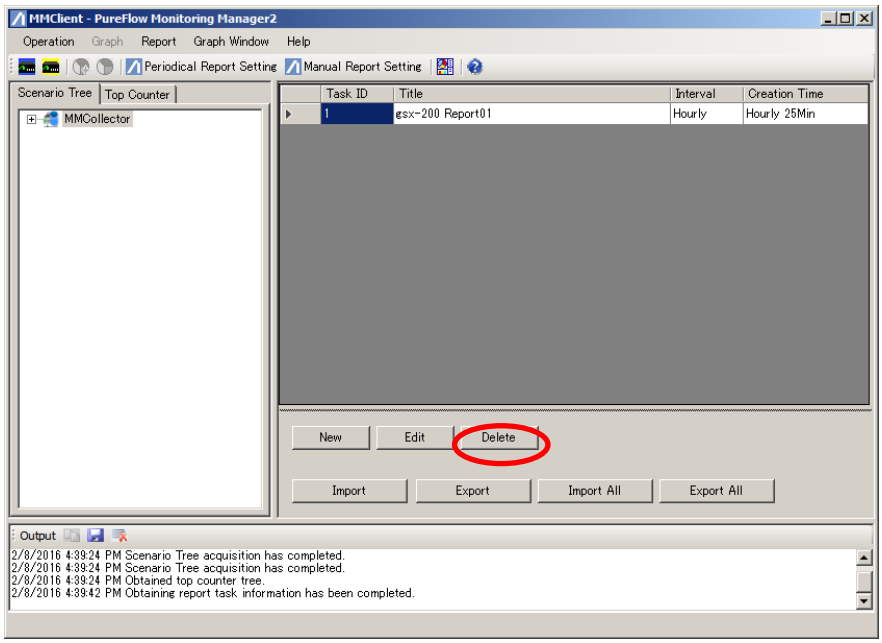


Figure 5.2.6-1 Periodic report list pane

A confirmation dialog box appears. Click **Yes**. The periodic report is deleted. If you click **No**, deletion of the periodic report is canceled.

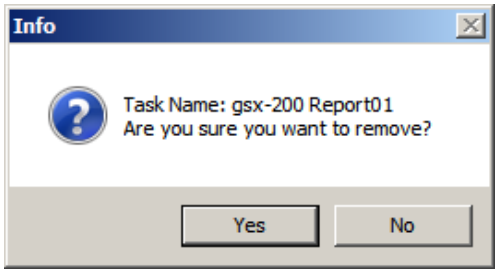


Figure 5.2.6-2 Periodic report deletion confirmation dialog box

5.2.7 Viewing periodic report data

Open the following web page file by using a web browser and select the report data that you want to view from the periodic report list. This periodic report list is automatically updated every time a periodic traffic report is created.

File path of periodic report list: `Report output folder\index.html`

Reference: The default value of `Report output folder` is `c:\reports`.

For how to check and change the report output folder, see 7.5.7 Specifying the report output folder.

5.3 Creating a manual report

When creating a manual report, you can freely select the time range for which the report is created and the graph on which the data is to be displayed.

Manual report tasks are registered as tasks excluded from periodic report management in the periodic report list. Tasks that are excluded from management can be executed as periodic report tasks again by reregistering them. For how to reregister report tasks, see 5.2.5 Reregistering report tasks excluded from the periodic report.

5.3.1 Creating a manual report

Create a manual report by using the following procedure:

Select **Report** then **Create Manual Report** from the menu bar. The **Create Manual Report** dialog box appears.

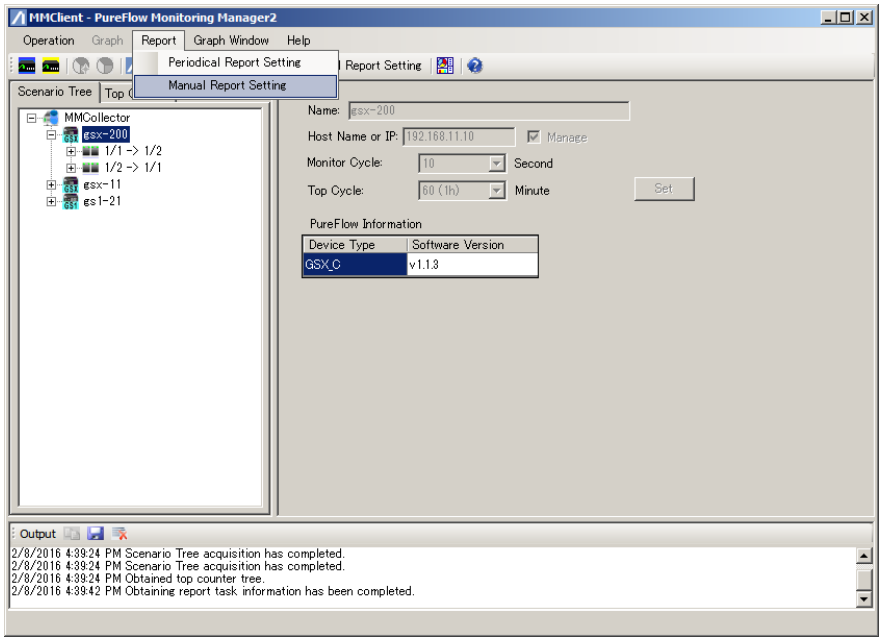


Figure 5.3.1-1 Creating a manual report by using the menu bar

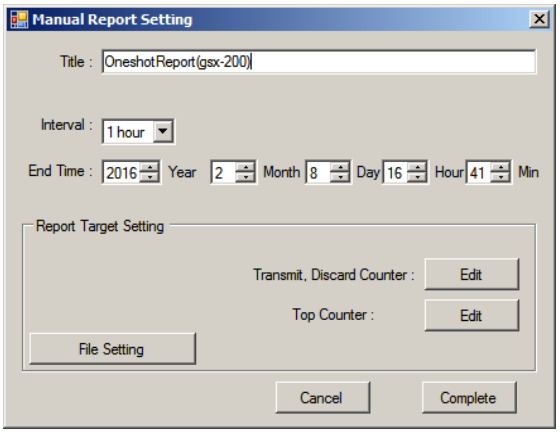


Figure 5.3.1-2 Create Manual Report dialog box

Title

Enter the title of the manual report.

One-byte alphanumeric and two-byte characters can be used.

The symbols “"<>|:;*?\/0[]{},$&' ([{〔〈《「『【 〝‘“ ,)]}, 〕〉》」』】’”〟 ” cannot be used.

Up to 255 characters can be registered.

Interval

Specify the period for which the manual report is to be created.

Select from **10 minutes**, **1 hour**, **1 day**, **1 week**, **1 month**, and **1 year**.

Ending time

Specify the ending time of the manual report in minute units. Specify a time before the current time.

A manual report is output for the time range indicated by the above period and ending time.

Setting of report target

Same as the periodic report.

Click the **Edit** button. The dialog box for selecting the target of the manual report appears in the same way as for a periodic report. Select the report output items, and then click the **Close** button.
Set the above items and click the **Complete** button. The manual report is created.

Notes:

1. When the time zone is set to Local, the displayed time in the report may differ from the actual local time depending on the time zone of the area. For details, see Chapter 8.

2. Manual report is started to create after 5 minutes from the time set.

5.3.2 Viewing manual report data

Open the following web page file by using a web browser and select the report data that you want to view from the manual report list. This manual report list is automatically updated every time a manual traffic report is created.

File path of manual report list: `Report output folder\oneshot\index.html`

Reference: The default value of `Report output folder` is `c:\reports`.

For how to check and change the report output folder, see 7.5.7 Specifying the report output folder.

5.4 Exporting and importing report settings

You can export (back up) and import (restore) report settings.

5.4.1 Exporting report settings

Select **Report** then **Create Periodic Report** from the menu bar. The periodic report list pane appears.

To back up a specific report, click the **Export** button.

To back up all the reports, click the **Export All** button.

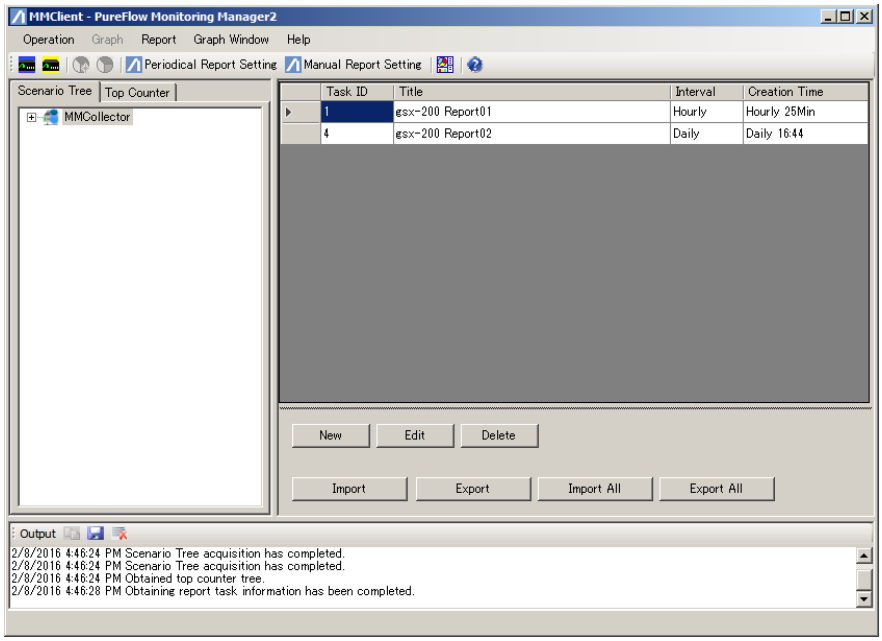


Figure 5.4.1-1 Periodic report list pane

A dialog box to specify the file to be exported appears.

Specify the directory and the name of the file in which the exported settings are to be saved.

Select ZIP (`*.zip`) for the file type.

Click **Save** to create the file.

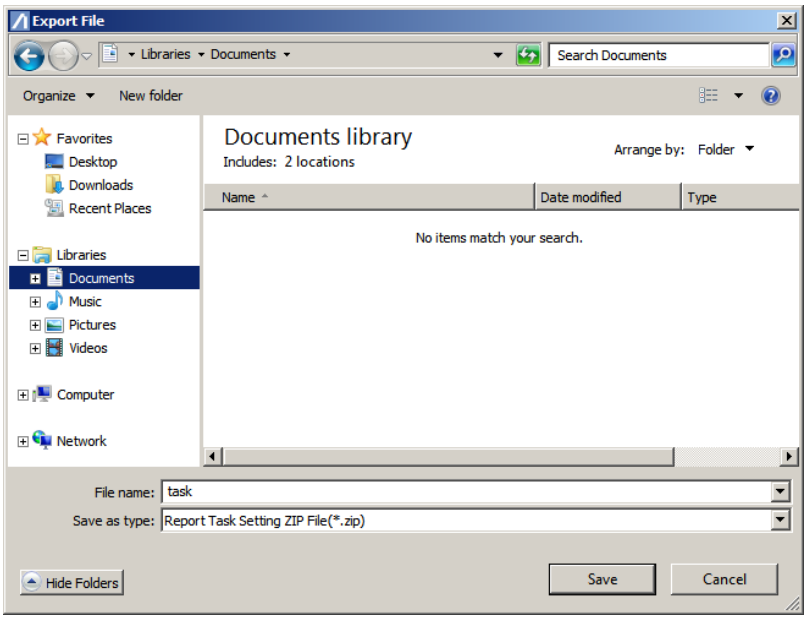


Figure 5.4.1-2 Dialog box for saving the file to be exported

Notes:

1. The purpose of exporting/importing report settings is to back up or restore the file. Do not edit the file saved in the exported ZIP file. If edit the exported ZIP file, export will be failed.

2. When saving the file, determine the saving folder and file name so that the number of characters including the folder path and file name does not exceed 255 bytes. Otherwise, the information may not be obtained because Windows OS restrictions stipulate that the characters of the names of the paths and files cannot exceed 255 bytes.

5.4.2 Importing report settings

Select **Report** then **Create Periodic Report** from the menu bar. The periodic report list pane appears.

To restore a specific report, click the **Import** button.

To restore all the reports, click the **Import All** button.

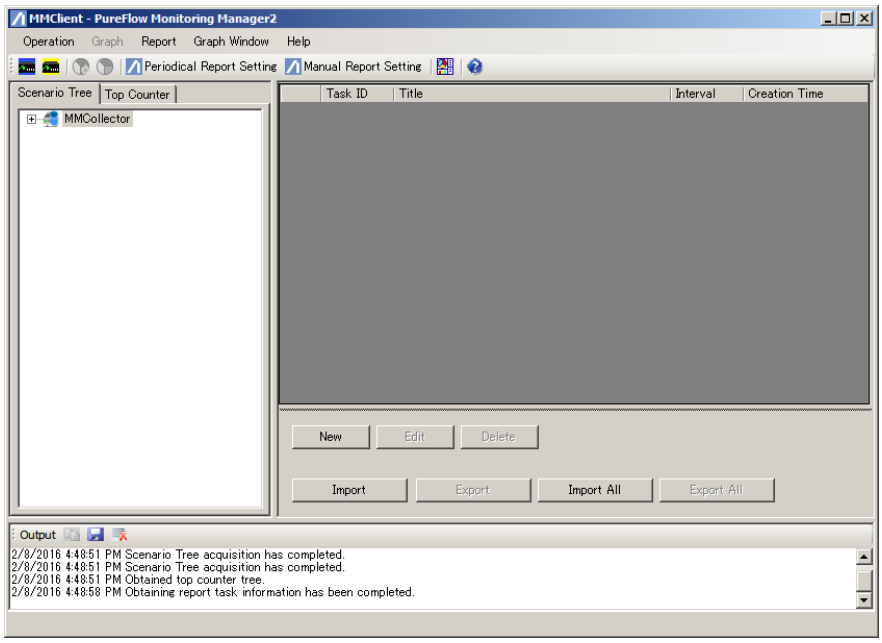


Figure 5.4.2-1 Periodic report list pane

If you click the **Import All** button, a dialog box to confirm whether you want to delete all the existing reports appears.

To delete all the existing reports, click **Yes**.

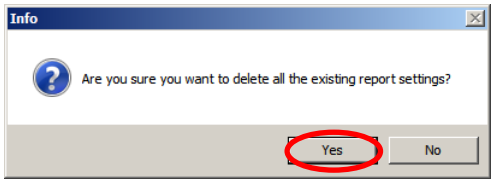


Figure 5.4.2-2 Confirmation dialog box

A dialog box to specify the file to be imported appears.

Select the file to be imported, and then click the **Open** button.

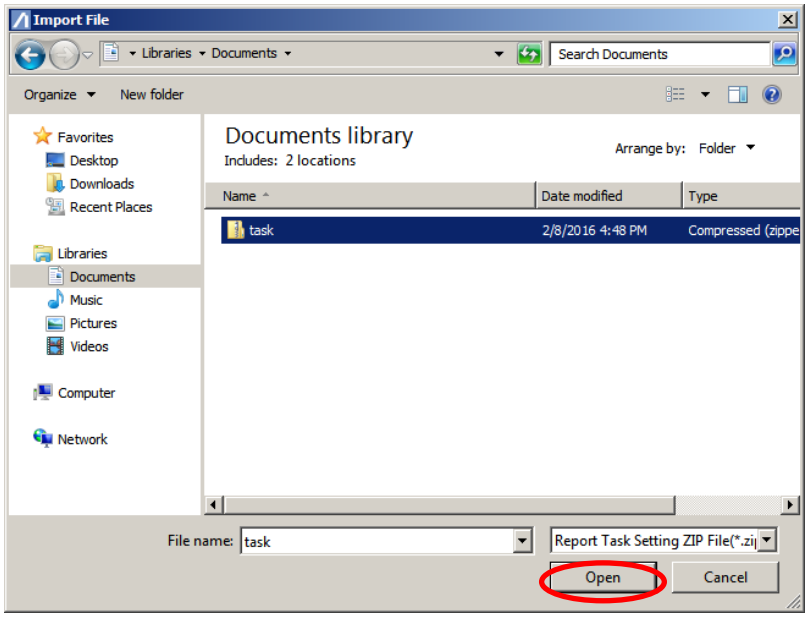


Figure 5.4.2-3 Dialog box for selecting the file to be imported

Check that the report has been restored on the periodic report list pane.

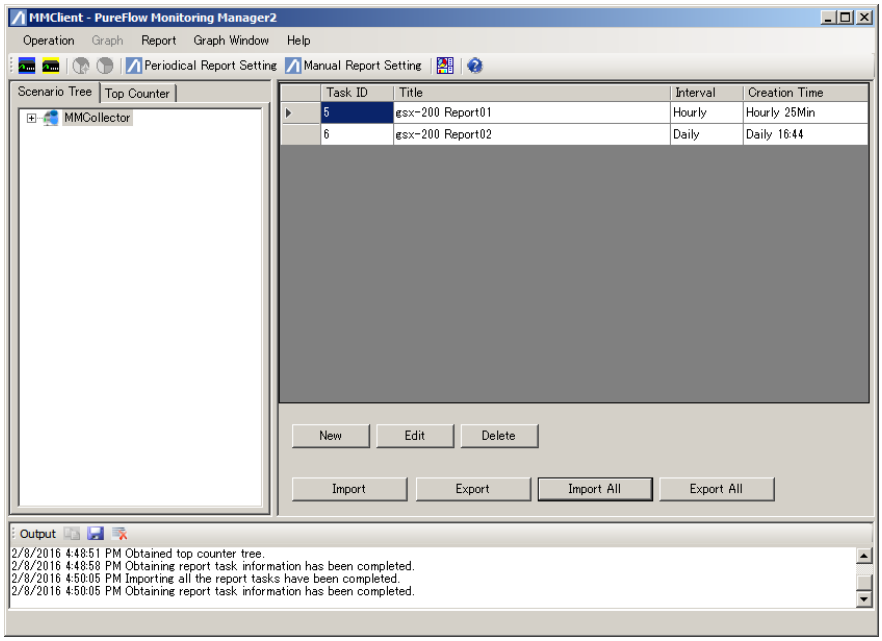


Figure 5.4.2-4 Periodic report list pane

Notes:

1. When the report task is imported, the unused task ID is allocated. The previously used task ID is not allocated.

2. When server software version v1.2.4 or earlier is used in Windows Server 2012 or Windows Server 2012 R2, import of the report settings (task.zip) after uninstalling the server software and re-installing it does not allow you to correctly register the report task in the Windows task scheduler and create the periodic report until the server is restarted. If you want not to restart server, delete all the report tasks before uninstalling the server software.

5.5 Report data

This section describes the format of the report data created by the report feature.

Reports can be created in the following two data formats:

- HTML format
  HTML-format reports are traffic reports that includes graphical images of monitor and top information saved in HTML format.
- CSV format
  CSV-format reports are traffic reports that include the numerical data of the monitor information and top information saved in CSV format.

5.5.1 HTML-format reports

HTML-format reports include graphical images in HTML format showing the how the monitor and top information for each port or scenario changes over time. The report title, graphs, and top graph of the specified node or scenario appear in order.

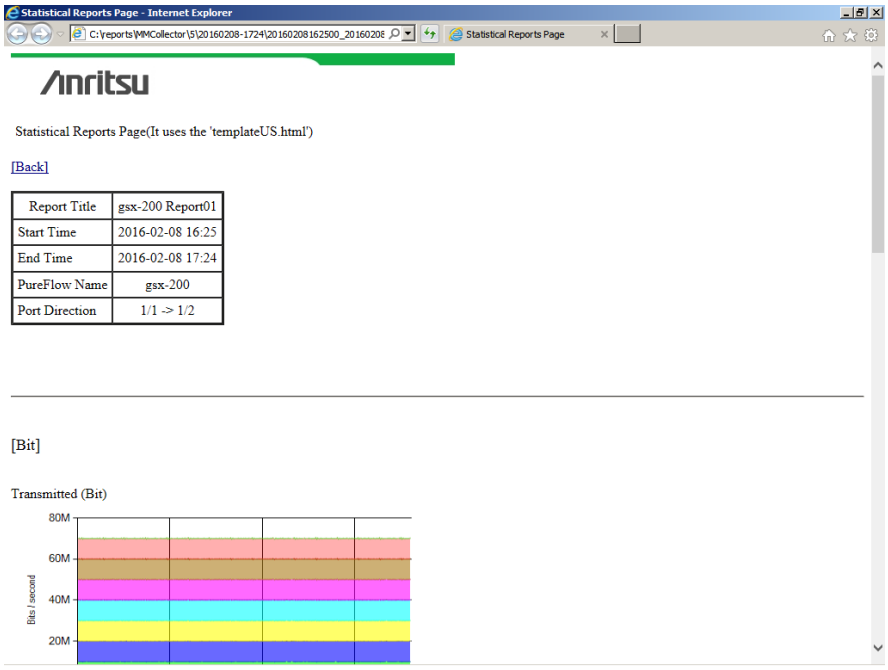


Figure 5.5.1-1 Example of HTML report

The header of the report is a template. The Anritsu logo is displayed by default. However, the header can be customized. The template in red in Figure 5.5.1-2 is recognized as a keyword in the software. Do not modify it.

```
<HTML>
  <HEAD>
    <TITLE>Statistics report page</TITLE>
  </HEAD>
  <BODY>
    <img src="../images/header1.jpg" border="0" alt="Anritsu top page">
    …
    <!—#####—>
    <!—#####—>
    …
  </BODY>
</HTML>
```

A graph is displayed in this position.

Figure 5.5.1-2 HTML report template

File path of template file:

`Installation folder\MMReporter\HTML_Template\template.html`

The path of `Installation folder` is as follows:

`C:\Program Files\AnritsuNetworks\MonitoringManager2`

Note:

If a large number of HTML reports are created at the same time, not only is a large amount of disk space consumed, but also the server load increases because the server is accessed frequently. You should therefore set the report task so that the condition "Number of nodes × Number of scenarios < 100" is satisfied. If the task exceeds this, divide the report task into the multiple tasks and change the report creation times so that a large number of reports are not created at the same time.

5.5.2 HTML report graph display setting

In version v1.3.1 or later, the following graph display settings for HTML report can be selected.

- Setting for displaying leader lines of a circle graph
- Setting of background line color saturation of a bar graph
- Setting of unit display for stacked bar, line, and bar graphs

Select the setting according to the following procedure.
The change of settings is valid from the first report after the change.

1. Open MMReporter.config using the text editor.
   The location of MMReporter.config is given below.
   C:\ProgramData\AnritsuNetworks\MMReporter\MMReporter.config
2. Change the value of each setting tag.
3. Overwrite MMReporter.config and save it.

The tag names and set values are listed below.

