MasterScope SystemManager G 8.0 WebConsole Option

Function Reference Guide

First Edition
July, 2018

NEC Corporation
SMG0800E-FUNC-1820

Disclaimer

The copyrighted information noted in this document shall belong to NEC Corporation.

Copying or revising this document, in whole or in part, is strictly prohibited without the permission of NEC Corporation.

This document may be changed without prior notice.

NEC Corporation shall not be liable for any technical or editing errors or omissions in this document.

NEC Corporation shall not be liable for the accuracy, usability, or certainty of information noted in this document.

Copyright Information

- MasterScope is a registered trademark of NEC Corporation.
- Linux is a trademark or registered trademark of Linus Torvalds in the United States of America and other countries.
- Red Hat is a trademark or registered trademark of Red Hat, Inc. in the United States and other countries.
- PostgreSQL is a registered trademark or trademark of PostgreSQL in the United States and other countries.
- Intel and Itanium are trademarks or registered trademarks of Intel Corporation in the United States of America and other countries.
- Apache, Apache Tomcat, and Tomcat are trademarks or registered trademarks of Apache Software Foundation.
- Java is a registered trademark of Oracle Corporation and its subsidiaries and affiliates in the United States of America and other countries.
- Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries. Other Microsoft products mentioned in this guide are also registered trademarks of Microsoft Corporation in the United States of America and other countries.
- Adobe, the Adobe logo, and Acrobat are registered trademarks of Adobe Systems Incorporated in the United States of America and other countries.
- PATLITE is a registered trademark of PATLITE Corporation.

Other system names, company names, and product names in this document are trademarks or registered trademarks of their respective companies.

Note that the ® mark and the ™ mark are not indicated in this document.

Notes on exporting this product

This product (including software) may be applicable to the controlled cargo regulated by the Foreign Exchange and Foreign Trade Law. To export the product to outside of Japan, the export permit from Japanese government is required. If you require documents from NEC in order to obtain an export

license, please contact the dealer where you purchased your MasterScope product, or your local NEC sales office.

Preface

Target readers and objective

This document is intended for system administrators who use SystemManager G to perform operation management, and describes the management method.

Overview of the document

This chapter describes how to use SystemManager G.

Notation rules of this document

In this document, important notes and related information are described as follows:

Note

Notes, warnings, and supplements on functions, operations, and settings are described.

Tip

Additional information and reference information are described.

Notation list

The following conventions apply to this document.

Notation	Meaning	Example
Square brackets	Placed before and after an item (such as a text box, check box, or tab) on the screen	Enter the machine name in the **Machine name** text box. **All** check box
" " Double quotation marks	Placed before and after a screen name (such as a dialog box or window), and a name of other manuals	"Setting" window "*Installation Guide*"
Square brackets [ ] in a command line	Indicates that the specification of the value in [ ] can be omitted.	add [/a] Gr1
Pipe | in a command line	Indicates that either of the elements delimited with the pipe will be selected. The element selection can be omitted when a pipe is used in square brackets. The element selection must be made when a pipe is used in braces.	delete [/a|/f] group add {--code=*codeword*|--file=*file-path*}
Braces { } in a command line	Are used together with a pipe, indicating that either of the elements delimited with the pipe must be selected.	add {--code=*codeword*|--file=*file-path*}
Monospace font (Courier New)	Output from the command line (such as a message or prompt)	Run the following command. `replace Gr1`

Notation	Meaning	Example
Italicized monospace font (Courier New)	Indicates the items to be replaced with a valid value and input by users. If the value contains any spaces, surround it with " " (double quotation marks).	add *GroupName* `InstallPath="Install Path"`
Gray-scale background	Shows a concrete example of a command to run, a return value(s), and the like.	`msc_license_cmd.exe --register="C:\tmp\codeword.txt" --force`
JSON example	To improve readability, line breaks and indentation are added to the displayed JSON examples.	`{ "ID": [ "45ed3512" ], "Manager": { "ErrorMessage": "", "Name": "localhost", "Status": 200, "StatusCode": 200 } }`

Definitions

Definition	Description
<WebConsole-install-path>	Installation directory of SystemManager G WebConsole Option. The default installation directory varies depending on the environment as follows: In the Windows environment, the default installation directory is "C:\Program Files \NEC\pf\opm\manager". In the Linux environment, the default installation directory is "/opt/nec/pf/opm/manager".
<manager-install-path>	Installation directory of SystemManager G Manager. The default installation directory varies depending on the environment as follows: In the Windows environment, the default installation directory is "C:\Program Files (x86)\NEC\UMF\Operations". In the Linux environment, the default installation directory is "/opt/UMF/Operations".
<Tomcat-install-path>	Installation directory of Application Server. The default installation directory varies depending on the environment as follows: In the Windows environment, the default installation directory is "C:\Program Files (x86)\NEC\UMF\Operations\Tomcat". In the Linux environment, the default installation directory is "/opt/NEC/UMF/Operations/Tomcat".
<WebSAM Root>	Mounting directory of MasterScope media. The default installation directory varies depending on the environment.

Contents

List of Figures

List of Tables

Chapter 1. How to Operate the Web GUI

This chapter describes how to operate the Web GUI of SystemManager G.

Contents

1.1 Limitations on the operation of the Web GUI

- When an item is entered using a regular expression, a check is not made to see whether the syntax of that regular expression is valid. Be sure to enter a valid regular expression.
- Immediately after you add a service using the Windows service monitoring setting, the information you have just set may not be reflected in the screen. In that case, wait a while and then display the information again.
- When a performance monitoring counter set in the monitoring template applies to a node, the setting of the counter is registered even if that counter is nonexistent. The monitoring results will not be affected even if the setting of a nonexistent counter is registered. Note, however, that you cannot delete only this counter. To delete the counter, delete the resources or instances first and then register only the necessary counters again.
- Timezone of server side and client side should be configured as same, otherwise displayed time will include a difference.
- Summer time is not reflected in the time label of the graph.

1.2 User types and roles

With the Web GUI, the available screens and operations differ depending on the user type and role that are set on a user-by-user basis.

This section describes the screens and operations that are available to each individual user type and role.

- User type

  You can set the authority to perform system operations such as user management.

  - System Administrator

    User who manages the entire system. In addition to all the operations available to the other user types, this user can monitor system messages as well.

  - Manager

    User who can perform operations such as user management.

  - User

    General user who uses services. This user can view the user list but cannot perform operations such as making changes.

For details about the operations that are available to each individual user type, see the table below.

Table 1-1 User types

Function	Operation	System Administrator	Manager	User
Dashboard	Displaying and customizing the dashboard	Y	Y	Y
User management	Displaying a list and details of users	Y	Y	Y
User management	Registering, changing, and deleting a user	Y	Y	N
Monitoring	Handling system messages (changing the state, marking, and editing a comment)	Y	N	N

- Role

  You can set the authority to view and operate monitoring (node monitoring and message monitoring).

  You cannot set a role for a user whose user type is system administrator. (A user whose user type is system administrator cannot view or operate nodes and messages.)

  - MONITORING USER

    User who views monitoring states to detect errors. This user can view monitoring states but cannot perform message operations such as changing message states and marking.

  - MONITORING OPERATOR

    User who has the authority to perform message operations in addition to the authority of MONITORING USER.

  - MONITORING ADMINISTRATOR

    User who has the authority to group monitoring targets and results and to set filtering in addition to the authority of MONITORING OPERATOR.

For details about the operations that are available to each individual role, see the table below.

Table 1-2 Roles

Function	Operation	MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Monitoring	Displaying the monitoring state	Y	Y	Y
Monitoring	Handling messages (changing the state, marking, and editing a comment)	Y	Y	N
Monitoring	Registering, changing, and deleting groups, categories, and filters	Y	N	N

1.3 Login

This section describes how to log in to the Web GUI.

1. Using a browser, access one of the following URLs:

   http://*hostname*:*http_port*/portal

   https://*hostname*:*https_port*/portal

   In *hostname*, specify the host name or IP address of the host in which the SystemManager G WebConsole Option is installed.

   In *http_port*, specify the waiting port for HTTP connection. If installed by default, specify 12080.

   In *https_port*, specify the waiting port for HTTPS connection. If installed by default, specify 12443.

2. Start the Web GUI, enter the user ID and password, and then click the [Login] button.

   When you log in for the first time, use the user ID and password of the built-in user.

   Both the user ID and password of the built-in user is "admin".

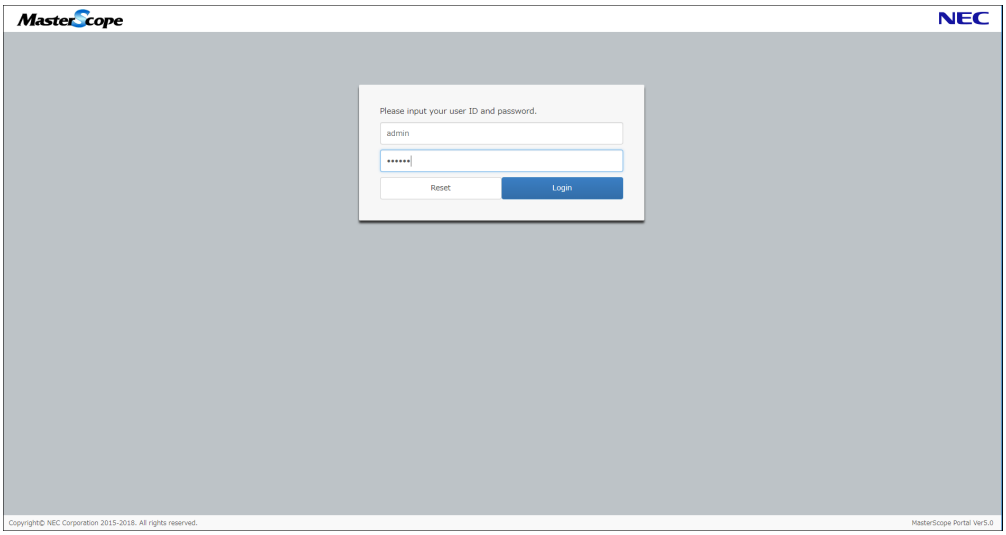

Figure 1-1 [Login] screen

Note

- After logging in to the Web GUI for the first time, register a new system administrator and disable the built-in user (admin).

  For details about registering a user, see "1.6.2 Registering a user (page 16)". For details about disabling the built-in user, see "1.6.4 Changing user information (page 19)".

- If you enter an incorrect password 10 times for the same account, the screen is locked and you cannot log in.

  * Until the 9th password input failure, the number of input failures is reset after 10 minutes.

  The screen can be unlocked by the system administrator or administrator enabling the target user.

  For information about how to enable a user, see "1.6.4 Changing user information (page 19)".

- If you become unable to log in because all administrators are locked or disabled

  Run the following command to enable the admin user. Then, log in as the admin user from the Web GUI, unlock the system administrators, and disable the admin user again.

  ```
  >psql -f <WebConsole-install-path>\portal\sql\enable_admin.sql -U msc_portal
  msc_portal
  ```

  * Execute this command on the host in which the SystemManager G WebConsole Option is installed.

- If "HTTP Status 404 - Not Found" is displayed, one of the following causes is likely to blame.
  - The database is not running.

    Check the status of the database that you set when using the WebConsole Option.

    For Windows, use the database whose displayed name is postgresql-x64-9.6 by default.

    For Linux, use the database that you have installed according to "Installation in a Linux environment" - "Installing the database" of the "Installation Guide."
  - The setup of the database is not complete.

    For Linux, check whether the setup is complete according to "Installation in a Linux environment" - "Setting up PostgreSQL" of the "Installation Guide."

3. When the [Dashboard] screen is displayed, the login is complete.

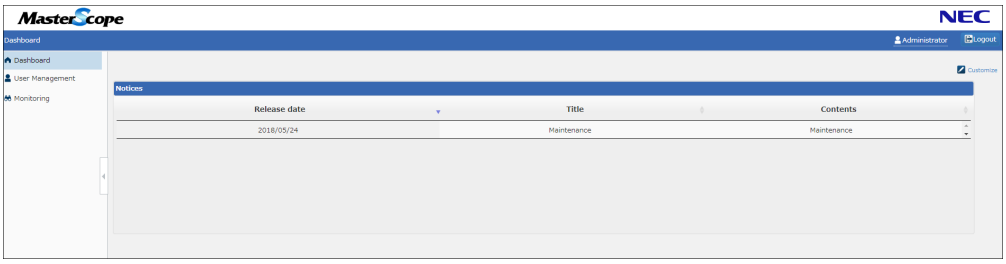

Figure 1-2 [Dashboard] screen

1.4 Setting up the login user (local user)

This section describes the following operations, which you can select from the login user operation dialog box that appears when you click the login user name (local user name) displayed at the upper right of the Web GUI.

- Viewing the information of the login user
- Changing the information of the login user
- Changing the password of the login user

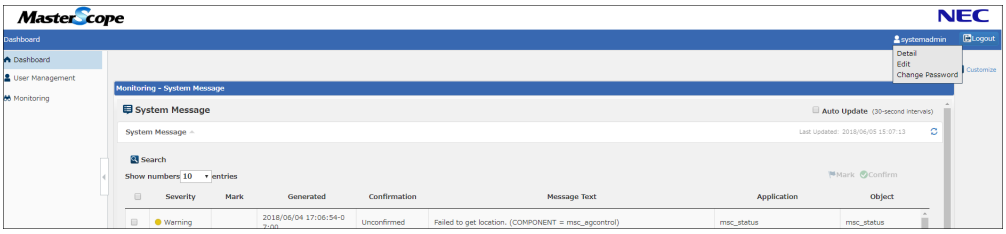

Figure 1-3 Login user operation dialog box

1.4.1 Viewing the information of the login user

The [Log-in User Detail] screen, which you can open by selecting [Detail] in the login user operation dialog box, lets you check information such as the user type and role.

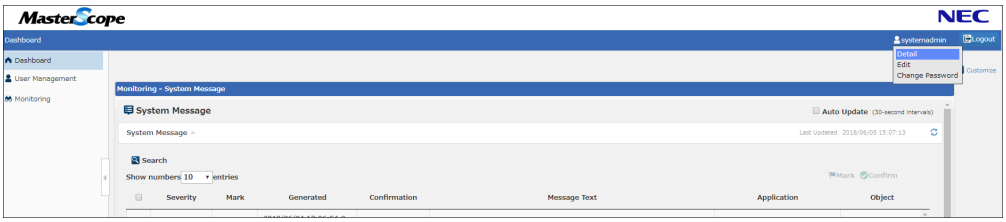

Figure 1-4 [Detail] on the Login user operation dialog box

Figure 1-5 [Log-in User Detail] screen

Details about each item are shown below.

Table 1-3 Item list ([Log-in User Detail] screen)

Item name	Details
User ID	ID specified when the user was registered and used to identify the user in the system
Name	Name (user name)
User type	User type. One of the following is displayed: • System Administrator • Manager • User
Role	Role. One of the following is displayed: • MONITORING ADMINISTRATOR • MONITORING OPERATOR • MONITORING USER This item is not displayed for a user who has [System Administrator] shown in [User type].
Status	Status of the account. Either [Active] or [Inactive] is displayed.
Notes	Remark.

1.4.2 Changing the login user information

You can change the following information of the login user (local user) by using the [Edit Log-in User(Form)] screen, which you can open by selecting [Edit] in the login user operation dialog box.

- Name
- Notes

To change the above information, follow the procedure below.

1. On the dashboard screen, click a user name and then click [Edit].

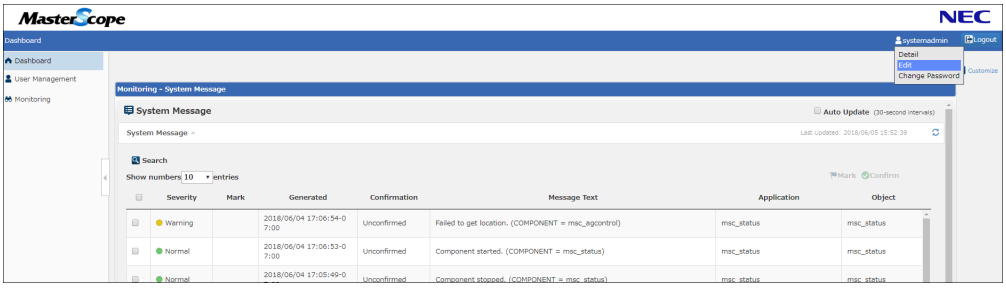

Figure 1-6 Login user operation dialog box

2. The [Edit Log-in User(Form)] screen is displayed. Edit the items by referring to the following table and then click the [Next] button.

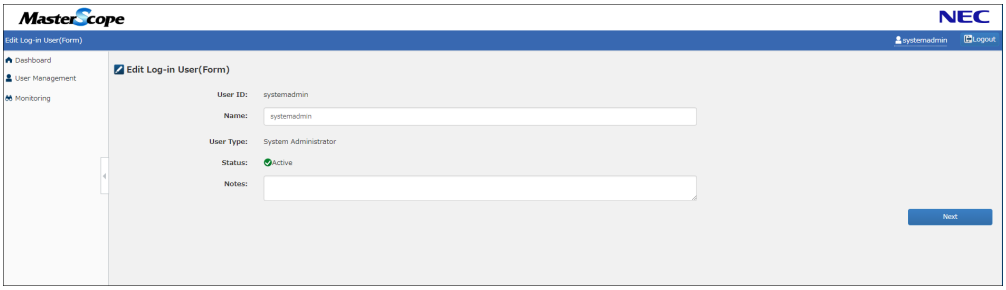

Figure 1-7 [Edit Log-in User(Form)] screen

Table 1-4 Item list ([Edit Log-in User(Form)] screen)

Item name	Input rule	Description
Name	Up to 1024 characters	Enter a name (user name).
Notes	Up to 255 characters	Enter a remark.

3. The [Edit Log-in User(Confirmation)] screen is displayed. Click the [Confirm] button to apply the changes.

Figure 1-8 [Edit Log-in User(Confirmation)] screen

1.4.3 Changing the password of the login user

You can change the password of the login user (local user) by using the [Change Log-in Password(Form)] screen, which you can open by selecting [Change Password] in the login user operation dialog box.

To change the password, follow the procedure below.

1. On the dashboard screen, click a user name and then click [Change Password].

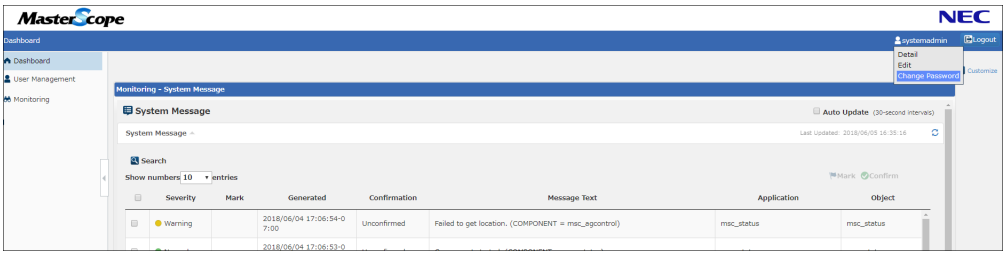

Figure 1-9 Login user operation dialog box - [Change Password]

2. The [Change Log-in Password(Form)] screen is displayed. Enter a password and click the [Next] button.

   When entering a password, following the rules described in "Table 1-11 Item list ([Create User(Form)] screen) (page 16)"in "1.6.2 Registering a user (page 16)".

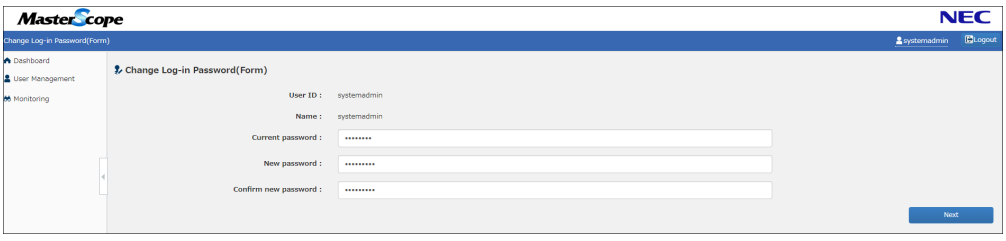

Figure 1-10 [Change Log-in Password(Form)] screen

3. The [Change Log-in Password(Confirmation)] screen is displayed. Click the [Submit] button to apply the changes.

Figure 1-11 [Change Log-in Password(Confirmation)] screen

1.5 Dashboard

In the [Dashboard] screen, you can have desired widgets arranged in a desired order and size. Since the arrangement of widgets is saved for each login user individually, you can customize the arrangement as you like.

This section describes the widget operations, such as the viewing, placement, and removal of widgets.

While the authority to perform the operations described in this section is controlled according to the user type, they are available to all users.

Table 1-5 Authority to operate the [Dashboard] screen

System Administrator	Administrator	User
Y	Y	Y

1.5.1 Displaying the widgets

By selecting [Dashboard] from the menu, the [Dashboard] screen is displayed and widgets are displayed on the dashboard.

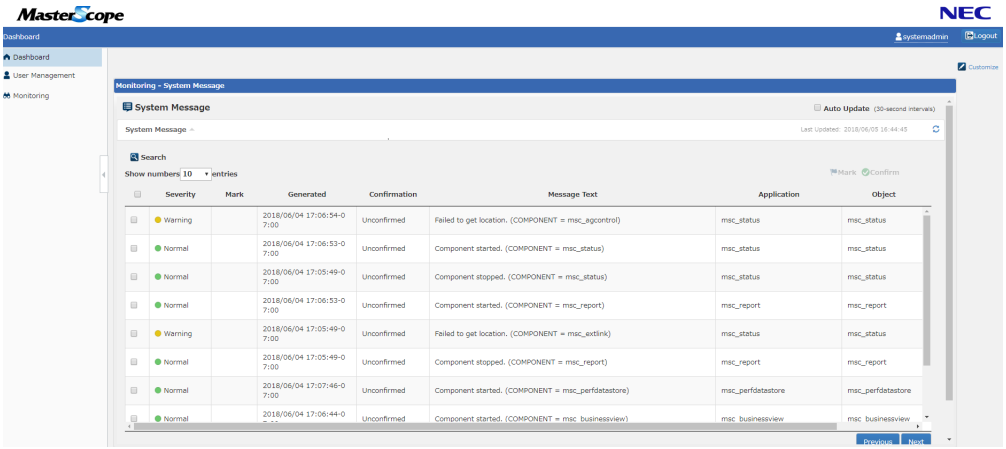

Figure 1-12 Displaying the widgets on the [Dashboard] screen

Widgets can be handled by using a mouse.

To return to the initial display of widgets after handling them, reload the page.

1.5.2 Adding a widget

This section describes how to add a widget to the dashboard.

1. On the [Dashboard] screen, click [Customize].

   The [Dashboard] screen changes to customize mode and the customize menu is displayed.

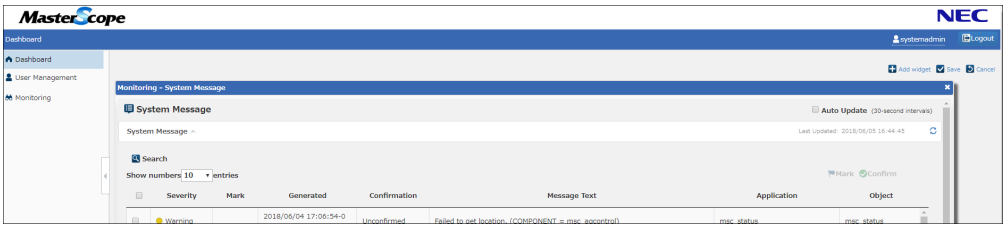

Figure 1-13 [Dashboard] screen with the customize menu

2. On the [Dashboard] screen, click [Add widget].

   The [Add widget] dialog box is displayed.

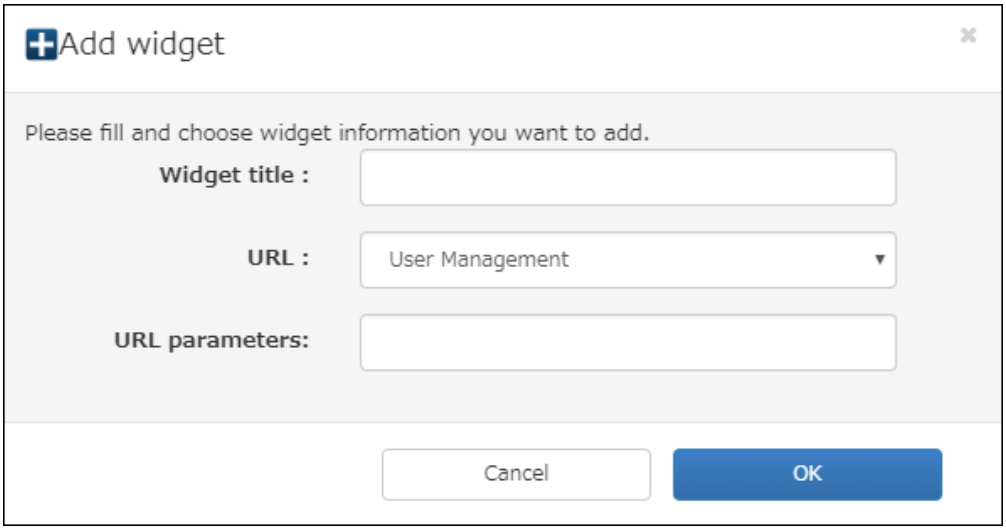

Figure 1-14 [Add widget] dialog box

3. On the [Add widget] dialog box, enter the information of the widget that you want to add.

Table 1-6 Item list ([Add widget] dialog box)

Item name	Input rule	Initial value	Description
Widget title	0 to 64 characters	-	Specify the name to be displayed as the widget title. Make sure that it is easy to identify from the name what the widget is for. If a widget name is omitted, "(No name)" is displayed. Multiple widgets with the same name can be registered.
URL	-	-	Select the item to be displayed as the widget. Multiple widgets with the same URL can be registered.
URL parameters	0 to 2048 characters	-	Use this item when specifying an option parameter for the widget URL. The format of the option parameter is *key*=*value*. When specifying multiple parameters, separate them with "&". The character string must have been encoded.

4. Click [OK].

   The [Add widget] dialog box is closed.

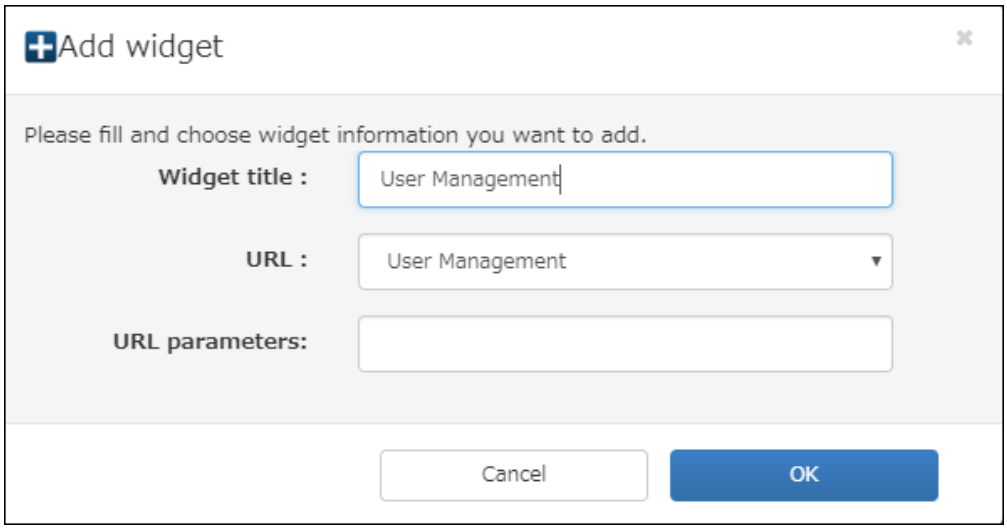

Figure 1-15 [Add widget] dialog box

A new widget is displayed at the end of the displayed widgets on the dashboard.

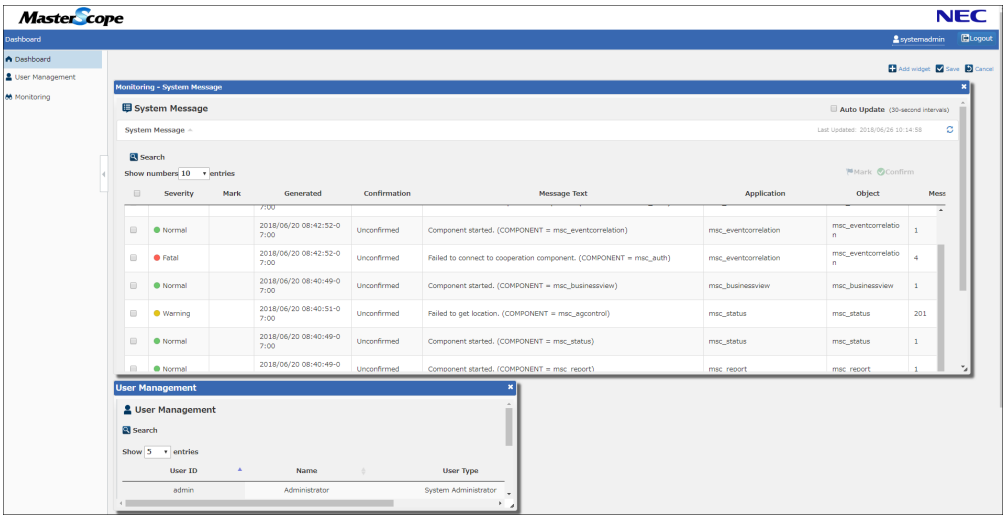

Figure 1-16 Displaying the dashboard and a new widgets

After adding widgets, save the added widgets. For details about the procedure, see "1.5.5 Saving the widget settings (page 13)".

1.5.3 Removing a widget

This section describes how to remove a widget from [Dashboard].

1. On the [Dashboard] screen, click [Customize].

   The [Dashboard] screen changes to customize mode.

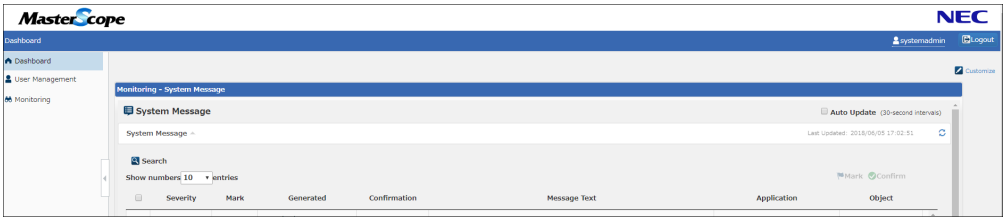

Figure 1-17 [Dashboard] screen - Customize

2. Click [×] displayed at the upper right of the widget that you want to remove.

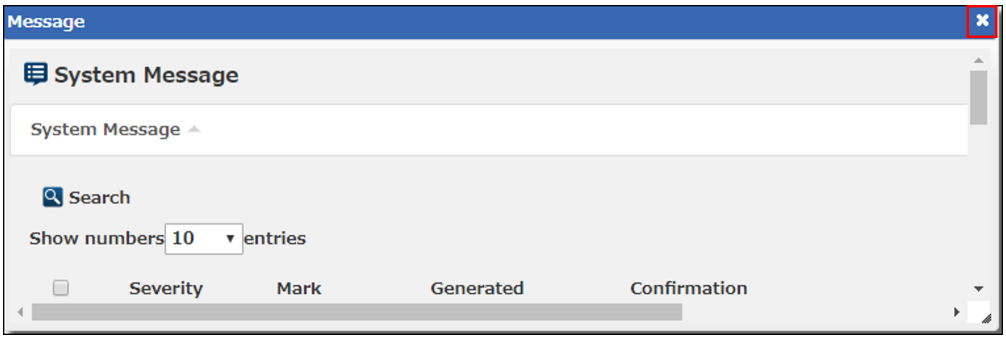

Figure 1-18 Removing a widget from the dashboard

The [Confirmation - remove widget] dialog box is displayed.

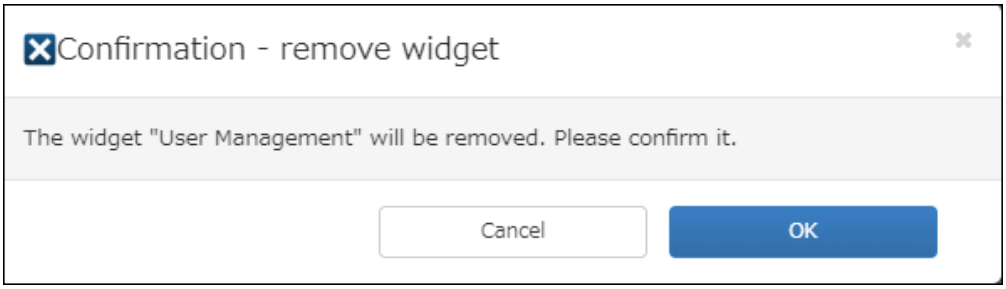

Figure 1-19 The [Confirmation - remove widget] dialog box

3. Check the contents of the [Confirmation - remove widget] dialog box. If you want to remove the displayed widget, click [OK].

   Otherwise, click [Cancel].

   The [Confirmation - remove widget] dialog box is closed.

Click [OK] to delete the selected widget is removed.

After removing the widget, click [Save]. For details about the procedure, see "1.5.5 Saving the widget settings (page 13)".