Table 5.5.2-1 Tag name and set value

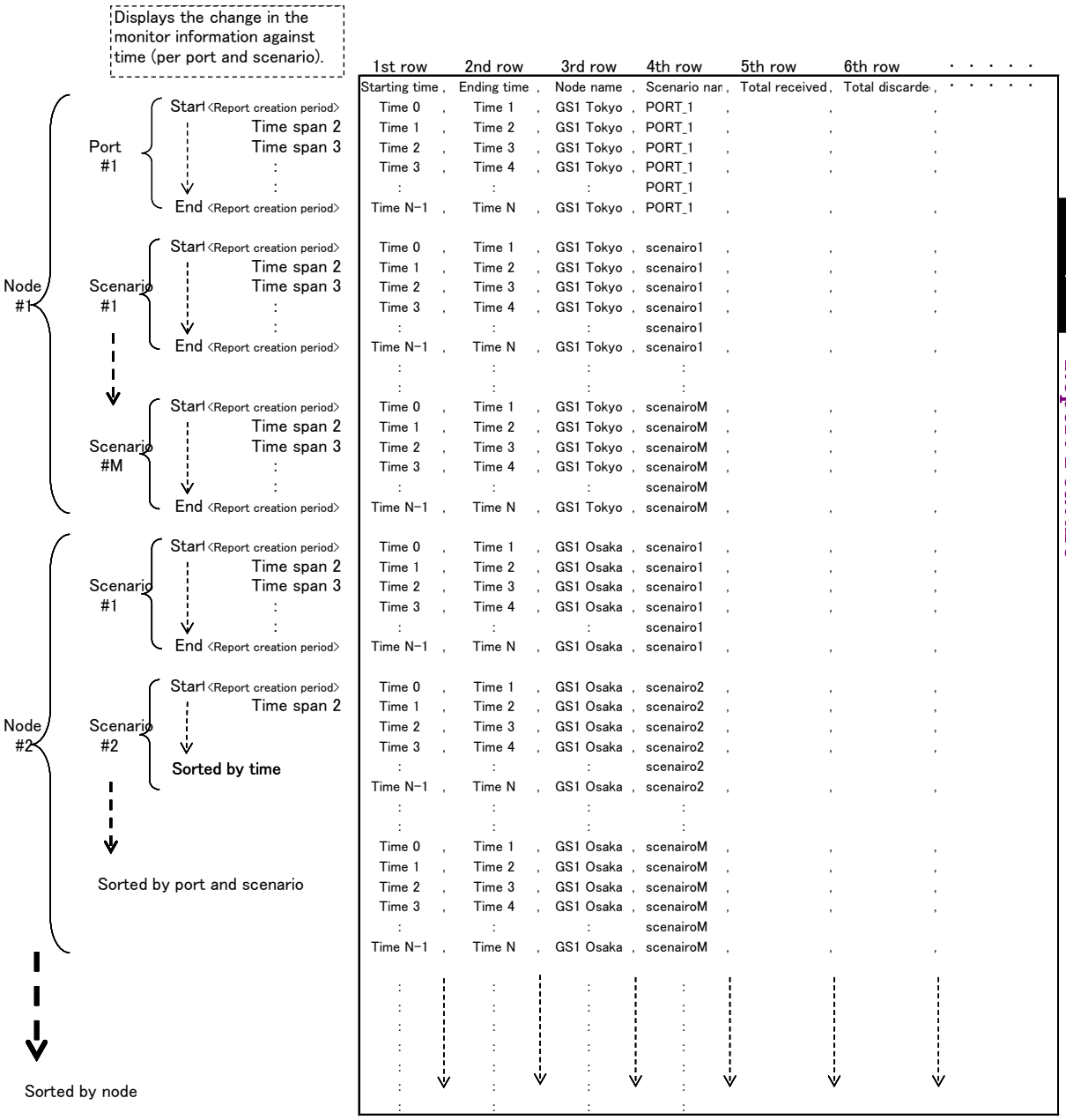
Displayed contents	Tag name	Set value
Setting for displaying leader lines of a circle graph	PieBarDisableLabel AndExtendLegend	true: No leader line appears. false: Leader lines appear (compatible display for versions v1.2.4 or earlier) Default value: true
Setting of background line color saturation of a bar graph	BarHorizontalLine LookBehind	true: Displays in darker color. false: Display in lighter color (compatible display for versions v1.2.4 or earlier) Default value: true
Setting of unit display for stacked bar, line, and bar graphs (K/M/G display)	EnableGraphUnit	true: Displays a unit false: Does not display a unit (compatible display for versions v1.2.4 or earlier) Default value: true

5.5.3 Monitor information CSV reports

Monitor information CSV reports include the statistics for each port or scenario in CSV format. The statistics between the starting and ending times of the report creation period are separated by certain time spans and displayed line by line.

(1) Display format

The following figure shows an example of a monitor information CSV report. The lines are sorted in port or scenario units as shown in the figure below, and the rows are separated by commas (,).



(2) Statistics to be displayed

The statistics to be displayed in the monitor information CSV report are described in Table 5.5.3-1. The statistics of ports and scenarios are displayed for each time span.

Table 5.5.3-1 Monitor information statistics (statistics for each port/scenario)

Row position	Item name	Maximum storage size	Description
1	Starting time	20 bytes	Displays the starting time of 1 time span.
2	Ending time	20 bytes	Displays the ending time of 1 time span.
3	Node name	257 bytes (Note 1)	Displays the PureFlow node name.
4	Port direction/Scenario name	257 bytes (Note 2)	Displays the port direction or scenario name.
5	Total packets received	21 bytes	Total number of packets received from the start of data collection
6	Total packets discarded	21 bytes	Total number of packets discarded from the start of data collection
7	Total packets sent	21 bytes	Total number of packets sent from the start of data collection
8	Total bytes received	21 bytes	Total number of bytes received from the start of data collection
9	Total bytes discarded	21 bytes (Note 3)	Total number of bytes discarded from the start of data collection
10	Total bytes sent	21 bytes	Total number of bytes sent from the start of data collection
11	Total bits received	21 bytes	Total number of bits received from the start of data collection
12	Total bits discarded	21 bytes (Note 3)	Total number of bits discarded from the start of data collection
13	Total bits sent	21 bytes	Total number of bits sent from the start of data collection
14	Delta packets received	21 bytes	Number of packets received during a certain time span
15	Delta packets discarded	21 bytes	Number of packets discarded during a certain time span
16	Delta packets sent	21 bytes	Number of packets sent during a certain time span
17	Delta bytes received	21 bytes	Number of bytes received during a certain time span
18	Delta bytes discarded	21 bytes (Note 3)	Number of bytes discarded during a certain time span
19	Delta bytes sent	21 bytes	Number of bytes sent during a certain time span
20	Delta bits received	21 bytes	Number of bits received during a certain time span
21	Delta bits discarded	21 bytes (Note 3)	Number of bits discarded during a certain time span
22	Delta bits sent	21 bytes	Number of bits sent during a certain time span

Row position	Item name	Maximum storage size	Description
23	Average packets received (pps)	11 bytes	Average number of packets received during a certain time span (one second)
24	Average packets discarded (pps)	11 bytes	Average number of packets discarded during a certain time span (one second)
25	Average packets sent (pps)	11 bytes	Average number of packets sent during a certain time span (one second)
26	Average bytes received (pps)	11 bytes	Average number of bytes received during a certain time span (one second)
27	Average bytes discarded (pps)	11 bytes (Note 3)	Average number of bytes discarded during a certain time span (one second)
28	Average bytes sent (pps)	11 bytes	Average number of bytes sent during a certain time span (one second)
29	Average bits received (pps)	11 bytes	Average number of bits received during a certain time span (one second)
30	Average bits discarded (pps)	11 bytes (Note 3)	Average number of bits discarded during a certain time span (one second)
31	Average bits sent (pps)	11 bytes	Average number of bits sent during a certain time span (one second)
32	Peak Transmitted bytes (Bps)	11 bytes	Maximum Bps rate in a 1-minute time span
33	Enable Peak: 1 Disable Peak: 0	2 bytes	1 (enabled), 0 (disabled)
34	Bypass state Disable:0 Standby:1 Measuring:2 Acceleration:3 Bypass:4 Forced Bypass:5	1 byte	Bypass state of the acceleration scenario (Scenarios other than the acceleration scenario are always set to 0 (Disable)). 1 (Standby), 2 (Measuring), 3 (Acceleration), 4 (Bypass), 5 (Forced Bypass), 0 (Disable)

Notes:

1. The node name is saved in up to 257 bytes. If the node name is defined to be less than 256 bytes, the data size is "(node name length) + 1 byte".

2. If the scenario name is displayed, it is saved in up to 257 bytes. If the port direction is displayed, it is saved in up to 12 bytes. If the scenario name is defined to be less than 256 bytes, the data size is "(scenario name length) + 1 byte".

3. For the monitor information of a port, total bytes discarded, delta bytes discarded, average bytes discarded, total bits discarded, delta bits discarded, and average bits discarded are not displayed. If the data described above is not displayed, the storage data size is 2 bytes.

4. In a CSV-format report, data from the same node is all output to a single file, so the scenario name is important because it identifies the data. Define the scenario name in PureFlow node so that the data can be identified. If the scenario name is duplicated, scenario name that displays can be substituted by setting the scenario comment. See "4.7.3 scenario comment setting", "7.7 scenario import and export of comment".

5. For the peak rate values of each particle-size data, check the peak rate value of the particle-size data smaller by one size, and adopt the maximum value within the related time range. Referenced data time range is same as the filtered data. See "4.6 Counter data type".

   Real-time data: Data itself sent from the PureFlow node is adopted.

   5-minute particle-size data: The maximum value is adopted within the related time range by referring to the real-time data.

   1-hour particle-size data: The maximum value is adopted within the related time range by referring to the 5-minute particle-size data

   3-hour particle-size data: The maximum value is adopted within the related time range by referring to the1-hour particle-size data

   1-day particle-size data: The maximum value is adopted within the related time range by referring to the 3-hour particle-size data

6. Data output order of the CSV report is in ascending order of port ID and scenario ID. For WSX (TCP acceleration) and WS1, the data is output in the following order.
   Network port 1/1
   Scenarios included in /port1 (scenario ID order)
   /port1
   Network port 1/2
   Scenarios included in /port2 (scenario ID order)
   /port2
   Network port 1/3
   Scenarios included in /port3 (scenario ID order)
   /port3
   Network port 1/4
   Scenarios included in /port4 (scenario ID order)
   /port4

(3) Output method of peak bytes

In v1.2.3 and later, user can select one of the following methods to output data to a CSV report for the peak transmitted bytes of 1/1 → 1/2 and 1/2 → 1/1. Output method I is an output method that can be chosen from v1.2.3 and later. Output method II is an output method earlier than v1.2.3.

I. The peak bytes transmitted at scenario "/port2" will be output to line of "1/1 → 1/2" in the report.

   The peak bytes transmitted at scenario "/port1" will be output to line of "1/2 → 1/1" in the report.

II. The peak bytes transmitted at scenario "/port1" will be output to line of "1/1 → 1/2" in the report.

   The peak bytes transmitted at scenario "/port2" will be output to line of "1/2 → 1/1" in the report.

The peak transmission byte of WSX (TCP acceleration) and WS1 is effective for the port scenario and scenario. The peak transmission byte for the port scenario is not affected by the output method due to output respectively to /port1, /port2, /port3, and /port4. The Network port is output while the peak transmission byte output is always set to 0.

An output example of the above mentioned output method is as follows. The following example is a CSV output report when PureFlowGSX only receive traffic from port 1/1.

Table 5.5.3-2 Output result of Output method I

Start time	End time	Node name	Port direction/ Scenario name	・・・	Total received bytes	Total transmit bytes	・・・	Peak transmit bytes (Bps)
2014/03/18-11:00:02	2014/03/18-11:01:02	GSX	1/1 → 1/2	・・・	8628488088	0	・・・	0
2014/03/18-11:01:02	2014/03/18-11:02:02	GSX	1/1 → 1/2	・・・	9368863746	0	・・・	0
2014/03/18-11:02:02	2014/03/18-11:03:02	GSX	1/1 → 1/2	・・・	10108993488	0	・・・	0
. .	. .	. .	. .	・・・	. .	. .	・・・	. .
2014/03/18-11:59:02	2014/03/18-12:00:02	GSX	1/1 → 1/2	・・・	52303377654	0	・・・	0
2014/03/18-11:00:02	2014/03/18-11:01:02	GSX	1/2 → 1/1	・・・	0	8628488088	・・・	12338300
2014/03/18-11:01:02	2014/03/18-11:02:02	GSX	1/2 → 1/1	・・・	0	9368863746	・・・	12338300
2014/03/18-11:02:02	2014/03/18-11:03:02	GSX	1/2 → 1/1	・・・	0	10108993488	・・・	12338300
. .	. .	. .	. .	・・・	. .	. .	・・・	. .
2014/03/18-11:59:02	2014/03/18-12:00:02	GSX	1/2 → 1/1	・・・	0	52303377654	・・・	12338300

Table 5.5.3-3 Output result of Output method II

Start time	End time	Node name	Port direction/ Scenario name	・・・	Total received bytes	Total transmit bytes	・・・	Peak transmit bytes (Bps)
2014/03/18-11:00:02	2014/03/18-11:01:02	GSX	1/1 → 1/2	・・・	8628488088	0	・・・	12338300
2014/03/18-11:01:02	2014/03/18-11:02:02	GSX	1/1 → 1/2	・・・	9368863746	0	・・・	12338300
2014/03/18-11:02:02	2014/03/18-11:03:02	GSX	1/1 → 1/2	・・・	10108993488	0	・・・	12338300
・ ・	・ ・	・ ・	・ ・	・・・	・ ・	・ ・	・・・	・ ・
2014/03/18-11:59:02	2014/03/18-12:00:02	GSX	1/1 → 1/2	・・・	52303377654	0	・・・	12338300
2014/03/18-11:00:02	2014/03/18-11:01:02	GSX	1/2 → 1/1	・・・	0	8628488088	・・・	0
2014/03/18-11:01:02	2014/03/18-11:02:02	GSX	1/2 → 1/1	・・・	0	9368863746	・・・	0
2014/03/18-11:02:02	2014/03/18-11:03:02	GSX	1/2 → 1/1	・・・	0	10108993488	・・・	0
・ ・	・ ・	・ ・	・ ・	・・・	・ ・	・ ・	・・・	・ ・
2014/03/18-11:59:02	2014/03/18-12:00:02	GSX	1/2 → 1/1	・・・	0	52303377654	・・・	0

Procedure for changing the output method is as follows. Please do the change of this setting while a periodic reporting that has not started by the scheduler. If the output report is activated while changing the settings, the report may not correctly output.

[1] Open the configuration file "MMReporter.config" with a text editor such as Notepad.

[2] Choose<IsPortPeakAndTransmitCombined>true</IsPortPeakAndTransmit Combined>, then please change the [true] to match the output method. Parameter settings are as follows.

True: Output format I. Output method I is the default value in V1.2.3 and later.

False: Output method II. Please set as false if you want to change it to the output method that is earlier than V1.2.3..

After saving the “MMReporter.config”, make a manual report and please make sure that it is output by the peak transmit bytes of CSV report by the set output method.

(4) Output of the bypass state

Whether to output the bypass state of the acceleration scenario or not can be changed. This is not output in the default state.

The procedure for changing the output method is described below. Change this setting while the report output is not activated. If the report output is activated when changing the setting, the report may not be output correctly.

<1> Open the setting file "MMReporter.config" by using a text editor such as a notepad.

<2> Select <IsScenarioStateOutput>false</IsScenarioStateOutput>, and change [false] according to the output method to be changed. The parameter set values are described below.

true: Outputs the bypass state information.

false: Does not output the bypass state information.

After overwriting "MMReporter.config", execute a manual report to check that the peak transmission byte of the CSV report is output according to the specified output method.

(5) Time span

In a monitor information CSV report, the data is displayed line by line, with each line representing a certain time span. The time spans are shown in the table below. For details about the report creation period, see the **Create Periodic Report** and **Create Manual Report** dialog boxes.

Table 5.5.3-4 Time spans in monitor information (CSV report)

Report creation period	Time spans in CSV report
Hourly report	Monitor information notification interval (60 seconds by default)
Daily report	1 line represents 5 minutes
Weekly report	1 line represents 1 hour
Monthly report	1 line represents 3 hours
Yearly report	1 line represents 1 day

(6) How to calculate the storage disk size

How to calculate the maximum disk size for storing monitor information CSV reports is described below.

The maximum data size of a monitor information CSV report is as follows:

(Maximum data size) = (Header information data volume) +
{(Number of report creation targets) × (Report creation period ÷ Time span) × (Maximum statistics size)}

- Header information data volume
  A description of the statistics for each row is displayed in the first line of the CSV data. The header information data volume is 648 bytes.

- Number of report creation targets
  This is the number of ports or scenarios for which report creation is specified. This number corresponds to the number of the selected check boxes for the ports and scenarios on the report creation pane.
- (Report creation period ÷ Time span)
  Corresponds to the number of times the monitor information is saved. The time span changes according to the length of the report creation period. For details, see Table 5.5.3-4.
  (Number of times monitor information is saved) = (Report creation period) ÷ (Time span)
- Maximum size of statistics
  The maximum size of the statistics is 1045 bytes.

Example of calculating the hourly report data size

A calculation example when the report creation period is specified as 1 hour is provided below. In this calculation example, the monitor information notification interval is set to 60 seconds (default value). Note that if you set the monitor information notification interval to 10 seconds (minimum value), the data is 6 times the size calculated in the example below.

[1] Creating a CSV report for a 1-hour period (per scenario)
If you create a CSV report with the report period set to 1 hour, the data size is approx. 64 KB.

(Maximum data size) = (Header information data volume) +
{(Number of report creation targets) × (Report creation period ÷ Time span) × (Maximum statistics size)}
= (648 bytes) + {(1 scenario) × (1 hour ÷ 60 seconds) × (1045 bytes)}
= 63,348 bytes
≈ 64 KB

[2] Creating an hourly period report for 1 month (1 node × 1 scenario)
If you create an hourly periodic report for 1 month, the total data size is approx. 48 MB.

(CSV data size for 1 month) = 64 KB × (31 days ÷ 1 hour)
= 47,616 KB (46 MB)

[3] Creating an hourly period report for 1 month (10 nodes × 100 scenarios)
If you create an hourly periodic report specifying 10 nodes each of which have 100 scenarios, the CSV data size per hour is approx. 64 MB. If you create a periodic report for 1 month, the total data size is 48 GB.

(CSV data size for 1 hour) = 64 KB × 10 nodes × 100 scenarios
= 64 MB

(CSV data size for 1 month) = 64 MB × (31 days ÷ 1 hour)
= 47,616 MB (46 GB)

Example of calculating the daily report data size

A calculation example when the report creation period is specified as 1 day is provided below.

[1] Creating a CSV report for a 1-day period (per scenario)
If you create a CSV report with the report period set to 1 day, the data size is approx. 302 KB.

(CSV data size) = (648 bytes) + {(1 scenario) × (1 day ÷ 5 minutes) × (1045 bytes)}
= 301,608 bytes
≈ 302 KB

[2] Creating an daily period report for 1 month (1 node × 1 scenario)
If you create a daily periodic report for 1 month, the total data size is approx. 9.4 MB.

(CSV data size for 1 month) = 302 KB × 31 days
= 9,362 KB (9.4 MB)

[3] Creating a daily period report for 1 month (10 nodes × 100 scenarios)
If you create a daily periodic report specifying 10 nodes each of which have 100 scenarios, the CSV data size for one month is approx. 9.4 GB.

(CSV data size for 1 month) = 9,362 KB × (10 nodes × 100 scenarios)
= 9,362 GB

Example of calculating the monthly report data size

A calculation example when the report creation period is specified as 1 month is provided below.

[1] Creating a CSV report for a 1-month period (per scenario)
If you create a CSV report with the report period set to 1 month, the data size is approx. 260 KB.

(CSV data size) = (648 bytes) + {(1 scenario) × (1 month ÷ 3 hours) × (1045 bytes)}
= 259,808 bytes
≈ 260 KB

[2] Creating a monthly period report for 1 month (10 nodes × 100 scenarios)
If you create a monthly periodic report specifying 10 nodes each of which have 100 scenarios, the CSV data size for one month is approx. 260 MB.

(CSV data size) = 260 KB × 10 nodes × 100 scenarios
≈ 260 MB.

Example of calculating the yearly report data size

A calculation example when the report creation period is specified as 1 year is provided below.

[1] Creating a CSV report for a 1-year period (per scenario)

If you create a CSV report with the report period set to 1 year, the data size is approx. 373 KB.

(CSV data size) = (648 bytes) + {(1 scenario) × (1 year ÷ 1 day) × (1045 bytes)}
= 372,668 bytes
≈ 373 KB

[2] Creating a yearly period report for 1 month (10 nodes × 100 scenarios)

If you create a yearly periodic report specifying 10 nodes each of which have 100 scenarios, the CSV data size is approx. 373 MB.

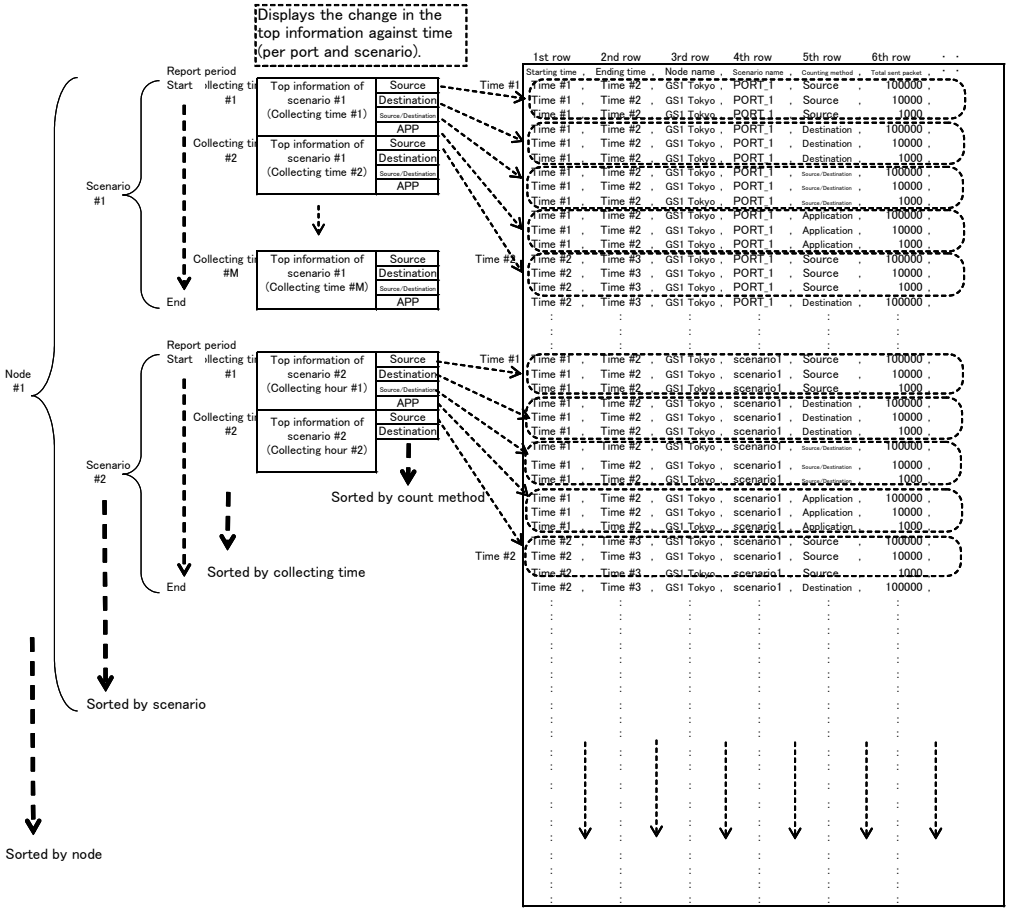
(CSV data size) = 373 KB × 10 nodes × 100 scenarios
≈ 373 MB

5.5.4 Top information CSV reports

Top information CSV reports include data showing how the top information changes over time for each port or scenario in CSV format. The top information between the starting and ending times of the report creation period is displayed for each top counter collection interval.

(1) Display format

The following figure shows an example of a top information CSV report. The lines are sorted in port or scenario units as shown in the figure below, and the rows are separated by commas (,).



(2) Statistics to be displayed

The statistics to be displayed in the top information CSV report are described in Table 5.5.4-1. The statistics of ports and scenarios are displayed for each top information collection interval.

Table 5.5.4-1 Top information statistics

Row position	Item name	Maximum storage size	Description
1	Starting time	20 bytes	Displays the starting time of top information collection.
2	Ending time	20 bytes	Displays the ending time of top information collection.
3	Node name	257 bytes (Note 1)	Displays the PureFlow node name.
4	Port direction/Scenario name	257 bytes (Note 2)	Displays the port direction or scenario name.
5	Counting target	17 bytes	Displays the source, destination, source and destination, or application.
6	Total packets sent	21 bytes	Displays the number of packets sent for all the sessions that passed through the scenario or port.
7	Total bytes sent	21 bytes	Displays the number of bytes sent for all the sessions that passed through the scenario or port.
8	Total bits sent	21 bytes	Displays the number of bits sent for all the sessions that passed through the scenario or port.
9	Source IP address	41 bytes (Note 3)	Displays the source IP address.
10	Destination IP address	41 bytes (Note 3)	Displays the destination IP address.
11	Protocol	28 bytes (Note 4)	Displays the TCP/UDP port number and application name.
12	Packets sent	21 bytes	Displays the number of packets sent for the ranked sessions.
13	Bytes sent	21 bytes	Displays the number of bytes sent for the ranked sessions.
14	Bits sent	21 bytes	Displays the number of bits sent for the ranked sessions.

Notes:

1. The node name is saved in up to 257 bytes. If the node name is defined to be less than 256 bytes, the data size is "(node name length) + 1 byte".

2. If the scenario name is displayed, it is saved in up to 257 bytes. If the port direction is displayed, it is saved in up to 12 bytes. If the scenario name is defined to be less than 256 bytes, the data size is "(scenario name length) + 1 byte".

3. For the source IP address and destination IP address, only the item specified by the counting target is displayed. If the data described above is not displayed, the storage data size is 2 bytes. The IPv4 address is saved in up to 17 bytes. The IPv6 address is saved in up to 41 bytes.

4. For the protocol, only the item whose application is specified by the counting target is displayed. If the data described above is not displayed, the storage data size is 2 bytes. If the application name consists of the maximum 20 characters, the protocol data size is up to 28 bytes.

5. Data output order of the CSV report is in ascending order of port ID and scenario ID.

(3) How to calculate the storage disk size

How to calculate the maximum disk size for storing top information CSV reports is described below.

The maximum data size of a top information CSV report is as follows:

(Maximum data size) = (Header information data volume)
+ {(Report creation period ÷ Top information notification cycle) × (Number of report creation targets) × (Maximum number of counting targets) × (Maximum number of display sessions + 1) × (Maximum statistics size)}

- Header information data volume
  A description of the statistics for each row is displayed in the first line of the CSV data. The header information data volume is 158 bytes.
- Number of report creation targets
  This is the number of ports or scenarios for which report creation is specified. This number corresponds to the number of the selected check boxes for the ports and scenarios on the report creation pane.
- (Report creation period ÷ Top information notification interval)
  Corresponds to the number of times the top information is saved.
  (Number of times monitor information is saved) = (Report creation period) ÷ (Top information notification interval)
- Maximum number of counting targets
  The maximum number of counting targets is 4. Four types of top information CSV reports are displayed: one for each source IP address, one for each destination IP address, one for each source and destination IP address, and one for each application.
- Maximum number of display sessions
  The maximum number of the display sessions is 25. For the top information, the top 25 communication sessions are displayed. Additionally, the sessions ranked 26th or lower are summed up and displayed as "Other sessions".
- Maximum size of statistics
  The maximum size of the statistics is 808 bytes. This maximum value is calculated when both the node and scenario names are defined as 256 bytes. If these names are defined to be smaller sizes, the maximum size of the statistics is also smaller.

Example of calculating the data size of a top information CSV report

An example of calculating the data size of a top information CSV report is shown below. The size of the top information CSV report varies depending on the total number of top counter measurement targets set for the nodes and the top information notification interval. Note that if you set the top information notification interval to 10 seconds (minimum value), the data is 6 times the size calculated in the example below.

[1] Creating a daily top information CSV report (notification interval = 60 seconds; one scenario)

If you create a daily CSV report for one scenario specifying a notification interval of 60 seconds, the maximum data size is approx. 2.0 MB.

(Data size per day) = (184 bytes) +
{(1440 minutes ÷ 60 minutes) × (1 node x 1 scenario) × (4 targets) × (25 sessions + 1) × (808 bytes)

= 2,016,952 bytes
≈ 2.0 MB

[2] Daily top information CSV report (notification interval = 480 minutes; 100 nodes × 32 scenarios)

If you create a daily CSV report for a total of 3,200 scenarios specifying a top information notification interval of 480 minutes, the maximum data size is approx. 807 MB.

(Data size per day) = (184 bytes) +
{(1440 minutes ÷ 480 minutes) × (100 nodes × 32 scenarios) × (4 targets) × (25 sessions + 1) × (808 bytes)

= 806,707,384 bytes
≈ 807 MB

Notes:

1. If a large volume of yearly report data is created, the server hard disk is accessed more frequently, leading to an increase in server load.
   Set the report task so that the condition "Number of nodes × Number of scenarios < 100" is satisfied. If the task exceeds this, divide the report task into the multiple tasks and change the report creation times so that a large number of reports are not created at the same time.

2. The size of the top information CSV report varies depending on the total number of top counter measurement targets for which a report is specified to be created and the top information notification interval. If the top information notification interval is short, the report data size increases, and it takes longer for the report to be created.

3. If a large number of top information CSV reports are created at the same time, the hard disk is accessed more frequently, leading to an increase in server load. Be sure to satisfy the following condition when creating a top information CSV report: Do not specify top information CSV reports to be created at the same time as periodic reports.
   {Total number of scenarios × (Report period [minutes] ÷ Top information notification interval [minutes])} ≤ 9600

   For example, to create a top information CSV report when the top information collection interval is 8 hours (480 minutes) and the top information consists of 3200 scenarios (100 nodes × 32 scenarios), set the report creation interval to 1 day or less.
   {3200 scenarios × (1 day ÷ 480 minutes)} = 9600

5.6 Deleting report data

This section describes how to delete report data.

This software does not delete the report data automatically. Periodical report will consume hard-disk capacity continually. If a large amount of the report data is created, the server hard-disk capacity is consumed. Therefore, be sure to delete the report data periodically. If the periodic report has been created continuously for a long time, the capacity of the index.html file in the "Task ID folder" is expanded, and the time taken to create a report may increase. Back up the report output folder or delete it periodically.

When creating a periodic or manual report, also create a sub folder under the report output folder and save the data there. The default setting of the report output folder is "c:\reports". For how to check the report output folder, see 7.5.7 Specifying the report output folder.

Note:

Do not delete the report output folder at the time at which the report is created. The file may not be deleted since it is being edited.

Report data is stored in the starting-time folders under each task-ID folder.

If the report output folder is `c:\reports`, you can check the relationship between the task ID and report title in `c:\reports\index.html` (periodic report) or `c:\reports\oneshot\index.html` (manual report).

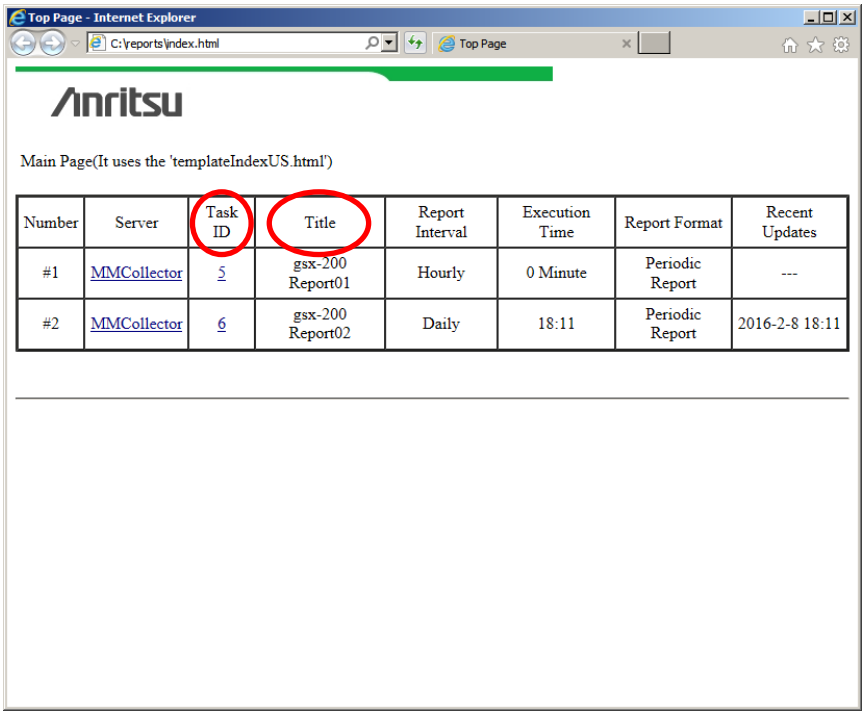


Figure 5.6-1 Relationship between task ID and report title

Delete the starting-time folders that are allowed to be deleted under each task ID folder.

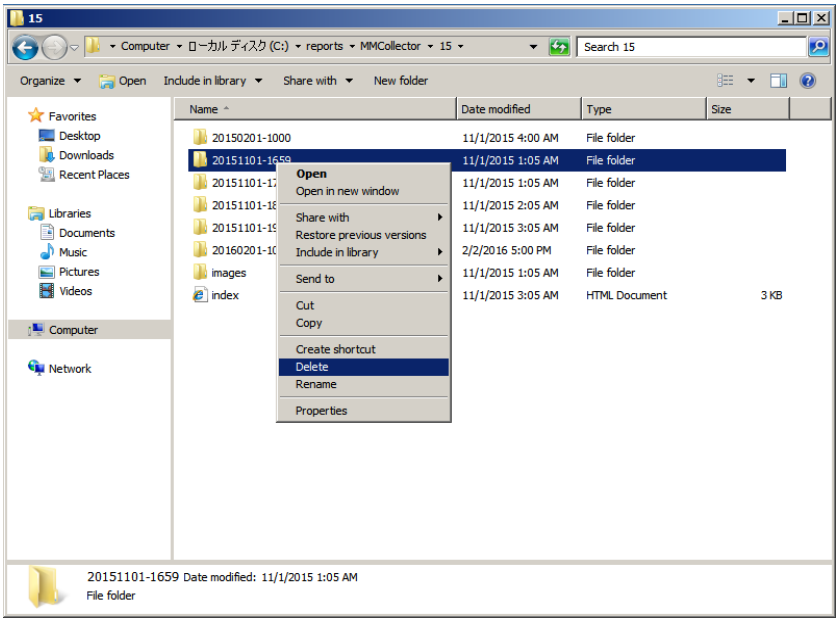


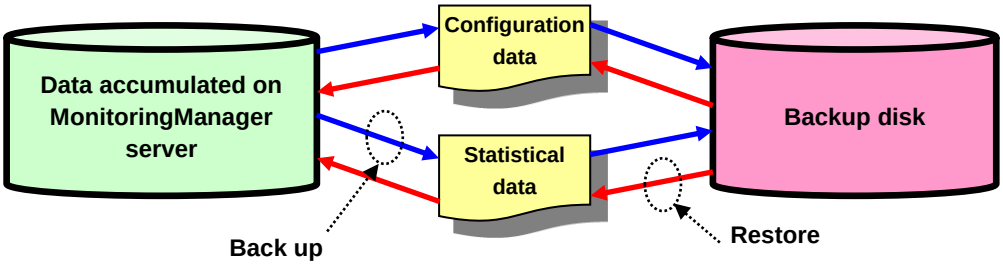
Figure 5.6-2 Deleting report data

This chapter describes how to back up and restore the settings and statistics of MonitoringManager2.

6.1 Backing up and restoring data

Data accumulated by MonitoringManager2 can be lost due to unforeseen problems such as a hardware failure. It is therefore recommended to regularly back up data in the MonitoringManager2 server.

The data that should be backed up in the MonitoringManager2 server consists of the setting information and the statistics. Regularly backing up this data helps in restoring the system in case of failure.



Data in server	Description
Setting information	This is the setting information of PureFlow, etc. registered in MonitoringManager2.
Statistics	These are the collected PureFlow traffic statistics.

This chapter describes how to perform the following:

- Online data backup and restoration
- Offline data backup and restoration

Notes:

1. This chapter focuses on only backing up the setting information (excluding language setting) and statistics required for operating MonitoringManager2. The license file and periodic and manual reports created by using the report feature are not included in the backup targets described in this chapter.
   Back up the license file (license_mm.txt) and report files by copying or exporting the report output folders as required. For the location for storing the license file, refer to "2.2 Installing the basic license file" or" "2.3 Installing an additional license file" in this manual.

2. In server software of PureFlow MonitoringManager2 version 1.2.4 or earlier, the online backup command and restore command cannot back up or restore the database if the folder where the database is saved is changed from the default setting. Back up or restore the database according to the offline backup procedure if the folder where the database is saved is changed from the default setting.

6.2 Online data backup and restoration

This section describes how to back up the data in the MonitoringManager2 server and restore the backed up data online.

A special command is provided to back up and restore data online. To back up and restore the data, click **Start - All Programs - Accessories - Command Prompt** to open the command prompt of Windows. On the command prompt, enter the name of the folder to which the special command used for backup and restoration is allocated, and then execute the command.

Folder to which the special command used for backup and restoration is allocated

`Installation folder\MMBackupAndRestoreTool\`

Reference: The path of `installation folder` is described below.
`C:\Program Files\AnritsuNetworks\MonitoringManager2`

An example of executing the command to move to the folder in which the special command is allocated is shown below. Enter the command without a linefeed.

Execution example

```
cd "c:\Program Files\AnritsuNetworks\MonitoringManager2\
MMBackupAndRestoreTool\"
```

For details of the backup and restore commands, see Appendix D Online Backup Command in this document.

Note:

If an error occurs during the online backup or restore, the OS event viewer shows a message. For the displayed message, see "Appendix F Event Viewer Message List".

6.2.1 Backing up data online

This section describes how to back up the data in the MonitoringManager2 server online. You can perform online back up even when MonitoringManager2 is running.

The following table shows an overview of the backup procedure described in this section.

Backup	
Backup data range	Can be selected by using a command option.
Backup method	Back up the data by using the special command.
Operation of MonitoringManager2 during backup process	Does not stop.
Restoration method	Described in the next section.

Back up the data by using the following procedure:

1. Check the capacity of the data directory and free space of the backup destination disk. Prepare a backup destination disk that is accessible from MonitoringManager2 in advance. The data directory "pure2" of this software is located by default as described below.
   C:\ProgramData\AnritsuNetworks\MMSql\MM2DataBase\pure2

2. Use the special command to back up the data.
   Click **Start - All Programs - Accessories - Command Prompt** to open the command prompt of Windows. On the command prompt, enter the name of the folder to which the special command used for backup is allocated, and then execute the command.

A backup command execution example is shown below. By executing this command, all the statistics and setting information in MonitoringManager2 is backed up. The backup data is output to the following folder:

Backup data folder

"{Folder to which special command for backup is allocated}\all-backup\"

Execution example

```
cd "c:\Program Files\AnritsuNetworks\MonitoringManager2\
MMBackupAndRestoreTool\"

.\mmbackup.exe -a -f all-backup -l backup-log.txt
```

This completes backup.

Notes:

1. In the online backup process, the data size, load on the server, and processing time increase in accordance with the backup period and data type.
   To prevent this, reduce the backup targets by using the -t option and reduce the backup period by using the -d or -r option so as to back up only the required data.
   For details of options, refer to "Appendix D Online Backup Command".

2. If MonitoringManager2 is managing a large number of nodes or scenarios, the backup process might not finish due to an excessive reading/writing load on the disk. In this case, consider backing up the statistics offline.

3. The backup process will be canceled without completing if there is insufficient free disk space.

4. The online backup function recognizes the folder where the database is saved by referring to the database configuration file created at installing of this software. If this software was installed in another folder previously, the folder where the current database is saved may not be recognized since the old database configuration file is the one referred to. Additionally, the same problem occurs if the previous database configuration file is backed up.
   In this case, specify the folder where the database is saved clearly by using the --db-path option.
   The folder where the database is stored recognized by the online backup function can be checked by the following message output to the console during online backup.
   "[main] DB instance path finded. Path = {Path of the folder where the database is saved}"

5. If the database configuration file cannot be searched since the access right for the installation folder of this software is specified or for other reasons, the folder where the database is saved cannot be recognized, and the online backup function is not enabled. In this case, specify the folder where the database is saved clearly by using the --db-path option.

6. If you will restore the backup data, you must restore it to the same folder which you had run an online-backup. Do not restore it to a different folder. This software may not be operated correctly.

6.2.2 Restoring data backed up online

This section describes how to restore the backed up data to the MonitoringManager2 server. The data to be restored must have been backed up in accordance with the above procedure.

The following table shows an overview of the restoration procedure described in this section.

Restoration	
Range of data to be restored	Backed up setting information and statistics data
Restoration method	Restore the data by using the special command.
Operation of MonitoringManager2 during restoration process	Must be stopped.
Backup method	Described in the above section.

Restore the data by using the following procedure:

1. Check the path of the backup data to be restored.
   Check the data backed up by using the special command for backup described in the above section. Check which data is to be restored and make a note of the target data path.
2. Check and correct the storage period setting.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **MMCollector Service** tab and click **Set Storage Period**. Confirm that the specified storage period is suitable for the data to be restored. Correct it as required.
   For how to set the storage period, see 7.4.1 Specifying the data storage period.
3. Stop the MonitoringManager2 services.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **Service** tab and stop **MMCollector Service** and **MMController Service**. These services stop according to this procedure.
   For how to stop these services, see 7.3 Service management.
4. Start the database service of MonitoringManager2.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **Service** tab and start **MMSql Service**. If this service is already running, it does not have to be started again.
   For how to start this service, see 7.3 Service management.
5. Restore the backup data by using the special command for restoration.
   Click **Start - All Programs - Accessories - Command Prompt** to open the command prompt of Windows. On the command prompt, enter the name of the folder that noted in step 1 to which the special command used for restoration is allocated, and then execute the command.

Specify the folder of the restoration target data noted in step 1 as an argument. An example of executing the command to restore the folder in which the backup data was output in the example above is shown below.

Backup data folder

```
Folder to which special command for backup is allocated\all-backup\
```

Execution example

```
cd "c:\Program Files\AnritsuNetworks\MonitoringManager2\
MMBackupAndRestoreTool\"

.\mmrestore.exe -f .\all-backup -l restore-log.txt
```

6. Start the MonitoringManager2 services.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **Service** tab, once start and stop **MMSql Service**, and start **MMCollector Service** and **MMController Service**. These services start according to this procedure.
   For how to start these services, see 7.3 Service management.
7. Enable periodic report execution.
   After restoration, the periodic report setting is reflected as report execution is disabled. To enable periodic report execution, click the **Edit** button on the periodic report list screen of the client software, and click the **Complete** button on the **Periodic Report Setting** pane that newly appears.
   To configure the previously backed-up report, restore the report configuration file. Click **Start** menu, **MonitoringManager2**, and **MMClient** to start it, and import (restore) all the previously backed-up report tasks.
   For how to import the tasks, see 5.4.2 Importing report settings.
8. Check that MonitoringManager2 is running.
   Start MMClient and display real-time graphs and other data to check that the MonitoringManager2 server is running in the same way as before the data was backed up.

This completes restoration.

Notes:

1. Be sure to stop MMCollector Service and MMController Service before restoring the data. Otherwise, the data might not be restored correctly.

2. The storage period setting cannot be restored by using the special command. The storage period setting immediately before restoration is retained as is. Be sure to set an appropriate storage period before restoring the data. If you do not set a storage period, the period is set to the default value.
   If data is restored without setting a storage period, data that is outside the storage period range is deleted when the MonitoringManager2 services are started (after the data has been restored).

3. If there is still MonitoringManager2 statistics and setting information remaining during the restoration process, that information is overwritten by the backup data as a result of executing the special command for restoration. If the incorrect data is restored, the statistics and setting information might be corrupted, causing MonitoringManager2 to malfunction.
   Also if data is restored after statistics and setting information has been corrupted, the restoration might not finish successfully or the data might be damaged during the restoration process, causing MonitoringManager2 to malfunction.

4. Do not change the folder name of the online back-up data. Restore function will not work.

5. The restoration function by the dedicated command recognizes the folder where the database is saved by referring to the database configuration file created at installing of this software. If this software was installed in another folder previously, the folder where the current database is saved may not be recognized since the old database configuration file is the one referred to. Additionally, the same problem occurs if the previous database configuration file is backed up.
   In this case, specify the folder where the database is saved clearly by using the --db-path option.
   The folder where the database is stored recognized by the restoration function by the dedicated command can be checked by the following message output to the console during the restoration.
   "[main] DB instance path finded. Path = {Path of the folder where the database is saved}"

6. If the database configuration file cannot be searched since the access right for the installation folder of this software is specified or for other reasons, the folder where the database is saved cannot be recognized, and restoration is not enabled. In this case, specify the folder where the database is saved clearly by using the --db-path option.

7. If you will restore the backup data, you must restore it to the same folder which you had run an online-backup. Do not restore it to a different folder.

6.3 Offline backup and restoration

Data can be backed up offline only by copying the directory.

6.3.1 Backing up data offline

This section describes how to back up the data in the MonitoringManager2 server offline.

The following table shows an overview of the backup procedure described in this section.

Backup	
Backup data range	All backed up setting information and statistics data currently existing in the data directory
Backup method	Manually copy the entire data directory. Back up all the setting information of MonitoringManager2.
Operation of MonitoringManager2 during backup process	Must be stopped.
Restoration method	Described in the next section.

Back up the data by using the following procedure:

1. Check the capacity of the data directory and free space of the backup destination disk.
   Prepare a backup destination disk that is accessible from MonitoringManager2 in advance.
   Make sure that the free space of the backup destination disk is more than size of the data directory `pure2` of MonitoringManager2.
   The default location of the data directory `pure2` of MonitoringManager2 is:
   `C:\ProgramData\AnritsuNetworks\MMSql\MM2DataBase\pure2`
2. Exit the client software.
   If MMClient is running, close the window to exit the software.
3. Stop all the MonitoringManager2 services.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **Service** tab and stop **MMCollector Service**, **MMController Service**, and **MMSql Service**. These services stop according to this procedure.
   For how to stop these services, see 7.3 Service management.
4. Copy the data directory to the backup disk.
   Copy the entire data directory `pure2` (whose capacity was checked above) in MonitoringManager2 to the backup destination. Copy the directory by using the usual directory copy command of Windows.
   For easy management, specify a name that includes the backup date, such as `D:\backup\mm\20161028`, as the directory name in the backup destination.
5. Back up the operation settings of MonitoringManager2.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **Backup/Restore** tab and back up the configuration file.
   For how to back up the configuration file, see 7.8.1 Backing up operation settings.

6. Start the MonitoringManager2 services.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **Service** tab and start **MMSql Service**, **MMCollector Service** and **MMController Service**. These services stop according to this procedure.
   For how to start these services, see 7.3 Service management.
7. Back up the report settings.
   Click **Start - MonitoringManager2 – MMClient** and export all the report tasks.
   For how to back up the report settings, see 5.4.1 Exporting report settings.
8. Check that MonitoringManager2 is running.
   Start MMClient and display real-time graphs and other data to check that the MonitoringManager2 server is running in the same way as before the data was backed up.

This completes backup.

6.3.2 Restoring data backed up offline

This section describes how to restore the backed up data to the MonitoringManager2 server. The data to be restored must have been backed up in accordance with the above procedure.

The following table shows an overview of the restoration procedure described in this section.

Restoration	
Range of data to be restored	All backed up setting information and statistics data
Restoration method	Manually copy the entire data directory. Restore all the setting information of MonitoringManager2.
Operation of MonitoringManager during restoration process	Must be stopped.
Backup method	Described in the above section.

Restore the data by using the following procedure:

1. Stop all the MonitoringManager2 services.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **Service** tab and stop **MMCollector Service**, **MMController Service**, and **MMSql Service**. These services stop according to this procedure.
   For how to stop these services, see 7.3 Service management.
2. Delete the old data in the MonitoringManager2 data restoration destination.
   If an older copy of the data directory `pure2` exists in the data directory of the MonitoringManager2 data restoration destination, delete this directory first.
   The default location of the data directory `pure2` of MonitoringManager2 is:
   `C:\ProgramData\AnritsuNetworks\MMSql\MM2DataBase\pure2`
   Make sure that the size of the backup directory `pure2` of MonitoringManager2 to be restored is less than the free space of the restoration destination disk.
3. Copy the backup data directory to the restoration destination directory.
   Copy the entire backup data directory `pure2` of MonitoringManager2 to the restoration destination directory. Copy the directory by using the usual directory copy command of Windows.
   The default copy destination of the data directory `pure2` of MonitoringManager2 is:
   `C:\ProgramData\AnritsuNetworks\MMSql\MM2DataBase\pure2`
4. Restore the operation settings of MonitoringManager2.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **Backup/Restore** tab and restore the configuration file.
   For how to restore the configuration file, see 7.8.1 Backing up operation settings.
5. Start the MonitoringManager2 services.
   Click **Start - MonitoringManager2 - MMAdminTool**, open the **Service** tab and start **MMSql Service**, **MMCollector Service** and **MMController Service**. These services stop according to this procedure.
   For how to start these services, see 7.3 Service management.