1.5.4 Changing the display order and size of the widgets

This section describes how to change the display order and size of the widgets displayed on the dashboard.

1. On the [Dashboard] screen, click [Customize].

   The [Dashboard] screen changes to customize mode.

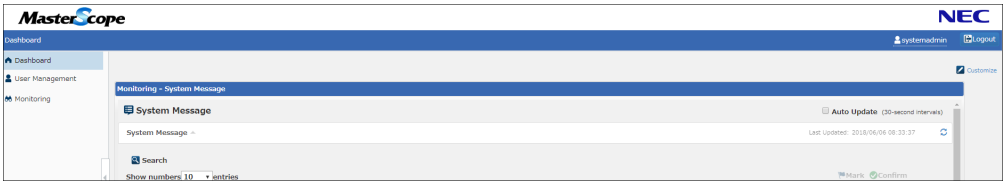

Figure 1-20 [Dashboard] screen - Customize

2. To change the widget display order, drag and drop the desired widget with a mouse.

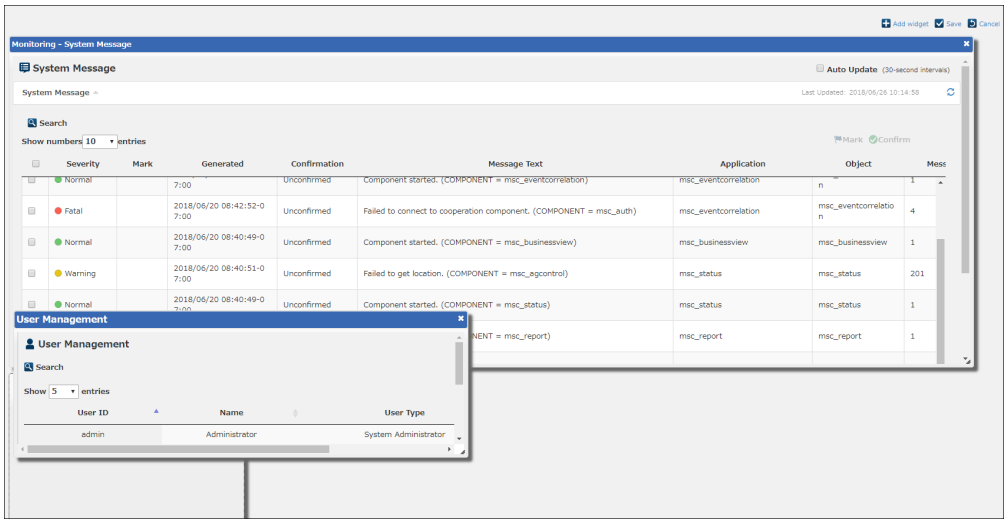

Figure 1-21 Changing the display order of the widgets

The widget display order is changed.

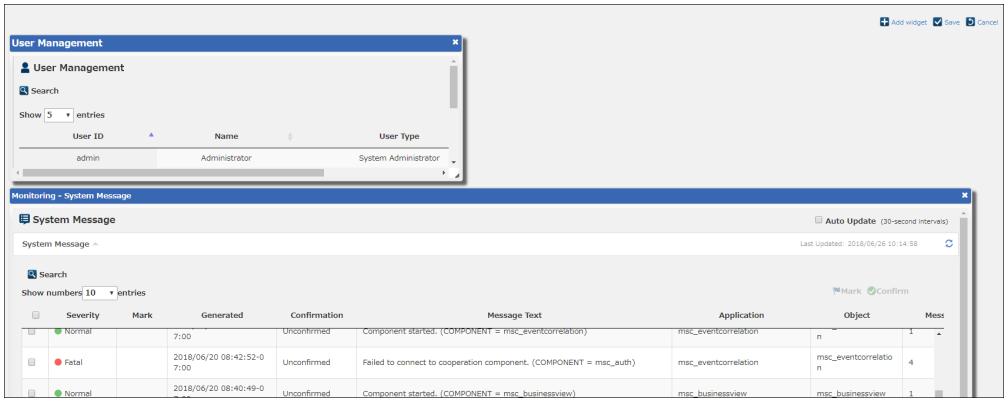

Figure 1-22 Changing the display order of the widgets

3. To change the widget size, drag the frame of the desired widget with a mouse.
   - To change the height of the widget, drag the bottom frame of the desired widget with a mouse.
   - To change the width of the widget, drag the right frame of the desired widget with a mouse.
   - To change the height and width of the widget, drag the bottom right corner of the desired widget with a mouse.

The widget size is changed.

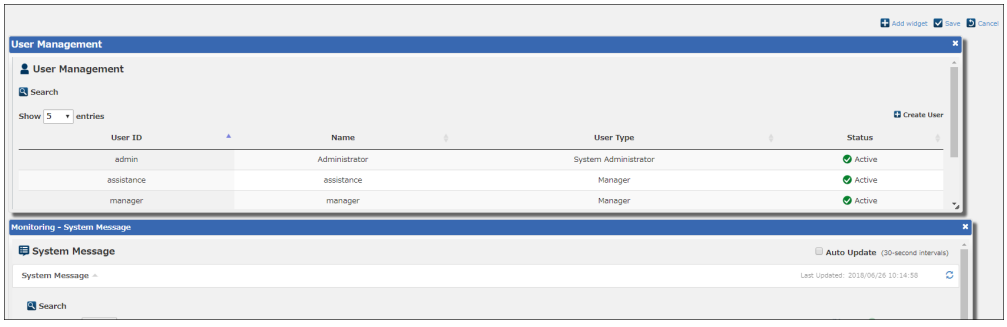

Figure 1-23 Changing the display size of the widgets

After changing the widget display order or size, click [Save]. For details about the procedure, see "1.5.5 Saving the widget settings (page 13)".

1.5.5 Saving the widget settings

This section describes how to save the settings of the widget on the dashboard.

It is assumed that the dashboard is already in customize mode and the widgets are being handled. For the operations for widgets, see the following:

- "1.5.2 Adding a widget (page 8)"
- "1.5.3 Removing a widget (page 10)"
- "1.5.4 Changing the display order and size of the widgets (page 11)"

1. On the [Dashboard] screen, click [Save].

   The [Confirmation - save widgets] dialog box is displayed.

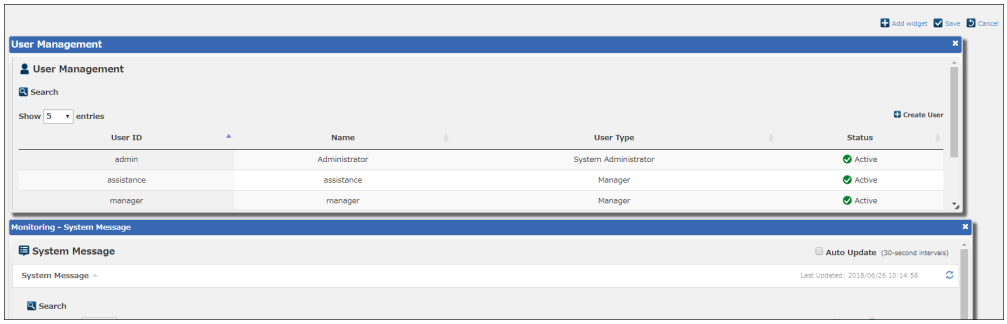

Figure 1-24 Saving the widget settings

2. Check the contents of the [Confirmation - save widgets] dialog box. If you want to save the displayed contents, click [OK].

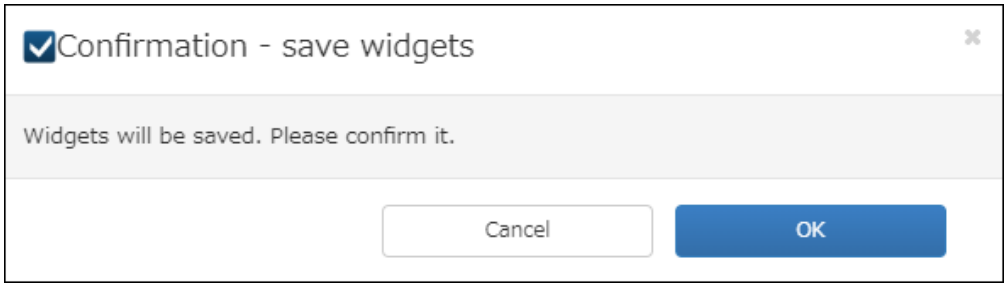

Figure 1-25 [Confirmation - save widgets] dialog box

   Otherwise, click [Cancel].

   The [Confirmation - save widgets] dialog box is closed.

Information of the added or remove widget and the widget display order and size are saved.

1.5.6 Discarding the settings of the widget

This section describes how to discard the settings of the widget on the dashboard.

It is assumed that the dashboard is already in customize mode and the widgets are being handled. For details about how to handle the widgets, see the following:

- "1.5.2 Adding a widget (page 8)"
- "1.5.3 Removing a widget (page 10)"
- "1.5.4 Changing the display order and size of the widgets (page 11)"

1. On the [Dashboard] screen, click [Cancel].

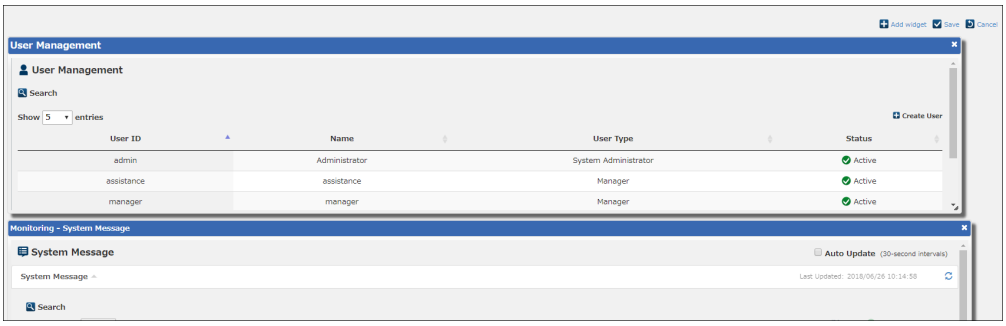

Figure 1-26 Discarding the settings of the widget

The [Confirmation - cancel] dialog box is displayed.

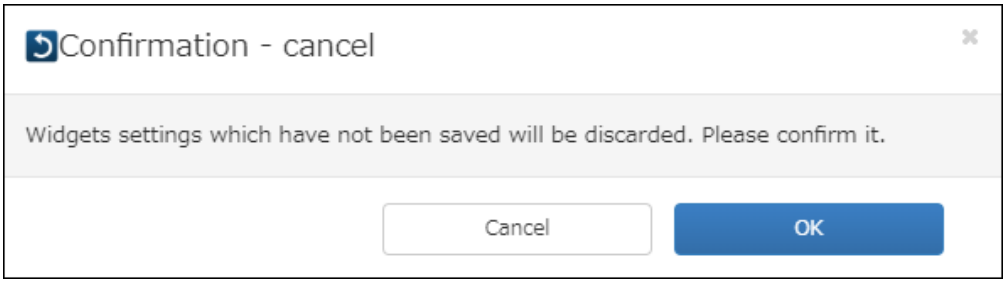

Figure 1-27 [Confirmation - cancel] dialog box

2. Check the contents of the [Confirmation - cancel] dialog box. If you want to discard the displayed contents, click [OK].

   Otherwise, click [Cancel].

   The [Confirmation - cancel] dialog box is closed.

The widget editing contents that have not been saved are discarded and the widget display returns to the last saved state.

1.6 User management

This section describes the user management menu that enables you to perform operations such as viewing, registering, and deleting users.

1.6.1 Displaying the user list

Clicking [User Management] in the menu displays the [User Management] screen.

While the authority to perform the operations described in this section is controlled according to the user type, they are available to all users.

System Administrator	Administrator	User
Y	Y	Y

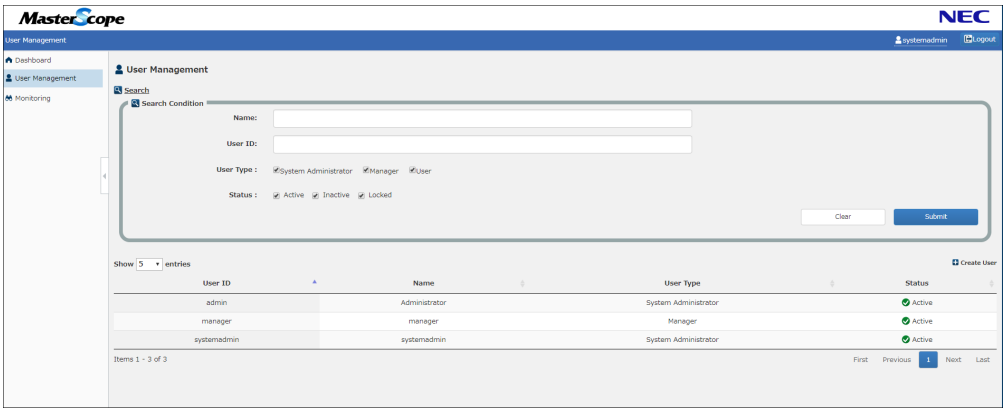

Figure 1-28 [User Management] screen

The [User Management] screen displays the following items and buttons.

Table 1-8 Item list ([User Management] screen)

Item name	Description
Show [ ] entries	The number of users to be displayed per page in the user list shown in the lower part of the screen. You can select the number of users to be displayed from 5, 10, 50, and 100.
Search	Displays the [Search] screen used to search for users who match the specified conditions.
Create User	Displays the [Create User(Form)] screen used to register new users. This button is displayed only for a user whose user type is System Administrator or Manager.
User list	Displays a list of users.

The user list displays the following items.

Table 1-9 Item list ([User Management] screen - User list)

Item name	Description
User ID	ID specified when the user was registered and used to identify the user in the system
Name	Name (user name)
User type	User type. One of the following is displayed: • System Administrator • Manager • User
Status	Status of the account. One of the following is displayed: • Active • Inactive • Locked

To search for a user, click the [Search] button to display the [Search] screen, enter search conditions, and then execute the search.

The [Search] screen displays the items and buttons shown below. A string search is a partial match search.

Table 1-10 Item list ([User Management] screen - Search)

Item name	Input rule	Description
Name	-	Searches for the entered name (user name).
User ID	-	Searches for the entered user ID.
User Type	-	Searches for the selected user type (system administrator, administrator, or user).
Status	-	Searches for the selected status (Active, Inactive, or Locked).
Clear	-	Resets the entered (specified) values to the initial values.
Submit	-	Click this button to start searching.

1.6.2 Registering a user

This section describes how to add a user.

Note that the authority to perform the operations described in this section is controlled according to the user type, and these operations are available to the following users.

System Administrator	Administrator	User
Y	Y	N

1. On the [User Management] screen, click [Create User].

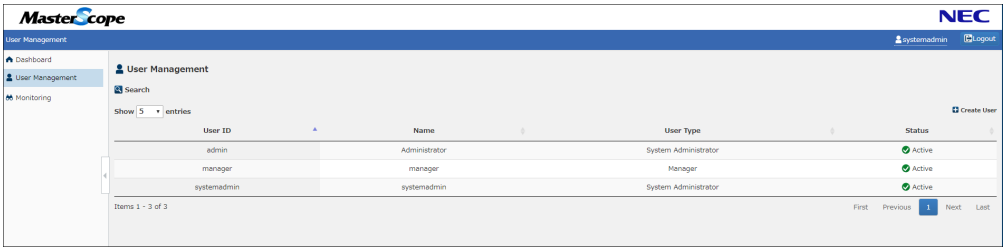

Figure 1-29 [User Management] screen - Create User

2. The [Create User(Form)] screen is displayed. Edit the items by referring to the following table and then click the [Next] button.

Figure 1-30 [Create User(Form)] screen

Table 1-11 Item list ([Create User(Form)] screen)

Item name	Input rule	Initial value	Description
User type	-	User	Select a user type. When the type of the registering user is [System Administrator], a user type can be selected from the following:

Item name	Input rule	Initial value	Description
			• System Administrator • Manager • User When the type of the registering user is [Manager], a user type can be selected from the following. • Manager • User
Role	-	-	Select the role to be assigned to the user. This item is not displayed when the type of the user to be registered is system administrator. • MONITORING USER • MONITORING OPERATOR • MONITORING ADMINISTRATOR
User ID	3 to 16 characters One-byte alphanumeric characters, underscores (_), and hyphens (-) can be used.	-	Enter an ID to identify the user in the system.
Name	Up to 1024 characters	-	Enter a name (user name).
Password	6 to 16 characters One-byte alphanumeric characters and the following symbols are available: !"#$ %&'()* +,./:;<=>? @[¥]^_`{|}~ -.	-	Enter the user password.
Password(Confirmation)	Enter the same character string that you entered in [Password].	-	Enter the user password for confirmation.
Status	-	Active	Select any of the following user states: • Active • Inactive
Note	Up to 255 characters	-	Note

3. The [Create User(Confirmation)] screen is displayed. Click the [Confirm] button to add the user.

Figure 1-31 [Create User(Confirmation)] screen

1.6.3 Displaying the detailed information of a user

Clicking the line of the user whose contents you want to check displays its detailed information.

While the authority to perform the operations described in this section is controlled according to the user type, they are available to all users.

System Administrator	Manager	User
Y	Y	Y

Figure 1-32 [User Management] screen - User details

The detailed information displays the following items.

Table 1-12 Item list ([User Management] screen - User details)

Item name	Description
User ID	ID specified when the user was registered and used to identify the user in the system
Name	Name (user name)
User Type	User type. One of the following is displayed: • System Administrator • Manager • User
Role	Role. One of the following is displayed: • MONITORING ADMINISTRATOR • MONITORING OPERATOR • MONITORING USER This item is not displayed for a user who has "System Administrator" shown in [User Type].
Status	Status of the account. One of the following is displayed: • Active • Inactive • Locked
Note	Note.
Edit User	The [Modify User(Form)] screen is displayed. If the user type of the operator is "System Administrator", this item is displayed when a user other than the local user is selected.

Item name	Description
	If the user type of the operator is a Manager, this item is displayed when a user other than the local user is selected whose user type is one of the following. • Manager • User This item is not displayed when the user type of the operator is User.
Change Password	The [Changing password(Form)] is displayed. If the user type of the operator is "System Administrator", this item is displayed when a user other than the built-in user or local user is selected. If the user type of the operator is a Manager, this item is displayed when a user other than the local user is selected whose user type is one of the following. • Manager • User This item is not displayed when the user type of the operator is a User.
Delete User	The [Delete User(Confirmation)] screen is displayed. If the user type of the operator is system administrator, this item is displayed when a user other than the built-in user or local user is selected. If the user type of the operator is a Manager, this item is displayed when a user other than the local user is selected whose user type is one of the following. • Manager • User This item is not displayed when the user type of the operator is a User.

1.6.4 Changing user information

This section describes how to change user information.

Note that the authority to perform the operations described in this section is controlled according to the user type, and these operations are available to the following users.

System Administrator	Administrator	User
Y	Y	N

1. On the [User detail] screen, click [Edit User].

Figure 1-33 [User Management] screen - Change User

2. The [Modify User(Form)] screen is displayed. Edit each item by referring to "Table 1-11 Item list ([Create User(Form)] screen) (page 16)" of "1.6.2 Registering a user (page 16)" and click the [Next] button.

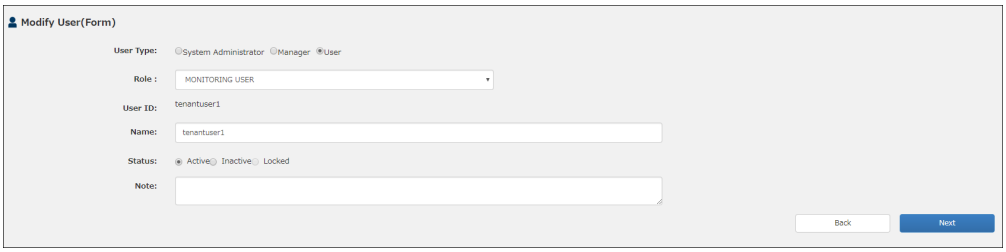

Figure 1-34 [Modify User(Form)] screen

Note

The user information of the built-in user can be changed only by a system administrator, and [Status] is the only item that can be changed.

3. The [Change User(Confirmation)] screen is displayed. Click the [Confirm] button to apply the changes.

Figure 1-35 [Change User(Confirmation)] screen

1.6.5 Changing the password

This section describes how to change the password.

Note that the authority to perform the operations described in this section is controlled according to the user type, and these operations are available to the following users.

System Administrator	Administrator	User
Y	Y	N

1. On the [User detail] screen, click [Change Password].

Figure 1-36 [User detail] screen - Change Password

2. The [Changing password(Form)] screen is displayed.

   Change the password by referring to the password entry rule described in "1.6.2 Registering a user (page 16)" and click the [Next] button.

Figure 1-37 [Changing password(Form)] screen

3. The [Changing password(Confirmation)] screen is displayed. Click the [Submit] button to apply the changes.

Figure 1-38 [Changing password(Confirmation)] screen

1.6.6 Deleting a user

This section describes how to delete a user.

Note that the authority to perform the operations described in this section is controlled according to the user type, and these operations are available to the following users.

System Administrator	Administrator	User
Y	Y	N

1. On the [User detail] screen, click [Delete User].

Figure 1-39 [User Management] screen - Delete User

2. The [Delete User(Confirmation)] screen is displayed. Click the [Confirm] to delete the user.

Figure 1-40 [Delete User(Confirmation)] screen

Note

If the deleted user is currently logged in, that user is automatically logged out during the ongoing operation.

1.7 Monitoring

This section describes the monitor menu.

The following item is displayed in the monitor menu for a user whose user type is system administrator.

Item name	Details
System messages	View messages related to the system, such as the system operation state, and perform the operations to change the confirmation status, assign a mark, etc.

The following items are displayed in the monitor menu for a user whose user type is administrator or user.

Item name	Details
Node	View a node list, statuses, and a message list, and perform operations for them.
Message	View monitoring messages, and perform the operations to change the confirmation status, assign a mark, etc.
Analysis / Report	Display the information obtained from each monitored node in a graph.
Setting	Specify the settings related to monitoring.

1.7.1 System messages

This section describes the system messages.

Note that the authority to perform the operations described in this section is controlled according to the user type, and these operations are available to the following users.

System Administrator	Administrator	User
Y	N	N

The [System Message] screen is displayed by selecting [Monitoring] and then [System Message] from the menu.

On the [System Message] screen, messages related to a system such as the system operation state can be browsed. For messages, a user can also perform the operations to change the confirmation status, assign a mark, and edit comments. You can search for a message by specifying a condition.

Selecting the [Auto Update] check box automatically updates a list of system messages every 30 seconds.

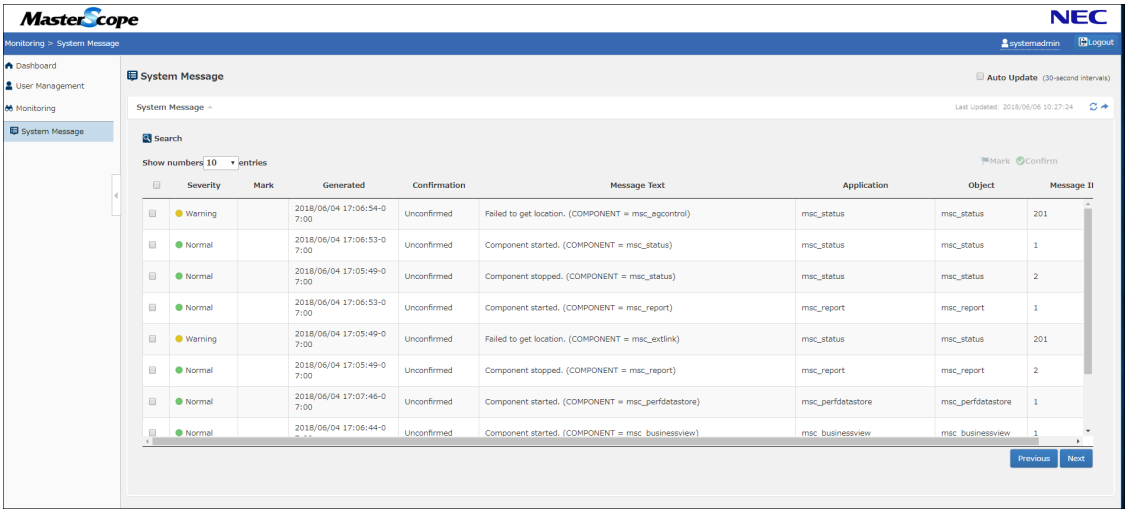

Figure 1-41 [System Message] screen

1.7.1.1 Displaying the message list

This section describes how to display the list of system messages and what each item of the list is for.

The [System Message] screen is displayed by selecting [Monitoring] and then [System Message] from the menu.

The [System Message] screen lists unconfirmed system messages.

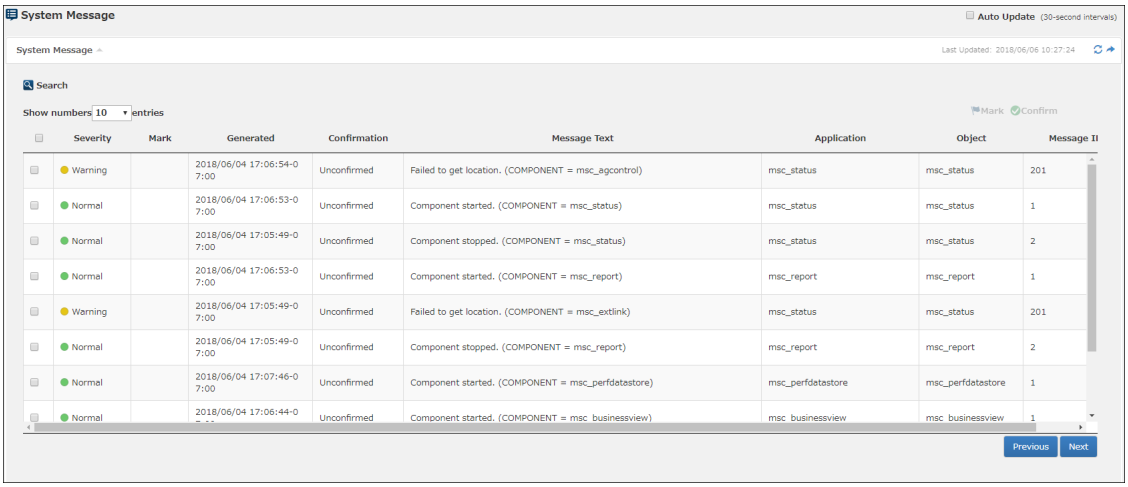

Figure 1-42 Message panel and messages

The items and buttons shown in the [System Message] screen are as follows.

Table 1-12 Item list ([System Message] screen - Message panel)

Item name	Description
[System Message] toggle	Opens and closes the message panel.
[Update] button	Updates the message panel.
[Add widget] button	Pastes the currently displayed message panel to the dashboard as a widget.
[Search] toggle	Opens and closes the search condition. This is hidden initially.
Show numbers [ ] entries	The number of messages to be displayed in the list per page. You can select the number of messages to be displayed from 10, 100, 500, and 1000.
[Mark] button	Marks the selected message.
[Confirm] button	Changes the confirmation status of the selected message.
[Previous] button	Displays messages newer than the displayed messages.
[Next] button	Displays messages older than the displayed messages.

The items and buttons shown in the message list of the [System Message] screen are as follows.

Table 1-13 Item list ([System Message] screen - Message list)

Item name	Description
Check box	The message whose check box is selected is an operation target.
Severity	Displays the severity.
Mark	Displays the mark.
Generated	Displays the generation date and time.
Confirmation	Displays the confirmation status.
Message Text	Displays the message text.
Application	Displays the application.
Object	Displays the object.
Message ID	Displays the message ID.

1.7.1.2 Searching messages

This section describes how to search system messages.

Clicking the [Search] toggle on the [System Message] screen displays the items for which a search condition can be specified.

Specifying a search condition and clicking the [Submit] button displays messages that meet the specified search condition in a list. For the items whose search condition is specified by using a character string (Message Text and Description), a regular expression search is performed

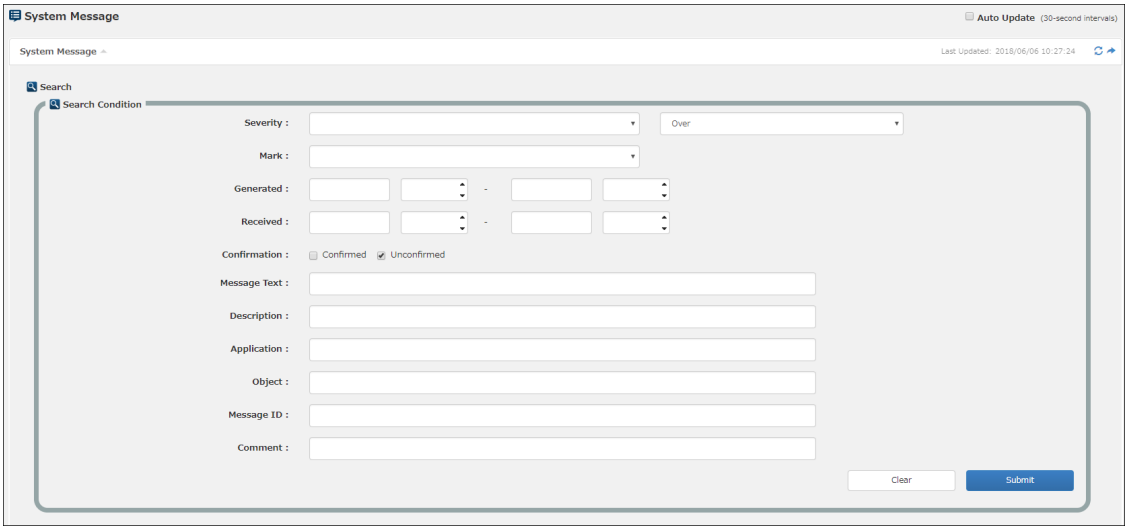

Figure 1-43 [System Message] screen - Search

Table 1-14 Item list ([System Message] screen - Search)

Item name	Input rule	Description
Severity	-	The selected severity and severity range ([Over], [Equal], or [Under]) are searched. If the severity is not selected, all severity levels are searched.
Mark	-	The selected mark is searched. If the mark is not selected, all marks are searched.
Generated	1970/01/01 00:00:00 to 2999/12/31 23:59:59	The selected or entered range of the generation dates and times are searched. This is the date and time when an agent generated the message on the monitored server machine. The time zone depends on the system time of the manager.
Received	1970/01/01 00:00:00 to 2999/12/31 23:59:59	The selected or entered range of the reception dates and times are searched. This is the date and time when the manager received the message generated on the monitored server machine. The time zone depends on the system time of the manager.
Confirmation	-	The selected confirmation status ([Confirmed] or [Unconfirmed]) is searched. Be sure to select either check box.
Message Text	Up to 1024 characters	The entered message text is searched.
Description	Up to 256 characters	The entered message summary is searched.
Application	Up to 1024 characters	The entered application is searched.
Object	Up to 1024 characters	The entered object is searched.
Message ID	Up to 128 characters	The entered message ID is searched.
Comment	Up to 1024 characters	The entered comment is searched.

Item name	Input rule	Description
Clear	-	Resets the entered (specified) values to the initial values.
Submit	-	Click this button to start searching.

1.7.1.3 Displaying message details

This section describes how to display details of a system message and what each item of the details is for.

Selecting a message shown in the message list in the [System Message] screen displays details of that message.

Figure 1-44 [System Message] screen - Message details

The items shown in the message details are as follows.

Table 1-15 Item list ([System Message] screen - Message details)

Item name	Description
Severity	Displays the severity.
Mark	Displays the mark.
Generated	Displays the generation date and time. This is the date and time when an agent generated the message on the monitored server machine.
Received	Displays the reception date and time. This is the date and time when the manager received the message generated on the monitored server machine.
Confirmation	Displays the confirmation status.
Message Text	Displays the message text.
Description	Displays the message summary.
Application	Displays the application.
Object	Displays the object.
Message Definition ID	Displays the message definition ID.
Message ID	Displays the message ID.
Comment	Displays the comment.
[Mark] button	Assigns the mark.
[Confirm] button	Changes the confirmation status.
[Edit comment] button	Edits the comment.

1.7.1.4 Changing the confirmation status of a message

This section describes how to change the confirmation status of a message.

The following two methods are available to change the confirmation status of a message.

- Changing method 1

  1. Select the check box of the target message in the list of messages and click the [Confirm] button.
  2. The confirmation statuses are displayed under the [Confirm] button. Select the status that you want to change.

     By selecting two or more messages, you can change the confirmation statuses of multiple messages simultaneously.

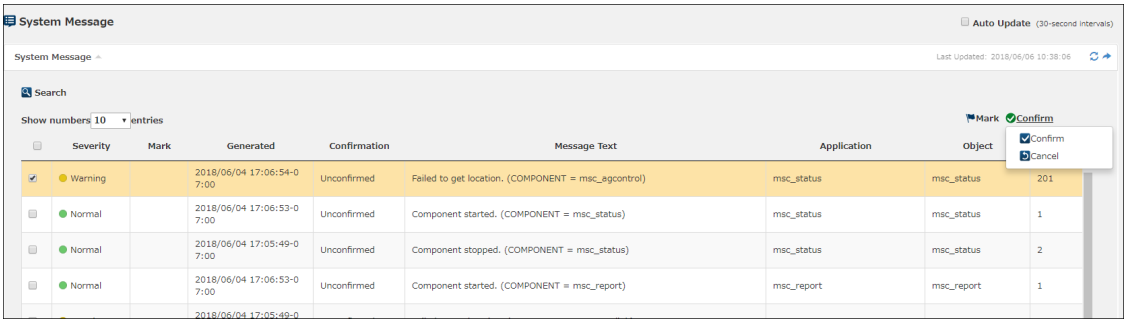

Figure 1-45 Confirmation status changing method 1

- Changing method 2

  1. Click the message whose comment you want to edit in the list of messages.
  2. [Message Details] is displayed. Click the [Confirm] button.