6. Enable periodic report execution.
   After restoration, the periodic report setting is reflected as report execution is disabled. To enable periodic report execution, click the **Edit** button on the periodic report list screen of the client software, and click the **Complete** button on the **Periodic Report Setting** pane that newly appears.
   To configure the previously backed-up report, restore the report setting file.
   Click **Start - MonitoringManager2 – MMClient** and import (restore) all the backed up report tasks. For how to restore the report settings, see 5.4.2 Importing report settings.
7. Check that MonitoringManager2 is running.
   Start MMClient and display real-time graphs and other data to check that the MonitoringManager2 server is running in the same way as before the data was restored.

This completes restoration.

6.4 Upgrading the software

6.4.1 Upgrade procedure

This section describes how to upgrade MonitoringManager2 to the latest version.
Back up any required data such as configuration information before starting the upgrade process.

The following table shows an overview of the upgrade procedure described in this section.

Upgrade	
Operation of MonitoringManager2 during upgrade process	Must be stopped.
Backup and restoration methods	Described in the above section.

Upgrade MonitoringManager2 and the database by using the following procedure:

1. Back up previous-version data.
   Back up all required data. For details, see 6.2.1 Backing up data online or 6.3.1 Backing up data offline.
2. Uninstall the old version of MonitoringManager2.
   For details, see 3.1 Uninstallation procedure.
3. Install the new version of MonitoringManager2.
   For details, see 2.1 Installation procedure.
4. Restore the database backed up from the old version.
   For details, see 6.2.2 Restoring data backed up online or 6.3.2 Restoring data backed up offline.

6.4.2 Upgrading from MonitoringManager (PX700003A)

This section describes how to upgrade MonitoringManager (PX700003A) to the latest version of MonitoringManager2.

The database storage format of this product, MonitoringManager2 (NF7201A), is different from that of Anritsu's previous product, MonitoringManager (PX700003A). Therefore, data migration is not possible.
Output the required statistics in a CSV-format report and save it.

1. Uninstall MonitoringManager (PX700003A).
   For details, see 3.1 Uninstallation procedure in the instruction manual of MonitoringManager (PX700003A).
2. Install MonitoringManager2.
   For details, see 2.1 Installation procedure.

This chapter describes MMAdminTool, which is the server management tool of MonitoringManager2.

7.1 Overview

MMCollector Service, MMController Service, and MMSql Service are the services used by MonitoringManager2.

MMCollector Service

This service collects the counter information of the PureFlow series device. If this service is not enabled, the information reported by PureFlow cannot be collected.

MMController Service

This service creates reports based on the PureFlow counter information accumulated in the database. This service also communicates with MMClient to specify settings and manage nodes. If this service is not enabled, reports cannot be output and nodes cannot be managed by MMClient.

MMSql Service

This service accumulates the PureFlow statistics in the database. This service communicates with each service of MonitoringManager2 to reference and update the database information. If this service is not enabled, MonitoringManager2 cannot operate.

MMAdminTool is used to manage the services above, perform operation settings for MonitoringManager2, and obtain information required for technical support.

MMAdminTool performs general service management, MMCollector Service management, and MMController Service management.

Service management

You can start and stop services.
You can also check the operating status of each service.

MMCollector Service management

You can specify the data storage period for MMCollector.
You can also check the PureFlow connection status.

MMController Service management

You can specify the following settings:
Local user settings, RADIUS server settings, server settings, SNMP settings, SYSLOG server settings, detection event settings, authentication mode switch settings, report output folder settings, and language settings of MMController and MMReporter.

You can also check the connection status of MMClient and view a list of reports.

Importing and exporting the scenario comments

You can specify or obtain the batch scenario comments.

Backing up and restoring operation settings

You can back up and restore the configuration files of MonitoringManager2.

Language selection

You can select in which language to display the MonitoringManager2 GUI.

Time mode specification

You can check the time mode.

Obtaining technical support information

You can obtain information for technical support.

7.2 Starting up MMAdminTool

Click **Start - All Programs - AnritsuNetworks – MMAdminTool** to start admintool. If the **User Account Control** dialog box appears, click **Yes**.

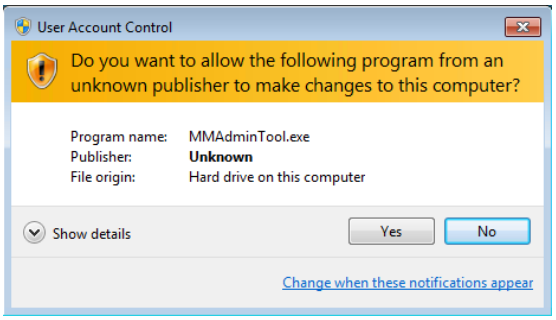


Figure 7.2-1 User Account Control dialog box

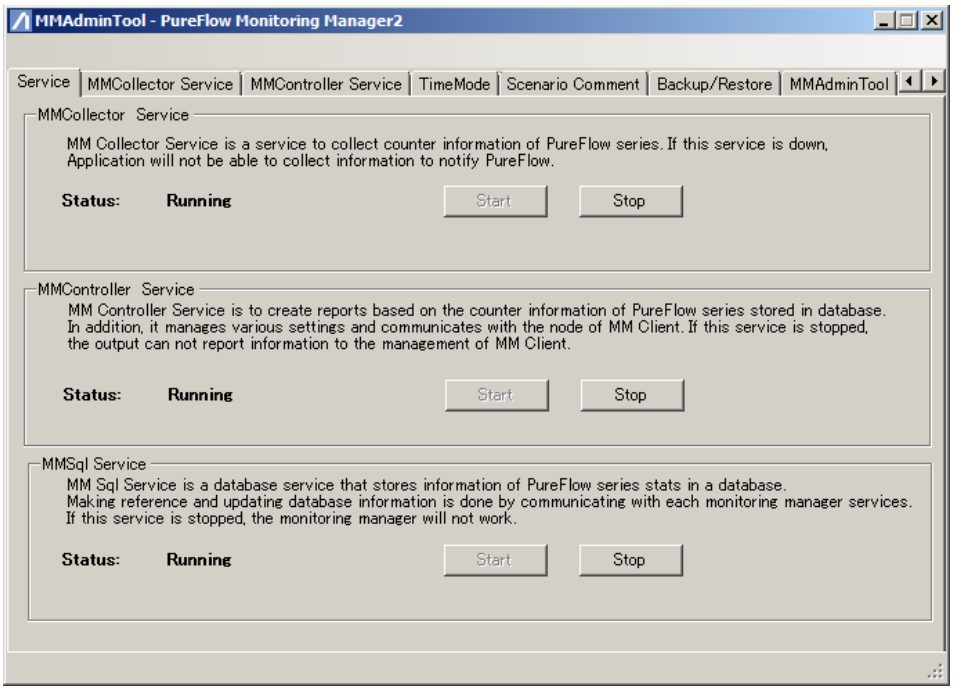


Figure 7.2-2 MMAdminTool main window

Note:

When saving the file, determine the saving folder and file name so that the number of the characters including the folder path and file name does not exceed 255 bytes. Otherwise, the information may not be obtained as Windows OS restrictions stipulate that the characters of the names of the paths and files cannot exceed 255 bytes.

7.2.1 Starting up MMAdminTool by using the task tray icon

If the minimize ("_") button on the active title bar is clicked, MMAdminTool is not displayed on the task bar. In this case, MMAdminTool is displayed as a task tray icon.

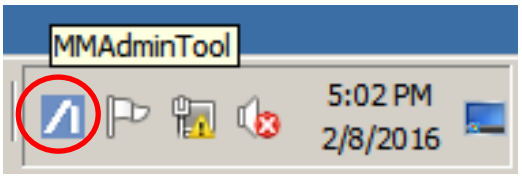


Figure 7.2.1-1 MMAdminTool task tray icon

Click the MMAdminTool icon on the task tray to open the MMAdminTool currently running in the system.

If an attempt is made to start up MMAdminTool by using the normal startup procedure while the MMAdminTool icon is displayed in the task tray, an "MMAdminTool is already running" error message is displayed to prevent multiple booting.

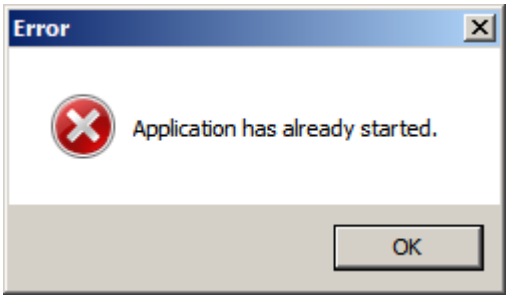


Figure 7.2.1-2 Message to prevent multiple booting

7.3 Service management

You can start and stop services on the **Service** tab. You can also check the operating status of each service on this tab.

Open the **Service** tab in the **MMAdminTool** window.

Click **Start** to start the service, and click **Stop** to stop the service.

When the service is running, **Running** is displayed, and when the service is stopped, **Stopped** is displayed.

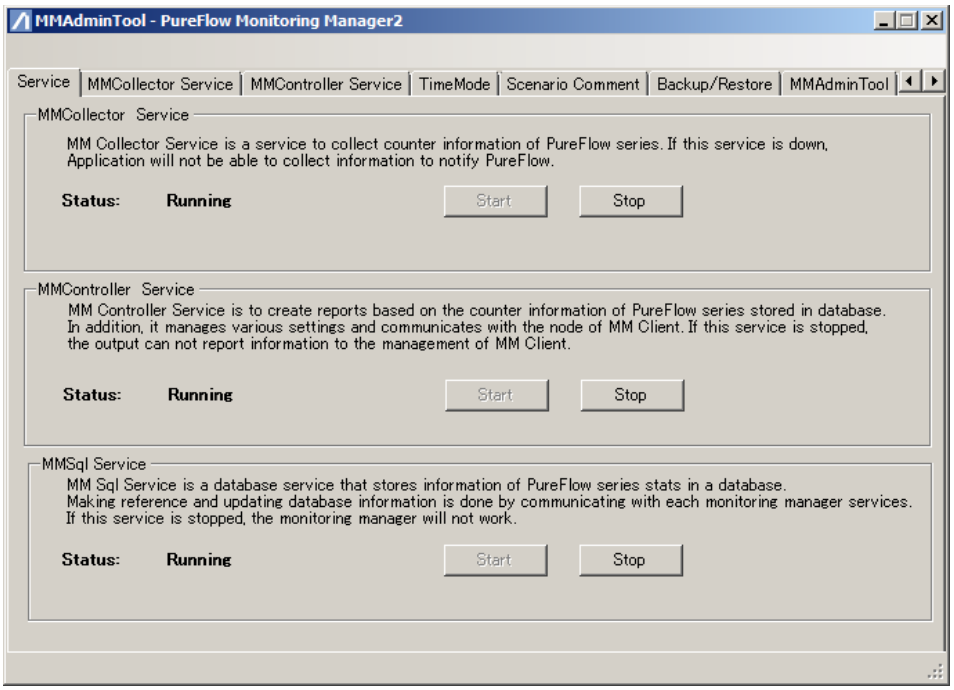


Figure 7.3-1 Service tab

When MMSql Service is stopped, MMCollector Service also stops.

7.4 MMCollector Service management

7.4.1 Specifying the data storage period

You can specify how long to store data in the database on the **MMCollector Service** tab. Once the specified storage period has expired, the corresponding data is deleted from the database to prevent the database becoming excessively large.

To specify the data storage period, **MMCollector service** has to be started.
Open the **MMCollector Service** tab in the **MMAdminTool** main window, and click **Set storage period** to display the **Set Data Storage Period** dialog box.

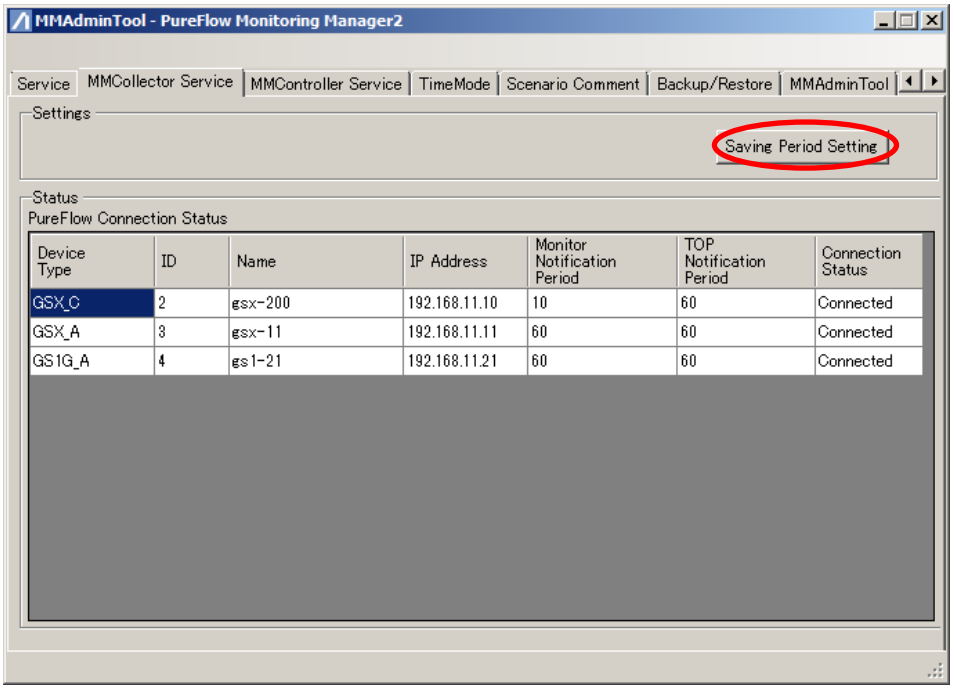


Figure 7.4.1-1 MMCollector Service tab

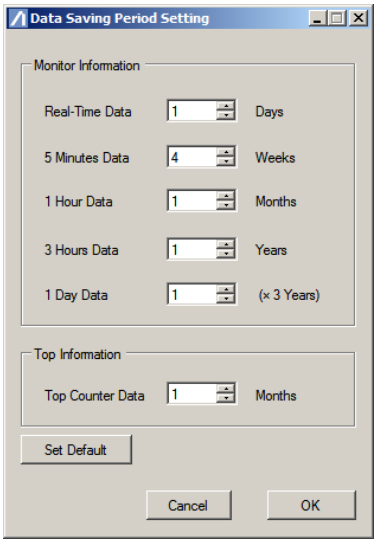


Figure 7.4.1-2 Set Data Storage Period dialog box

Specify the data storage period for monitor information and top information.

For monitor information, a storage period can be specified for each data granularity.

When the data with a fine time granularity is stored, the data can be displayed on a graph with fine granularity. However, this consumes a large amount of hard disk capacity. A longer storage period equates to higher hard disk capacity consumption, although storing information for a long time allows more past data to be referenced.

Granularity cannot be specified for top information; it can only be specified for real-time data.

Change the data storage period settings according to the available hard disk capacity and the granularity required for the past monitor data.

Monitor information

Real-time Data

Specify the storage period for real-time data.
Valid values are from 1 to 60 days. The default value is 1 (day).

5 Minutes Data

Specify the storage period for 5-minute granularity data.
Valid values are from 1 to 300 weeks. The default value is 4 (weeks).

1 Hour Data

Specify the storage period for 1-hour granularity data.
Valid values are from 1 to 24 months. The default value is 1 (month).

3 Hours Data

Specify the storage period for 3-hour granularity data.
Valid values are from 1 to 5 years. The default value is 1 (year).

1 Day Data

Specify the storage period for 1-day granularity data.
Valid values are from 1 to 3. 1 stands for 3 years, 2 for 6 years, and 3 for 9 years.
The default value is 1.

Top information

Specify the storage period for top counter data. Valid values are from 1 to 24 months.

Restore initial values

Click **Restore initial values** to display the initial settings.

Click **OK** to finalize the data storage period settings. Click **Cancel** to cancel the settings.

The data storage period settings become effective when starting MMCollector service next time. Restart MMCollector servie if these settings need to be enabled immediately. For how to restart MMCollector service, see 7.3 Service management.

Notes:

1. Time to delete the data will be 0:00 in the local time of the server
2. Data will also be deleted when restart the MMCollector Service

7.4.2 Checking the PureFlow connection status

Open the **MMCollector Service** tab in the **MMAdminTool** main window to display the connection status of PureFlow.

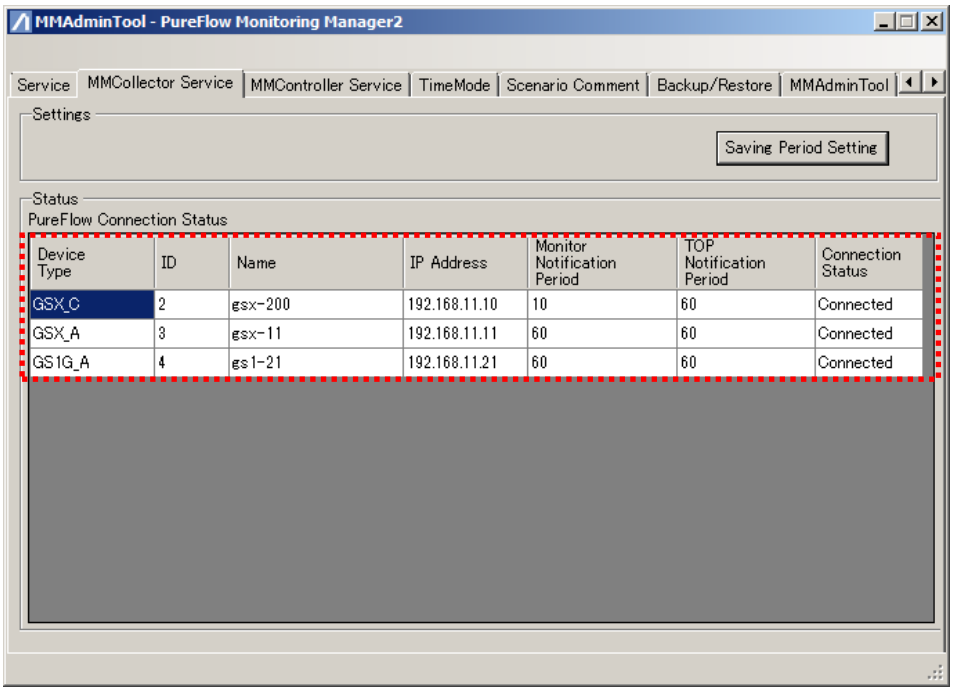


Figure 7.4.2-1 Checking the PureFlow connection status

7.5 MMController Service management

The MMController Service management feature can be used to perform actions such as adding, editing, or deleting Radius servers, specifying settings for over- or under-threshold events, and changing the report output folder. After changing any of the MMController Service management settings, click **Save Settings** button and restart MMController service. For how to restart MMController service, see 7.3 Service management.

7.5.1 Switching authentication mode

You can check and change the login authentication mode on the **MMController Service** tab.

The following login authentication modes are provided to log into MonitoringManager2:

Local authentication mode

Authentication is processed based on the account information stored in the MonitoringManager2 server.

RADIUS authentication mode

Authentication is processed based on the account information stored in the specified RADIUS server instead of the MonitoringManager2 server.

Open the **MMController Service** tab in the **MMAdminTool** main window to check the currently-selected authentication mode. Click **Switch authentication mode** to display the **Authentication Mode** dialog box.

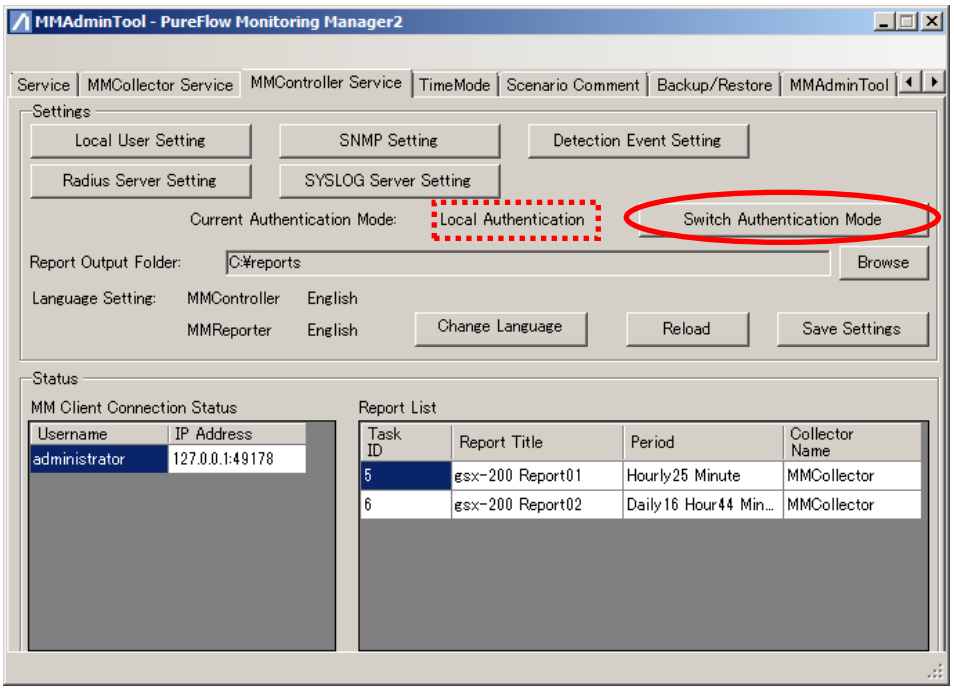


Figure 7.5.1-1 MMController Service tab

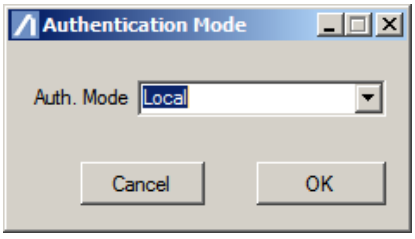


Figure 7.5.1-2 Authentication Mode dialog box

Select either **Local** (local authentication mode) or RADIUS (RADIUS authentication mode) from the **Authentication mode** pull-down menu. Click **OK** to finalize the authentication mode setting. Click **Cancel** to cancel the setting.

For the local user settings in local authentication mode, see 7.5.2 Specifying local user settings.

For the RADIUS server settings in RADIUS authentication mode, see 7.5.3 Specifying RADIUS server settings.

7.5.2 Specifying local user settings

You can add, change, or delete local users who use MonitoringManager2 in local authentication mode.

Open the **MMController Service** tab in the **MMAdminTool** main window to check the currently-selected authentication mode. The **Set Local Users** button is available if the selected mode is local authentication mode. Local authentication mode is specified as the login authentication mode at installation. When selecting local authentication mode, RADIUS authentication mode cannot be selected.

Open the **MMController Service** tab in the **MMAdminTool** main window, and click the **Set Local Users** button to display the **Set Local Users** dialog box.

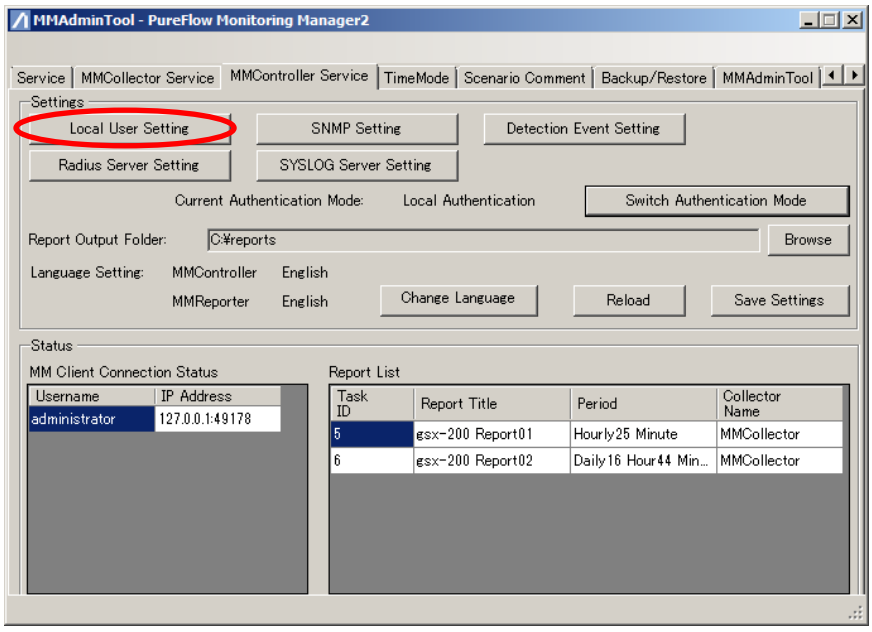


Figure 7.5.2-1 Set Local Users button

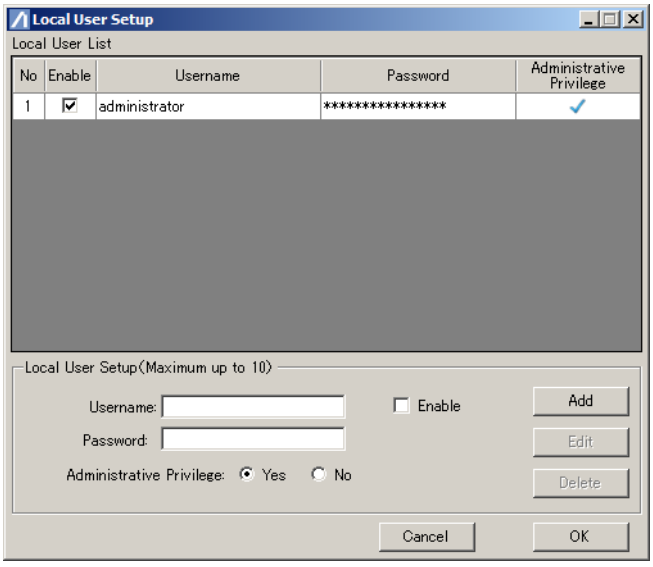


Figure 7.5.2-2 Set Local Users dialog box

This dialog box shows the list of local users. Local users can be added, changed, or deleted here. Up to 10 local users can be added.

Adding users

User name

Enter the user name.
Only one-byte alphanumeric characters can be used for user names.
Up to 255 characters can be registered.

Password

Enter the password.
One-byte alphanumeric and two-byte characters and symbols can be used for passwords. The symbols &<>'"\;, cannot be used. Up to 255 characters can be registered.

Administrative Privilege

Select **Enabled** or **Disabled** for **Administrator authority**.
Users with Administrator authority can register, delete, and edit PureFlow units, and specify report and threshold value settings.
Users without Administrator authority can only check the set values.
When enabling local users, select **Enabled**.

Click **Add** to add a user.

Editing user settings

Select the user whose settings are to be edited in the local user list, edit the relevant items, and click **Change**.

Deleting users

Select the user to be deleted in the local user list and click **Delete**. Note that users with administrator authority cannot be deleted. More than one user with administrator authority must be registered.

7.5.3 Specifying RADIUS server settings

You can add, edit, or delete the RADIUS servers used in the RADIUS authentication mode.

Open the **MMController Service** tab in the **MMAdminTool** main window to check the currently-selected authentication mode. The **Set RADUIS Server** button is available if the selected mode is RADIUS authentication mode. When selecting RADIUS authentication mode, local authentication mode cannot be selected.

Open the **MMController Service** tab on the **MMAdminTool** main window, and click the **Set RADIUS Servers** button to display the **Set RADIUS Servers** dialog box.

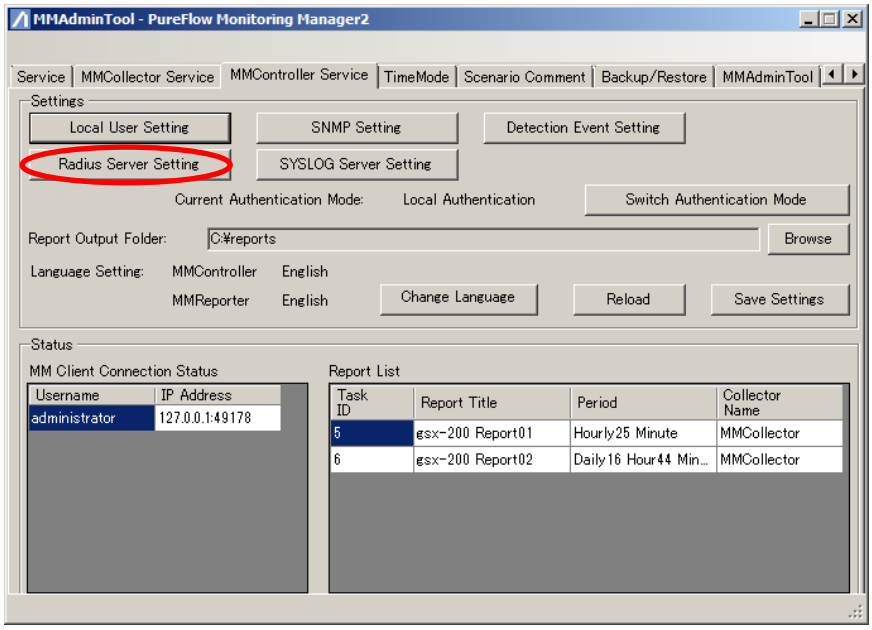


Figure 7.5.3-1 Set RADIUS Servers button

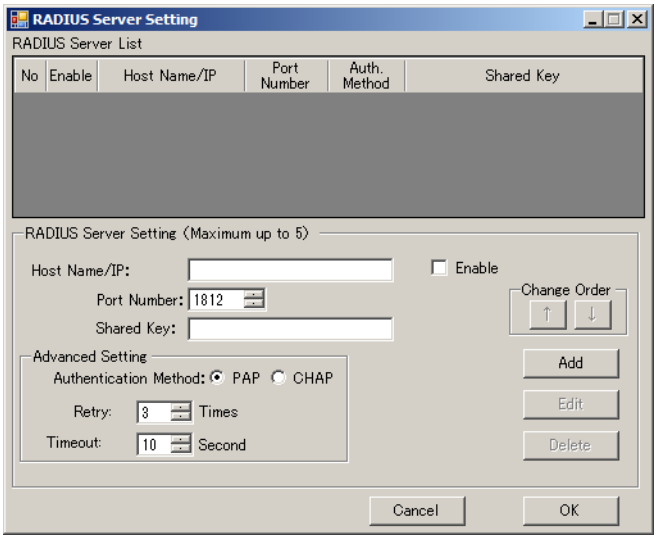


Figure 7.5.3-2 Set RADIUS Servers dialog box

This dialog box shows a list of RADIUS servers. RADIUS servers can be added, edited, or deleted here. Up to five RADIUS servers can be added.

The priority for RADIUS servers can be changed by using "↑"or button. Push "↑" button once to up server priority one. Push "↓" button once to down server priority one.

Adding RADIUS servers

Host Name/IP

Enter the host name or the IP address.

Port Number

Specify the RADIUS server port No.
The default value is 1812.

Shared Key

Specify the shared key.
The following one-byte characters can be used for the shared key:

1234567890
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ!
#$%()=~-^|@`[]{}:*;+_/.

Enable

To enable RADIUS servers, select **Enable**.

Authentication Method

Specify either PAP or CHAP for the authentication protocol.
The default authentication protocol is PAP.

Retry

Specify the retry count. Valid values are from 0 to 30 retries.
The default retry count is 3 (retries).

Timeout

Specify the timeout timing. Valid values are from 1 to 10 seconds.
The default timeout time is 10 seconds.

Click **Add** to add a server.

Editing RADIUS servers

Select the server whose information is to be edited in the RADIUS server list, edit the relevant items, and click **Change**.

Deleting RADIUS servers

Select the server to be deleted in the RADIUS server list and click **Delete**.

Notes:

1. By specifying the administrator authority setting on the RADIUS server side, the same operations can be performed as when administrator authority is enabled or disabled in the local user settings. For details about these operations, see “Adding users” in “7.5.2 Specifying local user settings”.

2. For the authentication packet NAS-IP-ADDRESS of this software, the initially found IPv4 address is used among the enabled IPv4 addresses in the server to which this software is installed. Change NAS-IP-ADDRESS as required according to the following procedure.

   (1) Stop the MMController service. If this software has not been started after installation, start the MMController service, and then stop it.

   (2) Open MMController.config using the text editor. The location of MMController.config is given below.
   C:\ProgramData\AnritsuNetworks\MMController\MMController.config

   (3) Give the IPv4 address used for the NAS-IP-ADDRESS value in the RadiusFixedNASIPAddressString setting tag value.

   (4) Overwrite MMController.config and save it.

   (5) Start the MMController service.

   If the IPv4 address is wrongly given, the initially found IPv4 address is used.

7.5.4 Specifying SNMP settings

You can add, edit, or delete the destination of SNMP traps indicating over- or under-threshold events.

Open the **MMController Service** tab in the **MMAdminTool** main window, and click the **Set SNMP** button to display the **Set SNMP Servers** dialog box.

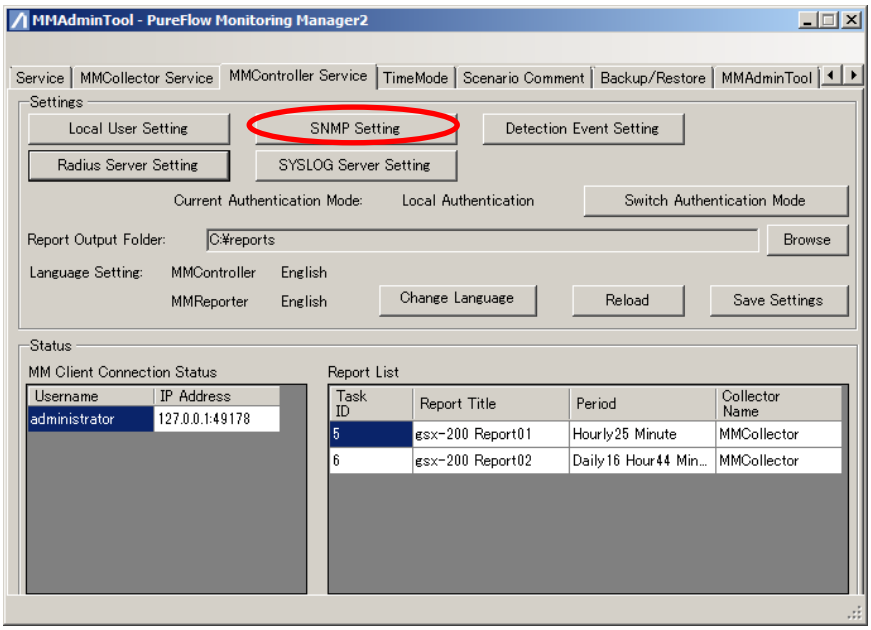


Figure 7.5.4-1 Set SNMP button

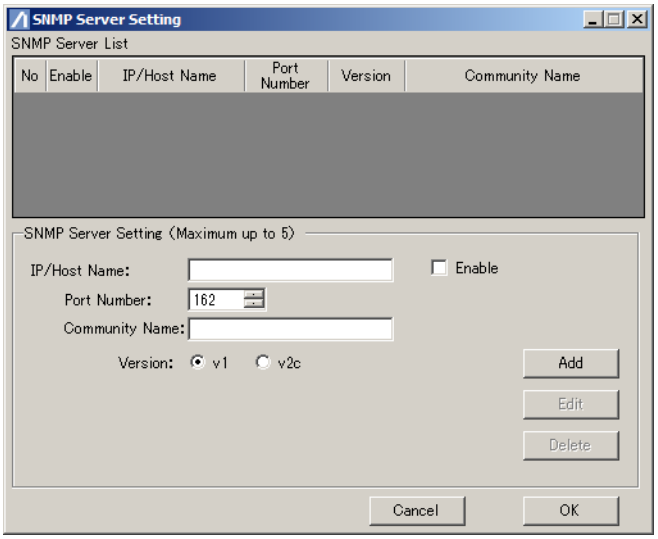


Figure 7.5.4-2 Set SNMP Servers dialog box

This dialog box shows a list of hosts to which SNMP traps are transmitted. Hosts can be added, edited, or deleted here. Up to five SNMP servers can be added.

Adding SNMP servers

IP/Host Name

Enter the host name or the IP address.

Port Number

Specify the SNMP trap UDP port No.
The default value is 162.

Community Name

Enter the SNMP community name.

Version

Specify either v1 or v2c as the SNMP version.
The default version is v1.

Enable

To enable SNMP servers, click **Enable**.

Click **Add** to add a server.

Editing SNMP servers

Select the server whose information is to be edited in the SNMP server list, edit the relevant items, and click **Change**.

Deleting SNMP servers

Select the server to be deleted in the SNMP server list and click **Delete**.

7.5.5 Specifying SYSLOG server settings

You can add, edit, or delete the destination of syslog messages indicating over- or under-threshold events.

Open the **MMController Service** tab in the **MMAdminTool** main window, and click the **Set SYSLOG Servers** button to display the **Set SYSLOG Servers** dialog box.

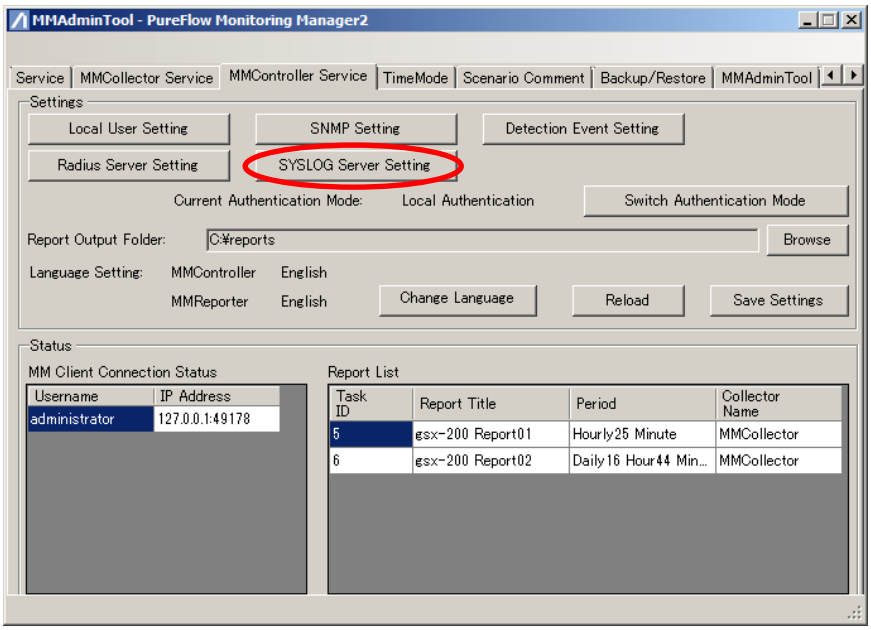


Figure 7.5.5-1 Set SYSLOG Servers button

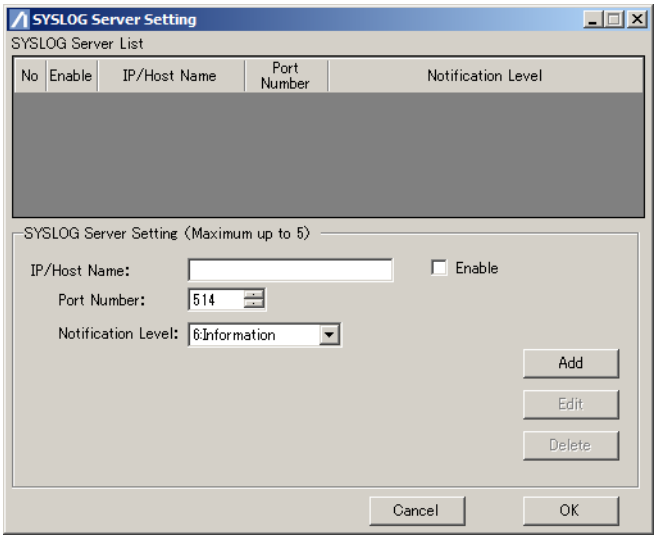


Figure 7.5.5-2 Set SYSLOG Servers dialog box

This dialog box shows the list of the hosts to which syslog messages are transmitted. Hosts can be added, edited, or deleted here. Up to five SYSLOG servers can be added.

Adding SYSLOG servers

IP/Host Name

Enter the host name or the IP address.

Port Number

Specify the port No. The default value is 514.

Notification Level

Specify the notification level. The logs below the specified level are not sent to the specified SYSLOG server.

Keyword	Severity	Level
Emergency	0	Highest
Alert	1	
Critical	2	
Error	3	
Warning	4	
Notice	5	
Information	6	Lowest

Enable

To enable SYSLOG servers, select **Enable**.

Click **Add** to add a server.

Editing SYSLOG servers

Select the server whose information is to be edited in the SYSLOG server list, edit the relevant items, and click **Change**.

Deleting SYSLOG servers

Select the server to be deleted in the SYSLOG server list and click **Delete**.

7.5.6 Specifying detection event settings

You can specify common settings for reporting over- or under-threshold events.

Open the **MMController Service** tab in the **MMAdminTool** main window, and click the **Set Detection Event** button to display the **Set Threshold Detection Notification** dialog box.

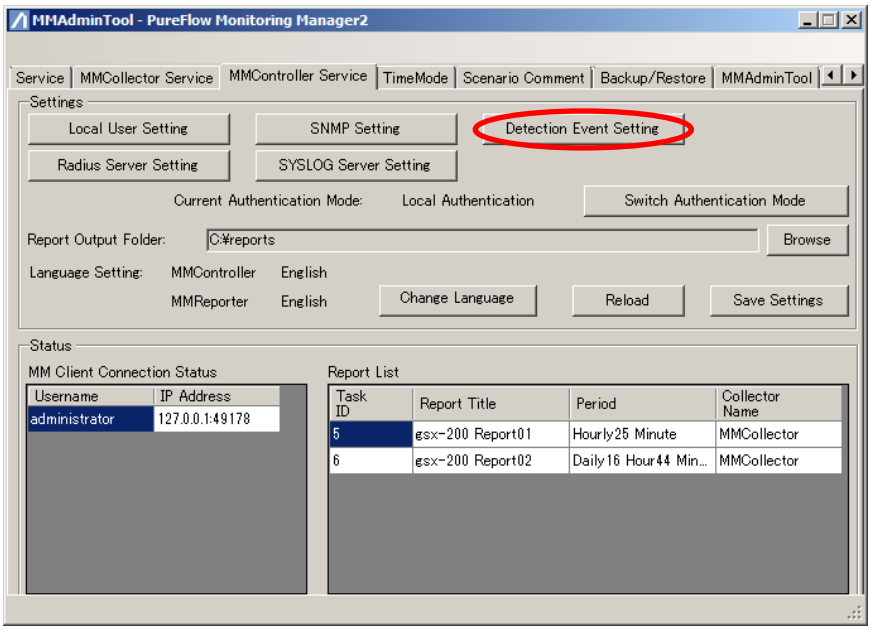


Figure 7.5.6-1 Set Detection Event button

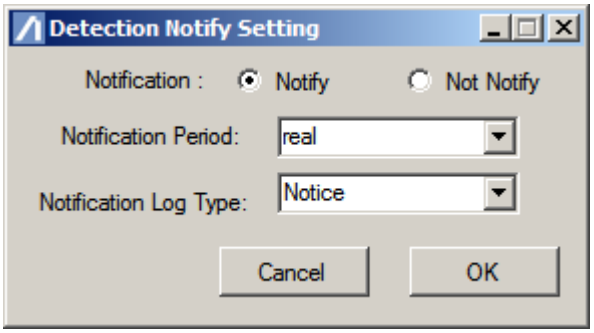


Figure 7.5.6-2 Set Threshold Detection Notification dialog box

Notification

Select **Notify** to enable over- or under-threshold event notification.
Select **Do not notify** to disable over- or under-threshold event notification.

Notification interval

Select the interval at which to report the detection of over- or under-threshold events from one of the following: **real** (real-time), **Every 5 minutes**, **Hourly**, **3-hourly**, and **Daily**.
When selecting **real** (real-time), the actual notification interval is synchronized with the interval specified for **Monitor information notification interval** in each PureFlow node. See 4.3.2 Editing the PureFlow settings to change the monitor information notification interval.

Notification log type

Select the log type for notification.

7.5.7 Specifying the report output folder

You can specify the report output folder settings.

Open the **MMController Service** tab in the **MMAdminTool** main window, and click **Browse** to specify the report output folder.

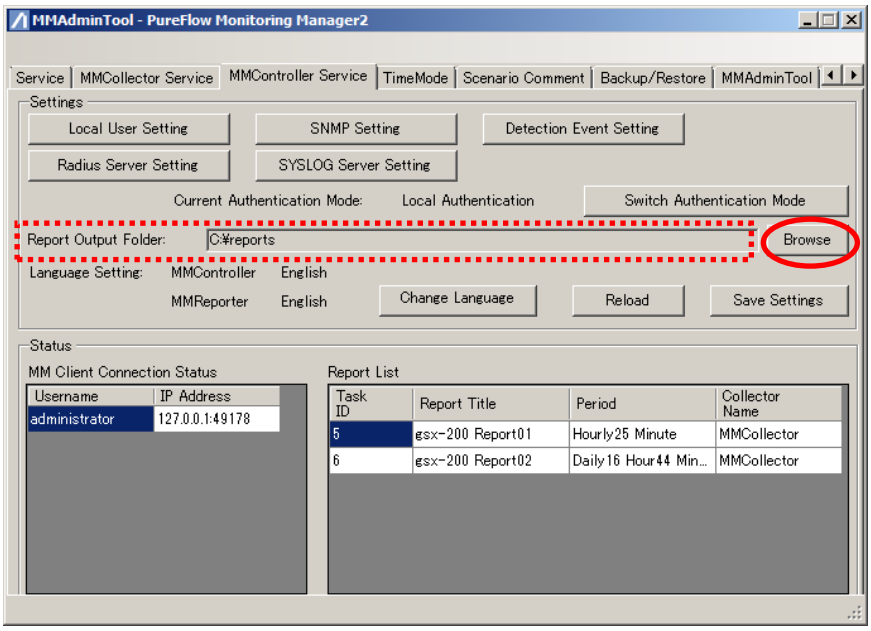


Figure 7.5.7-1 Specifying the report output folder

* Do not specify the root directory of the disk drive as the report output folder for the following reasons:

1) Reports might not be able to be output due to problems with access authority.

2) When creating a report under a root directory, the report is stored in the root directory with other system files, which makes harder to identify the report. Therefore, the user may accidentally delete system files instead of the report when attempting to delete a report.

   Example: Do not specify a drive root such as "C:\".

7.5.8 Selecting the language for the MMController and MMReporter GUI

You can select the language in which the MMController and MMReporter GUI is displayed.

Open the **MMController Service** tab in the **MMAdminTool** main window, and click **Select Language** to display the **Select Language** dialog box.

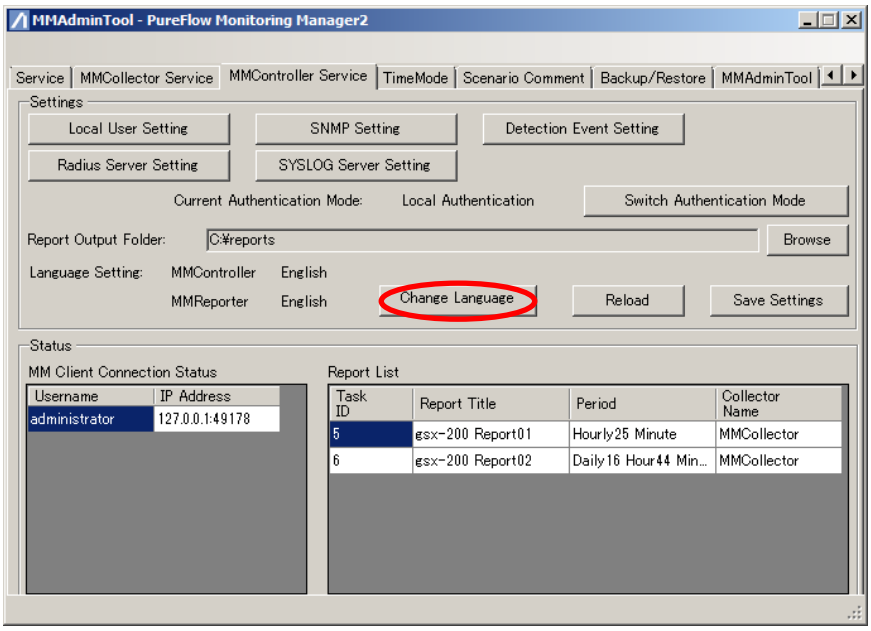


Figure 7.5.8-1 Set Language button

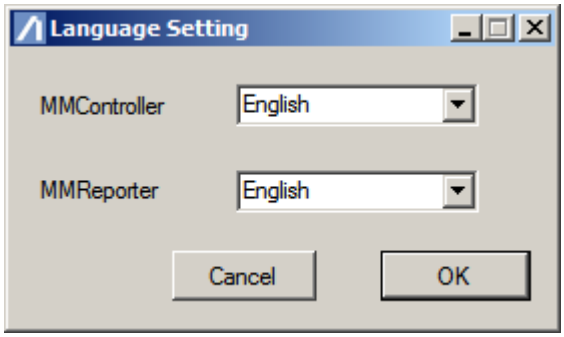


Figure 7.5.8-2 Set Language dialog box

Selecting the language

Select the language in which the MMController GUI is displayed (Japanese or English).