Figure 1-46 Confirmation status changing method 2

  3. The [Confirm] dialog box is displayed. Click the [Submit] button.

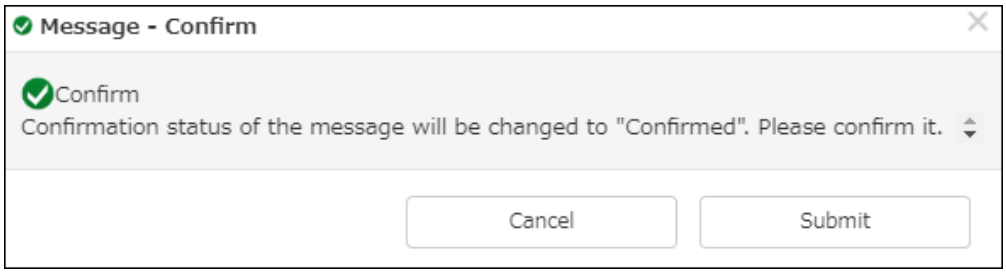

Figure 1-47 [Confirm] dialog box

1.7.1.5 Assigning a mark to a message

This section describes how to assign a mark to a message.

The following two methods are available to assign a mark to a message.

- Assignment method 1

  1. Select the check box of the target message in the list of messages and click the [Mark] button.
  2. The [Marking up] dialog box is displayed. Select the mark that you want to assign to the message and click the [Submit] button.

     By selecting two or more messages, you can assign marks to multiple messages simultaneously.

Figure 1-48 Mark assignment method 1

- Assignment method 2

  1. Click the message whose comment you want to edit in the list of messages.
  2. [Message Details] is displayed. Click the [Mark] button.

Figure 1-49 Mark assignment method 2

  3. The [Marking up] dialog box is displayed. Select the mark that you want to assign to the message and click the [Submit] button.

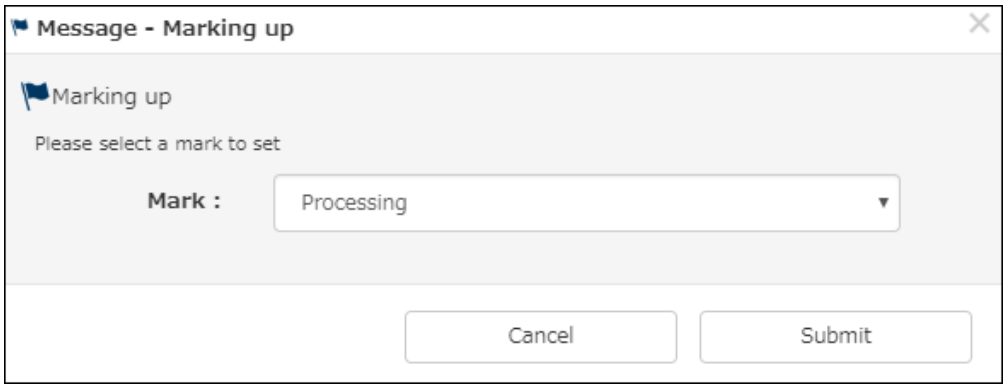

Figure 1-50 [Marking up] dialog box

1.7.1.6 Editing the comment of a message

This section describes how to edit the comment of a message.

1. Click the message whose comment you want to edit in the message list.
2. [Message Details] is displayed. Click the [Edit comment] button.

Figure 1-51 Editing the comment

3. The [Edit comment] dialog box is displayed. Enter a comment and click the [Submit] button.

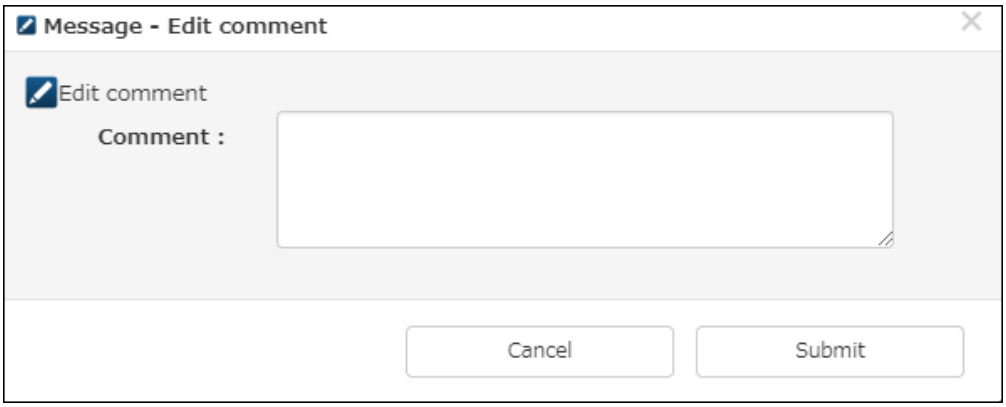

Figure 1-52 [Edit comment] dialog box

1.7.2 Node

This section describes the node function.

The [Node] screen is displayed by selecting [Monitoring] and then [Node] from the menu.

On the [Node] screen, the node list panel, status panel (initially hidden), message panel (initially hidden) are displayed.

On the node list and status panels, the current status of the node to be monitored is displayed. The displayed node severity is the most urgent severity among the monitoring items (such as process and performance information) of the node. Also, nodes can be grouped in any hierarchy. The group severity is the most urgent severity among the nodes (groups) in the group. Therefore, the failed node can be identified by tracing groups with high severity from the top of the group tree.

At the root of the group tree, a filter can be set that is used to issue a report according to preregistered settings if a specific message is generated. For information about how to display the filter setting screen, see "1.7.2.1 Displaying the node list (page 29)". For details about the filter settings, see "1.7.2.10 Setting a reporting filter (page 39)".

On the message panel, messages of the node or group selected on the node list panel are displayed and can be operated. For details about the displayed content, see "1.7.3.1 Displaying the message list (page 53)".

Selecting the [Auto Update] check box automatically updates each panel every 30 seconds.

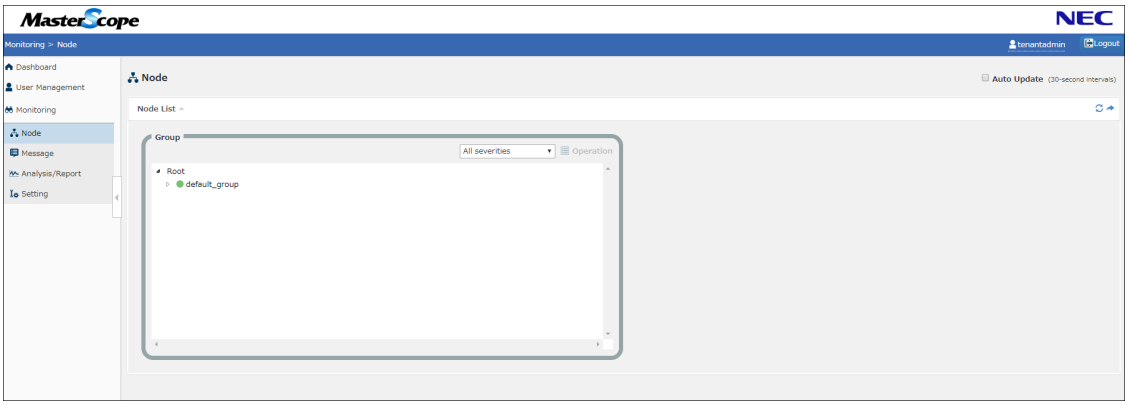

Figure 1-53 [Node] screen

1.7.2.1 Displaying the node list

This section describes the [Node List] panel that displays the node list.

While the authority to perform the operations described in this section is controlled according to the role, they are available to all users except system administrators.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

The node list panel is displayed on the [Node] screen by selecting [Monitoring] and then [Node] from the menu. The group tree is displayed at the left to the [Node List] panel.

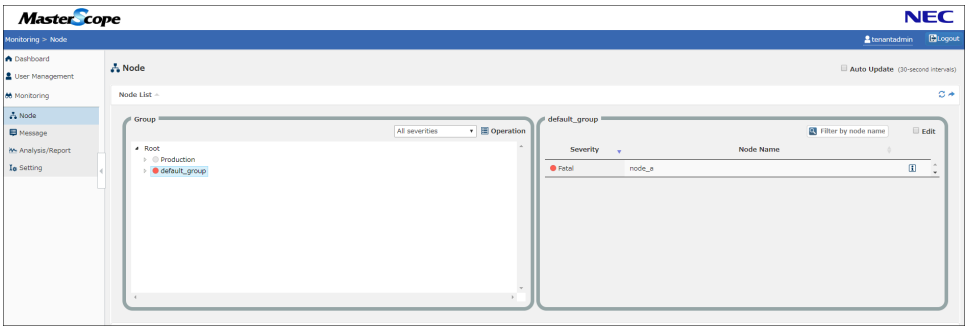

Figure 1-54 [Node] screen - [Node List] panel and group tree

Table 1-17 Item list ([Node] screen - [Node List] panel and group tree)

Item name	Description
[Node List] toggle	Opens and closes the [Node List] panel.
[Update] button	Updates the [Node List] panel.
[Add widget] button	Pastes the currently displayed node list panel to the dashboard as a widget.
Severity selection	Displays the groups whose severity is more urgent than the selected severity in the tree.
[Operation] menu button	Displays the [Operation] menu available for the selected group. • "1.7.2.4 Creating a group (page 34)" • "1.7.2.5 Changing a group name (page 35)" • "1.7.2.6 Moving a group (page 36)" • "1.7.2.7 Deleting a group (page 37)" • "1.7.2.11 Applying a monitoring template (group) (page 47)"

Item name	Description
	• "1.7.2.10.1 Displaying a list of filters (page 40)" The operation described in "1.7.2.10.1 Displaying a list of filters (page 40)"is available only when the selected group is the root.

The list of nodes is displayed by selecting a group from the group tree on the [Node List] panel.

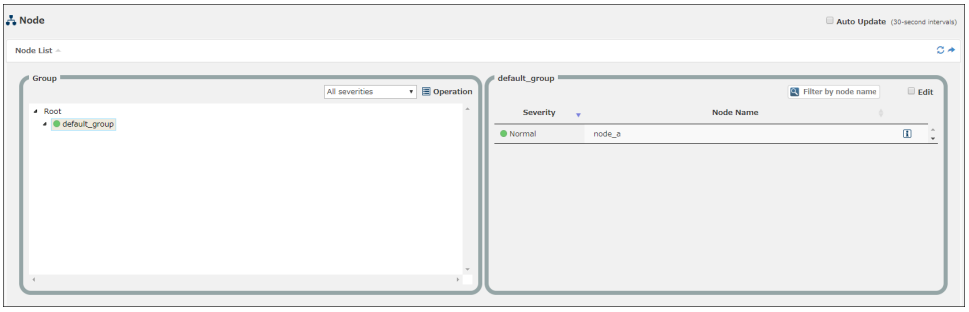

Figure 1-55 [Node] screen - Node List

Table 1-18 Item list ([Node] screen - Node List)

Item name	Description
[Edit] check box	Selecting this check box enables to move a node. For details, see "1.7.2.8 Moving a node (page 38)".
Search field	Searches the node name. Lines of the node names including the entered character string are extracted.
Severity	Displays the severity.
Node Name	Displays the node name.
Details icon	Clicking this icon displays the [Node Detail] dialog box.

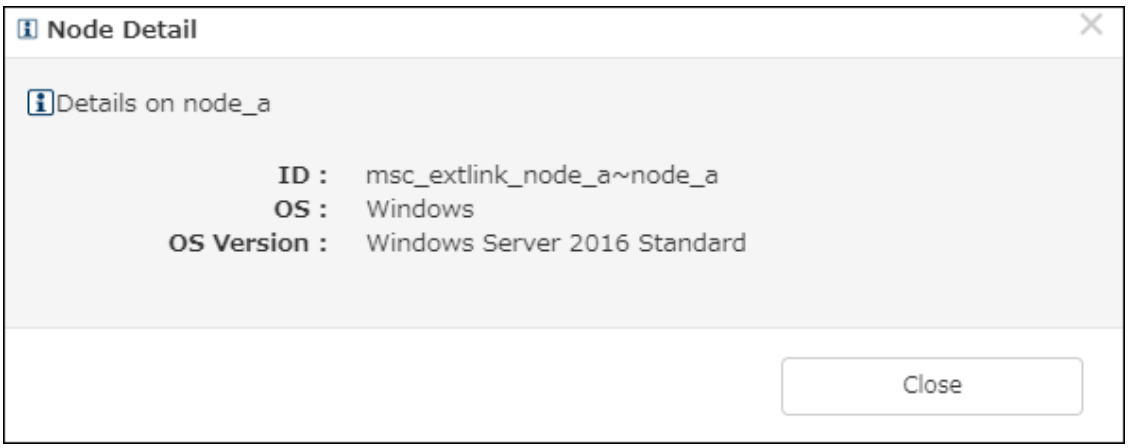

Figure 1-56 [Node Detail] dialog box

Table 1-19 Item list ([Node Detail] dialog box)

Item name	Description
ID	ID to identify a node. (The node ID or agent ID might be displayed.)
OS	Displays the OS type.
OS Version	Displays the OS version.

1.7.2.2 Displaying the status panel

This section describes the status panel that displays the status of a group or node.

While the authority to perform the operations described in this section is controlled according to the role, they are available to all users except system administrators.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

The status of a group is displayed by selecting the group in the group tree.

The status of a node is displayed by selecting the node on [Node List].

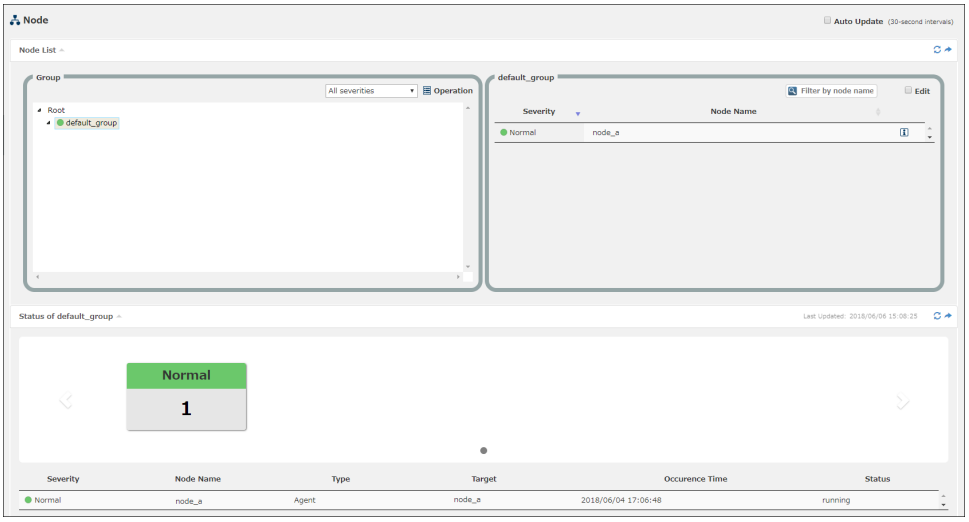

Figure 1-57 [Node] screen - Status panel

Table 1-20 Item list ([Node] screen - Status panel)

Item name	Description
Status toggle	Opens and closes the status panel.
[Update] button	Updates the status panel.
[Add widget] button	Pastes the currently displayed status panel to the dashboard as a widget. When the group status is displayed, both or either of the number of nodes of each severity and the list of statuses can be displayed.
Severity selection	Tallies and displays the number of nodes of each severity within the group. This is displayed when a group is selected.
Severity	Displays the severity.
Node Name	Displays the name. This is displayed when [Details] is performed for a group.
Type	Displays the type.
Target	Displays the target.
OccurenceTime	Displays the generation date and time.
Status	Displays the status.
Operation	Displays the Operation icons. This is displayed only when a node is selected. • If [Type] is [Performance], the performance graph display icon is displayed. For details of performance graph display, see "1.7.2.3 Displaying a performance graph (page 32)".

Item name	Description
	• If [Type] is [Process], the [start] and [stop] icons to recover processes are displayed. This is displayed for a user who has the operation management operation right. • If [Type] is [Windows Service], the [start], [stop], and [Other Operations] icons to recover Windows services are displayed. This is displayed for a user who has the operation management operation right. Clicking the [Other Operations] icon displays the pull-down menu. From the displayed pull-down menu, other operations such as [pause] and [resume] can be selected. Stopping a Windows service fails if there is any service that depends on the Windows service to be stopped. To stop a Windows service and a service that depends on the Windows service, select [force stop] from [Other Operations]. If a monitoring item is recovered, no operation can be performed for the monitoring item for a certain period (approximately 20 seconds).

1.7.2.3 Displaying a performance graph

This section describes the performance graph that is created based on the acquired performance values.

While the authority to perform the operations described in this section is controlled according to the role, they are available to all users except system administrators.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

Clicking a performance graph icon in the agent monitoring status displays a performance graph.

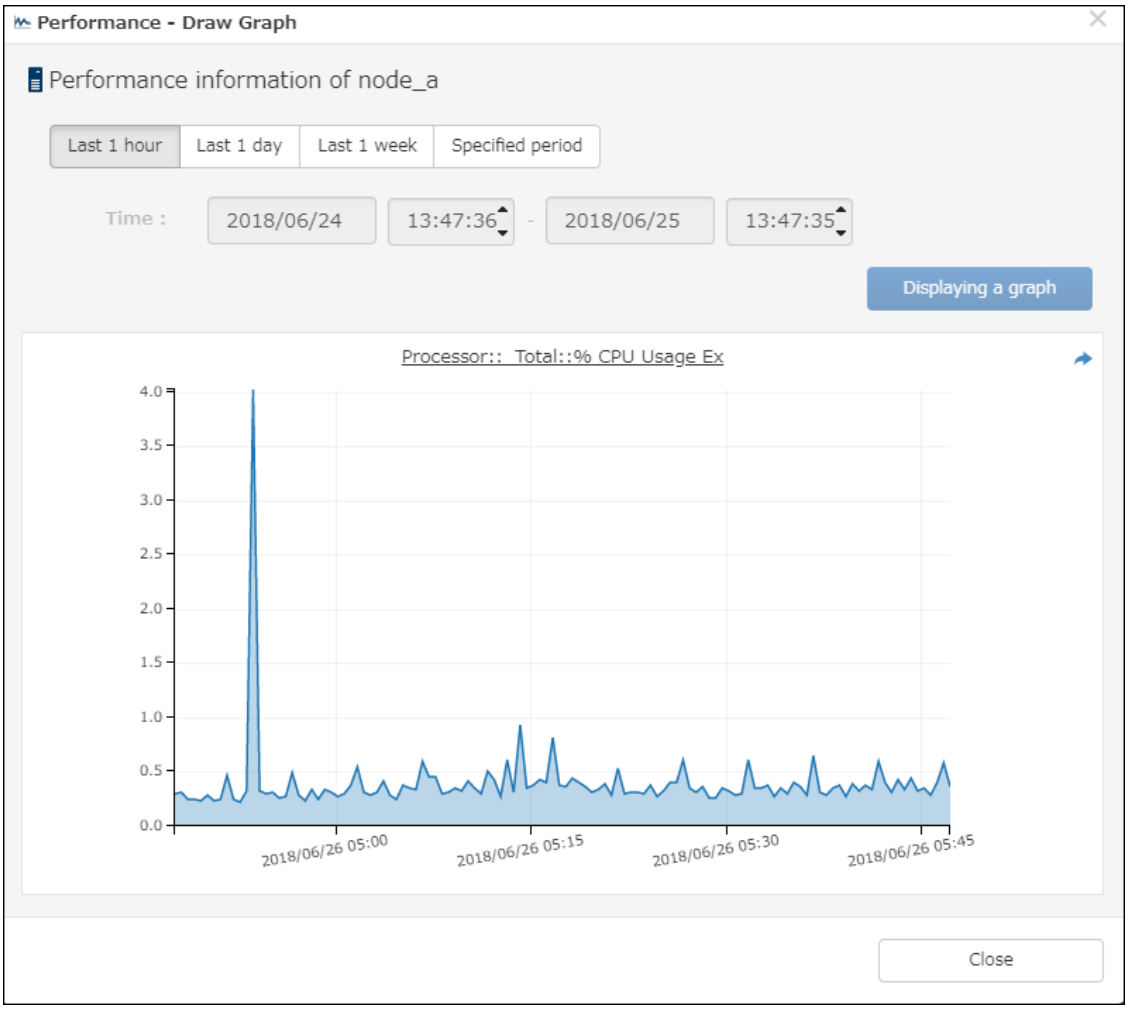

Figure 1-58 Performance graph

Table 1-21 Item list ([Performance graph])

Item name	Description
Last 1 hour	Displays a graph for the last hour. This button is selected at initial display.
Last 1 day	Displays a graph for the last day.
Last 1 week	Displays a graph for the last week.
Specified period	Specify the start time and end time and click the [Displaying a graph] button to display a graph for the specified period. The time range available for the start time and end time is 1971/01/01 00:00 to 2037/12/31 23:59. The interval between the start time and end time is up to one week.
[Add widget] button	Pastes the currently displayed status panel to the dashboard as a widget

Note

Depending on the display duration, some of the data may be omitted due to the limit of the rendering area. A graph can be displayed without omitting data for the following durations.

Table 1-22 Durations for which a graph can be displayed without omitting data

Monitoring interval	Duration
30 seconds (Default)	3 hours 7 minutes 30 seconds (11250 seconds)
10 seconds (Minimum)	1 hours 2 minutes 30 seconds (3750 seconds)

1.7.2.4 Creating a group

This section describes how to create a group.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

1. In the group tree, select the parent group in which to create a group.
2. Since [Create group] of the [Operation] menu becomes available, click it.

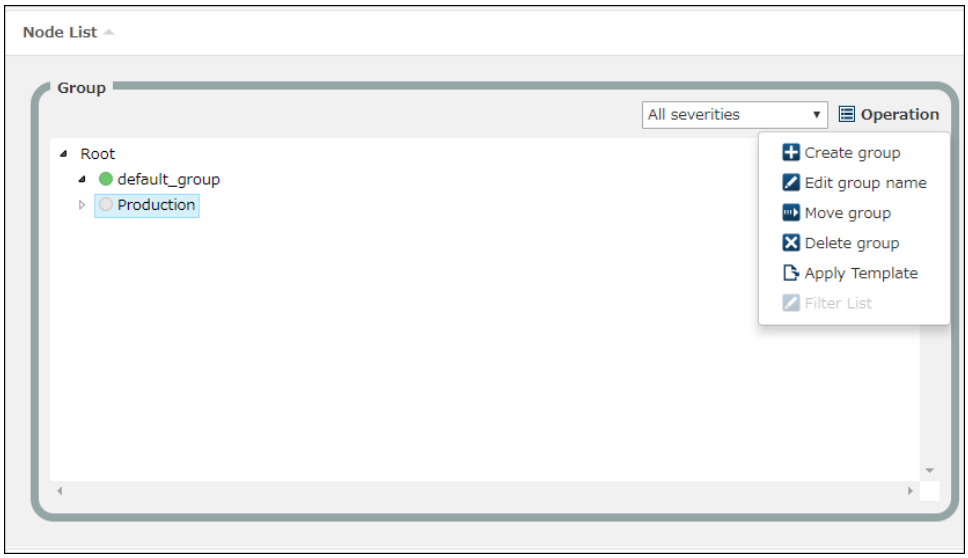

Figure 1-59 [Node] screen - Create group

3. The [Create group] dialog box is displayed. Enter the group name and click the [OK] button to create a group.

Figure 1-60 [Create group] dialog box

Table 1-23 Item list ([Create group] dialog box)

Item name	Input rule	Description
Group Name	Up to 128 characters	A group is created with the specified name.

1.7.2.5 Changing a group name

This section describes how to change the group name.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

1. In the group tree, select the group whose name you want to change.
2. Since [Edit group name] of the [Operation] menu becomes available, click it.

Figure 1-61 [Node] screen - Edit group name

3. The [Edit group name] dialog box is displayed. Enter the group name and click the [OK] button to change the group name.

Figure 1-62 [Edit group name] dialog box

Table 1-24 Item list (Edit group name)

Item name	Input rule	Description
Group Name	Up to 128 characters	The group name is changed to the specified name.

1.7.2.6 Moving a group

This section describes how to move a group.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

1. Select the group that you want to move in the group tree.
2. Since [Move group] of the [Operation] menu becomes available, click it.

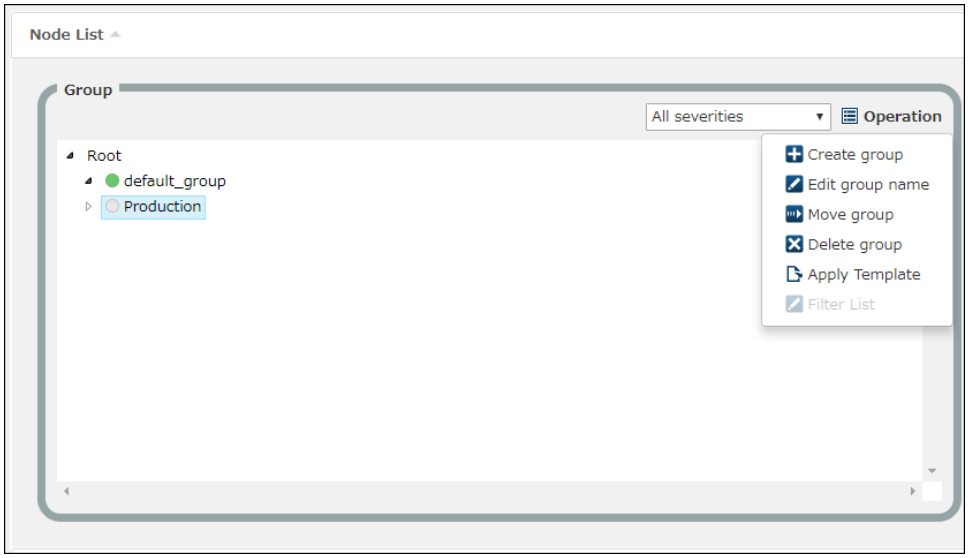

Figure 1-63 [Node] screen - Moving a group

3. The [Move group] dialog box is displayed. Select the group to which to move the group and click the [OK] button to move the group.

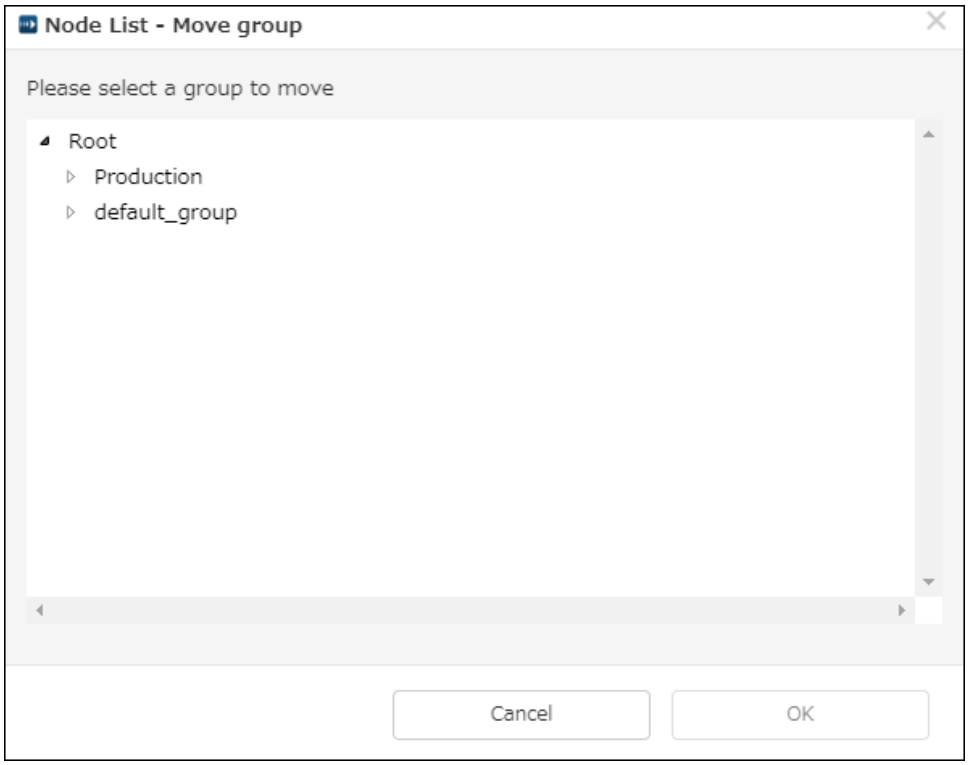

Figure 1-64 [Move group] dialog box

1.7.2.7 Deleting a group

This section describes how to delete a group.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Note

- If a group exists in the group that you want to delete, the target group cannot be deleted.
- If a node exists in the group that you want to delete, the node is moved to default_group after the group is deleted.

1. Select the group that you want to delete in the group tree.
2. Since [Delete group] of the [Operation] menu becomes available, click it.

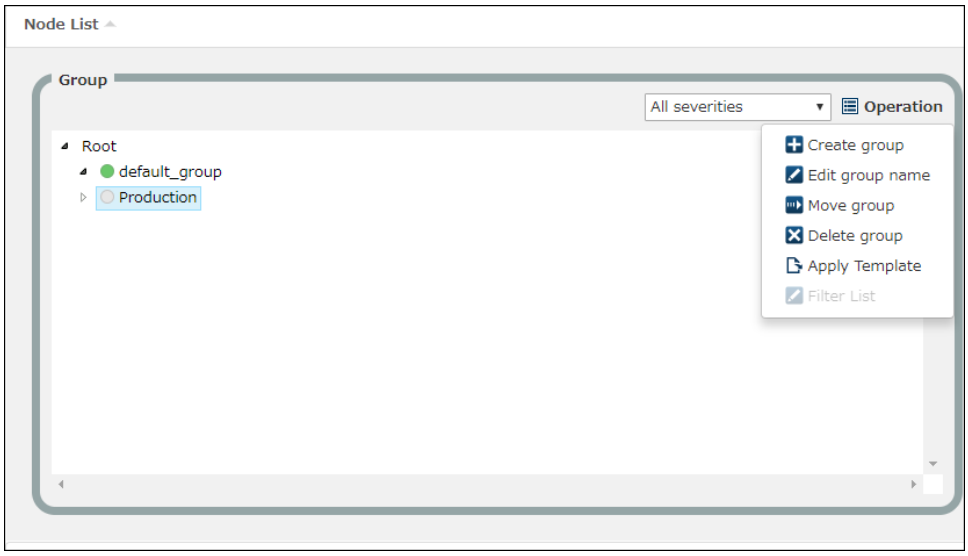

Figure 1-65 [Node] screen - Delete group

3. The [Delete group] dialog box is displayed. Click the [OK] button to delete the selected group.

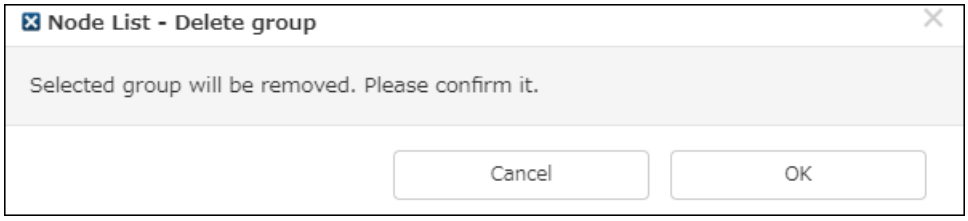

Figure 1-66 [Delete group] dialog box

1.7.2.8 Moving a node

This section describes how to move a node.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

1. Select the [Edit] check box above the node list table.
2. Select the node that you want to move.
3. Click the [Move] button under the node list table.

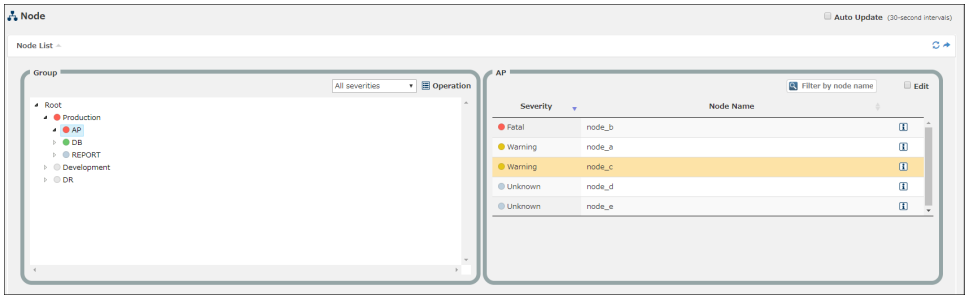

Figure 1-67 [Node] screen - Moving a node

4. The [NodeMove] dialog box is displayed. Select the group to which to move the node and click the [OK] button to move the node.