Select the language in which the MMReporter GUI is displayed (Japanese or English).

7.5.9 Checking the connection status and report list of MMClient

You can check the connection status and the report list of MMClient.

Open the **MMController Service** tab in the **MMAdminTool** main window to display the connection status and the report list of MMClient. The connection status and report list of MMClient can be updated by clicking the **Reload** button.

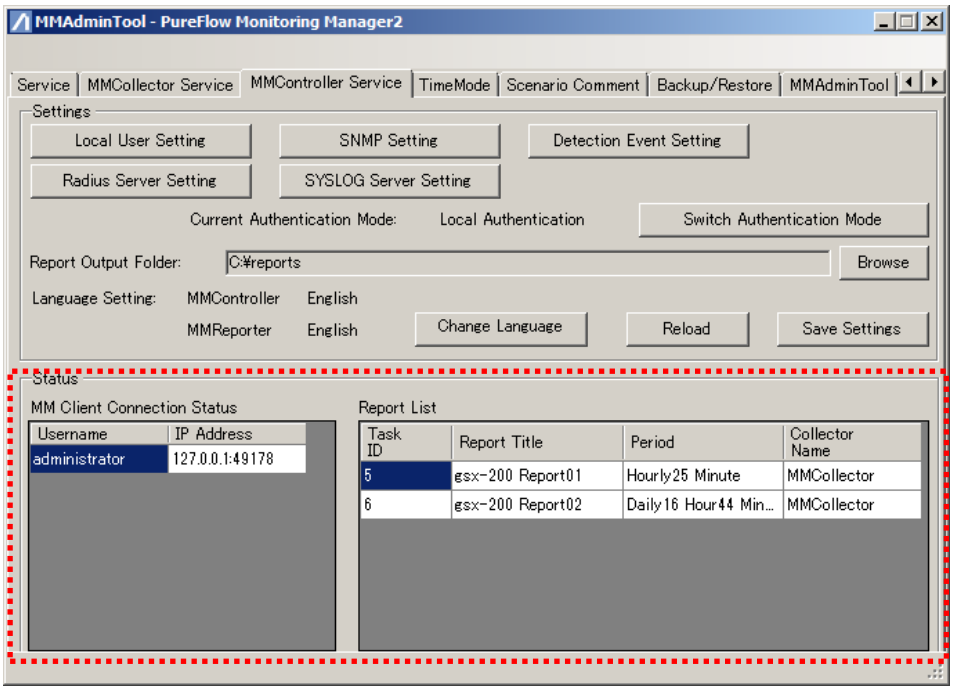


Figure 7.5.9-1 Checking the connection status and report list of MMClient

7.6 Specifying the time mode

You can check the time mode setting by selecting the **TimeMode** tab in the **MMAdminTool** main window. For details about the time modes, see Chapter 8. For how to specify the time modes, see 2.1.1 Installing the server software of PureFlow MonitoringManager2.

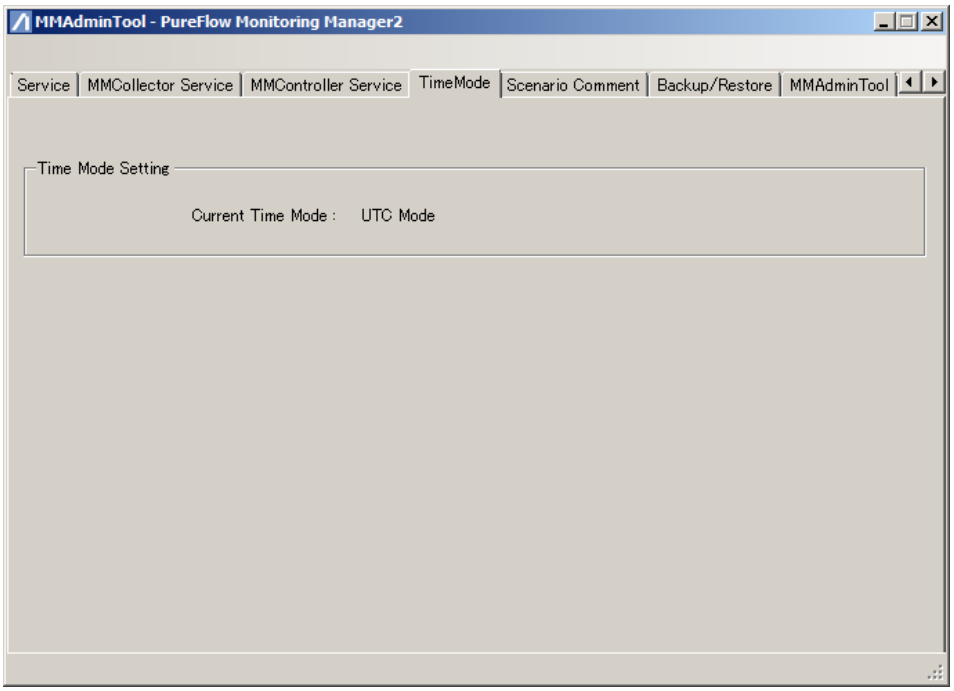


Figure 7.6-1 Set Time Mode button

Setting the time mode

UTC mode: Data is collected based on Coordinated Universal Time (UTC).
Local time mode: Data is collected based on the local time of MMServer.
Default value: UTC mode

Note:

Note that local time mode is provided to maintain compatibility with PureFlow GS1 v3.3.3 or earlier and PureFlow GSX (NF7101A) v1.1.1. Do not use this mode in the current version.

7.7 Importing and exporting the scenario comments

You can import or export the batch scenario comments by selecting the **Scenario Comment** tab in the **MMAdminTool** main window. The batch scenario comments are imported or exported in the CSV-format files used for the scenario comments as described in "7.7.3 CSV file format for scenario comments".
The software version v1.3.1 or later has this function.

7.7.1 Importing scenario comments

For the scenarios monitored by this software, the batch scenario comments are specified.

Select the [Scenario Comment] tab in the **MMAdminTool** main window, and click **Import scenario comment**.

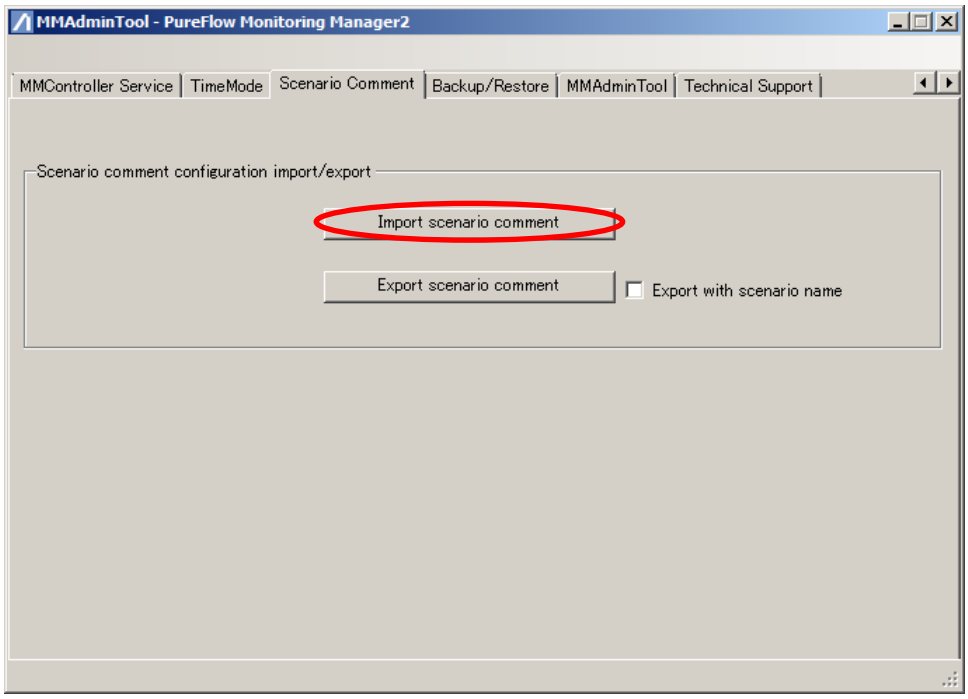


Figure 7.7.1-1 Importing scenario comments

A confirmation message appears to notify that all the scenario comments are deleted before importing, and they are replaced with the imported scenario comments. To continue import processing, click **Yes (Y)**.

Specify the CSV-format file including the scenario comment configuration. For details of the CSV file format for the scenario comments, see 7.7.3 CSV file format for the scenario comments.

Select CSV Files (*.csv) for the file type.

Click the **Open (O)** button to start import processing.

If import processing has been completed, a message to notify of completion of importing. Click **OK** to complete the processing.

If MMClient is activated, the scenario tree must be displayed again to reflect the scenario comments in the scenario tree. To display the scenario tree again, select PureFlow on the scenario tree on MMClient, right-click it, and select **Refresh**.

7.7.2 Exporting the scenario comments

You can obtain the batch scenario comments specified for the scenarios monitored by this software in the CSV file format that can be imported for the scenario comments.

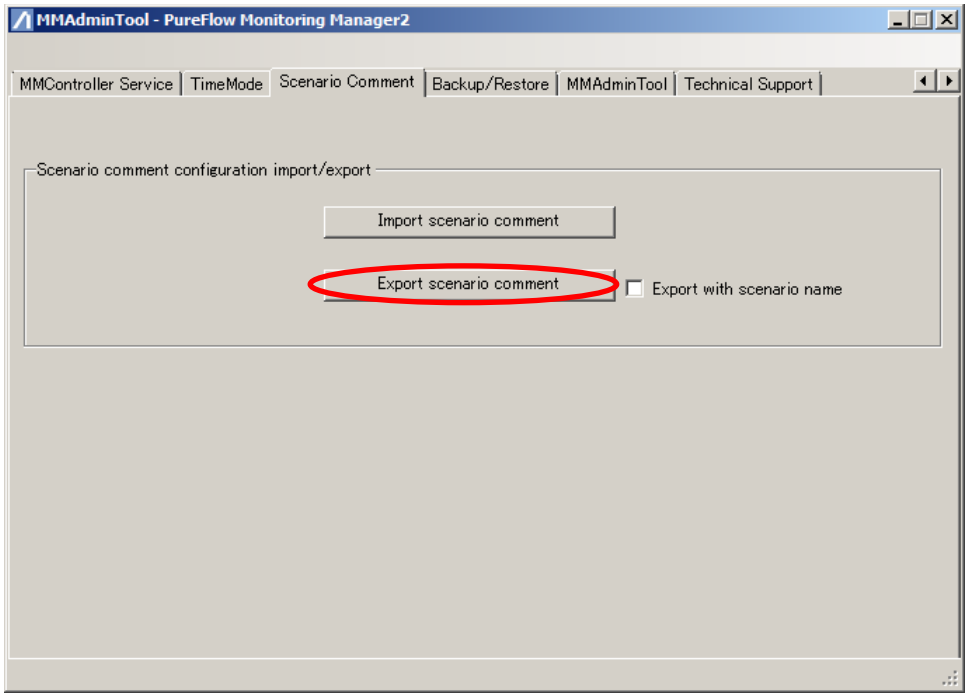


Figure 7.7.2-1 Exporting the scenario comments

Export with scenario name

If this check box is selected, the scenario name is added to the 4th column of the CSV file to be output.

Note:

When saving the file, determine the saving folder and file name so that the number of the characters including the folder path and file name does not exceed 255 bytes. Otherwise, the information may not be obtained as Windows OS restrictions stipulate that the characters of the names of the paths and files cannot exceed 255 bytes.

7.7.3 CSV file format for scenario comments

A CSV-format file is used for importing and exporting a scenario comment as described in this section. You can export the current scenario comment configuration and import the scenario comments after editing by using the spreadsheet software.

To determine the scenarios for which the scenario comments are specified, use the ID of PureFlow to which the related scenario belongs and the scenario ID. Additionally, you can add the scenario name to the CSV file by selecting the check box of the **Export with scenario name** option.

An example of description in the CSV file for the scenario comment is shown below.

```
pureflow_id,scenario_id,scenario_comment,scenario_name

1,100, base A, basepoint_a

1,101, service A, service_a

1,102, service B, service_b

1,110,,service_reserved
```

The items of the CSV file for the scenario comment are listed below.

Table 7.7.3-1 Description of the CSV items for the scenario comments

Line position	Item name	Description
1	pureflow_id	PureFlow ID
2	scenario_id	Scenario ID
3	scenario_comment	Scenario comment The contents in this column are specified as the scenario comment when importing a comment. If this column remains empty, the scenario comment setting is deleted. The current scenario comments are output for each scenario when exporting the comment. If no scenario comment is specified, this column remains empty when outputting.
4	scenario_name	Scenario name (without hierarchy) The scenario name is output when the **Export with scenario name** check box is selected for exporting the comment. The scenario name is used as the auxiliary information used for the configuration and management of the scenario comments. This item is ignored at importing a scenario comment.

Observe the following rules for the CSV files for the scenario comments as well as the normally used CSV files.

- "pureflow_id", "scenario_id", and "scenario_comment" are required items. To delete the scenario comments, "scenario_comment" can be kept empty.
- Provide either of two header lines for the first line. There must be descriptions in the CSV file to be output by exporting the scenario comment.
  pureflow_id,scenario_id,scenario_comment
  pureflow_id,scenario_id,scenario_comment,scenario_name
- Comments can be added to the CSV file for the scenario comment. Comments are not applied to scenario comment configuration. The empty line and the line starting with # are handled as the comment during import processing. Comments can be added prior to the header line. In this case, the line that does not include the initially given comment must be the header line.
- Set the file encoding to Shift_JIS. If a scenario comment is imported with other character codes, the scenario comment is not given in the normal manner.
- Use "pureflow_id" and "scenario_id" to relate the scenario to the scenario comment. "scenario_name" cannot be used.
- Up to 255 characters can be registered as a scenario comment. The word "port" cannot be used for a scenario comment. For details of the characters available for the scenario comment and for other rules, see 4.10.3 Setting scenario comments.
- The symbols ", ', \" cannot be used for the scenario comment to be imported.
- The same scenario comment as the existing scenario comment cannot be specified in the same PureFlow.
- If the scenario ID already exists in the same PureFlow, the scenario comment cannot be specified.

7.7.4 Precautions for importing scenario comments

This section describes other precautions for importing scenario comments.

1. By importing scenario comments, all the current scenario comments are deleted, and they are replaced with the imported comments. To use the current scenario comment continuously, export the current scenario comment, edit the CSV file for the exported scenario comment, and import the file.
2. The scenario comment given in the CSV file for the scenario comment but not currently registered in the scenario tree can also be specified and retained. When the PureFlow scenario is added after importing scenario comment, the retained scenario comment may be displayed. The scenario comment retained without the related scenario is sorted and deleted when editing the scenario comment for either scenario on MMClient.
3. Only for a scenario that currently exists on the scenario tree can a scenario comment be exported. Therefore, the scenario comment specified according to the scenario comment import procedure and retained without the related scenario cannot be exported.
4. Please note that the scenario ID may be replaced and the scenario comment for the assumed scenario may not be specified by deleting or adding the scenario on PureFlow GSX, WSX or WS1 since this software distinguishes the scenarios based on the scenario ID.
5. The exported CSV-format file for scenario comment has been encoded in UTF-8.

7.8 Backing up and restoring operation settings

You can back up and restore the operation settings of MonitoringManager2.
The following operation settings can be backed up and restored by using the commands described in this section:

Local user settings

RADIUS server settings

SNTP server settings

SYSLOG server settings

Detection event settings

Report output folder settings

Authentication mode

7.8.1 Backing up operation settings

Back up the operation settings of MonitoringManager2 as follows:

Open the **Backup/Restore** tab on the **MMAdminTool** main window, and click **Back Up Configuration File**.

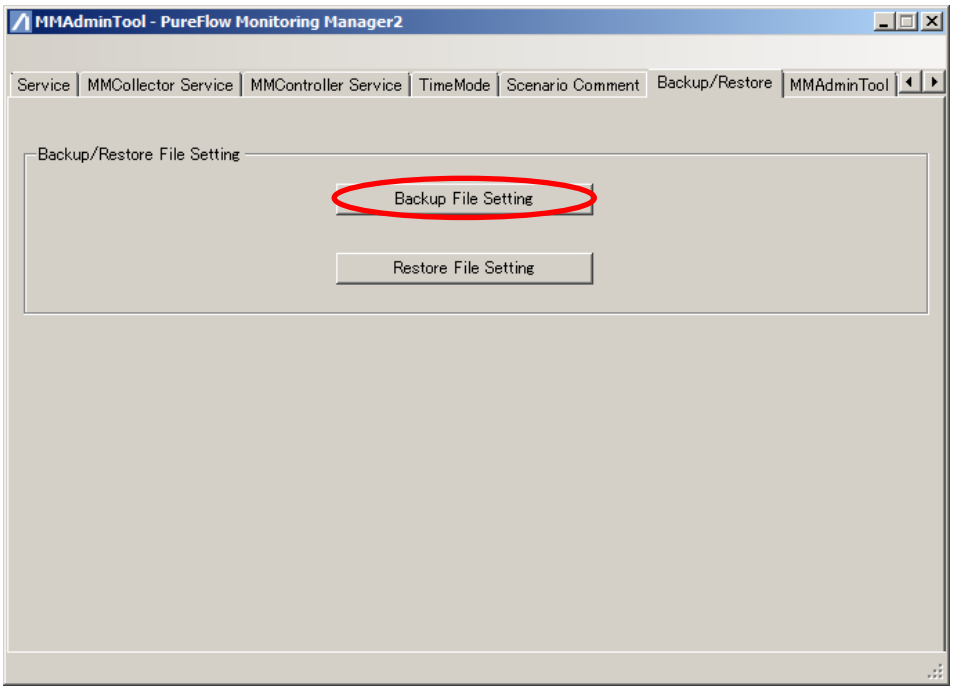


Figure 7.8.1-1 Backing up operation settings

A dialog box to specify the file to be exported is displayed.

Specify the directory and the name of the file to be saved.

Select ZIP (*.zip) for the file type.

Click **Save** to create the file.

Note:

When saving the file, determine the saving folder and file name so that the number of the characters including the folder path and file name does not exceed 255 bytes. Otherwise, the information may not be obtained as Windows OS restrictions stipulate that the characters of the names of the paths and files cannot exceed 255 bytes.

7.8.2 Restoring operation settings

Restore the operation settings of MonitoringManager2 as follows:

Open the **Backup/Restore** tab on the **MMAdminTool** main window, and click **Restore Configuration File**.

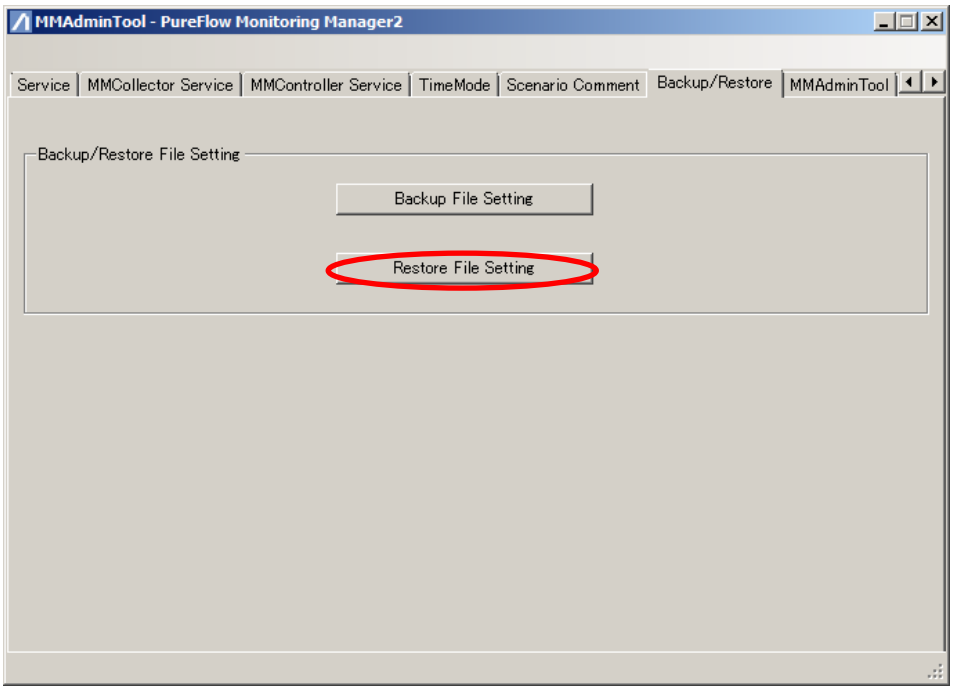


Figure 7.8.2-1 Restoring operation settings

A dialog box to specify the file to be restored is displayed.

Select the file to be restored, and click **Open**.

Once restoration is complete, click the **Service** tab and restart MMController Service. For how to restart MMController, see 7.3 Service management.

7.9 Selecting the language for MMAdminTool

You can select the language in which the MMAdminTool GUI is displayed.

Open the **MMAdminTool** tab in the **MMAdminTool** main window, select either **Japanese** or **English**, and click **OK**.

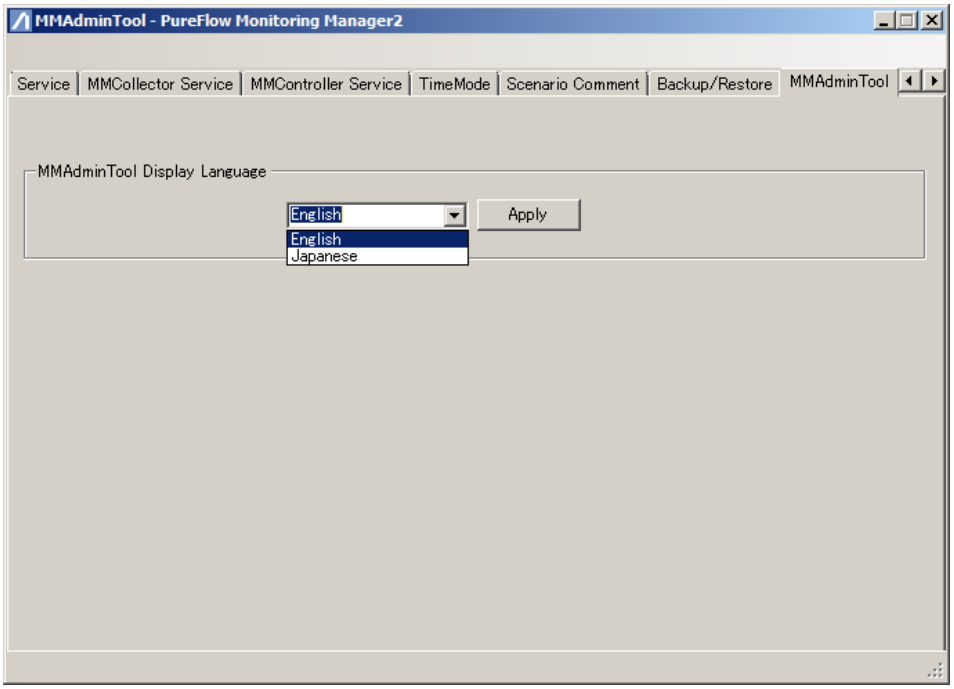


Figure 7.9-1 Selecting the language for MMAdminTool

After clicking **OK**, the language used for MMAdminTool is switched to the selected language. The default language setting is “Japanese” when using Japanese Windows and “English” when using English Windows.