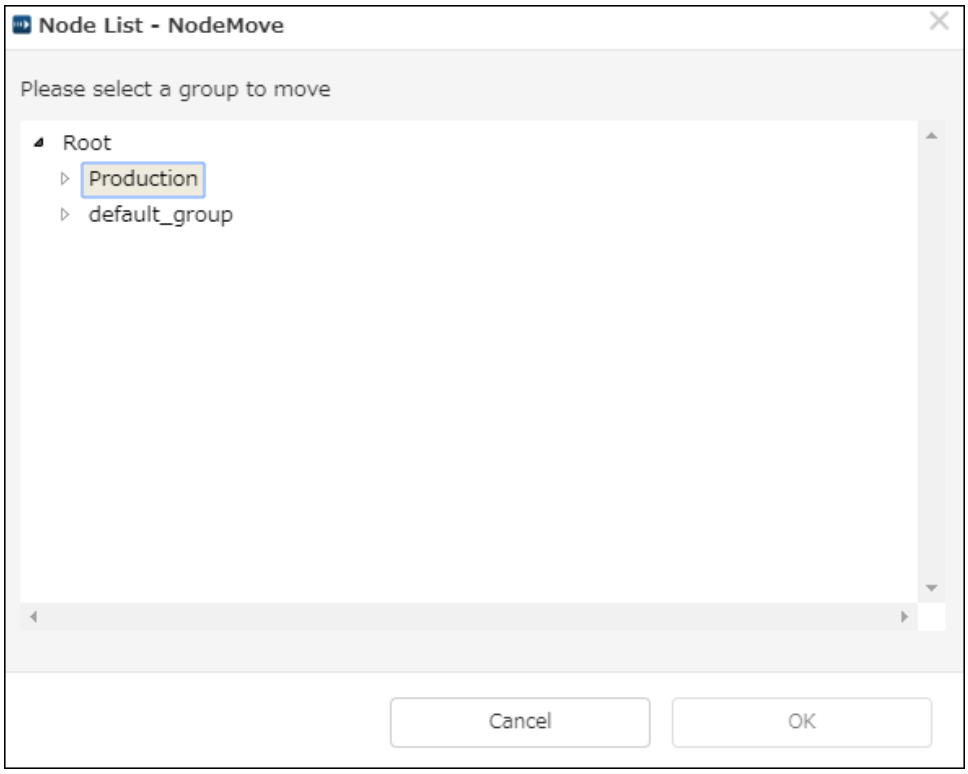

Figure 1-68 [NodeMove] dialog box

1.7.2.9 Start monitoring nodes

This section describes the setup of node monitoring.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

1. Select the [Edit] check box above the node list table.
2. Select the node for which to set up monitoring.
3. Clicking the [Node Monitoring] button below the node list table displays the [Node Monitoring] screen.

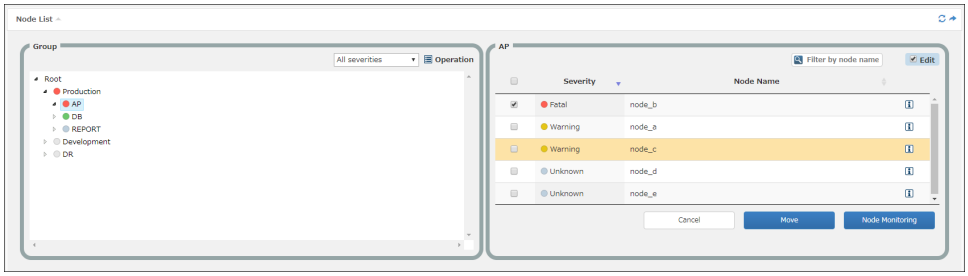

Figure 1-69 [Node] screen - Node monitoring

4. For details about monitoring setup, see "1.7.5.2 Setting up monitoring (page 102)".

1.7.2.10 Setting a reporting filter

This section describes the message filter function that reports messages via the [Node] screen.

The root node in the [Node] screen can centrally manage and reference the hardware and software messages of agents in the system. If a specific message is generated, it can report that message according to preregistered settings to notify the operator.

To perform reporting, you need to set a filter that determines whether to report a message generated by the system.

Displaying a list of filters

This section describes how to set a message filter that reports messages via the [Node] screen.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

To set a filter, use the [Filter List] screen.

For information about how to display the [Filter List] screen, see "1.7.2.1 Displaying the node list (page 29)".

The filters are displayed in priority order. When a message is output, it goes through the filters in order of priority and the action set in the first filter whose condition meets the message is executed.

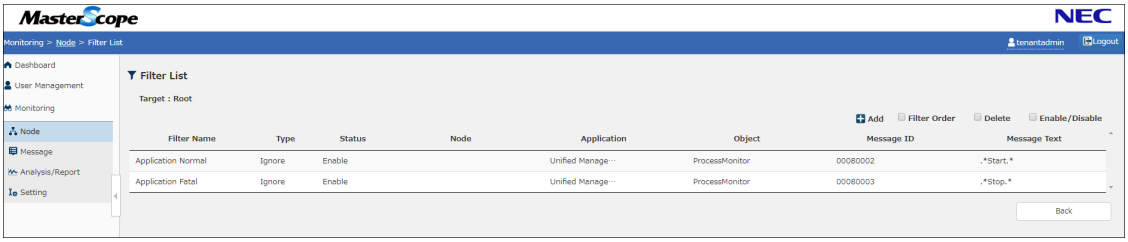

Figure 1-70 List of filters

Table 1-25 Item list ([Filter List] screen)

Item name	Description
Add	Add a filter.
Filter Order	Selecting this check box enables to change the filter order.
Delete	Selecting this check box enables to delete a filter.
Enable/Disable	Selecting this check box enables or disables to delete a filter.
Filter Name	Displays the filter name.
Type	Displays the filter type. Match: Messages that match the filter are reported. Ignore: Messages that match the filter are not reported. (The succeeding filtering is not performed.)
Status	Displays the filter status. Enable: Indicates that the filtering condition is applied. Disable: Indicates that the filtering condition is not applied temporarily.
Node	Displays the condition text (in regular expression) for the node name.

Item name	Description
Application	Displays the condition text (in regular expression) for the application.
Object	Displays the condition text (in regular expression) for the object.
Message ID	Displays the condition text (in regular expression) for the message ID.
Message Text	Displays the condition text (in regular expression) for the message text.
[Back] button	Returns you to the [Node] screen.

Clicking the filter at the top of the list displays the filter details.

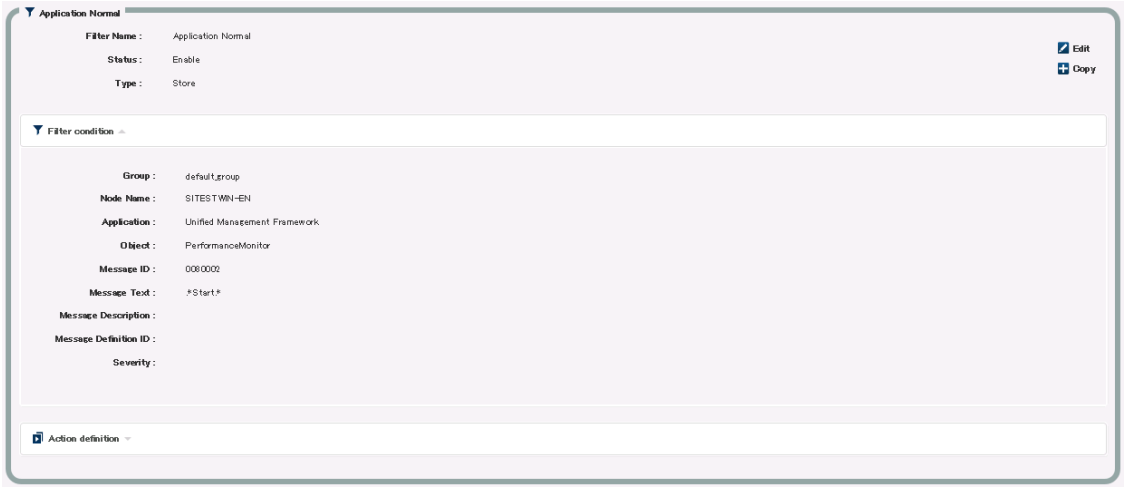

Figure 1-71 [Filter List] screen - Filter details

Table 1-26 Item list ([Filter List] screen - Filter details)

Item name	Description
Filter Name	Displays the filter name.
Status	Displays the filter status. Enable: Indicates that the filtering condition is applied. Disable: Indicates that the filtering condition is not applied temporarily.
Type	Type of the filter When [Match] is specified, the messages that match the filter are reported. When [Ignore] is specified, the messages that match the filter are not reported. (The succeeding filtering is not performed.) Action definitions cannot be set for a filter whose type is [Ignore].
Group	Displays the condition for the group.
Node Name	Displays the condition text (in regular expression) for the node name.
Application	Displays the condition text (in regular expression) for the application.
Object	Displays the condition text (in regular expression) for the object.
Message ID	Displays the condition text (in regular expression) for the message ID.
Message Text	Displays the condition text (in regular expression) for the message text.
Message Description	Displays the condition text (in regular expression) for the message summary.

Item name	Description
Message Definition ID	Displays the condition text (in regular expression) for the message definition ID.
Severity	Displays the severity condition.
[Edit] button	Changes the filter condition. For details, see "1.7.2.10.2 Adding or changing the filter (page 42)".
[Copy] button	Add a filter by quoting the filter information being displayed in the details. For details, see "1.7.2.10.2 Adding or changing the filter (page 42)". The added filter is inserted at one line above the quoted filter.

Note

For a "negative" condition (that is, targeting the filter that does not match the specified condition), an exclamation mark is displayed at the top of the condition.

When the type of the filter is [Store] and an action definition is set, the [Filter details] screen displays the following [Action definition] list.

Table 1-27 Item list ([Filter List] screen - Filter details - Action definition)

Item name	Description
Status	Sets the status of the action definition. Enable: In this status, the defined action (Email report or command execution) is taken when a message that matches the filter is generated. Disable: In this status, the defined action (Email report or command execution) is not taken even when a message that matches the filter is generated. It is used to suspend the execution of the action temporarily.
Email report	Displays the reporting name of the settings for the Email report to be executed when a message matches the filter.
Email report information button	Displays the details of the Email report settings in a dialog box. For details of the Email report settings, see "1.7.5.4.1 Adding or changing an email report setting (page 154)".
Command execution	Displays the reporting name of the settings for the command to be executed when a message matches the filter.
Command information button	Displays the details of the command settings in a dialog box. For details of the command settings, see "1.7.5.5.1 Adding or changing a command setting (page 161)".

Adding or changing the filter

This section describes how to add or change the message filter.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

The [Add Message Filter] screen is displayed by clicking [Add] on the [Filter List] screen or by selecting a filter on the [Filter List] screen and clicking [Copy]. When clicking [Copy], each condition input field is displayed with the selected condition set.

The [Edit Message Filter] screen is displayed by selecting a filter on the [Filter List] screen and clicking [Edit].

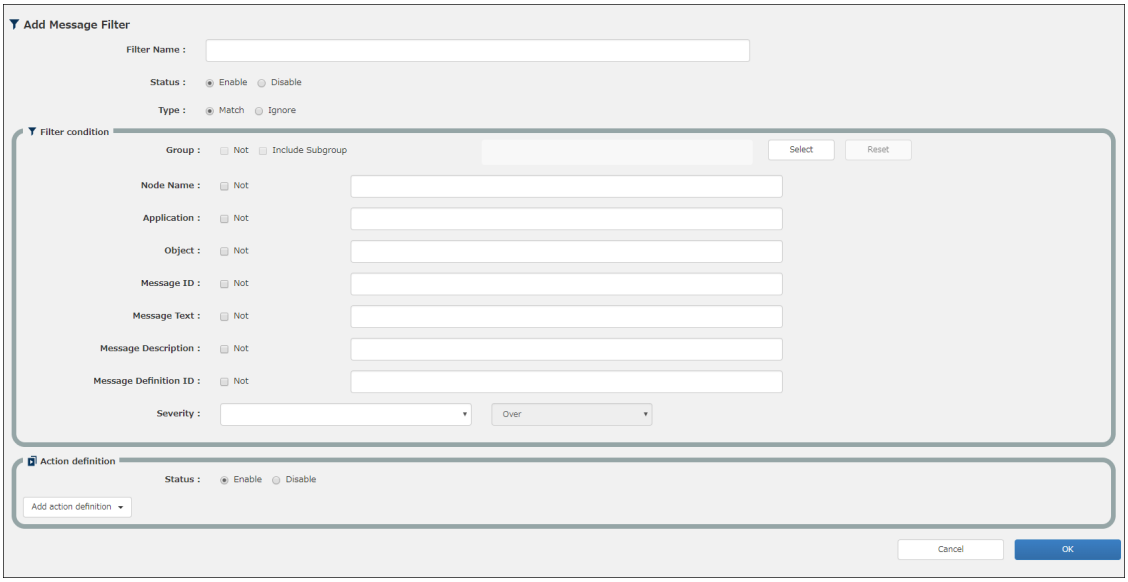

Figure 1-72 [Add Message Filter] screen

Table 1-28 Item list ([Add Message Filter] screen)

Item name	Description
Filter Name	Enter the filter name by using 0 to 128 characters.
Status	When [Enable] is specified, the status of the filter is "enabled". When [Disable] is specified, the status of the filter is "disabled".
Type	Type of the filter When [Match] is specified, the messages that match the filter are reported. When [Ignore] is specified, the messages that match the filter are not reported. (The succeeding filtering is not performed.) Action definitions cannot be set for a filter whose type is [Ignore].
Group	Select a group. Messages for the nodes in the selected group are targeted.
Include Subgroup	When this check box is selected, all groups in the selected group are targeted.
Not (Group)	When this check box is selected, groups other than the selected group are targeted. If [Include Subgroup] is also selected, groups other than "all groups in the selected group" are targeted.
Not (Node Name)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the node name, match the condition.
Node Name	Specify the filter condition for node names in regular expression.
Not (Application)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the application, match the condition.

Item name	Description
Application	Specify the filter condition for the application.
Not (Object)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the object, match the condition.
Object	Specify the filter condition for the object (name of the object in which a massage is generated) in regular expression.
Not (Message ID)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the message ID, match the condition.
Message ID	Specify the filter condition for the message ID.
Not (Message Text)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the message text, match the condition.
Message Text	Specify the filter condition for the message text.
Not (Message Description)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the message overview, match the condition.
Message Description	Specify the filter condition for the message overview.
Not (Message Definition ID)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the message definition ID, match the condition.
Message Definition ID	Specify the filter condition for the message definition ID to be used to generate a message text.
Severity	Specify the filter condition for the severity.
Severity Range	Select [Over], [Equal], or [Under] for the severity.

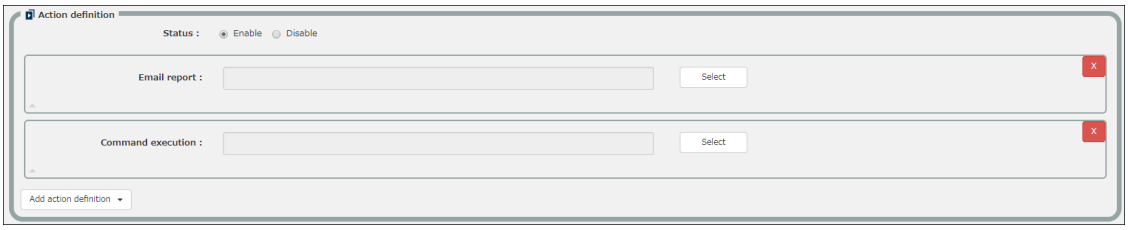

Figure 1-73 [Add Message Filter] screen - Action definition

Table 1-29 Item list ([Add Message Filter] screen - Action definition)

Item name	Description
Status	Sets the status of the action. Enable: In this status, the defined action (Email report or command execution) is taken when a message that matches the filter is generated. Disable: In this status, the defined action (Email report or command execution) is not taken even when a message that matches the filter is generated. It is used to suspend the execution of the action temporarily.
Add action definition	Add an action to be taken when a message matching the filter is generated. Select an action from the following.

Item name	Description
	Email report: A specified email is sent when the message is generated. Command execution: A specified command is executed when the message is generated. More than one action can be set per filter. To delete a set action definition, select [×] at the upper right of the action setting field.
Email report	When a message matching the filter is generated, an email with the preregistered content is sent. The [Email report Selection] dialog box, which appears when you click the [Select] button, displays the selected setting name. For information about how to set the content of the email to be sent, see "1.7.5.4.1 Adding or changing an email report setting (page 154)".
Command execution	When a message matching the filter is generated, a command is executed based on the preregistered setting. The [Command execution Selection] dialog box, which appears when you click the [Select] button, displays the selected setting name. For information about how to define the command to be executed, see "1.7.5.5.1 Adding or changing a command setting (page 161)".

When you have entered all necessary conditions, click [OK] to register them.

Clicking the [Cancel] button discards the data in the fields and returns you to the [Filter List] screen.

Changing the filter order

This section describes how to change the order of message filters.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Selecting [Filter Order] on the [Filter List] screen enables to change the filter order.

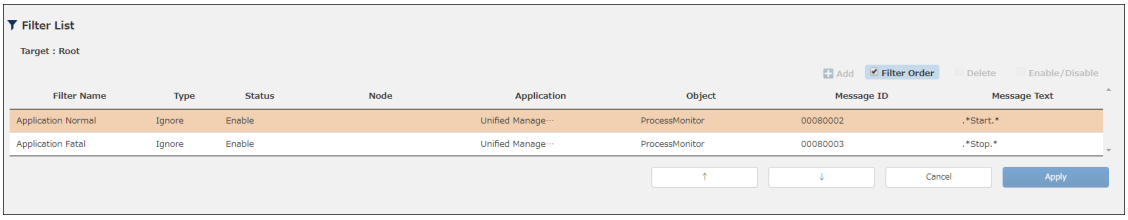

Figure 1-74 [Filter List] screen - Filter Order

Table 1-30 Item list ([Filter List] screen - Filter Order)

Item name	Description
↑	Moves the selected line up.
↓	Moves the selected line down.

Item name	Description
Cancel	Displays the [Filter List - Execution Order] dialog box (Cancel). "Table 1-31 Item list ([Filter List - Execution Order] dialog box (Cancel)) (page 46)"
Apply	Displays the [Filter List - Execution Order] dialog box (Apply). "Table 1-32 Item list ([Filter List - Execution Order] dialog box (Apply)) (page 46)"

[Filter List - Execution Order] dialog box (Cancel)

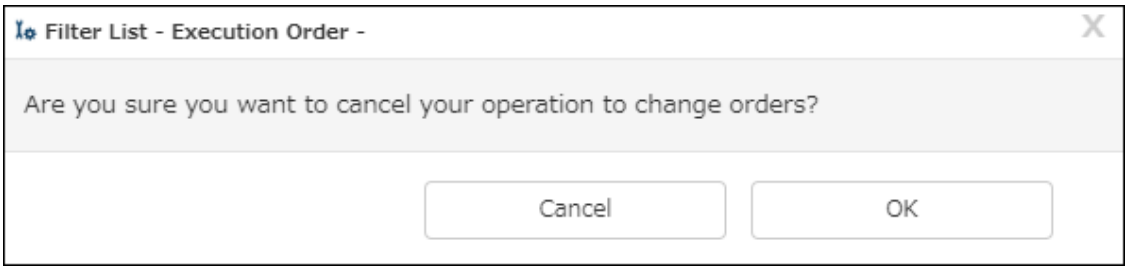

Figure 1-75 [Filter List - Execution Order] dialog box (Cancel)

Table 1-31 Item list ([Filter List - Execution Order] dialog box (Cancel))

Item name	Description
Cancel	Closes the dialog box without canceling the settings. (This returns you to the order change operation.)
OK	Stops changing the order and returns to the filter list display.

[Filter List - Execution Order] dialog box (Apply)

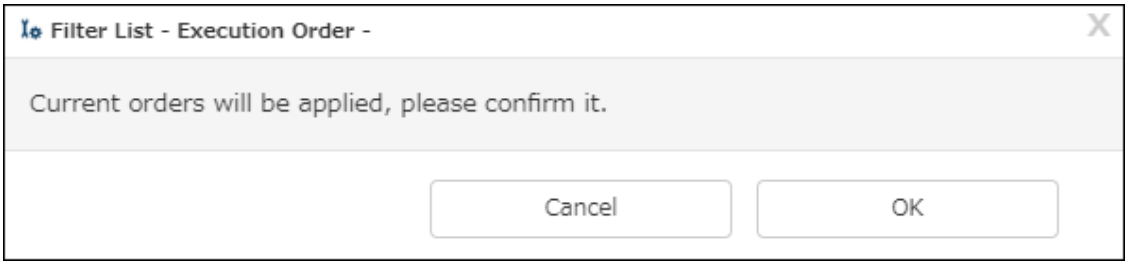

Figure 1-76 [Filter List - Execution Order] dialog box (Apply)

Table 1-32 Item list ([Filter List - Execution Order] dialog box (Apply))

Item name	Description
Cancel	Closes the dialog box without applying the order change. (This returns you to the order change operation.)
OK	Applies the order change and then closes the dialog box.

Deleting a filter

This section describes how to delete a message filter.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Selecting [Delete] on the [Filter List] screen enables to delete a filter.

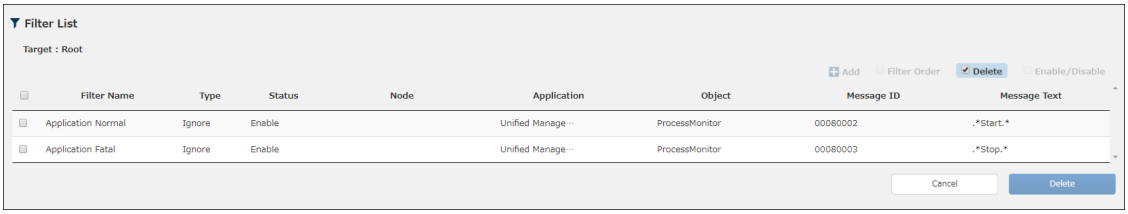

Figure 1-77 [Filter List] screen - Deleting

Selecting a filter that you want to delete from the list of filters and clicking the [Delete] button displays the [Filter List - Delete Filter] dialog box. Click [OK] to delete the selected filter.

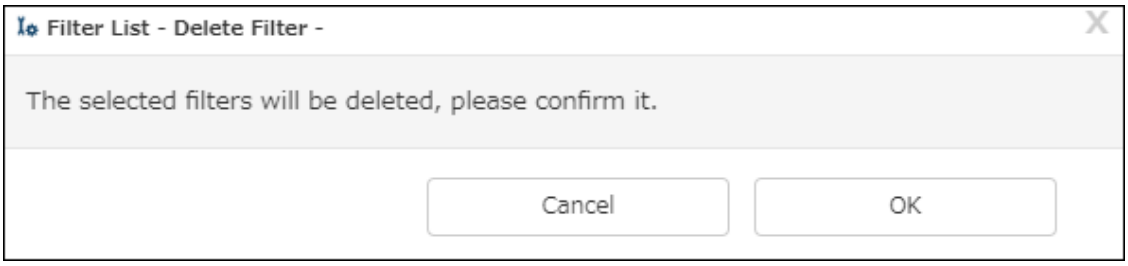

Figure 1-78 [Filter List - Delete Filter] dialog box

1.7.2.11 Applying a monitoring template (group)

This section describes how to apply a monitoring template from the node list.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

1. In the group tree of the [Node] screen, select the group to which you want to apply a template.
2. Click [Apply Template] in the [Operation] menu.

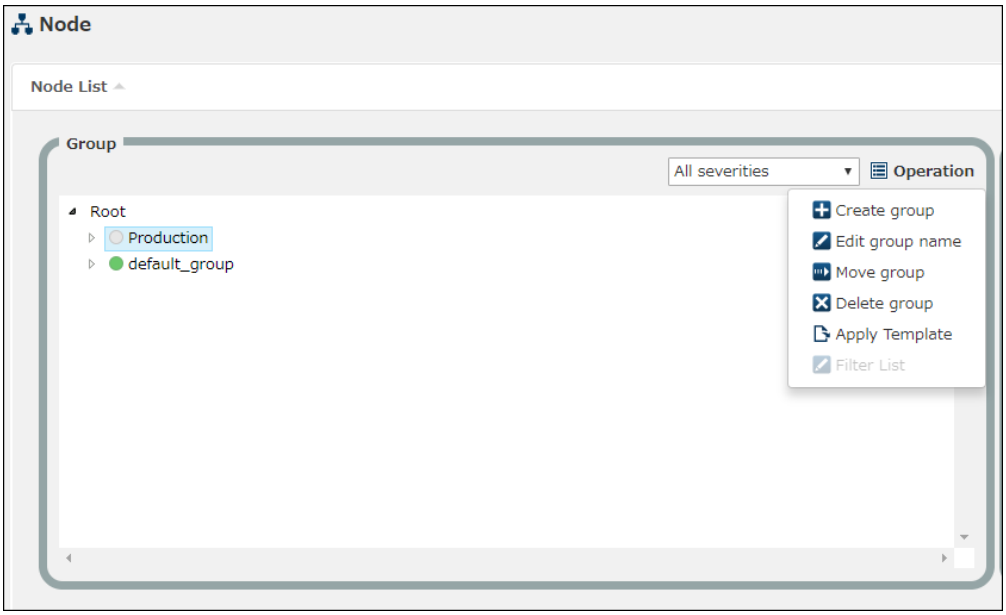

Figure 1-79 [Node] screen - Apply Template

3. The [Select Template] dialog box is displayed. Select the template you want to apply, and click the [OK] button.

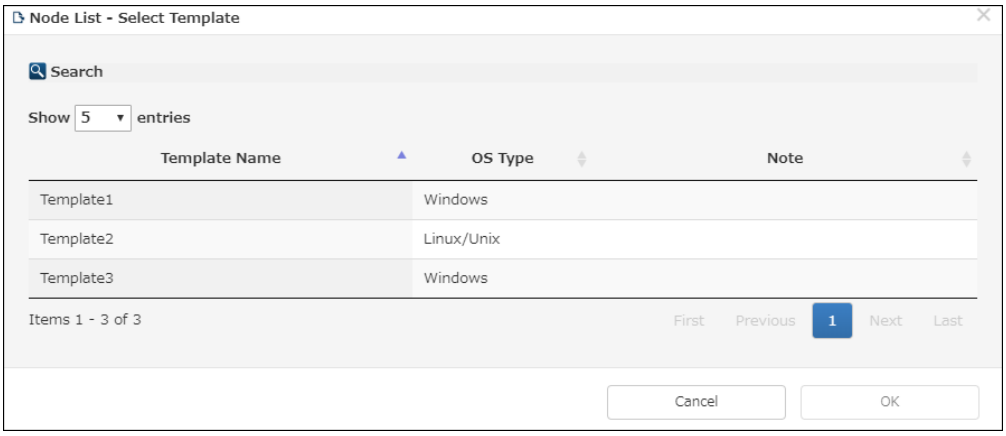

Figure 1-80 [Select Template] dialog box

4. A task list is displayed that shows the status of template application. For information about the items displayed in the task list, see "1.7.2.12 Task (page 49)".

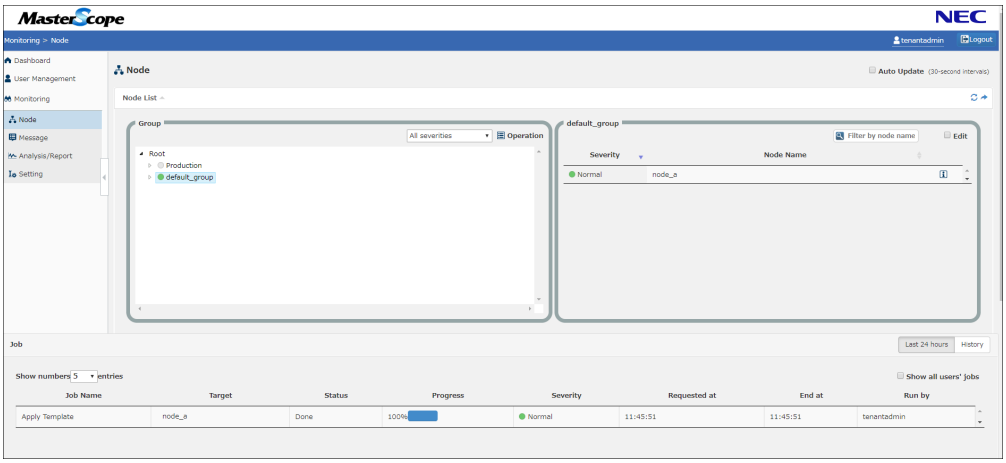

Figure 1-81 Task List

5. If you select a task in the task list, the [Task Detail] dialog box is displayed that lets you view the template application execution log. For information about the items displayed in [Task Detail], see "1.7.2.12 Task (page 49)".

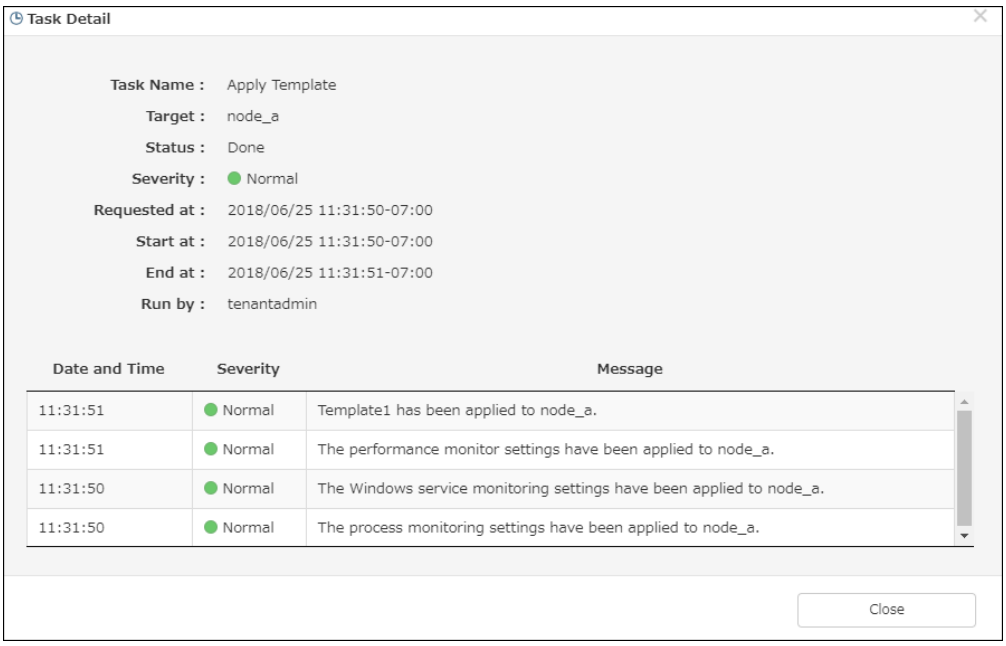

Figure 1-82 [Task Detail] dialog box

1.7.2.12 Task

This section describes tasks.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

Clicking [Task] in the lower part of the [Node] screen displays the task list. This is automatically displayed when a new task, such as the application of a template, arises.

Table 1-33 Task List

Item name	Description
[Last 24 hours] button	Displays the tasks executed in the most recent 24 hours.
[History] button	Displays the history of the executed tasks.

Clicking the [Last 24 hours] button lists the tasks executed in the most recent 24 hours.

Figure 1-83 Task list (Last 24 hours)

Table 1-34 Item list (Task list (Last 24 hours))

Item name	Default value	Description
[Show [ ] entries]	5	Select the number from 5, 10, 50, and 100. Specify the number of tasks to be displayed in the task list. The specified number of tasks are displayed in the list in the order of request dates, starting with the most recently executed task.
Show all users' tasks	Unchecked	If you do not select this check box, the tasks executed by the login user are listed. If you select this check box, the information about the tasks executed by other users is displayed. If you are an administrator, the information about the tasks registered by users is also displayed.
Task Name		Displays the type of the executed task. In this version, only [Apply Template] is displayed.
Target		Displays the node for which the task was executed.
Status		Displays the status of the task. • Stand by • Running • Done
Progress		Indicates the progress of the task execution. When the task is completed, 100% is shown.
Severity		Displays the severity of the task. One of the following severities is displayed: • Fatal • Warning • Unknown • Normal • Empty • Unmanaged
Requested at		Displays the execution request time of the task in the hh:dd:ss format.
End at		When the task is completed, the completion time is displayed in the hh:dd:ss format. When the task is not completed, the field is blank.
Run by		Displays the name of the user who executed the task.

Clicking the [History] button lets you view the history of tasks. The task history enables you to narrow down the task list by severity or by request date and time.

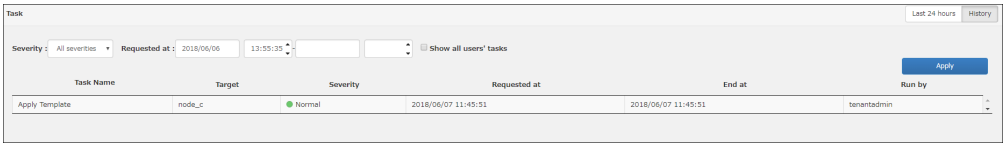

Figure 1-84 Task list (History)

Table 1-35 Item list (Task list (History))

Item name	Default value	Description
Severity	All severities	When narrowing down the task list, select a severity level from this pull-down list. You can select only one severity level. • All severities

Item name	Default value	Description
		• Fatal • Warning • Unknown • Normal • Empty • Unmanaged
Requested at(Search Range)	Time 24 hours ago	Specify the range of tasks to be displayed in the task list in the yyyy/mm/dd mm:dd:ss format.
Show all users' tasks	Unchecked	Specify whether to display the tasks executed by other users. Since this check box is not selected by default, only the tasks executed by the login user are displayed in the list.
[Apply] button		Applies the conditions specified in [Severity], [Requested at], and [Show all users' tasks] to the task list and displays the list again.
Task Name		Displays the type of the task. In this version, only [Apply Template] is displayed.
Target		Displays the node for which the task was executed.
Severity		Displays the severity set for the task.
Requested at		Displays the request date and time of the task in the yyyy/mm/dd mm:dd:ss format.
End at		When the task is completed, the completion time is displayed in the yyyy/mm/dd mm:dd:ss format. When the task is not completed, the field is blank.
Run by		Displays the name of the user who executed the task.

If you select a task in the task list, the [Task Detail] dialog box is displayed.

The [Task Detail] dialog box lets you view a list of task execution logs.

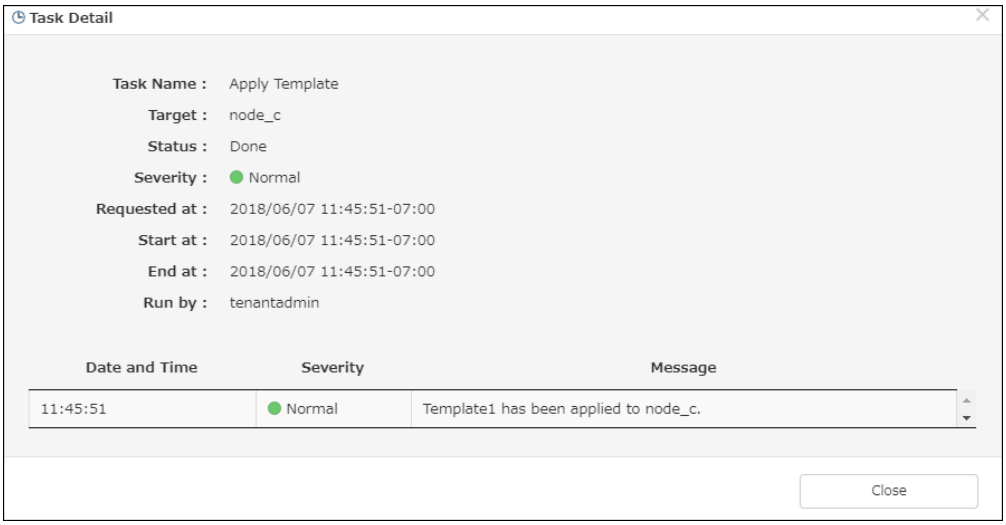

Figure 1-85 [Task Detail] dialog box

Table 1-36 Item list ([Task Detail] dialog box)

Item name	Description
Task Name	Displays the type of the task. In this version, only [Apply Template] is displayed.

Item name	Description
Target	Displays the node for which the task was executed.
Status	Displays the status of the task. • Stand by • Running • Done
Severity	Displays the status of the task. One of the following severity levels is displayed: • Fatal • Warning • Unknown • Normal • Empty • Unmanaged
Requested at	Displays the request date and time of the task in the yyyy/mm/dd mm:dd:ss format.
End at	Displays the completion time of the task in the yyyy/mm/dd mm:dd:ss format. When the task is not completed, the field is blank.
Run by	Displays the name of the user who executed the task.
Execution logs	Displays a list of task execution logs.
Date and Time	Displays the time when the message was output to the task execution log in the mm:dd:ss format.
Severity	Displays the severity of the task execution log.
Message	Displays the message of the task execution log.

1.7.3 Message

This section describes the message function.

The [Message] screen is displayed by selecting [Monitoring] and then [Message] from the menu.

The [Message] screen displays the [Category List] panel, [Number of Messages by Severity] panel (initially hidden), and [Message List] panel (initially hidden).

On the [Message] screen, messages can be categorized by specifying conditions and the message monitoring status can be displayed for each category. The category severity is the most urgent severity of the unconfirmed messages that are classified to that category. Also, categories can be grouped in any hierarchy. The category group severity is the most urgent severity among the categories (category groups) in the group. Therefore, the failed category can be identified by tracing groups with high severity from the top of the group tree.

On the [Message List] panel, messages of the category selected on the [Category List] panel are displayed and can be operated.

Selecting the [Auto Update] check box automatically updates each panel every 30 seconds.

Figure 1-86 [Message] screen

Table 1-36 Item list ([Message] screen - Category list)

Item name	Description
[Update] button	Updates the [Category List] panel.
[Add widget] button	Adds the [Category List] panel to the dashboard as a widget.
Severity selection	Displays the categories (category groups) whose severity is more urgent than the selected severity in the tree.
Operation	Displays the [Operation] pull-down menu. This is displayed only for a user who can change the operation management settings. For details, see "1.7.3.8 Performing an operation for a category (page 63)".
Category group node	Displays a category group name with a severity icon. The categories in the category group can be displayed or hidden by selecting the open or close icon.
Category node	Displays a category name with a severity icon. Clicking the category name shows a list of messages classified into the category and the number of unconfirmed messages of each severity. For the list of messages, see "1.7.3.1 Displaying the message list (page 53)". For the number of unconfirmed messages of each severity, see "1.7.3.7 Displaying the number of messages by severity level (page 62)".

1.7.3.1 Displaying the message list

This section describes how to display the list of messages and what each item of the list is for.

While the authority to perform the operations described in this section is controlled according to the role, they are available to all users except system administrators.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

Selecting a category in the [Category List] panel of the [Message] screen lists the messages of the selected category in the [Message] panel.

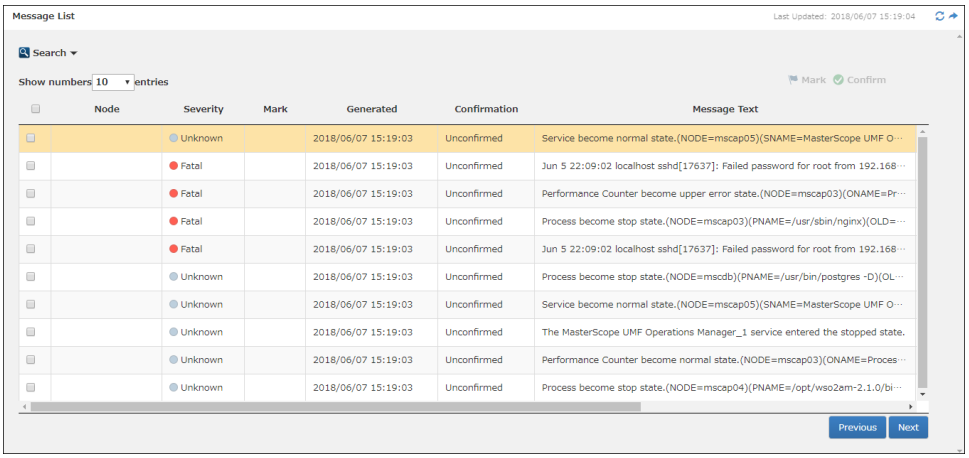

Figure 1-87 Message panel and messages

The items and buttons shown in the [Message] screen are as follows.

Table 1-38 Item list ([Message] panel)

Item name	Description
Message toggle	Opens and closes the message panel.
[Update] button	Updates the message panel.
[Add widget] button	Pastes the currently displayed message panel to the dashboard as a widget.
Search toggle	Opens and closes the search condition. This is hidden initially.
Show numbers [ ] entries	Specify the number of messages to be displayed in the list below. The number of messages to be displayed in the list per page. You can select the number of messages to be displayed from 10, 100, 500, and 1000.
[Mark] button	Marks the selected message.
[Confirm] button	Changes the confirmation status of the selected message.
[Previous] button	Displays messages newer than the displayed messages.
[Next] button	Displays messages older than the displayed messages.

The items and buttons shown in the message list of the [Message] screen are as follows.

Table 1-39 Item list (Message list)

Item name	Description
Check box	The message whose check box is selected is an operation target.
Node	Displays a node. This is displayed when a group is selected.
Severity	Displays the severity.
Mark	Displays the mark.
Generated	Displays the generation date and time.
Confirmation	Displays the confirmation status.
Message Text	Displays the message text.
Application	Displays the application.
Object	Displays the object.
Message ID	Displays the message ID.

1.7.3.2 Searching messages

This section describes how to search messages.

While the authority to perform the operations described in this section is controlled according to the role, they are available to all users except system administrators.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

Clicking the search toggle on the [Message] screen displays the items for which a search condition can be specified.

Specifying a search condition and clicking the [Submit] button displays messages that meet the specified search condition in a list. For the items whose search condition is specified by using a character string (Node, Message Text, Description, and Comment), a regular expression search is performed.

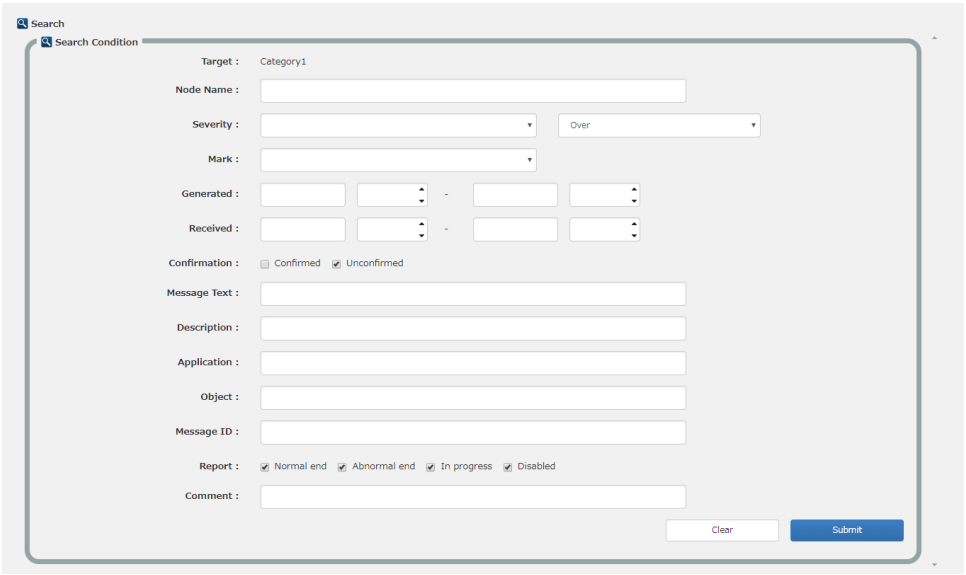

Figure 1-88 Searching messages

Table 1-40 Item list (Search Condition)

Item name	Input rule	Description
Target	-	Displays the search target. Selecting a group displays the check box to select whether to search groups in the specified group recursively.
Node Name	Up to 256 characters	Searches for the entered node name.
Severity	-	The selected severity and severity range are searched. If the severity is not selected, all severities are searched.
Mark	-	The selected mark is searched. If the mark is not selected, all marks are searched.
Generated	1970/01/01 00:00:00 to 2999/12/31 23:59:59	The selected or entered range of the generation dates and times are searched. This is the date and time when an agent generated the message on the monitored server machine. The time zone depends on the system time of the manager.
Received	1970/01/01 00:00:00 to 2999/12/31 23:59:59	The selected or entered range of the reception dates and times are searched. This is the date and time when the manager received the

Item name	Input rule	Description
		message generated on the monitored server machine. The time zone depends on the system time of the manager.
Confirmation	-	The selected confirmation status ([Confirmed] or [Unconfirmed]) is searched. Be sure to select either check box.
Message Text	Up to 1024 characters	The entered message text is searched.
Description	Up to 256 characters	The entered message summary is searched.
Application	Up to 1024 characters	The entered application is searched.
Object	Up to 1024 characters	The entered object is searched.
Message ID	Up to 128 characters	The entered message ID is searched.
Report	-	Searches for the selected reporting status (Normal end, Abnormal end, In progress, Disabled). Be sure to select either check box.
Comment	Up to 1024 characters	The entered comment is searched.
Clear	-	Resets the entered (specified) values to the initial values.
Submit	-	Click this button to start searching.

1.7.3.3 Displaying message details

This section describes how to display details of a message and what each item of the details is for.

While the authority to perform the operations described in this section is controlled according to the role, they are available to all users except system administrators.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

Selecting a message shown in the message list in the [Message] screen displays the [Message Details], [Knowledge], and [Action] tabs.

Figure 1-89 [Message Details] tab

The items shown in the [Message details] tab are as follows.

Table 1-41 Item list ([Message Details] tab)

Item name	Description
Node	Displays a node. This is displayed when a group is selected.
Severity	Displays the severity.
Mark	Displays the mark.

Item name	Description
Generated	Displays the generation date and time. This is the date and time when an agent generated the message on the monitored server machine.
Received	Displays the generation date and time. This is the date and time when the manager received the message generated on the monitored server machine.
Confirmation	Displays the confirmation status.
Message Text	Displays the message text.
Description	Displays the message summary.
Application	Displays the application.
Object	Displays the object.
Message Definition ID	Displays the message definition ID.
Message ID	Displays the message ID.
Report	Displays the reporting status.
Comment	Displays the comment.
[Mark] button	Assign the mark.
[Confirm] button	Changes the confirmation status.
[Edit comment] button	Edits the comment.

Figure 1-90 [Knowledge] tab

The [Knowledge] tab displays the content of the knowledge registered in [Display definition] of the message filter.

For information about how to set [Display definition], see "1.7.3.10 Adding or changing the filter (page 68)".

The [Knowledge] tab divides the display area into groups according to the number of knowledge definitions registered in [Display definition].

The following items are displayed for each displayed group.

Table 1-42 Item list ([Knowledge] tab)

Item name	Description
Group title	Displays the content of the display title of the knowledge registered in [Display definition].
Knowledge	Displays the content registered in the knowledge in either text or HTML format according to the display type of the registered knowledge. It is displayed according to the definition set in the message filter that first matches the condition when the message is generated. It is not displayed if the message filter is deleted.

Figure 1-91 [Action] tab

The [Action] tab displays the execution result of the action set in [Action definition] of the message filter.

For information about how to set [Action definition], see "1.7.3.10 Adding or changing the filter (page 68)".

The items to be displayed differ depending on the action type.

In the case of Email report, the following items are displayed.

Table 1-43 Item list ([Action] tab)

Item name	Description
Title	Displays the name of the report setting registered in the message filter.
Type	Displays the type of action. In the case of Email report, [E-mail Report] is displayed.
Execution Date & Time	Displays the date and time when Email report was executed.
Execution status	Displays one of the following as the execution status of Email report. ・Normal end ・In progress ・Abnormal end ・Unmanaged (displayed if the reporting definition is deleted or disabled when the message is generated)

Table 1-44 Item list ([Action] tab - Command execution)

Item name	Description
Title	Displays the name of the report setting registered in the message filter.
Type	Displays the type of action. [Command execution] is displayed when a command is executed.
Execution Date & Time	Displays the date and time when the command was executed.
Execution status	Displays one of the following as the status of command execution. ・Normal end ・In progress ・Abnormal end ・Unmanaged (displayed if the reporting definition is deleted or disabled when the message is generated)
Return value	Displays the value returned after command execution.
Execution information	Displays the content of the standard output and standard error output as the execution result of the command. If the command fails to be executed, the relevant error information is output.

1.7.3.4 Changing the confirmation status of a message

This section describes how to change the confirmation status of a message.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	N

The following two methods are available to change the confirmation status of a message.

- Changing method 1
  1. Select the check box of the target message in the list of messages and click the [Confirm] button.
  2. The confirmation statuses are displayed under the [Confirm] button. Select the status that you want to change.

     By selecting two or more messages, you can change the confirmation statuses of multiple messages simultaneously.

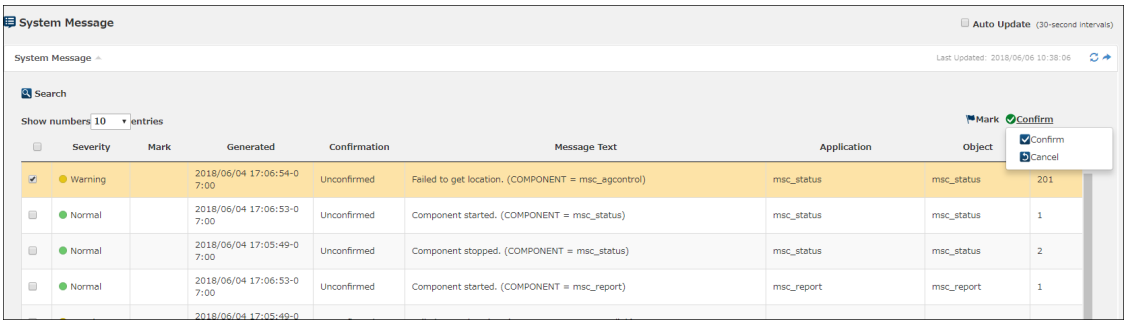

Figure 1-92 Confirmation status changing method 1

- Changing method 2
  1. Click the message whose comment you want to edit in the list of messages.
  2. [Message Details] is displayed. Click the [Confirm] button.

Figure 1-93 Confirmation status changing method 2

  3. The [Confirm] dialog box is displayed. Click the [Submit] button.

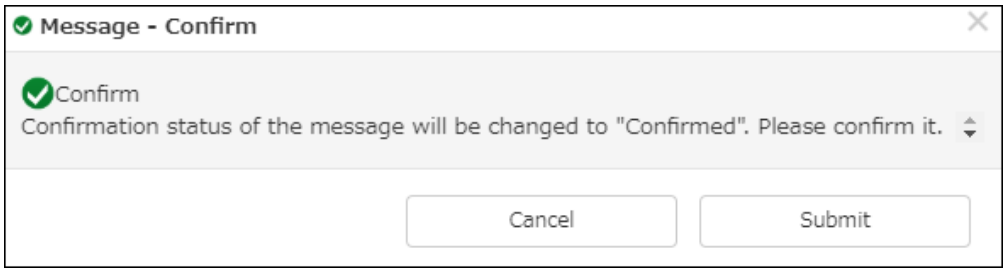

Figure 1-94 [Confirm] dialog box

1.7.3.5 Assigning a mark to a message

This section describes how to assign a mark to a message.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	N

The following two methods are available to assign a mark to a message.

- Assignment method 1
  1. Select the check box of the target message in the list of messages and click the [Mark] button.
  2. The [Marking up] dialog box is displayed. Select the mark that you want to assign to the message and click the [Submit] button.

     By selecting two or more messages, you can assign marks to multiple messages simultaneously.

Figure 1-95 Mark assignment method 1

- Assignment method 2
  1. Click the message whose comment you want to edit in the list of messages.
  2. [Message Details] is displayed. Click the [Mark] button.

Figure 1-96 Mark assignment method 2

3. The [Marking up] dialog box is displayed. Select the mark that you want to assign to the message and click the [Submit] button.

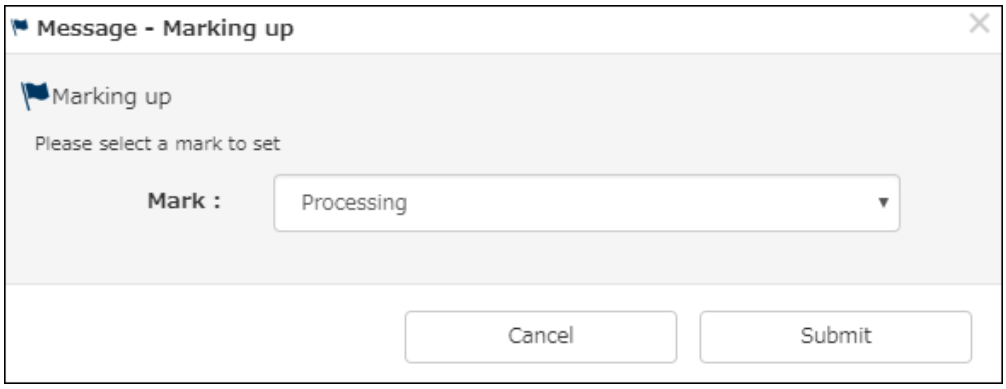

Figure 1-97 [Marking up] dialog box

1.7.3.6 Editing the comment of a message

This section describes how to edit the comment of a message.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	N

1. Click the message whose comment you want to edit in the list of messages.
2. [Message Details] is displayed. Click the [Edit comment] button.

Figure 1-98 Editing the comment

3. The [Edit comment] dialog box is displayed. Enter a comment and click the [Submit] button.

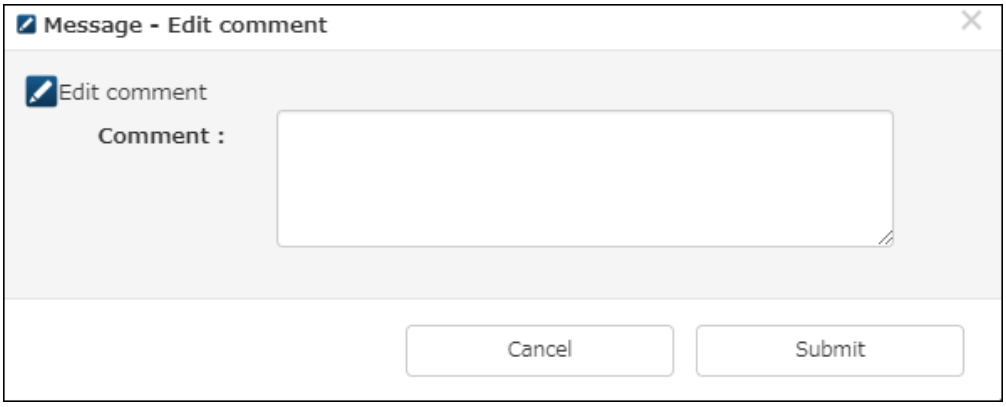

Figure 1-99 [Edit comment] dialog box

1.7.3.7 Displaying the number of messages by severity level

This section describes the number of messages displayed by severity level in the [Message] screen.

While the authority to perform the operations described in this section is controlled according to the role, they are available to all users except system administrators.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

Selecting a category from the list of categories displays the number of unconfirmed messages of each severity.

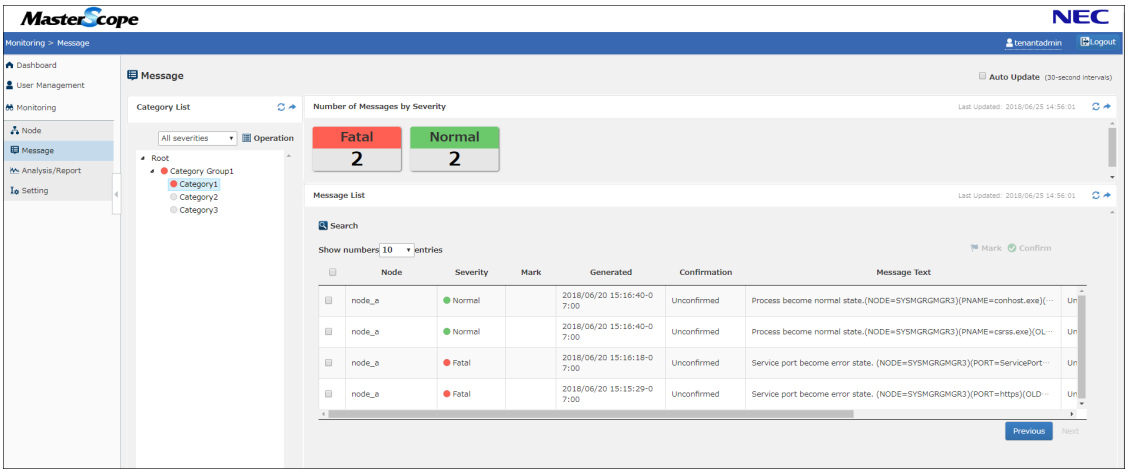

Figure 1-100 [Message] screen - Number of Messages by Severity

The search screen and messages can be narrowed down (searched again) by selecting a severity. It is also possible to select multiple severity levels. Click the selected severity to cancel the selection.

When the number of messages of each severity is displayed as a widget on the dashboard, the screen is changed to the [Message] screen by selecting a severity. Messages are displayed with narrowing down by the selected severity.

1.7.3.8 Performing an operation for a category

This section describes how to perform an operation for a category displayed in the [Message] screen.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Selecting an operation from the [Operation] pull-down menu on the category list displays the dialog box of the selected operation.

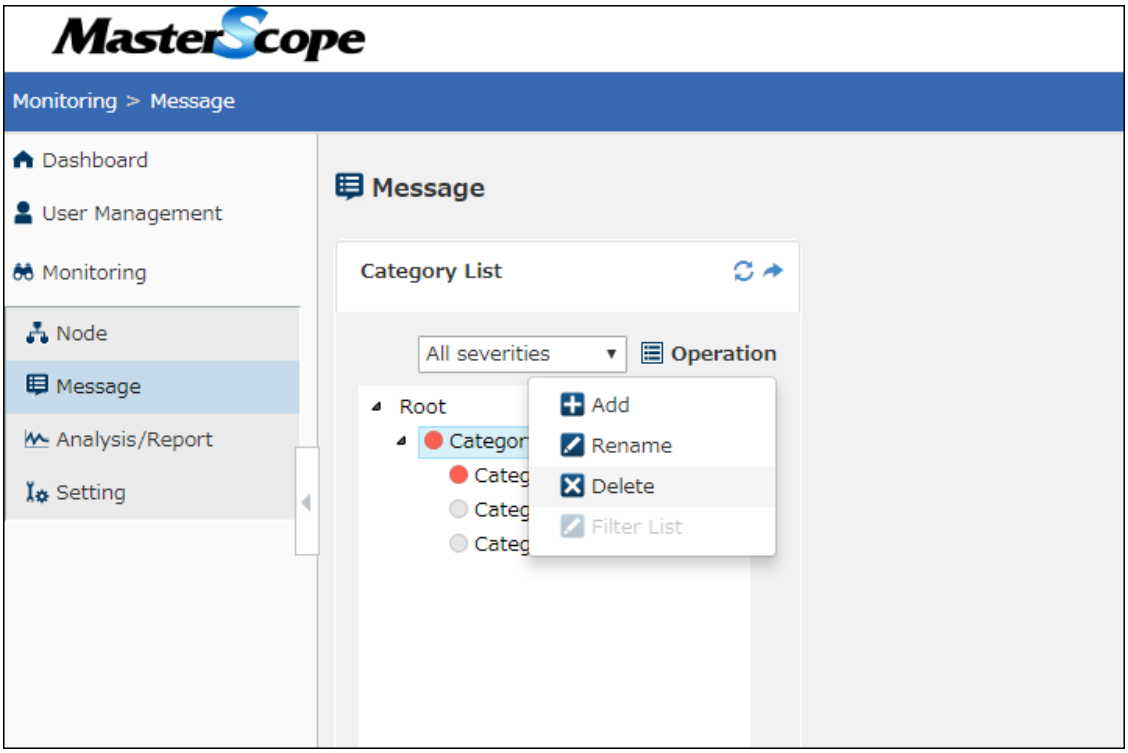

Figure 1-101 [Message] screen - Category list

- Creation

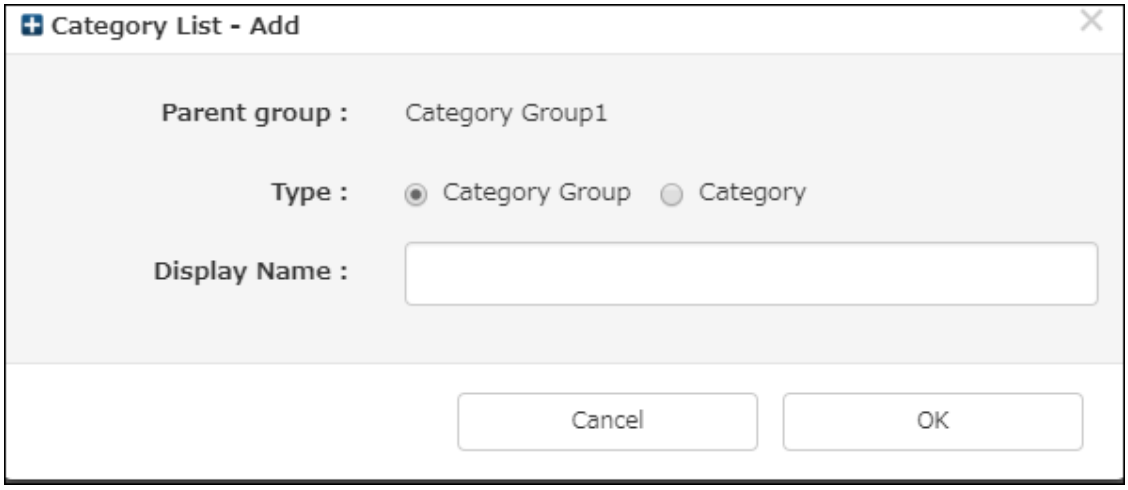

Figure 1-102 [Category List - Add] dialog box

Table 1-45 Item list ([Category List - Add] dialog box)

Item name	Description
Parent group	Displays the name of the parent category group in which a category group or category is created.
Type	Select the type of the [Category Group] or [Category] to be created.
Display Name	Enter the name of the category group or category to be created.
Cancel	Stops creating a category group or category and closes the dialog box.
OK	Creates the specified category group or category and closes the dialog box.

Click [OK] to create a category.

- Rename

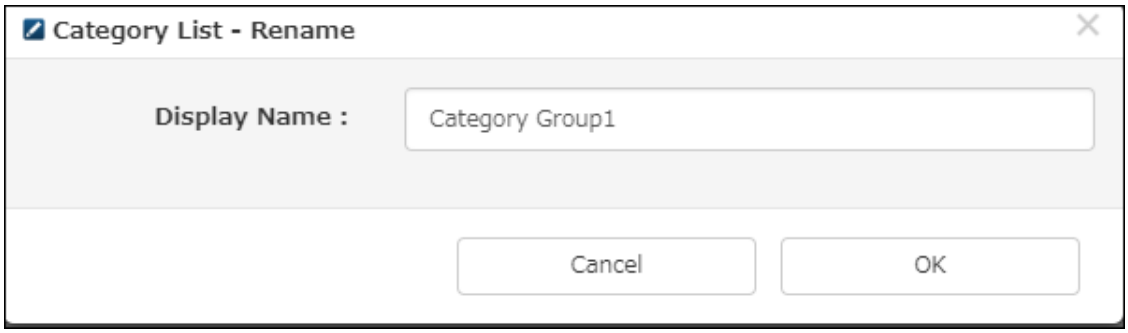

Figure 1-103 [Category List - Rename] dialog box

Table 1-46 Item list [Category List - Rename] dialog box)

Item name	Description
Display Name	Enter the name of the category group or category to be changed.
Cancel	Stops changing a category group or category name and closes the dialog box.
OK	Changes the specified category group or category name and closes the dialog box.

Click [OK] to change the category name.

- Delete

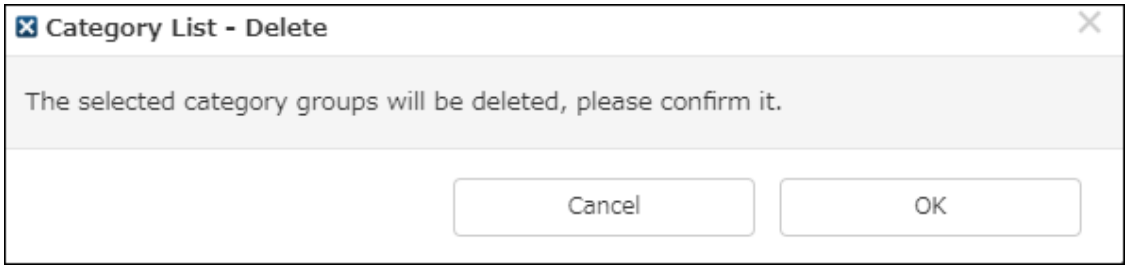

Figure 1-104 [Category List - Delete] dialog box

Click [OK] to delete the selected category group or category.

1.7.3.9 Displaying a list of filters

This section describes the screen that lists the message filters that can be set for a category.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

The [Filter List] screen is displayed by selecting a category from the list of categories and then select [Filter List] from the [Operation] menu.

The filters are displayed in priority order. The condition to classify messages to categories is set to each filter. The output message is filtered in descending order of priority. If the filter type that the message matches first is [Store], the message is classified to a category. If the filter type that the message matches first is [Ignore] or the message does not match any filtering conditions, the message is not classified to any category.