7.10 Obtaining technical support information

You can obtain information for technical support.
Open the **Technical Support** tab in the **MMAdminTool** main window.

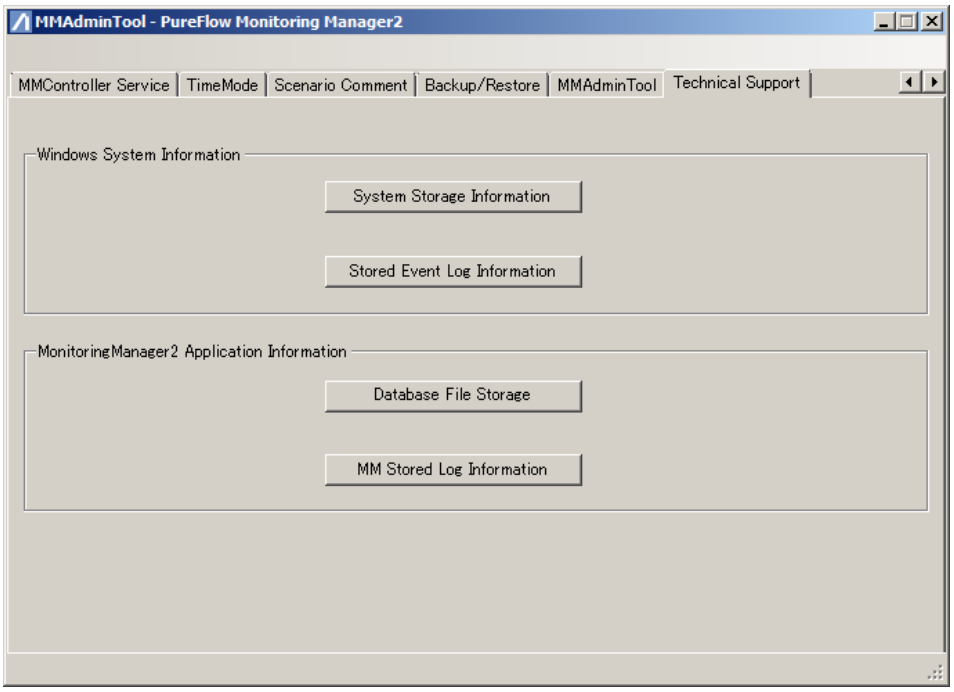


Figure 7.10-1 Obtaining technical support information

Note:

When saving the file, determine the saving folder and file name so that the number of the characters including the folder path and file name does not exceed 255 bytes. Otherwise, the information may not be obtained as Windows OS restrictions stipulate that the characters of the names of the paths and files cannot exceed 255 bytes.

7.10.1 Obtaining system information

You can obtain information about the system on which MonitoringManager2 is running.
Click **Save system information**. A confirmation dialog box will open.
Select the directory and the name of the file in which the information is to be saved, and click **Save**.

7.10.2 Obtaining event log information

You can obtain information about the event logs related to MonitoringManager2.
Click **Save event log information**. A confirmation dialog box will open.
Select the directory and the name of the file in which the information is to be saved, and click **Save**.

7.10.3 Obtaining database files

You can obtain information about the database of MonitoringManager2 on a table by table basis.
Click **Save database file information**. A confirmation dialog box will open.
Select the directory and the name of the file in which the information is to be saved, and click **Save**.

Note:

To execute this function, startup of MMSql Service is required. For how to start up MMSql Service, refer to "7.3 Service management".

7.10.4 Obtaining MM log information

You can obtain information about the MM logs of MonitoringManager2.
Click **Save MM log information**. A confirmation dialog box will open.
Select the directory and the name of the file in which the information is to be saved, and click **Save**.

Note:

For the log information to be obtained, the longer the running time is, the larger the file size is. It might take a few minutes to obtain the requested information. Although operations might not be able to be executed during the above process, this phenomenon is not an error. Therefore, be sure not to execute any operations until all the requested information is obtained.

7.11 Exiting MMAdminTool

To exit MMAdminTool, click the **Close (×)** button on the active title bar.

7.11.1 Exiting by using the task tray icon

If MMAdminTool is displayed as a task tray icon, right-click the task tray icon, and click **Exit**.

Figure 7.11.1-1 Exiting by using the task tray icon

(Blank page)

This chapter describes the time mode settings in MonitoringManager2.

8.1 Overview

A time mode setting feature is provided in MonitoringManager2 to support different time zones and the daylight saving time used in Europe, North America, and other countries. The time modes are UTC mode and local time mode.

If MonitoringManager2 is used in a region with a different time zone, a time difference will occur when data is collected. In UTC mode, the time difference is absorbed by converting the time at which the data was collected by the server to Coordinated Universal Time (UTC) before sending the data to the connected client computer. The time stamp of the sent data is then converted to the local time of the client computer. This mechanism is known as UTC mode.

Note that local time mode is provided to maintain compatibility with PureFlow GS1 v3.3.3 or earlier and PureFlow GSX (NF7101A) v1.1.1.In local time mode, the time zone of the server is used when collecting data. Even if a time difference occurs during data collection, the time is not adjusted.

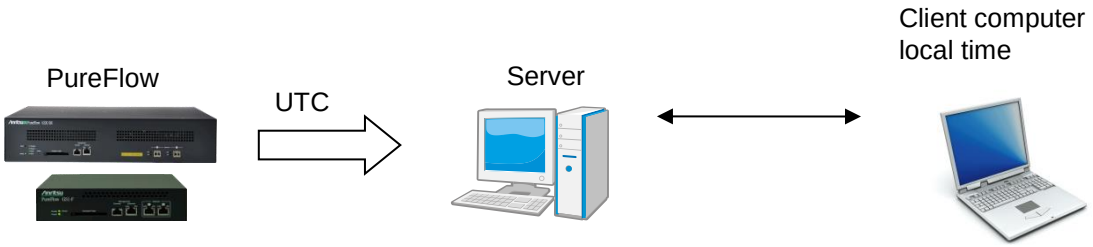


Figure 8.1-1 UTC mode

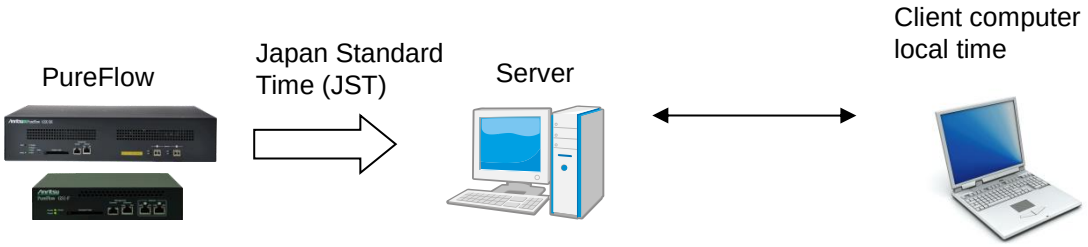


Figure 8.1-2 Local time mode

8.2 Graph display during daylight saving time

Graphs displayed by MonitoringManager2 are based on the local time of the computer in which the client software is installed. However, when daylight saving time starts (at the start of spring) and ends (at the end of autumn), graphs are displayed using a special method.
The way graphs are displayed at the start of spring and the end of autumn when MonitoringManager2 is used in a region that uses Pacific Standard Time is shown below.

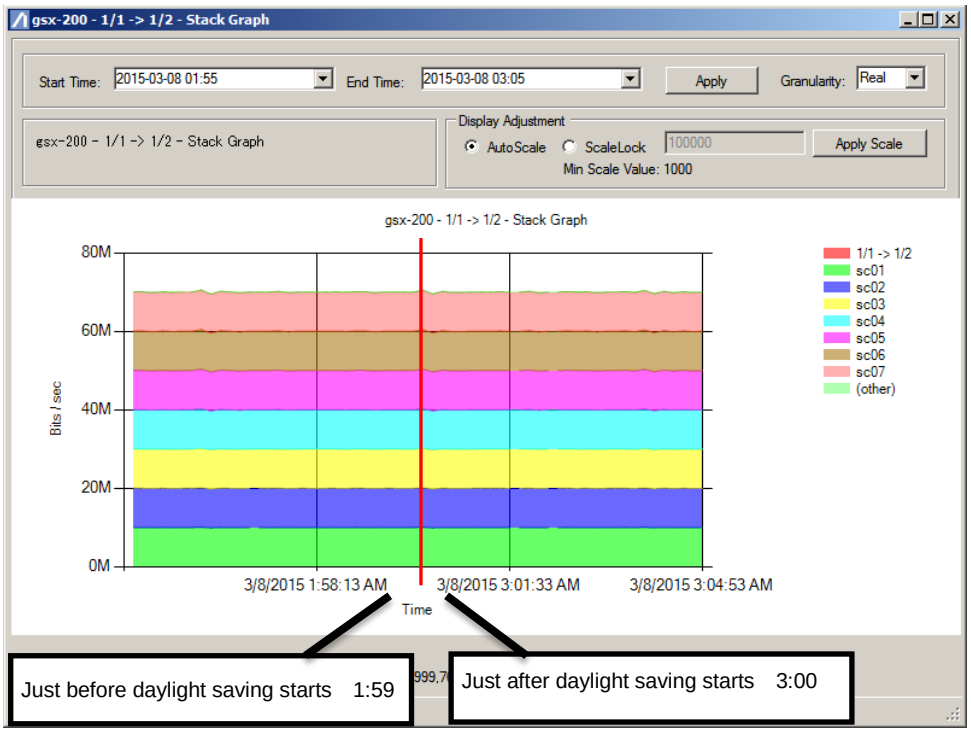


Figure 8.2-1 Graph showing the start of daylight saving

At the start of spring, data collected between 02:00 and 03:00, which is when daylight saving time starts, is not displayed, and the time skips from 01:59 to 3:00.

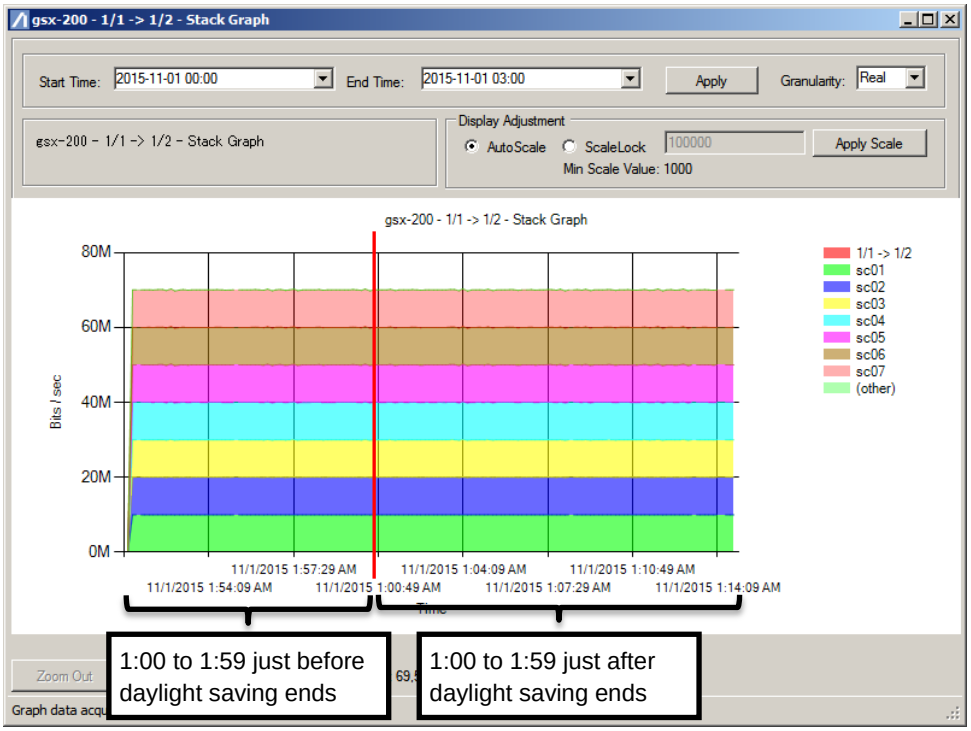


Figure 8.2-2 Graph showing the end of daylight saving

At the end of autumn, the period between 01:00 and 01:59 is displayed twice in succession.

8.3 Report creation during daylight saving time

Graphs displayed by MonitoringManager2 are based on the local time of the server in which the server software is installed.

For example, if a report is specified to be created at 05:30 everyday, the report will be created when the time of the OS used by the server reads 05:30.The report is created at this time regardless of whether the region in which the server is being used is currently operating on standard time or daylight saving time. However, if the report is specified to include a time period that is either skipped due to the start of daylight saving (at the start of spring) or is duplicated due to the end of daylight saving (at the end of autumn), the report will be output in a special format. The figures below show how the time changes at the start and end of daylight saving time.

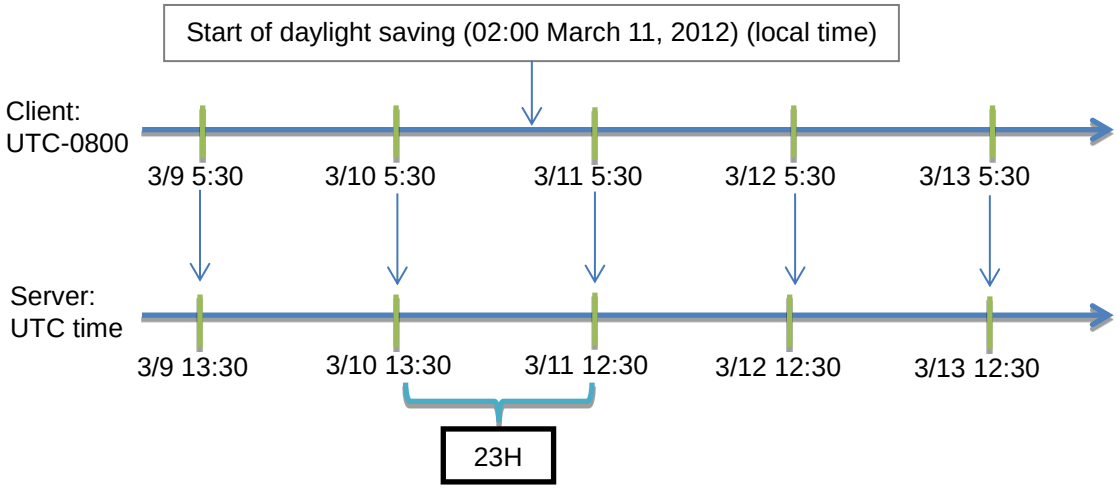


Figure 8.3-1 Change of time at the start of daylight saving time

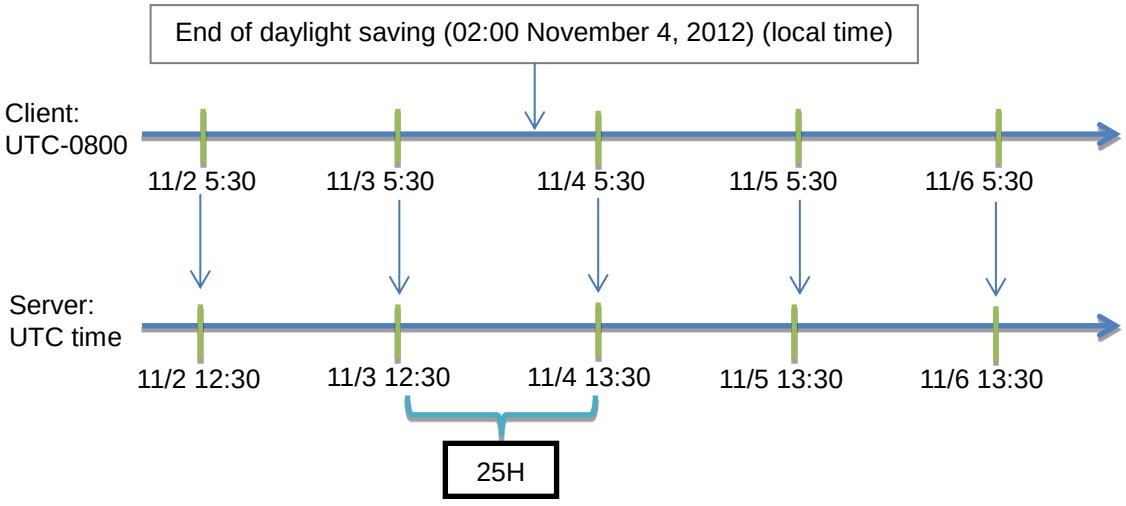


Figure 8.3-2 Change of time at the end of daylight saving time

As you can see in Figure 8.3-1, a report whose time span includes the start of daylight saving time does not include data from 02:00 to 03:00 on March 11th, and is therefore one hour shorter than normal. This behavior also occurs in the weekly report.
Also, as you can see in Figure 8.3-2, a report whose time span includes the end of daylight saving time include two sets of data from 02:00 to 03:00 on November 4th, and is therefore one hour longer than normal. This behavior also occurs in the weekly report.

Note:

MonitoringManager2 usually creates a graph based on a time axis (time), regardless of whether data exists or not. However, because the time axis is created based on data, if hourly and daily reports whose time span includes the start or end of daylight saving time include periods in which there is no data for reasons such as a server shutdown or node disconnection, a discrepancy can occur in the time axis, making the graph appear incorrect. Examples of graphs in which the time axis appears normal and then compacted due to the occurrence of a period with no data at the start of daylight saving are shown below.

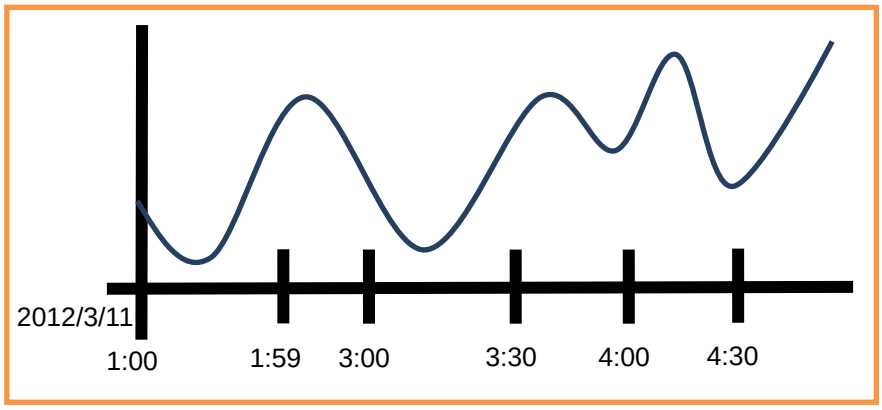


Figure 8.3-3 Graph at the start of daylight saving

A period with no data has occurred between 03:30 and 04:00 in the graph in Figure 8.3-3. If the time axis of the graph is displayed normally, the graph will look like the graph in Figure 8.3-4 below.

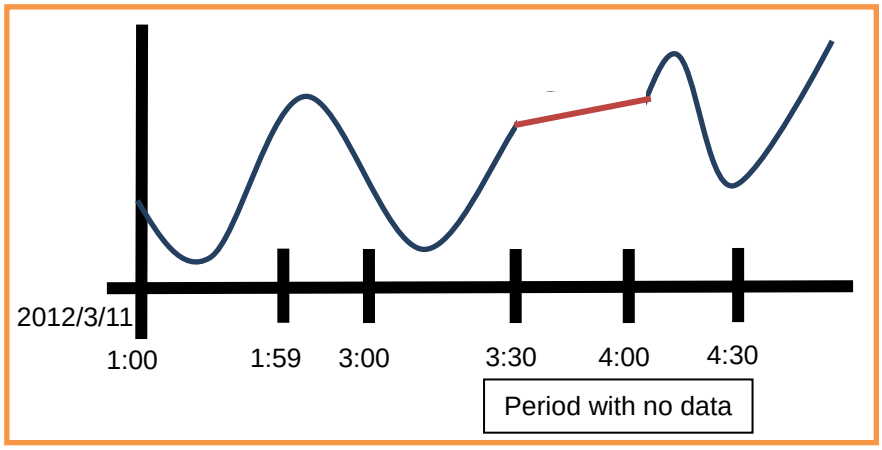


Figure 8.3-4 Graph with time axis displayed normally

As you can see in Figure 8.3-4, if the time axis is linear, the period with no data is shown as a straight line.
However, if the time axis is compacted, the graph looks like the graph in Figure 8.3-5 below.

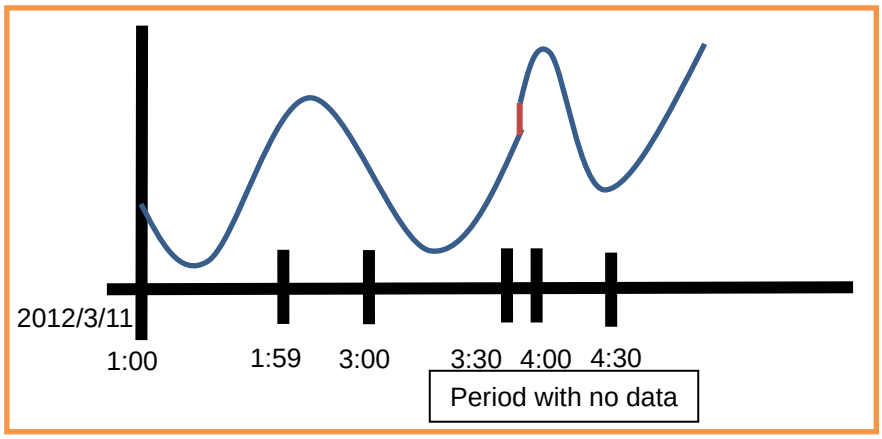


Figure 8.3-5 Graph with time axis compacted

As you can see in Figure 8.3-5, if the time axis is compacted, the period with no data is shown as a vertical line.

8.4 Specifying the time mode and displaying time mode information

For how to specify the time mode, see 2.1.1 Installing the server software of PureFlow MonitoringManager2.

8.4.1 Displaying time mode information

Information about the time mode can be found by selecting **Help** then **About time mode** on the menu bar.

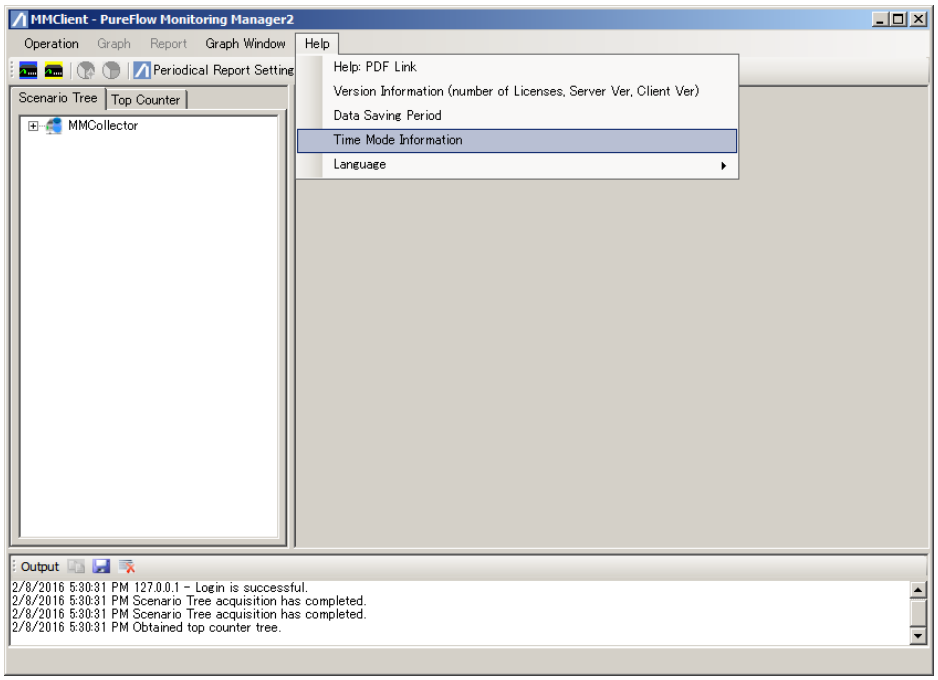


Figure 8.4.1-1 Time mode information

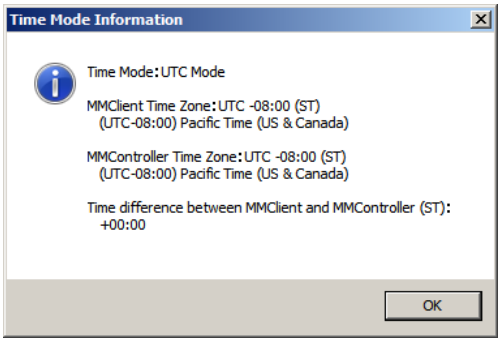


Figure 8.4.1-2 Time mode information dialog box

Reports record the local server time, so the client needs to ascertain the local server time. If the time mode is UTC mode, the difference between the current time of the client computer and the local server time can be checked by the client software from the time mode information, enabling the client to ascertain the local server time.
If the time mode is local time mode, the time difference is displayed, but because local time mode is only provided for compatibility with PureFlow GS1 v3.3.3 or earlier and PureFlow GSX (NF7101A) v1.1.1, if MonitoringManager2 is being used in a region operating in a different time zone, reports will not be output and graphs will not be displayed correctly.