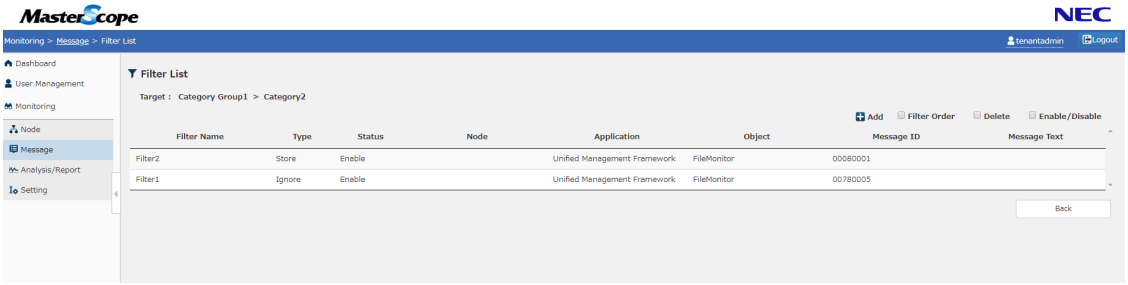

Figure 1-105 [Filter List] screen

Table 1-47 Item list ([Filter List] screen)

Item name	Description
Add	Add a filter. For details, see "1.7.3.10 Adding or changing the filter (page 68)". When adding the filter that is selected from the list of filters, the added filter is inserted above the selected filter. When adding a filter without selecting the filter, the added new filter is inserted at the top of the list.
Filter Order	Selecting this check box enables to change the filter order. For details, see "1.7.3.11 Changing the filter order (page 73)".
Delete	Selecting this check box enables to delete a filter. For details, see "1.7.3.12 Deleting a filter (page 74)".
Enable/Disable	Selecting this check box enables or disables to delete a filter. For details, see "1.7.3.13 Enabling or disabling multiple filters simultaneously (page 75)".
Filter Name	Displays the filter name.
Type	Displays the filter type. Store: Messages that match the condition is classified into the category. Ignore: Messages that match the condition are not classified into the category. (The succeeding filtering is not performed.)
Status	Displays the filter status. Enable: Indicates that the filtering condition is applied. Disable: Indicates that the filtering condition is not applied temporarily.
Node	Displays the condition text (in regular expression) for the node name.
Application	Displays the condition text (in regular expression) for the application.
Object	Displays the condition text (in regular expression) for the object.
Message ID	Displays the condition text (in regular expression) for the message ID.

Item name	Description
Message Text	Displays the condition text (in regular expression) for the message text.
[Back] button	Returns you to the [Message] screen.

Clicking the filter at the top of the list displays the filter details.

Figure 1-106 [Filter List] screen - Filter details

Table 1-48 Item list ([Filter List] screen - Filter details)

Item name	Description
Filter Name	Displays the filter name.
Status	Displays the filter status. Enable: Indicates that the filtering condition is applied. Disable: Indicates that the filtering condition is not applied temporarily.
Type	Displays the filter type. Store: Messages that match the condition is classified into the category. Ignore: Messages that match the condition are not classified into the category. (The succeeding filtering is not performed.)
Group	Displays the condition for the group.
Node Name	Displays the condition text (in regular expression) for the node name.
Application	Displays the condition text (in regular expression) for the application.
Object	Displays the condition text (in regular expression) for the object.
Message ID	Displays the condition text (in regular expression) for the message ID.
Message Text	Displays the condition text (in regular expression) for the message text.
Message Description	Displays the condition text (in regular expression) for the message summary.
Message Definition ID	Displays the condition text (in regular expression) for the message definition ID.
Severity	Displays the severity condition.
[Edit] button	Changes the filter condition. For details, see "1.7.3.10 Adding or changing the filter (page 68)".
[Copy] button	Add a filter by quoting the filter information being displayed in the details.

Item name	Description
	For details, see "1.7.3.10 Adding or changing the filter (page 68)". The added filter is inserted at one line above the quoted filter.

Note

For a "negative" condition (that is, targeting the filter that does not match the specified condition), an exclamation mark is displayed at the top of the condition.

When the type of the filter is [Store] and an action definition is set, the [Filter details] screen displays the following [Action definition] list.

Table 1-49 Item list ([Filter List] screen - Filter details - Action definition)

Item name	Description
Status	Sets the status of the action definition. Enable: In this status, the defined action (Email report or command execution) is taken when a message that matches the filter is generated. Disable: In this status, the defined action (Email report or command execution) is not taken even when a message that matches the filter is generated. It is used to suspend the execution of the action temporarily.
Email report	Displays the reporting name of the settings for the Email report to be executed when a message matches the filter.
E-mail Report information button	Displays the details of the Email report settings in a dialog box. For details of the Email report settings, see "1.7.5.4.1 Adding or changing an email report setting (page 154)".
Command execution	Displays the reporting name of the settings for the command to be executed when a message matches the filter.
Command information button	Displays the details of the command settings in a dialog box. For details of the command settings, see "1.7.5.5.1 Adding or changing a command setting (page 161)".

When the type of the filter is [Store] and a display definition is set, the [Filter details] screen displays the following [Display Definition] list.

Table 1-50 Item list ([Filter List] screen - Filter details - Display Definition)

Item name	Description
Message summary override	When [Message summary override] is set, the specified value is displayed. The overview of the message that matches the filter is updated with the specified content.
Knowledge	Displays the setting name of the knowledge settings to be displayed in [Message Ditails] of the message that matches the filter.
Knowledge information button	Displays the details of the knowledge settings in a dialog box. For the text type, the character strings of the specified knowledge are displayed within the specified display title frame. For the HTML type, the page generated from the specified HTML source code is displayed within the specified display title frame.

1.7.3.10 Adding or changing the filter

This section describes how to add or change the message filter.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

The [Add Message Filter] screen is displayed by clicking [Add] on the [Filter List] screen or by selecting a filter on the [Filter List] screen and clicking [Copy]. When clicking [Copy], each condition input field is displayed with the selected condition set.

The [Edit Message Filter] screen is displayed by selecting a filter on the [Filter List] screen and clicking [Edit].

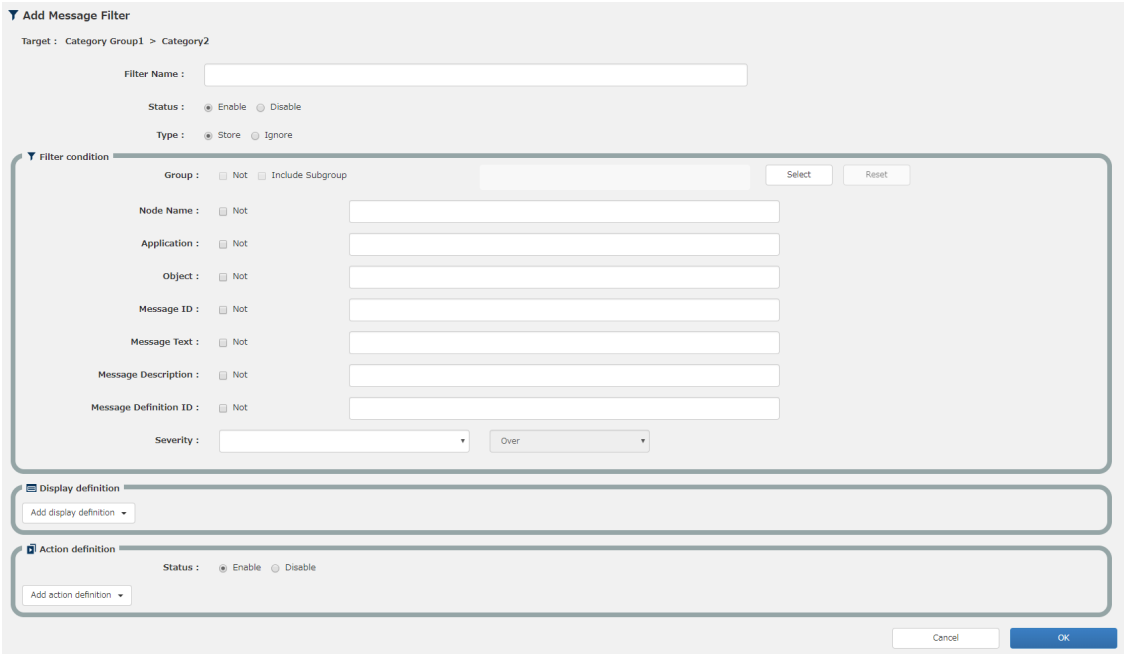

Figure 1-107 [Add Message Filter] screen

Table 1-51 Item list ([Add Message Filter] screen)

Item name	Description
Filter Name	Enter the filter name by using 0 to 128 characters.
Status	When [Enable] is specified, the status of the filter is "enabled". When [Disable] is specified, the status of the filter is "disabled".
Type	Type of the filter When [Store] is specified, messages that match the filter condition are to be classified into the category. When [Ignore] is specified, messages that match the filter condition are not to be classified into the category. In addition, comparison with the subsequent filtering definitions is not performed. Action definitions and display definitions cannot be set for a filter whose type is [Ignore].
Group	Select a group. Messages for the nodes in the selected group are targeted.

Item name	Description
Include Subgroup	When this check box is selected, all groups in the selected group are targeted.
Not (Group)	When this check box is selected, groups other than the selected group are targeted. If [Include Subgroup] is also selected, groups other than "all groups in the selected group" are targeted.
Not (Node Name)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the node name, match the condition.
Node Name	Specify the filter condition for node names in regular expression.
Not (Application)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the application, match the condition.
Application	Specify the filter condition for the application.
Not (Object)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the object, match the condition.
Object	Specify the filter condition for the object (name of the object in which a massage is generated) in regular expression.
Not (Message ID)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the message ID, match the condition.
Message ID	Specify the filter condition for the message ID.
Not (Message Text)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the message, match the condition.
Message Text	Specify the filter condition for the message text.
Not (Message Description)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the message overview, match the condition.
Message Description	Specify the filter condition for the message overview.
Not (Message Definition ID)	When this check box is selected, it is assumed that all messages, which do not match the filter condition for the message definition ID, match the condition.
Message Definition ID	Specify the filter condition for the message definition ID to be used to generate a message text.
Severity	Specify the filter condition for the severity.
Severity Range	Select [Over], [Equal], or [Under] for the severity.

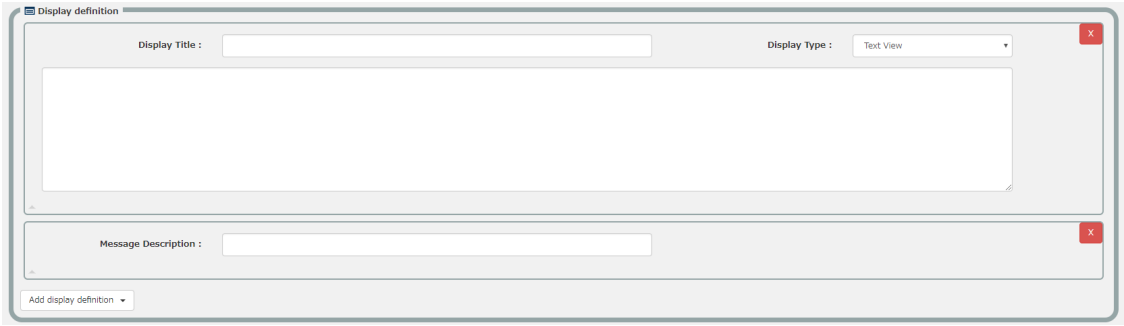

Figure 1-108 [Add Message Filter] screen - Display definition

Table 1-52 Item list ([Add Message Filter] screen - Display definition)

Item name	Description
Add display definition	From the following, select the display definition to be set for the message filter. ・Knowledge: This function displays the desired content in the details screen ([Knowledge] tab) of the message that matches the filter. You can set text describing the action to be taken for the generated message or a link to the Web page containing useful information. ・Message summary override: This function updates the overview of the message that matches the filter with the specified content. You can register up to two [Knowledge] definitions per filter and not more than one [Message summary override] definition per filter.
Display title	Set the display title of the knowledge to be displayed in the [Message Details] screen ([Knowledge] tab) within 1024 characters.
Display type	From the following, select the format of the knowledge information to be displayed in the [Message Details] screen ([Knowledge] tab). ・Text view ・HTML view
Displayed item	Set the information to be displayed in the [Message Details] screen ([Knowledge] tab) within 8192 characters. Replacement strings can be specified. When specifying any replacement string, take into account the number of characters to be actually displayed.
Message summary override	Set the overview of the message that matches the message filter, within 256 characters.

Table 1-53 Item list (Replacement strings)

Replacement string	Description
$message_id$	Message ID
$definition_code$	Message definition
$tenant_id$	Tenant ID
$severity$	Severity

Replacement string	Description
$create_time$	Occurrence date and time
$system_name$	System name
$node_id$	Node ID
$node_type$	Node type
$node_name$	Node name
$object$	Object
$summary$	Description of the message
$message_no$	Message number
$receive_time$	Reception date and time
$message_text$	Message text
$business_node_id$	Business category node ID set in the filter that triggered the reporting

Figure 1-109 [Add Message Filter] screen - Action definition

Table 1-54 Item list ([Add Message Filter] screen - Action definition)

Item name	Description
Status	Sets the status of the action definition. Enable: In this status, the defined action (email report or command execution) is taken when a message that matches the filter is generated. Disable: In this status, the defined action (Email report or command execution) is not taken even when a message that matches the filter is generated. It is used to suspend the execution of the action temporarily.
Add action definition	Add an action to be taken when a message matching the filter is generated. Select an action from the following. Email report: A specified email is sent when the message is generated. Command execution: A specified command is executed when the message is generated. More than one action can be set per filter. To delete a set action definition, select [×] at the upper right of the action setting field.
Email report	When a message matching the filter is generated, an email with the preregistered content is sent. The [Email report Selection] dialog box, which appears when you click the [Select] button, displays the selected setting name.

Item name	Description
	For information about how to set the content of the email to be sent, see "1.7.5.4.1 Adding or changing an email report setting (page 154)".
Command execution	When a message matching the filter is generated, a command is executed based on the preregistered setting. The [Command execution Selection] dialog box, which appears when you click the [Select] button, displays the selected setting name. For information about how to define the command to be executed, see "1.7.5.5.1 Adding or changing a command setting (page 161)".

When you have entered all necessary conditions, click the [OK] button to register them.

Clicking the [Cancel] button discards the data entered in the fields and returns you to the [Filter List] screen.

1.7.3.11 Changing the filter order

This section describes how to change the order of message filters.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Selecting [Filter Order] on the [Filter List] screen enables to change the filter order.

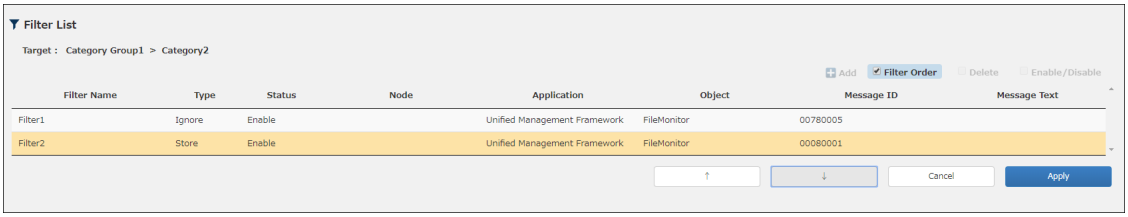

Figure 1-110 [Filter List] screen - Filter Order

Table 1-55 Item list ([Filter List] screen - Filter Order)

Item name	Description
↑	Moves the selected line up.
↓	Moves the selected line down.
Cancel	Displays the [Filter List - Execution Order] dialog box (Cancel). "Table 1-56 Item list ([Filter List - Execution Order] dialog box (Cancel)) (page 74)"
Apply	Displays the [Filter List - Execution Order] dialog box (Apply). "Table 1-57 Item list ([Filter List - Execution Order] dialog box (Apply)) (page 74)"

[Filter List - Execution Order] dialog box (Cancel)

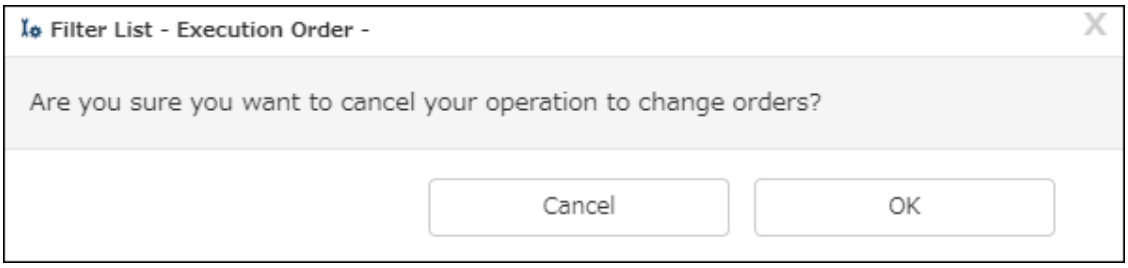

Figure 1-111 [Filter List - Execution Order] dialog box (Cancel)

Table 1-56 Item list ([Filter List - Execution Order] dialog box (Cancel))

Item name	Description
Cancel	Closes the dialog box without canceling the settings. (This returns you to the order change operation.)
OK	Stops changing the order and returns to the filter list display.

[Filter List - Execution Order] dialog box (Apply)

Figure 1-112 [Filter List - Execution Order] dialog box (Apply)

Table 1-57 Item list ([Filter List - Execution Order] dialog box (Apply))

Item name	Description
Cancel	Closes the dialog box without applying the order change. (This returns you to the order change operation.)
OK	Applies the order change and then closes the dialog box.

1.7.3.12 Deleting a filter

This section describes how to delete a message filter.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Selecting [Delete] on the [Filter List] screen enables to delete a filter.

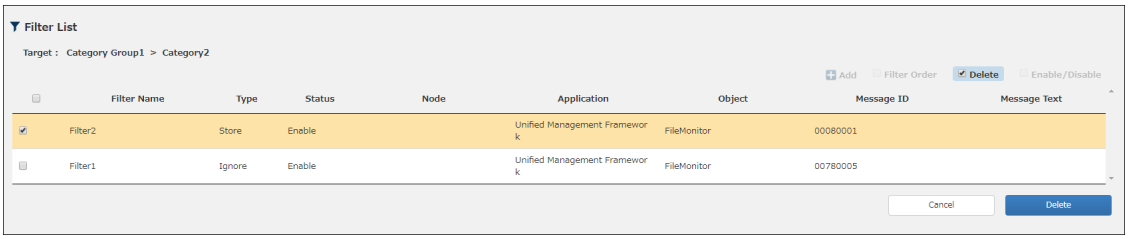

Figure 1-113 [Filter List] screen - Deleting

Selecting a filter that you want to delete from the list of filters and clicking the [Delete] button displays the [Filter List - Delete Filter] dialog box. Click [OK] to delete the selected filter.

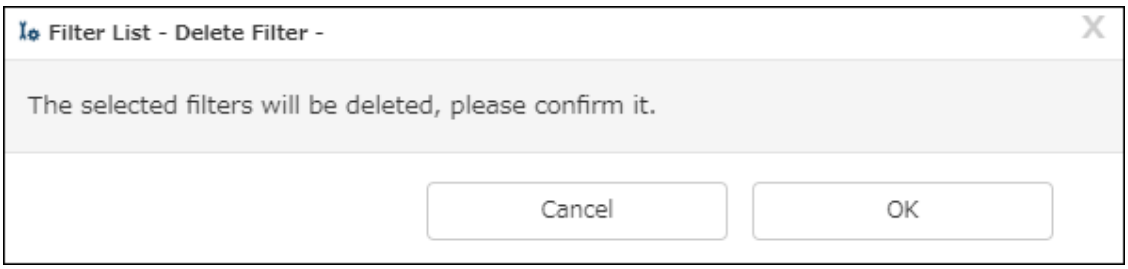

Figure 1-114 [Filter List - Delete Filter] dialog box

1.7.3.13 Enabling or disabling multiple filters simultaneously

This section describes how to enable or disable multiple message filters simultaneously.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Selecting [Enable/Disable] in the [Filter List] screen allows you to enable or disable multiple message filters simultaneously.

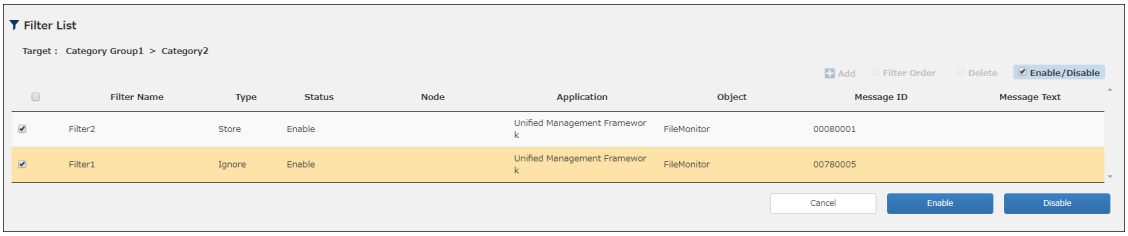

Figure 1-115 [Filter List] screen - Enable/Disable

Selecting a filter that you want to delete from the list of filters and clicking the [Enable] button displays the [Filter List - Change Status] dialog box. Click [OK] to enable the selected filter.

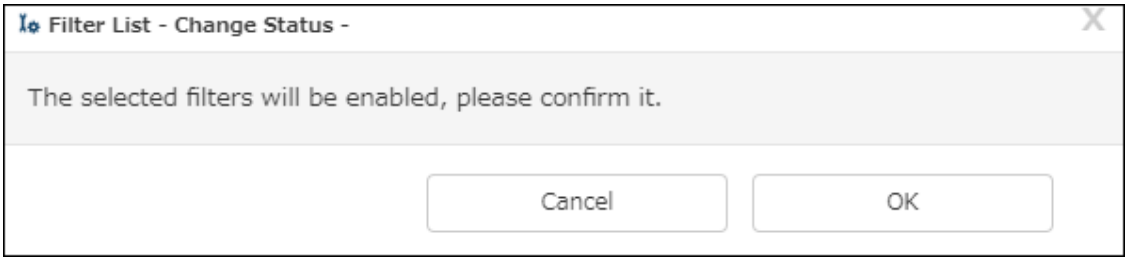

Figure 1-116 [Filter List - Change Status] dialog box (Enable)

Selecting a filter that you want to delete from the list of filters and clicking the [Disable] button displays the [Filter List - Change Status] dialog box. Click [OK] to disable the selected filter.

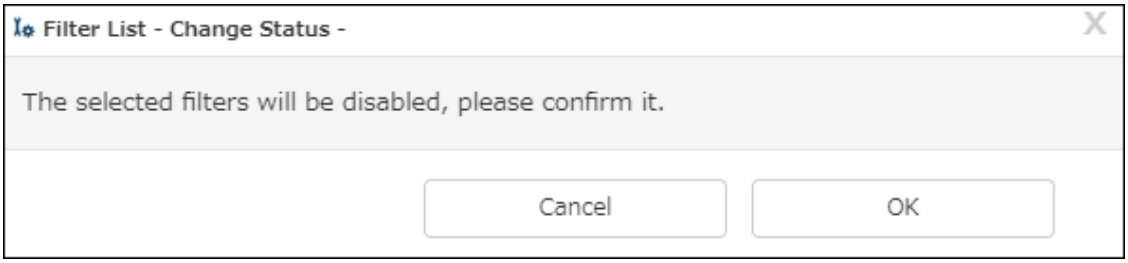

Figure 1-117 [Filter List - Change Status] dialog box (Disable)

1.7.4 Analysis / Report

This section describes the [Analysis / Report] screen that displays the information obtained from each monitored node in a graph.

While the authority to perform the operations described in this section is controlled according to the role, they are available to all users except system administrators.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

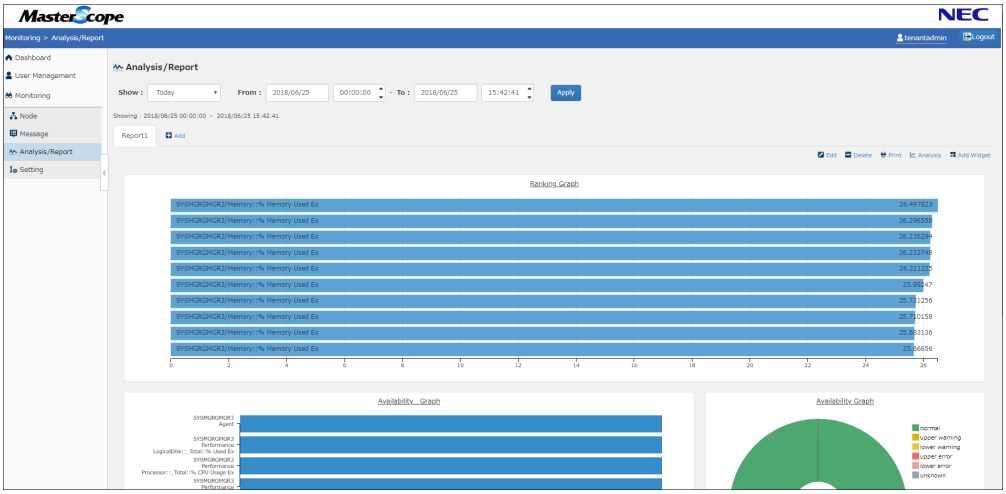

Figure 1-118 [Analysis / Report] screen

To use the analysis/report function, follow the procedure below. The view is the area in which a graph and analysis results are displayed.

Multiple graphs can be placed in the view.

1. Set the display period.

   Set the display period of the analysis and report.

Table 1-58 Item list (Display period)

Item name	Description
Last 1 hour	Displays a graph showing the data for the past 1 hour.
Today	Displays a graph showing the data for today from 00:00 to now. By default, this button is selected.

Item name	Description
Yesterday	Displays a graph showing the data for yesterday from 00:00 to 23:59.
n days	Displays a graph showing the data from 00:00 n days ago to 23:59 yesterday. In [n days], select 2 to 6 days from the pull-down menu.
n weeks	Displays a graph showing the data from 00:00 n weeks ago to 23:59 yesterday. In [n weeks], select 1 to 4 from the pull-down menu.
1 months	Displays a graph showing the data from 00:00 this day last month to 23:59 yesterday.
This month	Displays a graph showing the data from 00:00 the first day of this month to now.
Previous month	Displays a graph showing the data from 00:00 the first day of last month to 23:59 the last day.
From : To	Specify the start and end times of the graph display. The specifiable range is 1971/01/01 00:00 to 2037/12/31 23:59 for both the start and end times.
Apply	Clicking the [Apply] button displays a graph for the specified period. The data for the currently displayed period is updated.

2. Add a view. (Refer to "1.7.4.1 Setting an analysis/report view (page 77)".)
3. In the [Edit View] screen, select a graph type and specify settings for the selected graph type. For details, see below.
   - "1.7.4.2 Setting a performance graph (page 79)"
   - "1.7.4.4 Setting an availability graph (page 86)"
   - "1.7.4.3 Setting a ranking graph (page 83)"
4. For information about how to analyze data, see "1.7.4.7 Analysis function (page 91)".
5. To print the view, see "1.7.4.6 Printing an analysis/report view (page 91)".

1.7.4.1 Setting an analysis/report view

This section describes how to add and edit a view.

The procedure for adding an analysis view is described.

Click the [Add] button in the [Analysis / Report] screen.

The [Add View] dialog box is displayed. Enter a view name, and click [OK].

Figure 1-119 Analysis / Report - [Add View] dialog box

The view is added to the [Analysis / Report] screen.

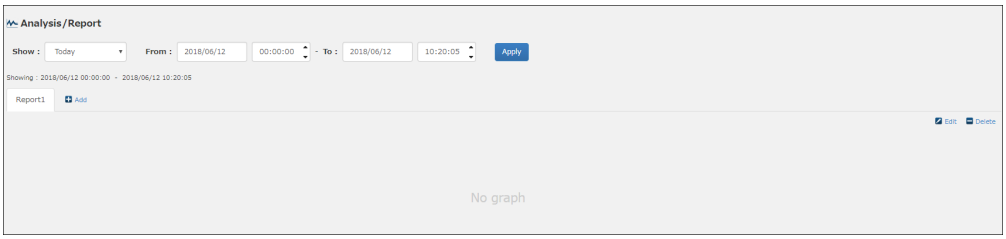

Figure 1-120 [Analysis / Report] screen immediately after a view is added

Click [Edit] to display the [Edit View] screen.

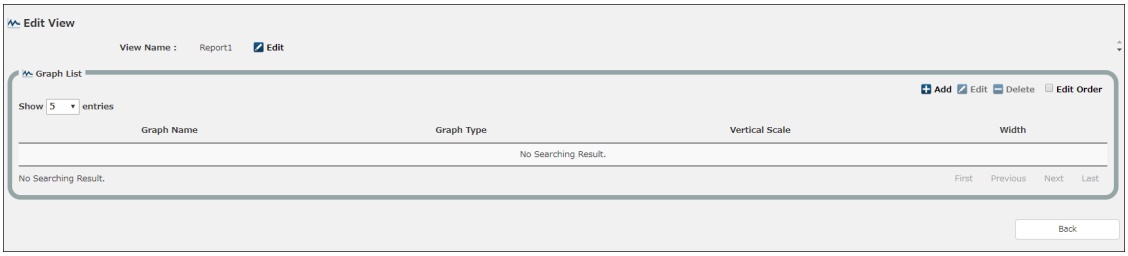

Figure 1-121 [Edit View] screen

In the graph list, click the [Add] button to display the [Graph Configuration] dialog box.

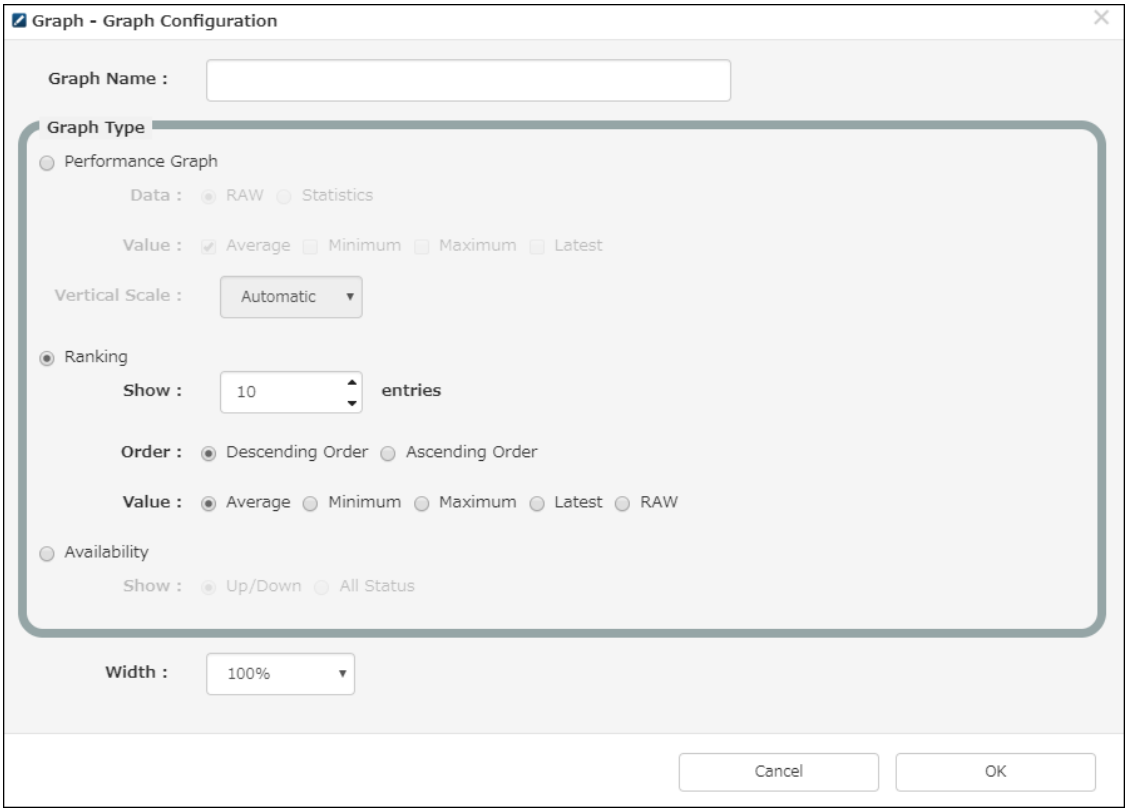

Figure 1-122 [Graph Configuration] dialog box

Table 1-58 Item list ([Graph Configuration] dialog box)

Item name	Required	Description
Graph name	Y	Enter the name of the graph within 128 characters.
Graph type	Y	Select one of the following. • Performance graph

Item name	Required	Description
		• Ranking • Availability
width	Y	Select the rendering size of the graph. • 100% - Use the whole display width for rendering. • 66% - Use two-thirds of the display width for rendering (2-column layout when combined with the 33% option). • 50% - Use a half of the display width for rendering (2-column layout). • 33% - Use one-third of the display width for rendering (3-column layout).

Note

While the number of graph definitions is not limited, rendering many graphs requires much of the client performance. It is recommended to render up to 50 graphs per view. Define graphs as appropriate for your operating environment.

1.7.4.2 Setting a performance graph

This section describes the settings you need to specify when you have selected [Performance Graph] for [Graph Type].

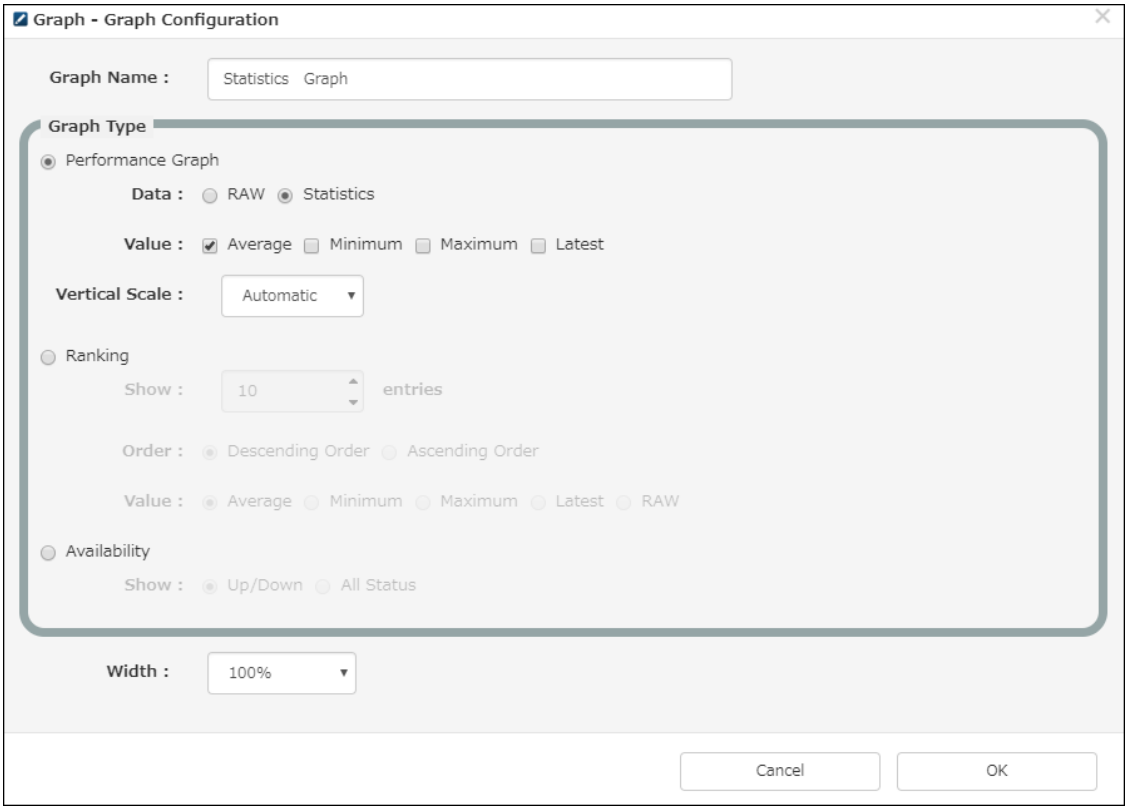

Figure 1-123 [Graph Configuration] dialog box (Performance graph)

Table 1-59 Item list ([Graph Configuration] dialog box (Performance graph))

Item name	Required	Description
Data	Y	Select one of the following.

Item name	Required	Description
		• RAW: The performance data collected for each server monitoring interval is displayed in a graph. This is used for a short-term data analysis for such a purpose as fault investigation. • Statistics: The statistical data generated on an hourly or daily basis (average, minimum, maximum, and latest) is displayed in a graph. This is used for a long-term data analysis for such a purpose as capacity planning.
Value	Y	Available only for a statistical graph. Select one or more of the following. • Average • Minimum • Maximum • Latest [Average], [Minimum], [Maximum], and [Latest] are the statistical data generated from [RAW].
Vertical Scale	Y	Specify how the graph is rendered. • Automatic: The graph is rendered with the minimum value among the values to be plotted being the bottom side and the maximum value being the top side. • Percent: The graph is rendered with 0% being the bottom side and 100% being the top side.

If you click [OK], the added performance graph is displayed in the graph list.

Have the performance graph selected in the list. Graph details are displayed.

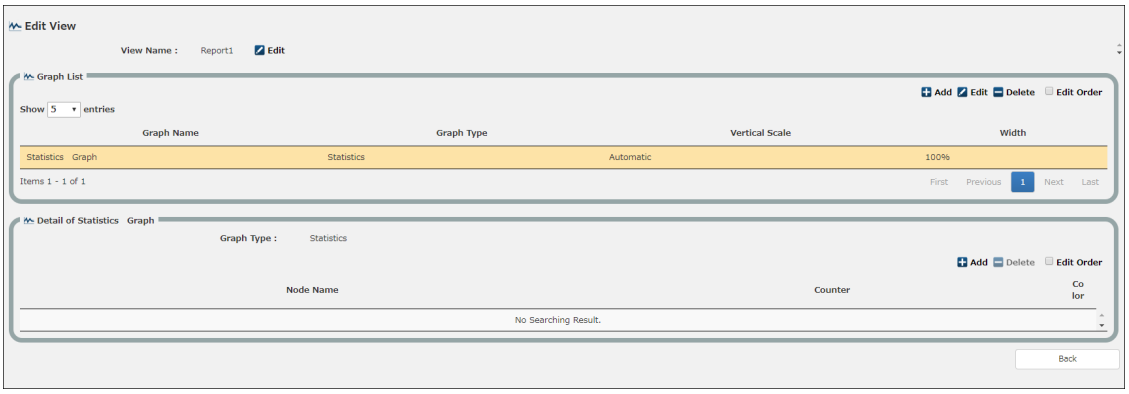

Figure 1-124 [Edit View] screen (Performance graph)

Select the node and counter to be displayed in the performance graph.

Click the [Add] button in the performance graph details to display the [Choose Counter] dialog box.

Entering a character string in the upper right field narrows down the counters to only those containing that character string.

You cannot add an already selected counter.

The display color of the counter is preset by the system.

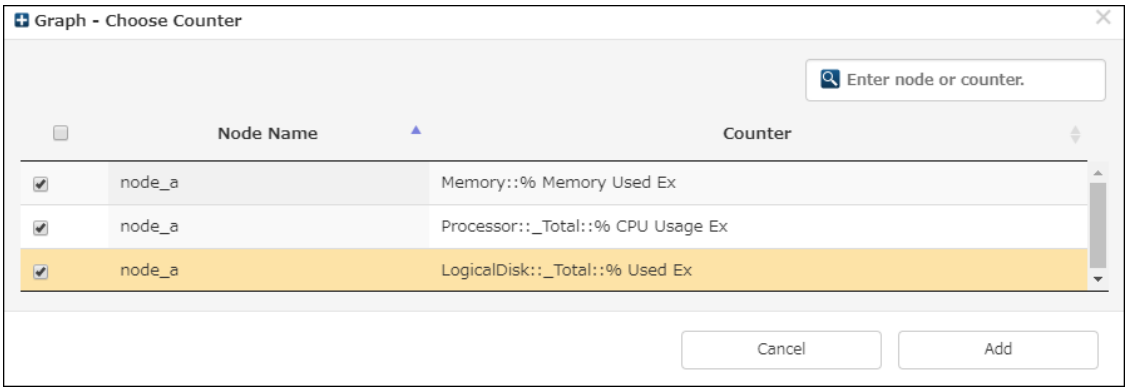

Figure 1-125 [Choose Counter] dialog box

Table 1-60 [Choose Counter] dialog box

Item name	Description
Counter	Select the combination of the graph to be displayed and the data to be acquired (counter). Multiple counters can be selected. You can select not more than 20 counters simultaneously. By clicking the header of the list, you can change the order by node or by counter.

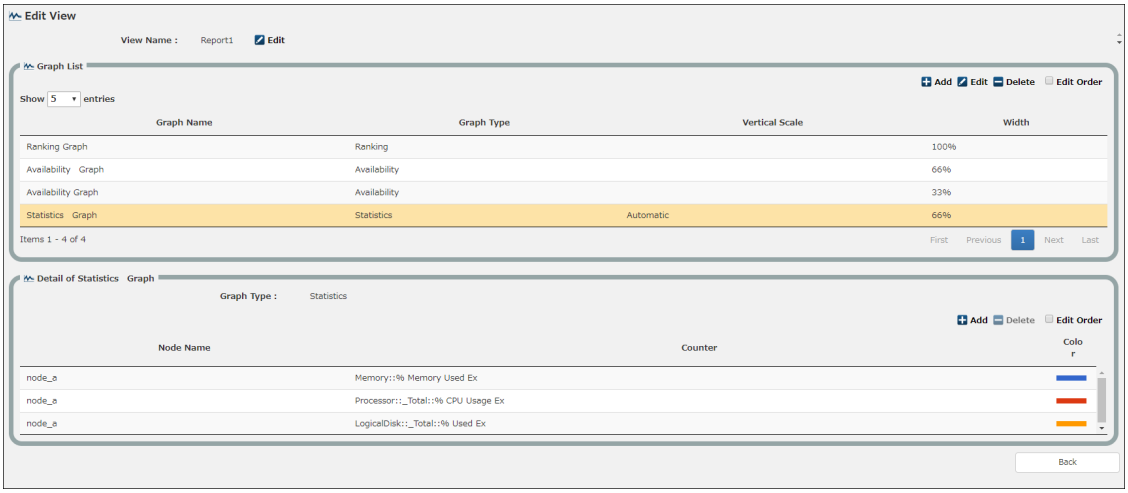

Figure 1-126 Detail of Statistics Graph

To delete a counter, follow the procedure below.

1. Select the desired counter by clicking it.
2. Click the [Delete] button.
3. When the Remove Counter dialog box is displayed, click the [OK] button.
4. Clicking the [Cancel] button closes the dialog box without deleting the counter.

Figure 1-127 Remove Counter dialog box

To change the display order of a counter, click the desired counter and click the [Edit Order] button in the [Detail] screen.

Change the order by using the edit button, and then click [Apply].

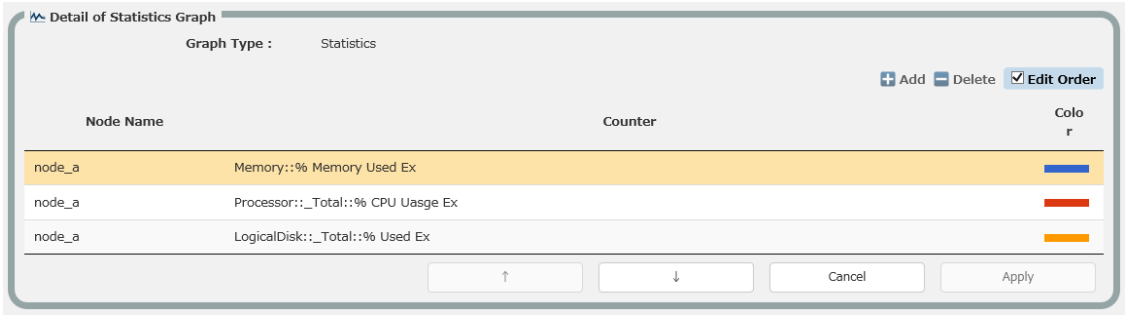

Figure 1-128 Edit Order

Table 1-61 Edit Order

Item name	Description
↑	Moves the selected line up. The line is moved as many times as the number of times you click.
↓	Moves the selected line down. The line is moved as many times as the number of times you click.
Cancel	Cancels the order change operation.
Apply	Applies the result of the order change.

Note

Depending on the display duration, some of the data may be omitted due to the limit of the rendering area. A graph can be displayed without omitting data for the following durations.

Table 1-62 Durations for which a graph can be displayed without omitting data

Data type	Monitoring interval	Duration			
		width: 100%	width: 66%	width: 50%	width: 33%
RAW	30 seconds (Default)	6 hours 35 minutes (23700 seconds)	4 hours 18 minutes 30 seconds (15510 seconds)	3 hours 10 minutes (11400 seconds)	2 hours 1 minutes 30 seconds (7290 seconds)
	10 seconds (Minimum)	2 hours 11 minutes 40 seconds (7900 seconds)	1 hours 26 minutes 10 seconds (5170 seconds)	1 hours 3 minutes 20 seconds (3800 seconds)	40 minutes 30 seconds (2430 seconds)

Data type	Monitoring interval	Duration			
		width: 100%	width: 66%	width: 50%	width: 33%
Statistics	-	32 days 22 hours (790 hours)	21 days 13 hours (517 hours)	15 days 20 hours (380 hours)	10 days 3 hours (243 hours)

1.7.4.3 Setting a ranking graph

This section describes how to set a ranking graph.

A ranking graph displays the indexes (counters) that are the top during the specified period according to the specified settings.

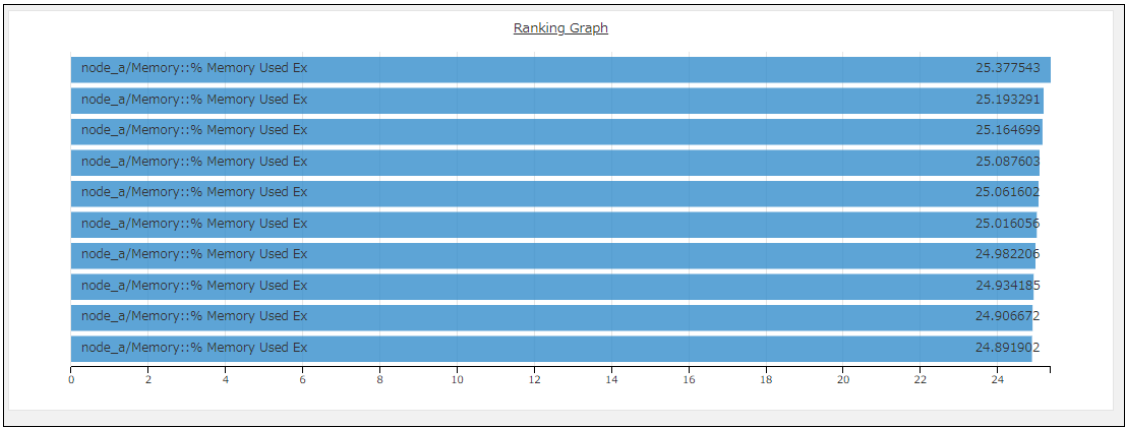

Figure 1-129 Ranking graph example

In the graph list, click [Add] and then select [Ranking] as the graph type.

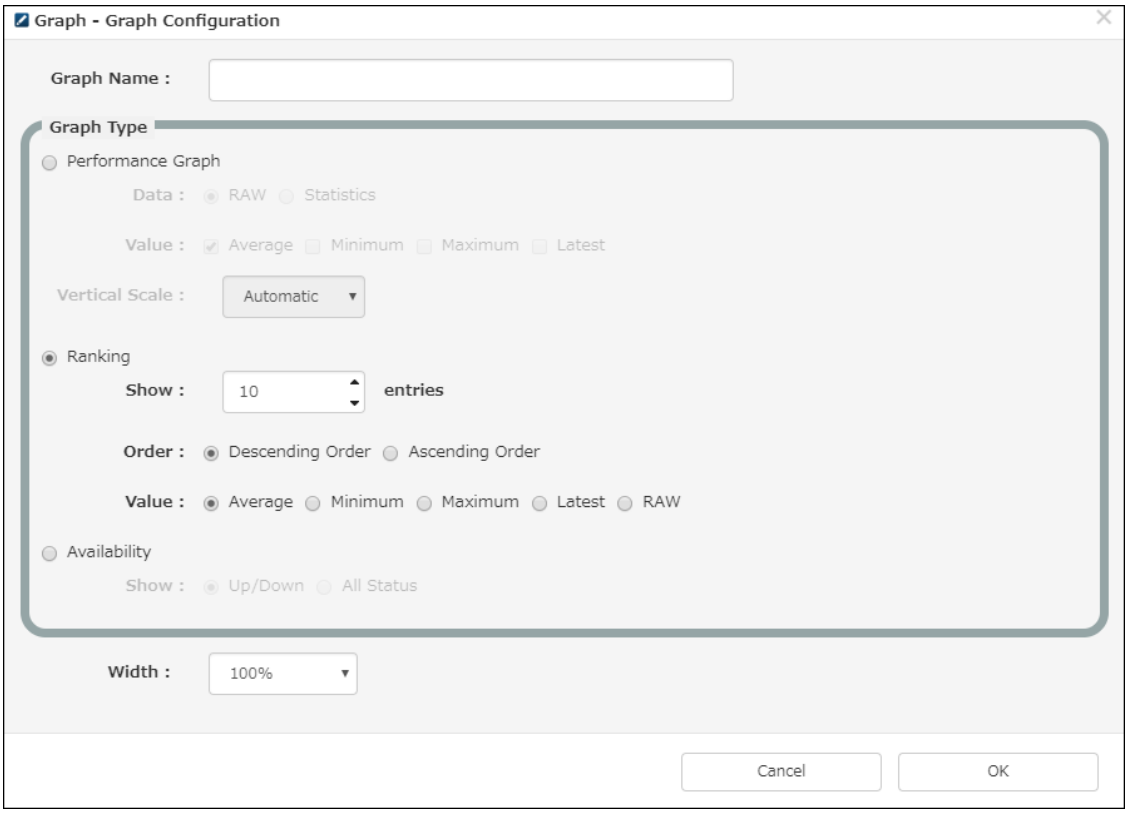

Figure 1-130 [Graph Configuration] dialog box (Ranking)

Table 1-63 Item list ([Graph Configuration] dialog box (Ranking))

Item name	Required	Description
Show [ ] entries	Y	Set the number of counters to be displayed in the ranking. If you will print the ranking on A4 paper in portrait orientation, set this number to 40 or so. • The default setting is 10. • Specify a value within the range of 1 to 100.
Order	Y	Set the sort order of the ranking. The default setting is descending. • Descending Order • Ascending Order
Value	Y	Select the data type of the ranking. • Average • Minimum • Maximum • Latest • RAW [RAW] is the values actually acquired by the monitoring system. [Average], [Minimum], [Maximum], and [Latest] are the statistical data generated from [RAW]. If you select [RAW], the ranking of the most recent monitoring data in the specified period is displayed. If you select [Average], [Minimum], [Maximum], or [Latest], the ranking of the statistical data in the specified period is displayed. The statistical data is calculated on the hour every hour based on the monitoring data obtained from 0 minutes to 59 minutes and 59 seconds. Therefore, depending on the specified range of the start and end dates and times, the same counter may be displayed multiple times in the ranking. To prevent the same counter from being displayed multiple times in the ranking, specify the ranking target time (the same time) as the start and end dates and times. For information about how to specify the start and end dates and times, see "1.7.4 Analysis / Report (page 76)".

Note

Since the statistical data is generated on the hour every hour, the specified range of the start and end dates and times and the maximum number of times the same counter is displayed in the ranking are as in the following examples.

- When the specified range of the start and end dates and times is 12:00:00 to 12:45:00, the maximum number of times the same counter is displayed in the ranking is 1.
- When the specified range of the start and end dates and times is 12:00:00 to 13:00:00, the maximum number of times the same counter is displayed in the ranking is 2.
- When the specified range of the start and end dates and times is 11:30:00 to 12:45:00, the maximum number of times the same counter is displayed in the ranking is 1.
- When the specified range of the start and end dates and times is 12:15:00 to 12:45:00, the maximum number of times the same counter is displayed in the ranking is 0.

If you click [OK], the added ranking is displayed in the graph list.

Have the ranking selected in the list. Graph details are displayed.

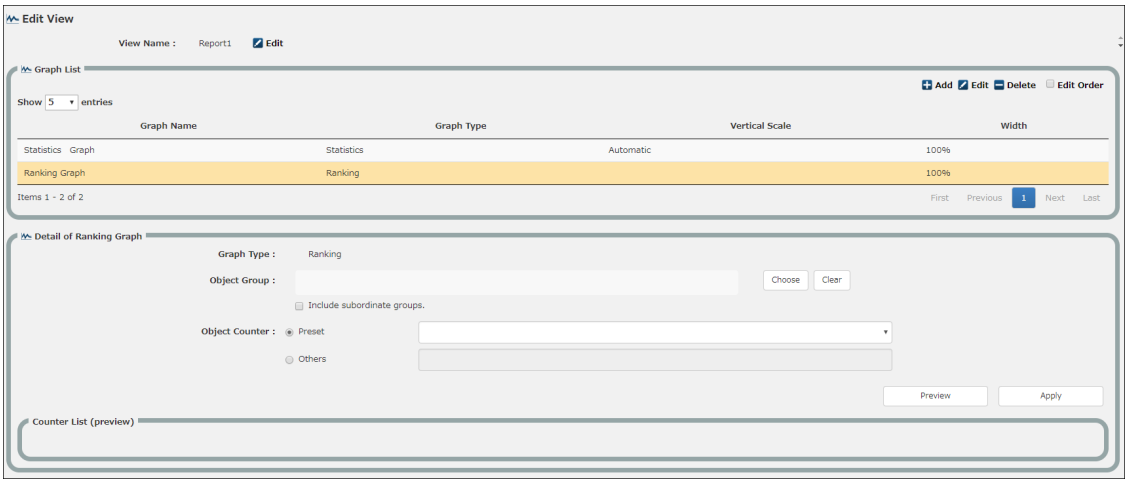

Figure 1-131 [Edit View] screen (Ranking graph setting)

Table 1-64 Item list ([Edit View] screen (Ranking graph setting))

Item name	Input value or display	Description
Graph type	Ranking	Indicates a ranking graph.
Object Group	Choose Group	The group that is the population for the ranking is displayed. Click [Choose] and, from the resulting group list, select the target group. Specify the selected group or selected counter or both. If you select [Include subordinate groups], the ranking includes all the groups below the selected group.
[Choose] button		Displays the [Choose Group] dialog box, which lets you select a group.
[Clear] button		Clears the selected group.
Object counter	Preset	Select one of the following preset items. • Memory Usage • Disk Usage • CPU Usage • CPU Usage of Process
Object counter	Others	Specify the name of the counter whose ranking you want to display, within 2048 characters in the regular expression format.
Preview		Clicking the [Preview] button displays the list in the target counter list.
Counter list (Preview)		Displays the list of ranking target counters.
Apply		Clicking the [Apply] button saves the specified settings.

Clicking the [Back] button displays the specified ranking in the [Analysis / Report] screen.

The following regular expressions are set for the preset items of the target counter.

Table 1-65 Object counter (Preset)

Item name	Regular expression
Memory Usage	^Memory::(% Memory Used Ex|%memusednocached|%MemoryUsedEx)$
Disk Usage	^LogicalDisk::(?!_Total::).+::(% Used Ex|Use%|%used|Capacity)$
CPU Usage	^Processor::(_Total::|all::|system::|ALL::)?% CPU Usage Ex$
CPU Usage of Process	^Process::(?!_Total::).+::(% Processor Time|%CPU)$

1.7.4.4 Setting an availability graph

This section describes how to set an availability graph. The availability is displayed as the operating ratio of the monitored target within the specified period. A circle graph is displayed when only one monitoring target is specified, and a bar graph is displayed when multiple monitoring targets are specified.

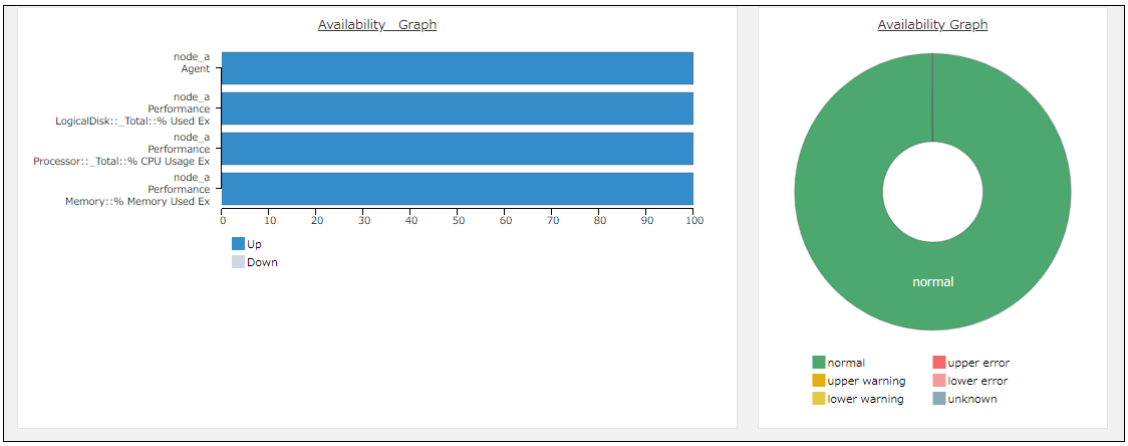

Figure 1-132 Availability graph example

In the graph list, click [Add] to display the [Graph Configuration] dialog box and then select [Availability] as the graph type. To display the graph, select [Up/Down] or [All Status] and click [OK].

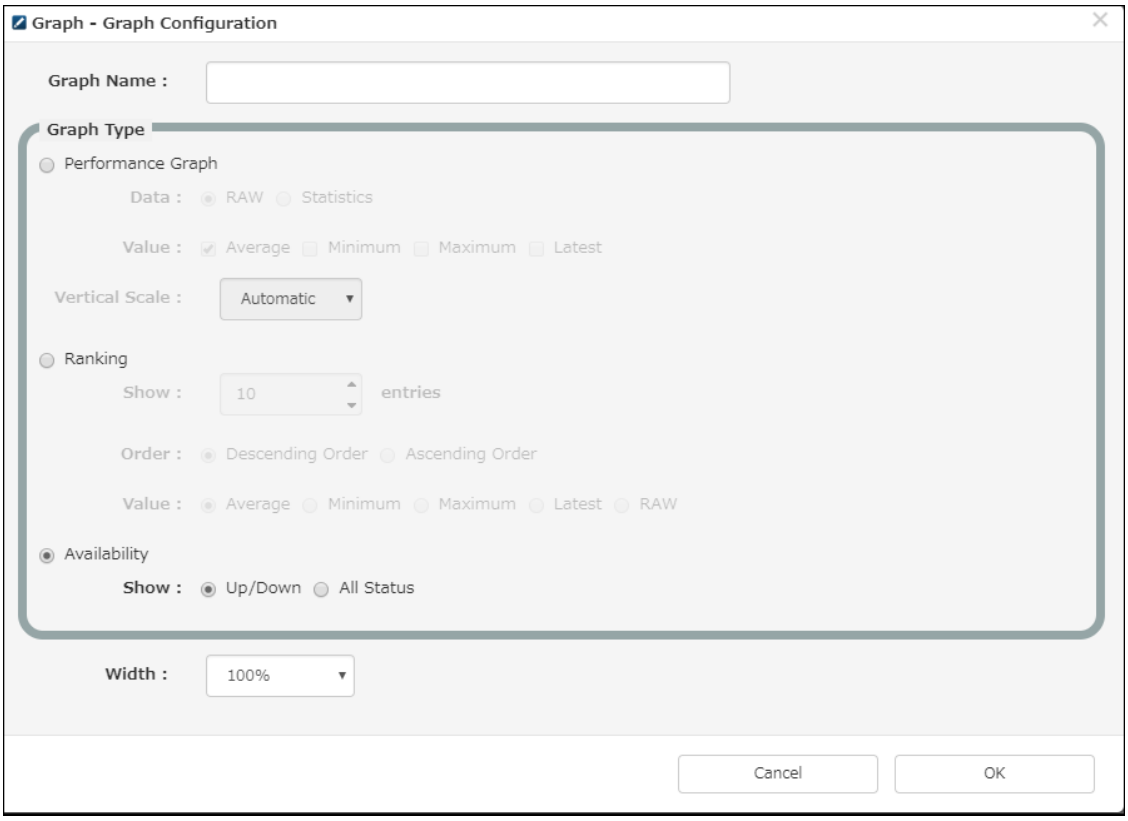

Figure 1-133 [Graph Configuration] dialog box (Availability)

Table 1-66 Item list ([Graph Configuration] dialog box (Availability)

Item name	Description
Up/Down	The graph displays only the information for the in-operation status, with all the other statuses shown as "out of operation."
All Status	Each status of the monitoring target is displayed, respectively.

The added graph is displayed in the graph list.

Have the availability graph selected in the list. Graph details are displayed.

Depending on the information to be displayed in the graph, select one of the following buttons:

- Add Agent Availability
- Add Other Availability

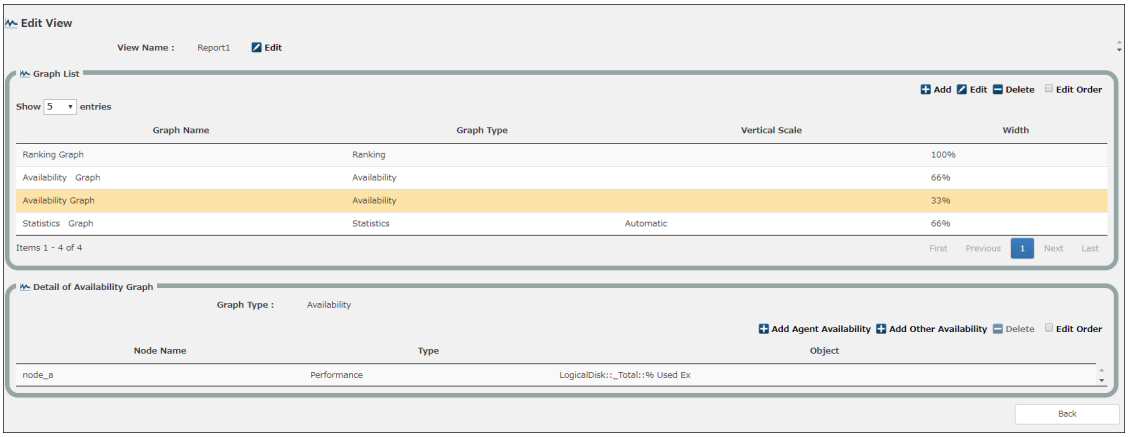

Figure 1-134 [Edit View] screen (Availability)

Adding an agent operating ratio

Clicking the [Add Agent Availability] button displays the [Choose Monitored Target] dialog box. Select a group from the group tree, and select the node to be monitored from the displayed node list. You cannot select an already selected node. Click the [Add] button.

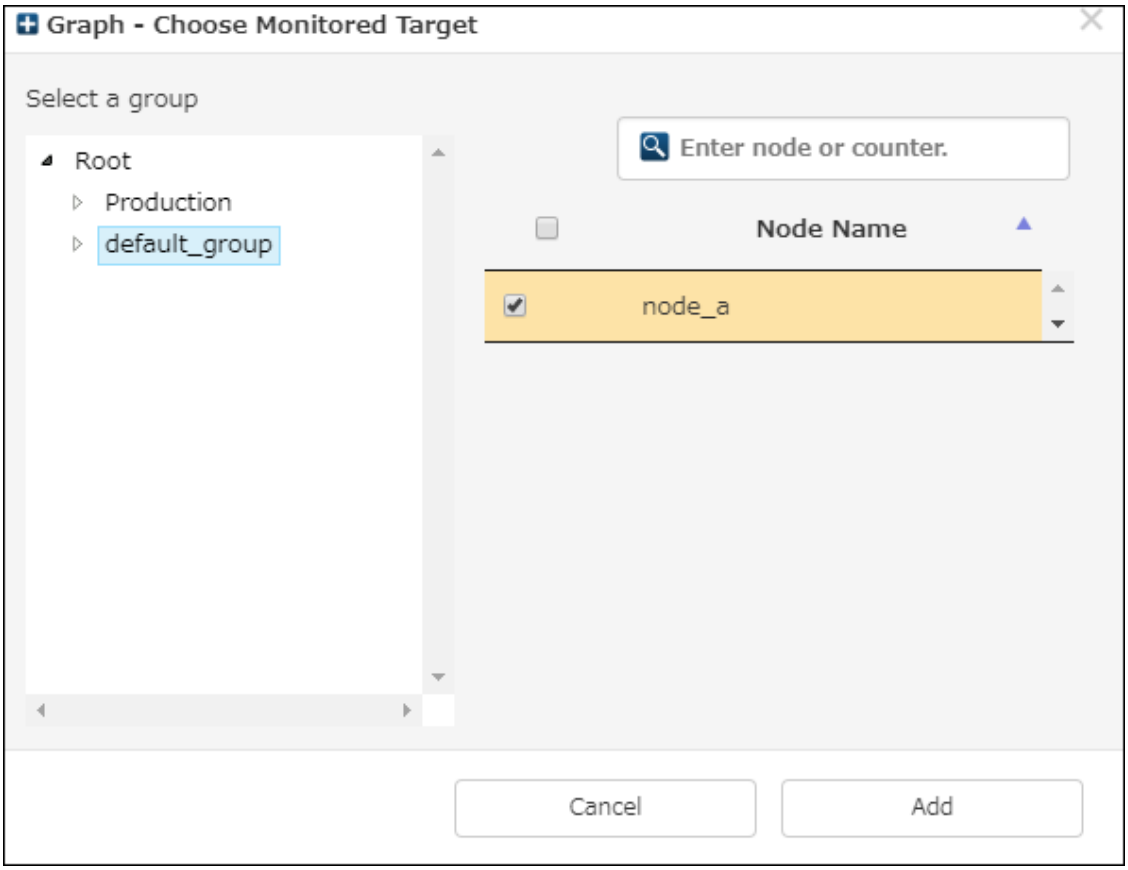

Figure 1-135 [Choose Monitored Target] dialog box

The selected node is displayed in the list.

Clicking the [Back] button displays the added availability graph in the [Analysis / Report] screen.

Adding another operating ratio

Clicking the [Add Other Availability] button displays the [Choose Monitored Target] dialog box. Select a group from the group tree, and select the node to be monitored from the displayed node list. From this node, select the monitoring target for which you want to display a graph. You cannot select an already selected monitoring target.

Selecting a filter narrows down the monitoring targets to be displayed.