Appendix A Third Party Software License

Apache log4net 1.2.10
(http://logging.apache.org/log4net/index.htmllog4net.dll)

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and limitations under the License.

Command Line Parser Library 1.8.0.0 (http://commandline.codeplex.com/CommandLine.dll)

License: The MIT License (MIT)
Copyright (c) 2005 - 2010 Giacomo Stelluti Scala

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DotNetZip Library1.9.1.5
(http://dotnetzip.codeplex.com/IonicZip.dll)

Microsoft Public License (Ms-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions
   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights
   (A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

   (B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations
   (A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

   (B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

   (C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

   (D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

(Blank page)

Appendix B List of syslog Messages

Table B-1 lists the syslog messages.

Syslog messages are output to registered hosts that the host notification level is higher or equal to the notification log type. Severity of a syslog message on Table B-1 replaces to the notification log type. Default of the notification log type is Notice.

For reference:

Some syslog messages have a hexadecimal number in brackets ([ ] or < >) added. The hexadecimal number in the brackets indicates the location in the source code or the variable value, which Anritsu will use for troubleshooting.

Table B-1 Syslog list

Severity	Syslog message	Occurs when	Action
Notice (5)	Upper threshold overflow [Host=xxx.xxx.xxx.xxx #S Threshold=#N Traffic=#M]	The amount of traffic exceeds the rate upper limit. (The volume of traffic is displayed in units of bytes per second ("Bps") or bits per second ("bps")).	Check the state of traffic flowing to ports or scenarios and make sure all the settings are correct.
	Upper threshold underflow [Host=xxx.xxx.xxx.xxx #S Threshold=#N Traffic=#M]	The amount of traffic falls below the rate upper limit. (The volume of traffic is displayed in units of bytes per second ("Bps") or bits per second ("bps")).	Check the state of traffic flowing to ports or scenarios and make sure all the settings are correct.
	Lower threshold overflow [Host=xxx.xxx.xxx.xxx #S Threshold=#N Traffic=#M]	The amount of traffic rises above the rate lower limit. (The volume of traffic is displayed in units of bytes per second ("Bps") or bits per second ("bps")).	Check the state of traffic flowing to ports or scenarios and make sure all the settings are correct.
	Lower threshold underflow [Host=xxx.xxx.xxx.xxx #S Threshold=#N Traffic=#M]	The amount of traffic falls below the rate lower limit. (The volume of traffic is displayed in units of bytes per second ("Bps") or bits per second ("bps")).	Check the state of traffic flowing to ports or scenarios and make sure all the settings are correct.

(Blank page)

Table C-1 lists the SNMP traps.

Traps are output to the registered SNMP trap destination.

Table C-1 SNMP Trap List

MIB object name (OID)	Occurs when	Action
pfMmUpperThresholdOverflowEvent (1.3.6.1.4.1.1151.2.1.9.20.0.1)	The amount of traffic exceeds the rate upper limit.	Check the state of traffic flowing to ports or scenarios and make sure all the settings are correct.
pfMmUpperThresholdUnderflowEvent (1.3.6.1.4.1.1151.2.1.9.20.0.2)	The amount of traffic falls below the rate upper limit.	Check the state of traffic flowing to ports or scenarios and make sure all the settings are correct.
pfMmLowerThresholdOverflowEvent (1.3.6.1.4.1.1151.2.1.9.20.0.3)	The amount of traffic rises above the rate lower limit.	Check the state of traffic flowing to ports or scenarios and make sure all the settings are correct.
pfMmLowerThresholdUnderflowEvent (1.3.6.1.4.1.1151.2.1.9.20.0.4)	The amount of traffic falls below the rate lower limit.	Check the state of traffic flowing to ports or scenarios and make sure all the settings are correct.

SNMP Trap: Conditions of trap raises and correspond MIB object.

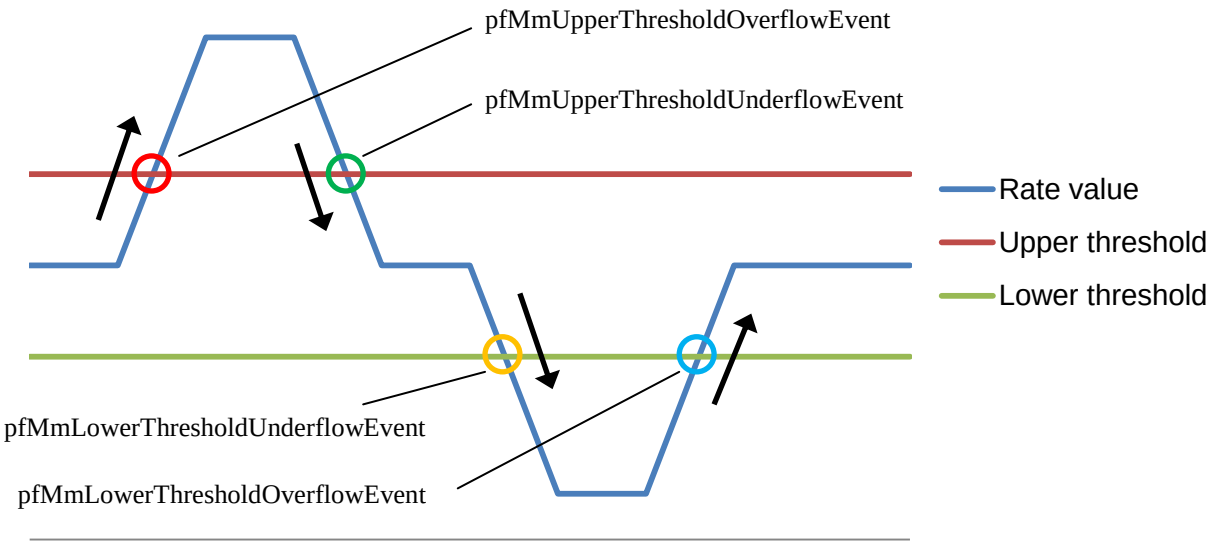


Table C-2 lists the informed objects with SNMP Traps.

Table C-2 Informed objects with SNMP Traps

MIB object name（OID）	Informed objects（OID）	Description
pfMmUpperThresholdOverflowEvent (1.3.6.1.4.1.1151.2.1.9.20.0.1)	pfMmGsHostname (1.3.6.1.4.1.1151.2.1.9.1.1.1.1)	Detected host name or IP address.
	pfMmScenarioThresholdScenarioIndex (1.3.6.1.4.1.1151.2.1.9.1.1.1.2)	Detected the index of the scenario or port.
	pfMmScenarioThresholdUpperThreshold (1.3.6.1.4.1.1151.2.1.9.1.1.1.3)	Detected upper threshold of the scenario or port.
	pfMmThresholdTrafficRate (1.3.6.1.4.1.1151.2.1.9.1.1.1.5)	Detected the traffic rate of the scenario.
pfMmUpperThresholdUnderflowEvent (1.3.6.1.4.1.1151.2.1.9.20.0.2)	pfMmGsHostname (1.3.6.1.4.1.1151.2.1.9.1.1.1.1)	Detected host name or IP address.
	pfMmScenarioThresholdScenarioIndex (1.3.6.1.4.1.1151.2.1.9.1.1.1.2)	Detected the index of the scenario or port.
	pfMmScenarioThresholdUpperThreshold (1.3.6.1.4.1.1151.2.1.9.1.1.1.3)	Detected upper threshold of the scenario or port.
	pfMmThresholdTrafficRate (1.3.6.1.4.1.1151.2.1.9.1.1.1.5)	Detected the traffic rate of the scenario.
pfMmLowerThresholdOverflowEvent (1.3.6.1.4.1.1151.2.1.9.20.0.3)	pfMmGsHostname (1.3.6.1.4.1.1151.2.1.9.1.1.1.1)	Detected host name or IP address.
	pfMmScenarioThresholdScenarioIndex (1.3.6.1.4.1.1151.2.1.9.1.1.1.2)	Detected the index of the scenario or port.
	pfMmScenarioThresholdLowerThreshold (1.3.6.1.4.1.1151.2.1.9.1.1.1.4)	Detected lower threshold of the scenario or port.
	pfMmThresholdTrafficRate (1.3.6.1.4.1.1151.2.1.9.1.1.1.5)	Detected the traffic rate of the scenario.
pfMmLowerThresholdUnderflowEvent (1.3.6.1.4.1.1151.2.1.9.20.0.4)	pfMmGsHostname (1.3.6.1.4.1.1151.2.1.9.1.1.1.1)	Detected host name or IP address.
	pfMmScenarioThresholdScenarioIndex (1.3.6.1.4.1.1151.2.1.9.1.1.1.2)	Detected the index of the scenario or port.
	pfMmScenarioThresholdLowerThreshold (1.3.6.1.4.1.1151.2.1.9.1.1.1.4)	Detected lower threshold of the scenario or port.
	pfMmThresholdTrafficRate (1.3.6.1.4.1.1151.2.1.9.1.1.1.5)	Detected the traffic rate of the scenario.

※Table C-3 lists the values of pfMmScenarioThresholdScenarioIndex. The type of all values are OCTET STRING.

Table C-3 Values of pfMmScenarioThresholdScenarioIndex

	Network port				Port scenario			
	Port 1	Port 2	Port 3	Port 4	Port 1	Port 2	Port 3	Port 4
GS1	1/1->1/2	1/2->1/1						
GSX	1/1->1/2	1/2->1/1						
WSX QoS	1/1->1/2	1/2->1/1						
WSX TCP	1/1	1/2	1/3	1/4	40001	40002	40003	40004
WS1	1/1	1/2	1/3	1/4	4097	4098	4099	4100

(Blank page)

Appendix D Online Backup Command

This section describes how to use the online backup and restore commands.

Backup command mmbackup.exe

Overview This command outputs all the log and configuration data of MonitoringManager2 to a single folder for backup purposes. You can specify the data to be backed up and the target period.

Execution example:

> mmbackup.exe --all

> mmbackup.exe --target real 5min --range 2012.04.01.00:00:00_2012.04.02.00:00:00

> mmbackup.exe -c command.txt

> mmbackup.exe -t real -p c:¥mmbak -l 20120402.log

Options

-a --all Back up all the configuration and log data of MonitoringManager2.

-l --log [filepath] Output detailed execution logs to a file.
Default: Do not output logs to a file.

Note:

If an error occurs during backup, logs might not be output.
To check whether logs have been output or not, check the data output to the console, or check the OS event viewer.

-t --target [setting | real | 5min | 1hour | 3hour | 1day | top | peak]
Specifies which database data is to be backed up.
Example: --target real 5min
Do not back up configuration tables; back up real-time logs and 5-minute logs.
--target setting real peak
Back up configuration tables, real-time logs, and peak logs.
When backing up configuration tables, also back up task scheduler data.
Default: Back up all data that can be backed up when the program is executed.

-r --range [from]_[to]
Specifies which period of data is to be backed up.
Data in the period from [from] to [to] is backed up.
[from] and [to] must be specified in the following format.
YYYY.MM.DD.hh:mm:ss
Example: --range 2012.04.01.00:00:00_2012.04.02.00:00:00
Default: Back up all existing data.

-b --base-folder [folderpath]

Specifies the base folder of the backup folder.
Example: --base-folder 'c':¥mmbak
Default: Create the backup folder under the program execution folder.

-f --folder [foldername]

Specifies the name the backup folder.
Specify the name the folder in which the data to be backed up will be output.
Example: --folder real_backup
--folder 20120401_real_setting
Default: Use the program execution date and time as the folder name.
The format is: YYYYMMDD.hhmmss

-c --command-file Load the option specifications from the command file. Use database folder path that specified in installing server software. If you use default database folder path, specifies following.
"C:¥Program Files¥AnritsuNetworks¥MMSql¥MM2Database"
If this option is specified, all options specified on the command line are ignored.
Default: Only use options specified on the command line.

--db-path Specifies clearly the folder where the database is saved.
If this option is specified, the folder where the database is saved is not searched automatically.
Example) --db-path D:¥mm2¥database
Default: The folder where the database is saved is searched automatically.

-h --help Output the Help file. (Do not perform backup.)

-q --quiet Minimize the execution logs (only include execution date and time and the error logs).
This option is ignored when the -l option (“output detailed execution logs to a file”) is specified.
Default: Show all possible data in the standard output.

Return value 0: Backup finished without error.
Other than 0: An error occurred during backup.

Note:

A very large amount of data might be backed up and backup might take a long time depending on the number of nodes and scenarios managed by MonitoringManager2, and the specified data storage period.
Make sure you consider the disk capacity and load on the server when executing this command.

Restore command mmrestore.exe

Overview This command restores the data backed up by using the mmbackup.exe command. Execute this command after specifying the data to be restored or the folder in which the data to be restored is stored.

Execution example:

> mmrestore.exe --base-folder c:¥mmbak¥

> mmrestore.exe -f c:¥mmbak¥20120401000000 c:¥mmbak¥20120402000000

Options

-l --log [filepath] Output execution logs to a file.
Default: Do not output logs to a file.

Note:

If an error occurs during restoration processing, the log may not be output.
In this case, output the log to the console, or check the OS event viewer.

-b --base-folder [folderpath]
Specifies the base folder from which data is to be restored.
Example: --base-folder c:¥mmbak
Restore all the data in the c:¥mmbak folder.
Default: Restore all the backup data from the base folder under the program execution folder.

-f --folder [folderpath,(folderpath,..)]
Specifies the backup folder from which data is to be restored.
More than one folder can be specified. Data is restored starting from the folders specified first (starting from the folders specified on the left).
Data restored later overwrites data restored earlier if data is duplicated when multiple folders are specified.
Example: --folder c:¥mmbak¥20120401000000
Restore the data in the c:¥mmbak¥20120401000000 folder.
--folder c:¥mmbak¥20120401000000 c:¥mmbak¥20120402000000
Restore the data in the c:¥mmbak¥20120401000000 folder and the c:¥mmbak¥20120402000000 folder.
Default: Execute the command assuming this option has not been specified.(That is, execute the command in the same way as when the --base-folder option is not specified.)

-c	--command-file	Load the option specifications from the command file. If this option is specified, all options specified on the command line are ignored. Default: The command file is not specified, so only use options specified on the command line.
	--db-path	Specifies clearly the folder where the database is saved. Use database folder path that specified in installing server software. If you use default database folder path, specifies following. "C:¥Program Files¥AnritsuNetworks¥MMSql¥MM2Database" If this option is specified, the folder where the database is saved is not searched automatically. Example) --db-path D:¥mm2¥database Default: The folder where the database is saved is searched automatically.
-h	--help	Output the Help file. (Do not perform restoration.)
-q	--quiet	Minimize the execution logs (only include execution date and time and the error logs). Default: Show all possible log data in the standard output.
Return value		0: Restoration finished without error. Other than 0: An error occurred during restoration.

The following table shows the creation colors and RGB set values.

Table E-1 Color name and RGB

Creation color	Set value			Remarks	
	R	G	B	HTML color name	HTML color code
■	0	0	0	black	#000000
■	0	0	128	navy	#000080
■	0	0	255	blue	#0000ff
■	0	128	0	green	#008000
■	0	128	128	teal	#008080
■	0	191	255	deepskyblue	#00bfff
■	0	255	0	lime	#00ff00
■	0	255	127	springgreen	#00ff7f
■	0	255	255	cyan	#00ffff
■	123	104	238	mediumslateblue	#7b68ee
■	127	255	0	chartreuse	#7fff00
■	127	255	212	aquamarine	#7fffd4
■	128	0	0	maroon	#800000
■	128	0	128	purple	#800080
■	128	128	0	olive	#808000
■	128	128	128	gray	#808080
■	148	0	211	darkviolet	#9400d3
■	224	255	255	lightcyan	#e0ffff
■	255	0	0	red	#ff0000
■	255	0	255	mgenta	#ff00ff
■	255	20	147	deeppink	#ff1493
■	255	128	128	salmon	#ff8080
■	255	140	0	darkorange	#ff8c00
■	255	240	245	lavenderblush	#fff0f5
■	255	250	205	lemonchiffon	#fffacd
■	255	255	0	yellow	#ffff00
□*	255	255	255	white	#ffffff

* The frame does not appear.

Note:

Transparency is set in the specified color, and then the color appears (50% by default). Change the color transparency settings as required according to the following procedure. Change the setting after exiting the client software.

1. Open MMClient.config using the text editor.
   The location of MMClient.config is given below.
   C:¥ProgramData¥AnritsuNetworks¥MMClient¥MMClient.config

2. Change the value of GraphCSVAlpha configuration tag.

3. Overwrite MMClient.config and save it.

Appendix F Event Viewer Message List

This section describes the messages displayed in the OS event viewer.

The following table shows the messages displayed in the event viewer related to the backup tool.

Table F-1 Backup tool message list

Event ID	Level	Error message	Command return value	Description	Countermeasures
19901	Error	Unhandled Exception occurred. It caught on top level of program.	-1	An unexpected error has occurred.	Contact an Anritsu Networks Co., Ltd. sales office.
16101	Error	[main] MMSQL Service does not running ! abort backup process.	-1	MMSql Service has not started up.	Start up MMSql Service, and execute it.
14301	Error	DB access parameter does not found.	-1	Access to the database cannot be allowed.	Contact an Anritsu Networks Co., Ltd. sales office.
15201	Error	Failed to access db.	-1		
14301	Error	[main] DB instance path is invalid. path = {DB folder path}	-1		
14301	Error	[main] Failed to find DB instance path setting. backup aborted.	-1		
14101	Error	Failed to parse option string.	-1	An option is wrongly specified.	Specify an option correctly.
14101	Error	backup - backup range parameter is invalid ! (start {Start date} > end {End date})	-1	When the time is specified by the range option, "from" and "to" are placed in reverse.	Specify the time so that the time in "from" is earlier than the time in "to".
15101	Error	Backup log table [{Table name}] - failed to get id1log.	-1	Obtaining the backup data has failed.	Contact an Anritsu Networks Co., Ltd. sales office.
15201	Error	[main] DB Move failed ! DB Base = {Saved DB name (pure2)}, DBName = {Temporary DB name}	-1	Copying the database has failed.	Contact an Anritsu Networks Co., Ltd. sales office.
14301	Error	[main] {Program name} config does not exists. backup skipped.	-1	Obtaining the software configuration file has failed.	Contact an Anritsu Networks Co., Ltd. sales office.
14301	Error	[main] mmsql.ini does not exists !!! checked path = {mmsql.ini path}	-1	The database configuration file cannot be found.	Contact an Anritsu Networks Co., Ltd. sales office.

Event ID	Level	Error message	Command return value	Description	Countermeasures
15301	Error	[main] task file {Task name} saved as {Renamed task name}, It ignored when restore backup data.	-1	Saving the report configuration file has failed.	Check the access right to the backup destination folder.
14301	Error	[main] file that append to list but not exists on filesystem ! path = {Backup file path}	-1	Some backup results are misaligned.	Contact an Anritsu Networks Co., Ltd. sales office.
13101	Error	backup info save : failed to save backup info !!! : save path = {Backup information file path}	-1	Saving the backup information file has failed.	Contact an Anritsu Networks Co., Ltd. sales office.

The following table shows the messages displayed in the event viewer related to the restore tool.

Table F-2 Restore tool message list

Event ID	Level	Error message	Command return value	Description	Countermeasures
19901	Error	Unhandled Exception occurred. It caught on top level of program.	-1	An unexpected error has occurred.	Contact an Anritsu Networks Co., Ltd. sales office.
16101	Error	[main] MMCollector service not stopped! abort restore process !!	-1	MM Collector has not stopped.	Stop MM Collector, and execute it.
16101	Error	[main] MMController service not stopped! abort restore process !!	-1	MM Controller has not stopped.	Stop MM Controller, and execute it.
16101	Error	[main] MMSQL Service does not running ! abort restore process.	-1	MMSql Service has not started up.	Start up MMSql Service, and execute it.
14301	Error	[main] no target folder specified !	-1	The restore target folder cannot be found.	Specify the restore target folder correctly.
14301	Error	[main] no backup information found on folder !	-1	The backup information file does not exist.	Specify the restore target folder correctly.
14103	Error	Failed to parse option string.	-1	An option is wrongly specified.	Specify an option correctly.
14301	Error	[main] restore target file missing !!! filepath = {File path}	-1	The restore target file cannot be found.	Specify the restore target folder correctly
14301	Error	[main] DB instance path is invalid. path = {DB folder path}	-1	Access to the database cannot be allowed.	Contact an Anritsu Networks Co., Ltd. sales office.
15201	Error	[main] failed to restore backup data table. tablename - {DB table name}	-1	An error has occurred during restoration processing.	Contact an Anritsu Networks Co., Ltd. sales office.
15101	Error	[main] restore tmp table not has ID1 log data! table name = {DB table name}	-1	Obtaining the backup data has failed.	Contact an Anritsu Networks Co., Ltd. sales office.
15201	Error	[main] backup table not found on restore temporary table ! table name = {DB table name}	-1	Access to the restore target database cannot be allowed.	Check the access right to the restore target folder.

Event ID	Level	Error message	Command return value	Description	Countermeasures
14301	Warning	[main] create restore target db	0	The restore destination folder (pure2) does not exist.	No measure is required.
15301	Warning	[main] config file already exist, renamed and overwrite., { Before renaming} -> {After renaming}	0	The software configuration file has been overwritten.	No measure is required.
15301	Warning	[main] mysql.ini already exist, renamed and overwrite., {Before renaming} -> {After renaming}	0	The database configuration file has been overwritten.	No measure is required.
15301	Warning	[main] restore target task scheduler task already exists. file removed. task name =	0	The report task has been overwritten.	No measure is required.

The following table shows the messages displayed in the event viewer related to the report function.

Table F-3 Report function message list

Event ID	Level	Error message	Description	Countermeasures
19901	Error	Unhandled Exception occured.	An unexpected error has occurred.	Contact an Anritsu Networks Co., Ltd. sales office.
19901	Error	Reporter execute errored. Process stopped.	A problem occurs during the creation of the report.	Contact an Anritsu Networks Co., Ltd. sales office.
14101	Error	Reporter argument is not valid. Parameter = {Delivered parameter}	Startup of the report creation task (reporter) has failed.	Contact an Anritsu Networks Co., Ltd. sales office.
13101	Error	Failed to got write access permission. Path = {Path by which obtaining the right has failed}	The right to write in the report output destination has not been obtained.	Check the access right to the report output destination.
15201	Error	Failed to access to database.	Access to the database cannot be allowed.	Contact an Anritsu Networks Co., Ltd. sales office.
13101	Error	Failed to create a report output directory. Path = {Path by which writing has failed}	Creation of the folder at the report output destination has failed.	Check the access right to the report output destination.
11101	Error	Not enough disk space. More than 1GB space required.	The disc free space at the report output destination is not sufficient.	Maintain 1 GB or more of disc free space at the report output destination.
15401	Error	Index.html write process is concurrent with MMReporter.	Competition has occurred when writing the common index.html.	Adjust the execution time of the report task.

(Blank page)