- Agent
- Process
- File size
- TCP/UDP port
- Windows service
- Performance

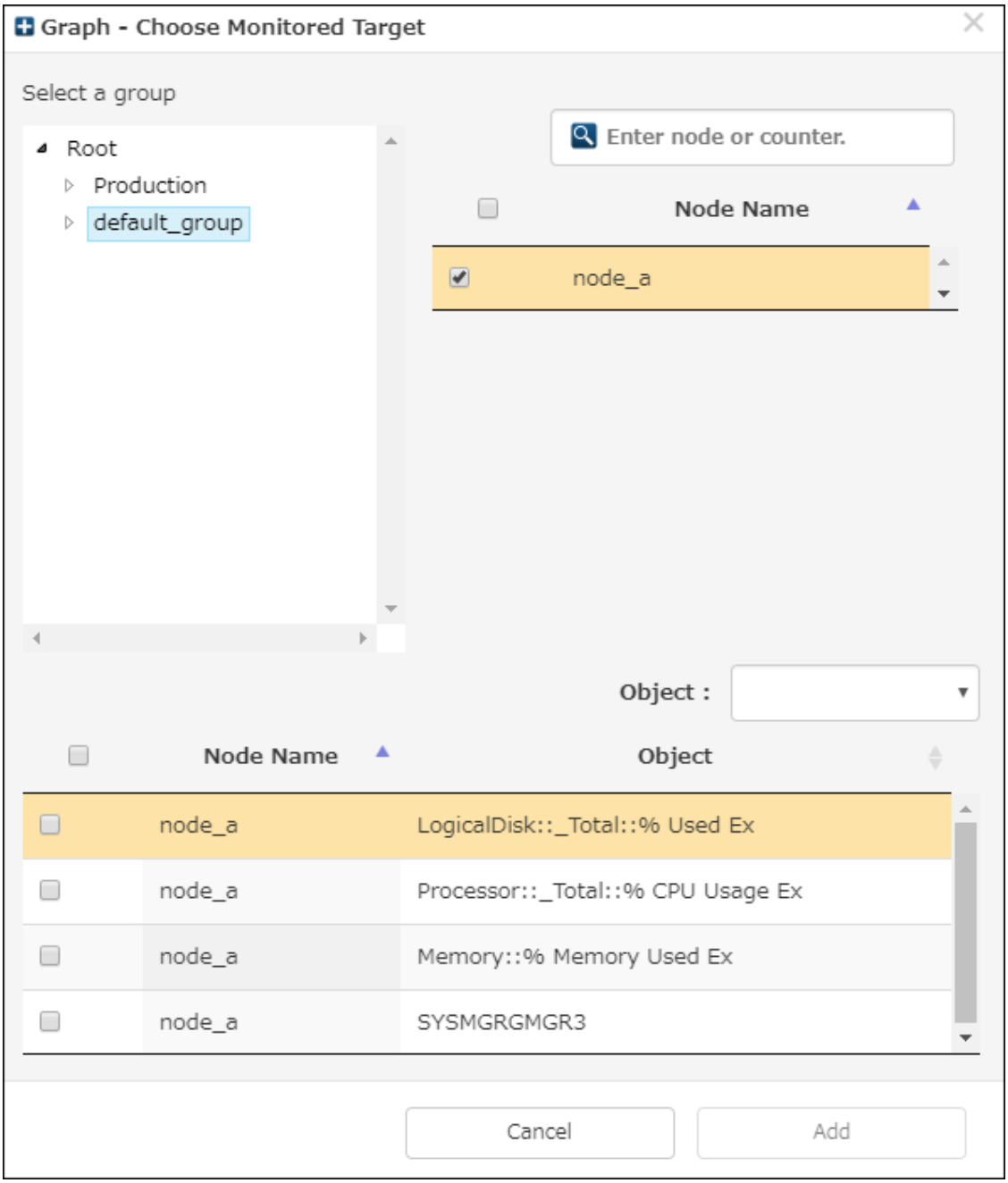

Figure 1-136 [Choose Monitored Target] dialog box

Select a monitoring target, and click [Add]. In the graph details, the monitoring targets to be displayed in the graph are listed.

Clicking the [Back] button displays the added availability graph in the [Analysis / Report] screen.

The statuses that are displayed in the availability graph are shown below.

Table 1-67 List of the information displayed for the availability

Monitoring target	Status	
	Display: Up/Down	Display: All Status
Agent	• running	• running • stop • disconnect

Monitoring target	Status	
	Display: Up/Down	Display: All Status
		• disable • function stop • unknown
Process	• running	• running • upper error • lower error • stop • unmanaged • unknown
File size	• normal	• normal • warning • fatal • unknown
TCP/UDP port	• open	• open • close • unknown
Windows service	• running	• running • stop • unknown
Performance	• normal	• normal • upper warning • lower warning • upper error • lower error • unknown

1.7.4.5 Deleting an analysis/report view

This section describes how to delete an analysis/report view.

Figure 1-137 Analysis / Report - [Delete View] dialog box

In the [Analysis / Report] screen, select a view from the tab and click the [Delete] button to display the [Delete View] dialog box.

Click the [OK] button to delete the view.

Clicking the [Cancel] button returns you to the [Analysis / Report] screen without deleting the view.

1.7.4.6 Printing an analysis/report view

This section describes how to print an analysis/report view.

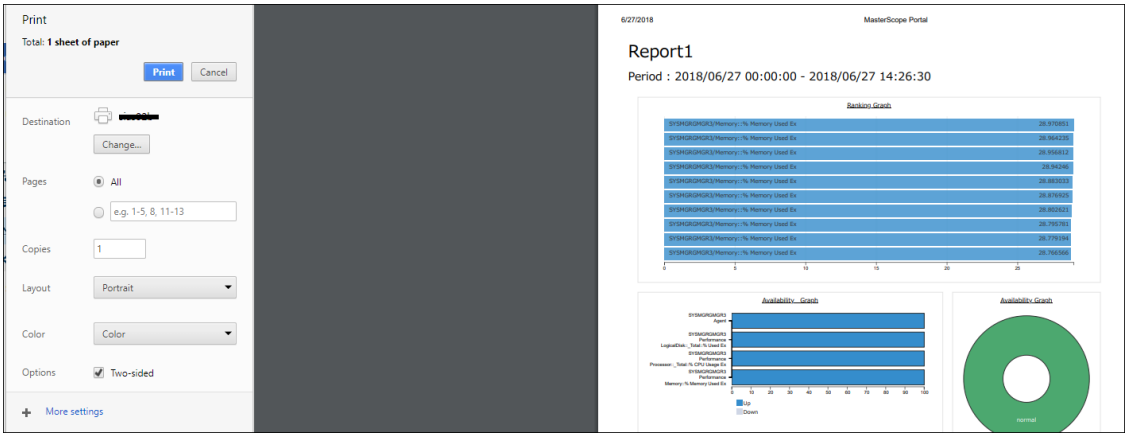

Figure 1-138 Printing an analysis/report view

In the [Analysis / Report] screen, select a view from the tab and click the [Print] button. The [Print] dialog box is displayed.

Clicking the [OK] button prints the view.

Clicking the [Cancel] button returns you to the [Analysis / Report] screen without printing the view.

1.7.4.7 Analysis function

This section describes the analysis function that conducts a future simulation based on performance data and displays the result in a graph.

While the authority to perform the operations described in this section is controlled according to the role, they are available to all users except system administrators.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

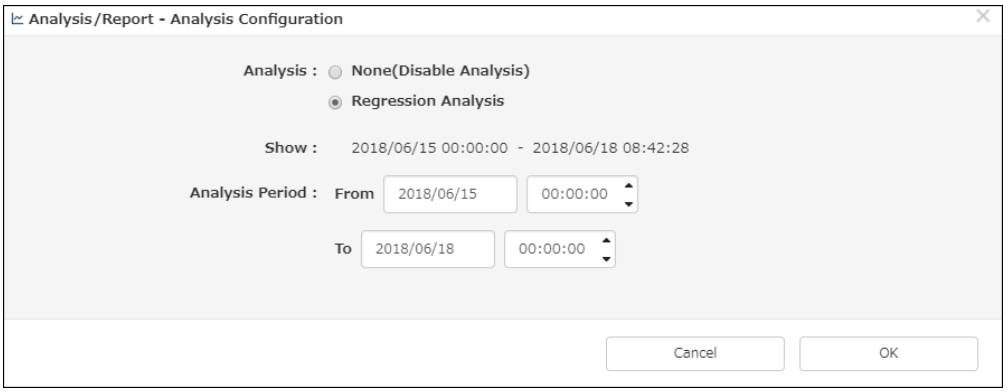

Figure 1-139 [Analysis Configuration] dialog box

To conduct a future simulation, follow the procedure below.

1. When specifying the display period in the [Analysis / Report] screen, set a future period.
2. Click [Analysis] with the view you want to analyze selected.
3. Display the [Analysis Configuration] dialog box.
4. In the [Analysis Configuration] dialog box, select an analysis period for which data is present.

5. Clicking the [OK] button displays the analysis result.
6. For a future period, an approximate straight line is shown.
7. To cancel the analysis, select [None] in the [Analysis Configuration] dialog box and click the [OK] button.

Table 1-69 Item list ([Analysis Configuration] dialog box)

Item name	Required	Description
Analysis	Y	Select one of the following. To cancel the analysis, select [None]. • None • Regression Analysis
Show		Shows the display period of the graph.
Analysis period		Specify the analysis period. The result of the future simulation conducted for the analysis period is displayed in the graph. This is required when you have selected [Regression Analysis] for [Analysis]. The analysis is conducted based on the data displayed in the graph. If the display period is long, some of the data may be omitted when the analysis is conducted. For details, see the note given at the end of "1.7.4.2 Setting a performance graph (page 79)".

An example of the analysis result is shown below.

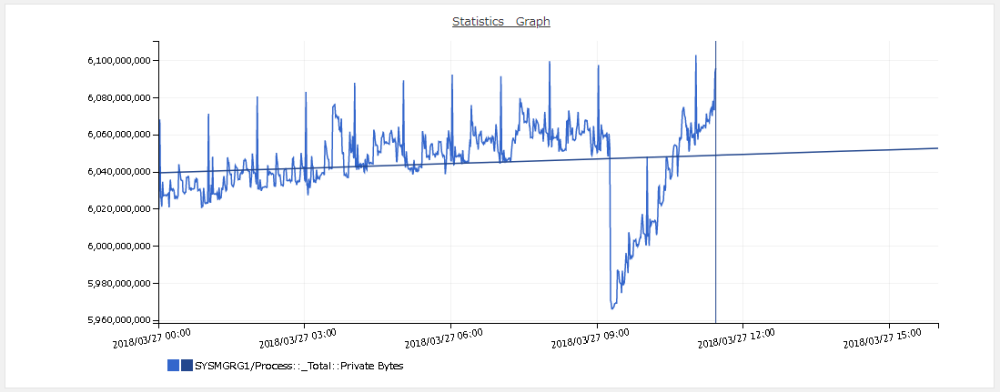

Figure 1-140 Analysis result display

1.7.5 Setting

This section describes the setting function.

The [Setting] screen is displayed by selecting [Monitoring] and then [Setting] from the menu.

1.7.5.1 Node monitoring

This section describes the [Node Monitoring] screen that displays the list of monitored nodes.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

The [Node Monitoring] screen is displayed by selecting [Monitoring], [Setting], and [Node Monitoring] from the menu.

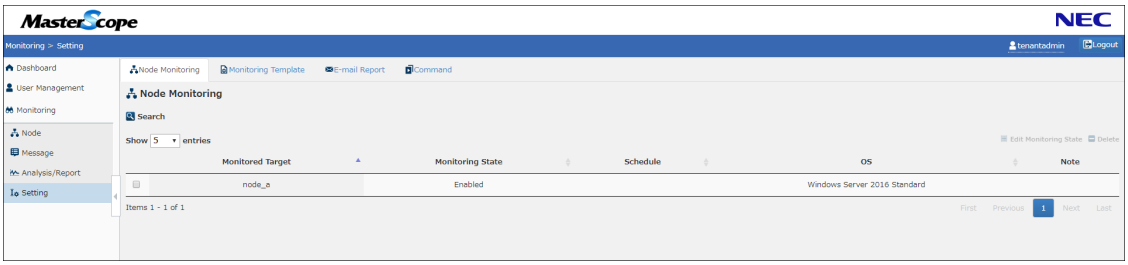

Figure 1-141 [Node Monitoring] screen

Table 1-70 Item list (Monitoring List)

Item name	Description
Monitored target	Displays the monitoring agent name of the monitored server.
Monitoring state	Displays the monitoring status. • Enabled • Disabled
Schedule	Displays the definition name of the monitoring schedule.
OS	Displays the OS of the monitored server.
Note	Displays the remark on the monitoring setting.

Note

- The [Node Monitoring] screen does not display those nodes that are registered as [Unregistered Host] on the SystemManager G 8.0 view. Move the nodes that are registered as [Unregistered Host] to a desired topology group.

Changing the monitoring status

This section describes how to enable or disable monitoring.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	N

The [Node Monitoring] screen has the [Edit Monitoring State] link in the upper right of the monitoring list. Selecting the check box for the monitoring target in the monitoring list enables the [Edit Monitoring State] link. (The link is not enabled if you select multiple monitoring targets.)

Clicking the [Edit Monitoring State] link displays the menu shown below, which lets you enable or disable monitoring.

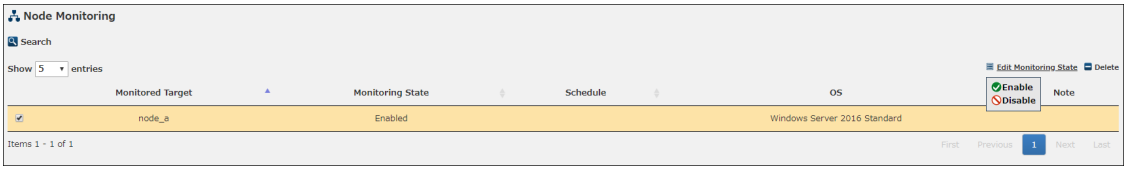

Figure 1-142 [Edit Monitoring State] menu

Figure 1-143 [Enable] dialog box

Table 1-71 Item list ([Enable] dialog box)

Item name	Description
Cancel	Closes the dialog box without enabling monitoring.
OK	Enables monitoring and then closes the dialog box.

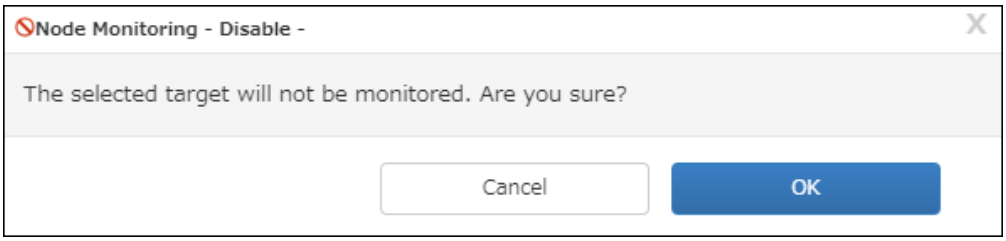

Figure 1-144 [Disable] dialog box

Table 1-72 Item list ([Disable] dialog box)

Item name	Description
Cancel	Closes the dialog box without disabling monitoring.
OK	Disables monitoring and then closes the dialog box.

Deleting the monitoring settings

This section describes how to delete the monitoring settings.

Note that the authority to perform the operations described in this section is controlled according to the user type and role.

The operations described in this section are available to the following users.

System Administrator	Manager	User
N	Y	N

The operations described in this section are available to the users of the following roles.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

The [Node Monitoring] screen has the [Delete] link in the upper right of the monitoring list. Selecting the check box for the monitoring target in the node list enables the [Delete] link. (The link is also enabled if you select multiple monitoring targets.)

Clicking the [Delete] link displays the [Delete Monitoring Settings] dialog box shown below, which lets you delete all the monitoring settings of a selected monitoring target.

Note

- Once you delete the monitoring settings, you cannot restore them. If you delete the monitoring settings by mistake, you will need to register all of them again.

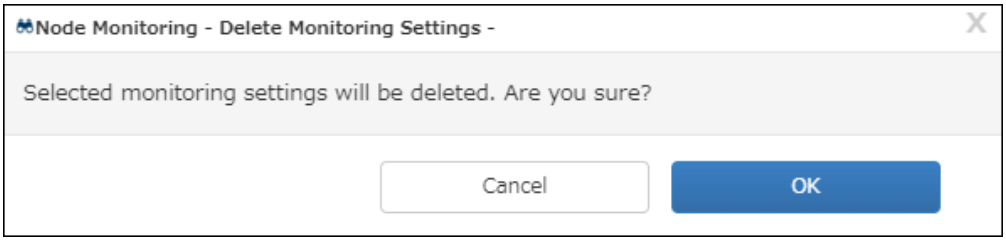

Figure 1-145 [Delete Monitoring Settings] dialog box

Table 1-74 Item list ([Delete Monitoring Settings] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the monitoring settings.
OK	Deletes the monitoring settings and then closes the dialog box.

[Details] tab

This section describes how to view the detailed information about monitoring settings.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

If you click the line of the monitoring target in the list of [Node List], the detailed information about the corresponding monitoring settings are displayed in the [Details] tab.

Figure 1-146 [Details] tab

Table 1-74 Item list ([Details] tab)

Item name	Description
Monitoring state	Displays the monitoring status. • Enabled • Disabled
State of monitoring agent	Displays the status of the monitoring agent. If no agent exists, "Already deleted" is displayed.

Item name	Description
Agent type	Displays the type of the monitoring agent. • Ordinary agent Normal monitoring agent • Remote host Agentless host (monitored by a remote monitoring agent)
Schedule	Displays the definition name of the monitoring schedule.
Scheduling status	Displays the status of the schedule if any. Either of the following statuses is displayed. • Active • Inactive
IP address	Displays the IP address of the monitored server.
OS	Displays the OS of the monitored server.
Note	Displays the remark on the monitoring setting.
Schedule setting	Clicking this item displays the [Schedule Setting] dialog box.
Edit note	Clicking this item displays the [Edit remark] dialog box.

Schedule setting

This section describes how to set a monitoring schedule.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	N

Clicking the [Schedule Setting] link displays the [Schedule Setting] dialog box shown below. By setting a schedule for the monitoring target (monitored agent) using this dialog box, you can have the target monitored for a specified period.

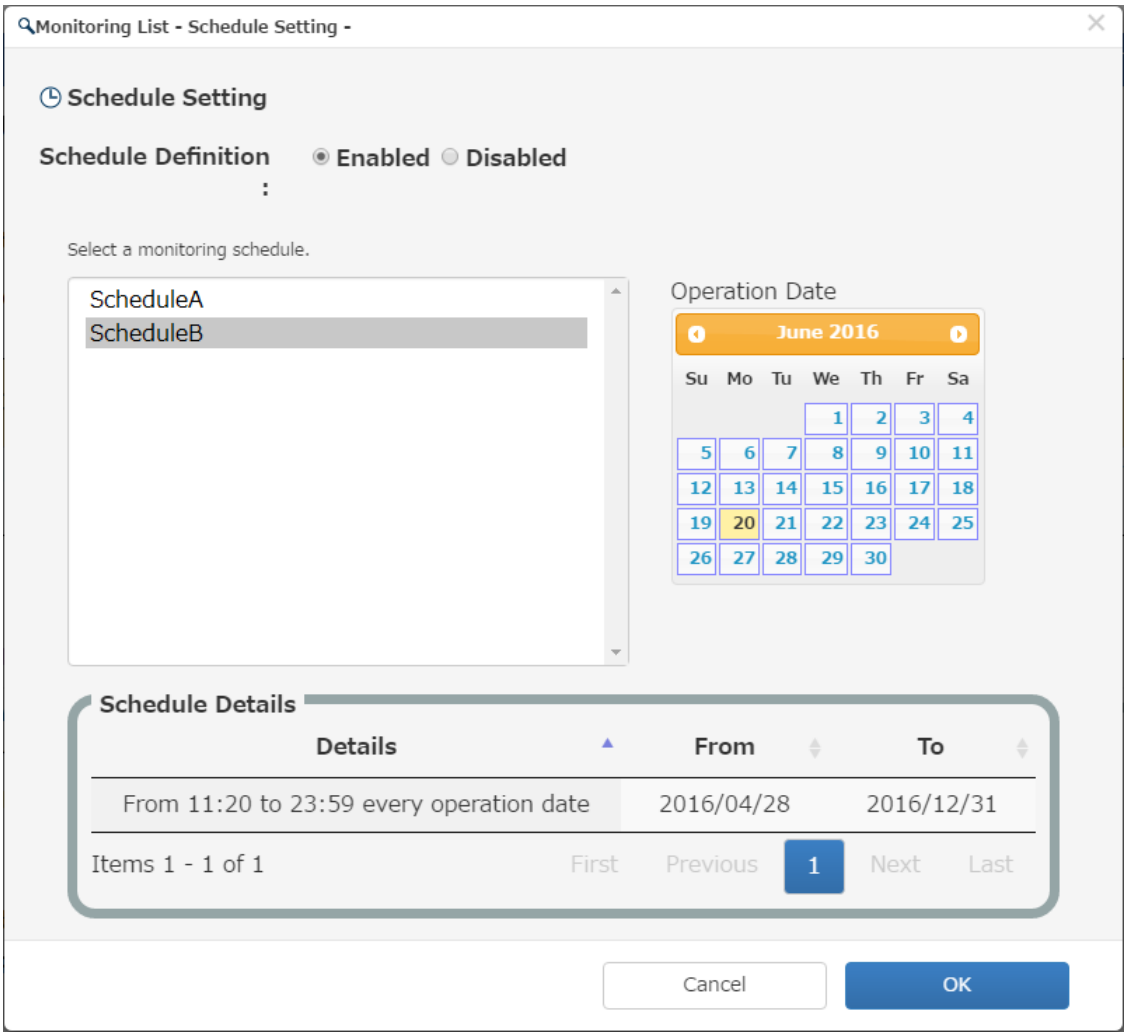

Figure 1-147 [Schedule Setting] dialog box

Table 1-75 Item list ([Schedule Setting] dialog box)

Item name	Description
Schedule definition	Select one of the following: • Enabled • Disabled If you select [Enabled], select a schedule definition from the list box.
Operating date	Displays the operating day of the selected schedule on the calendar. The operating day is indicated by a blue frame. A day other than the operating day is indicated by a gray frame.
Schedule details	Displays a table that lists the schedules registered for the selected schedule definition. [Schedule details] contains the following items. • Details Displays the description of the schedule. • From Displays the application start date of the schedule when it is a fixed-period schedule. • To Displays the application end date of the schedule when it is a fixed-period schedule. If this item is blank, there is no end date.

Item name	Description
Cancel	Discards the schedule setting and then closes the dialog box.
OK	Applies the schedule setting and then closes the dialog box.

Tip

The schedule set with SystemManager G is displayed. For information about how to set a schedule, see "Setting a schedule " in the "MasterScope SystemManager G Manual."

Editing the note

This section describes how to edit the note on a monitoring setting.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

Operation monitoring administrator	Operation monitoring operator	Operation monitoring referer
Y	N	N

Clicking [Edit Note] in the [Details] tab displays the [Edit Note] dialog box shown below. This dialog box lets you edit the remark on a monitoring setting.

Figure 1-148 [Edit Note] dialog box

Table 1-76 Item list ([Edit Note] dialog box)

Item name	Description
Edit note	Enter the content of the remark within 255 characters.
Cancel	Discards the edited remark and then closes the dialog box.
OK	Applies the edited remark and then closes the dialog box.

[Monitoring Settings] tab

Clicking the [Monitoring Settings] tab displays the major items of monitoring settings. Clicking one of these items displays an accordion, which lets you view monitoring settings and set monitoring items.

Note that the authority to view the individual monitoring setup panels of the [Monitoring Settings] tab is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

Note that the authority to change the individual monitoring settings is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

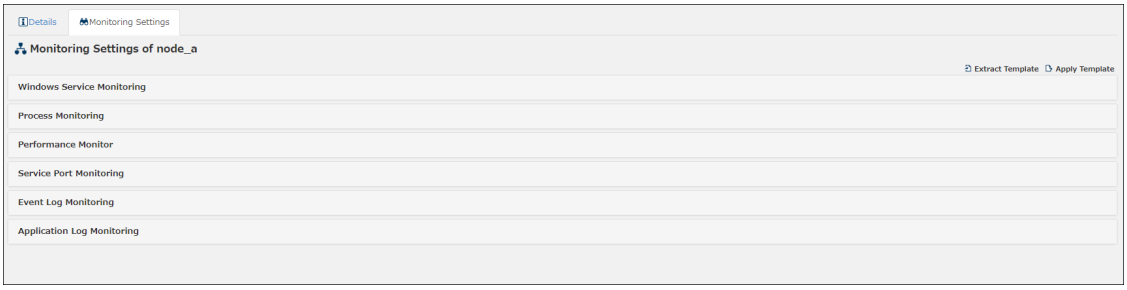

Figure 1-149 [Monitoring Settings] tab

Table 1-78 Item list ([Monitoring Settings] tab)

Item name	Description
Extract Template	Registers the monitoring settings of the node as a monitoring template. For details, see "1.7.5.1.5 Converting a monitoring setting into a monitoring template (page 99)".
Apply Template	Displays the remark on the monitoring template. For details, see "1.7.5.1.6 Applying a monitoring template (node) (page 101)".
Windows service monitoring panel	Displays the Windows service monitoring setting of the node. This is displayed only when the OS type is Windows. For details, see "1.7.5.2.1 Windows service monitoring (page 102)".
Process monitoring panel	Displays the process monitoring setting of the node. For details, see "1.7.5.2.2 Process monitoring (page 108)".
Performance monitor panel	Displays the performance monitor setting of the node. For details, see "1.7.5.2.3 Performance monitor (page 114)".
Service port monitoring panel	Displays the service port monitoring setting of the node. For details, see "1.7.5.2.4 Service port monitoring (page 118)".
Event log monitoring panel	Displays the event log monitoring setting of the node. This is displayed only when the OS type is Windows. For details, see "1.7.5.2.5 Event log monitoring (page 121)".
System log monitoring panel	Displays the system log monitoring setting of the node. This is displayed only when the OS type is Linux/Unix. For details, see "1.7.5.2.6 System log monitoring (page 128)".
Application log monitoring panel	Displays the application log monitoring setting of the node. For details, see "1.7.5.2.7 Application log monitoring (page 135)".

Converting a monitoring setting into a monitoring template

This section describes how to convert the monitoring setting of a node into a monitoring template.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Click the [Extract Template] button in the [Monitoring Settings] tab to display the [Extract Template] dialog box.

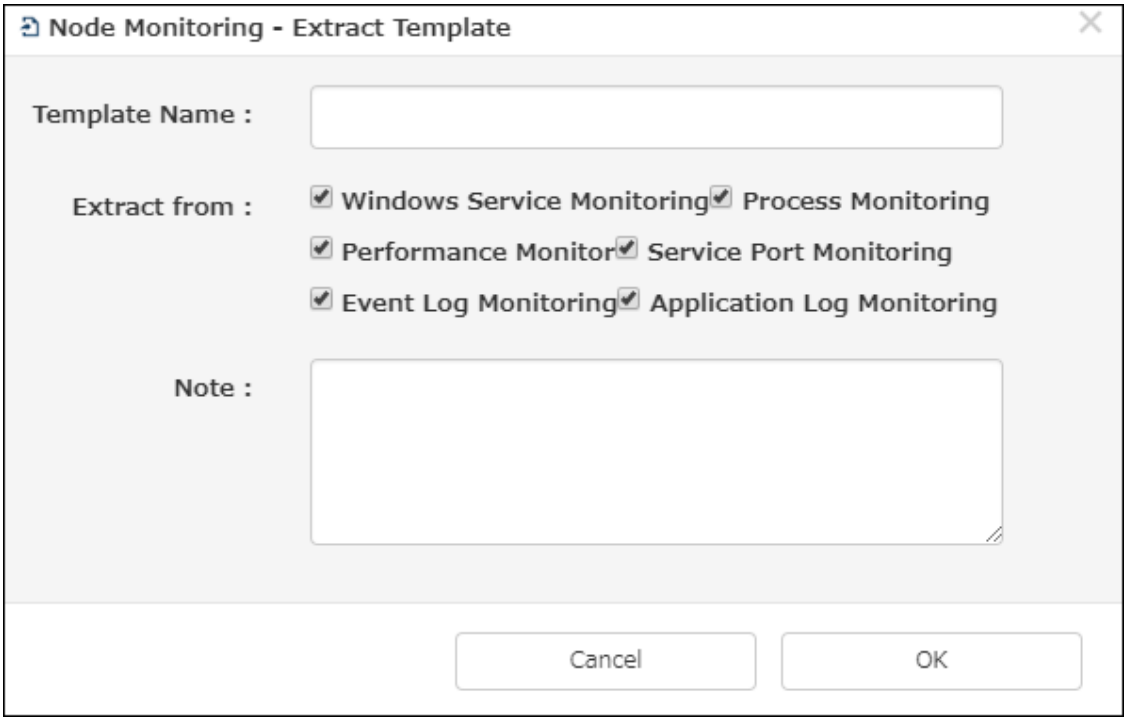

Figure 1-150 [Extract Template] dialog box

Table 1-78 Item list ([Extract Template] dialog box)

Item name	Required	Description
Template name	Y	Enter the name of the monitoring template within 256 characters.
Extract from	Y	Select the monitoring setting to be set as a monitoring template. • Windows service monitoring: The monitoring setting for the Windows service monitoring is set as a monitoring template. This is displayed when the OS type of the node is Windows. • Process monitoring: The monitoring setting for the process monitoring is set as a monitoring template. • Performance monitor: The monitoring setting for the performance monitoring is set as a monitoring template. • Service port monitoring: The monitoring setting for the service port monitoring is set as a monitoring template. • Event log monitoring: The monitoring setting for the event log monitoring is set as a monitoring template. This is displayed when the OS type of the node is Windows. • System log monitoring: The monitoring setting for the system log monitoring is set as a monitoring template. This is displayed when the OS type of the node is Linux or Unix. • Application log monitoring: The monitoring setting for the application log monitoring is set as a monitoring template.
Note		Enter the note on the monitoring template within 1024 characters.

When you have entered all necessary items, click the [OK] button to convert the setting into a monitoring template.

Clicking the [Cancel] button discards the data entered in the fields and returns you to the [Monitoring Settings] tab.

Applying a monitoring template (node)

This section describes how to apply a monitoring template from the [Monitoring Settings] tab.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

1. Click the [Apply Template] button in the [Monitoring Settings] tab.

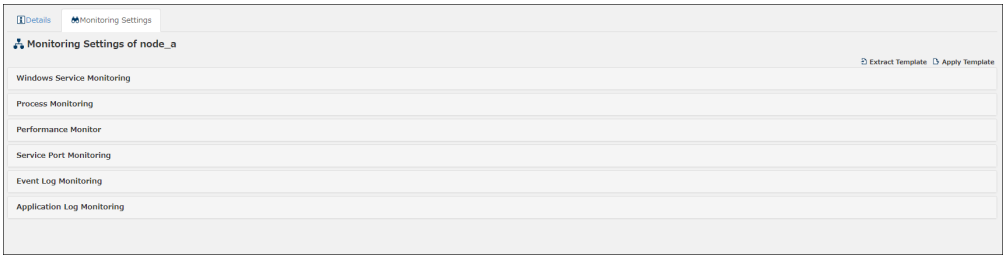

Figure 1-151 [Monitoring Settings] tab - Apply Template

2. The [Select Template] dialog box is displayed. Select the template you want to apply, and click the [OK] button.

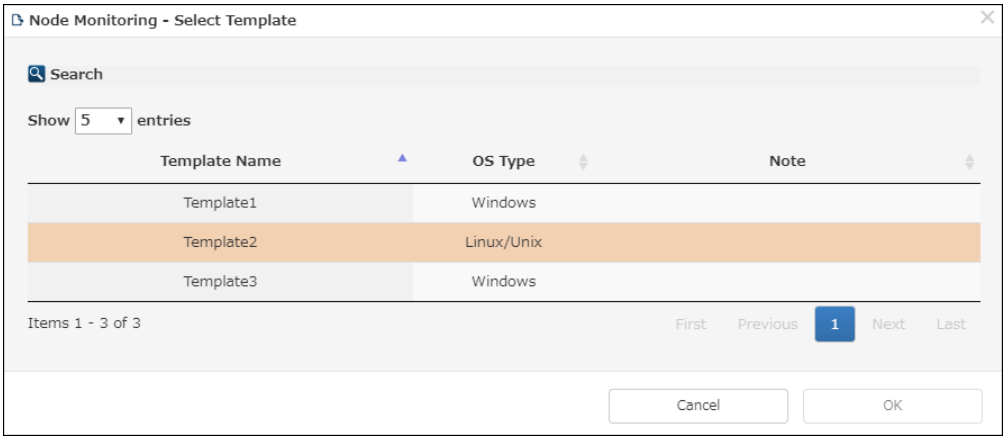

Figure 1-152 [Select Template] dialog box

3. A task list is displayed that shows the status of template application. For details about the items to be displayed on the task list, see "1.7.2.12 Task (page 49)".

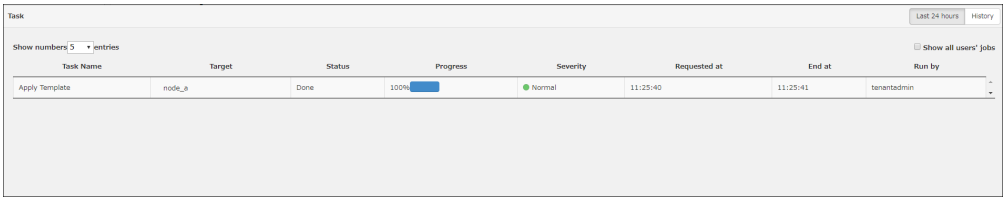

Figure 1-153 Task List

4. If you select a task in the task list, the [Task Detail] dialog box is displayed that lets you view the template application execution log. For details about the items to be displayed on the task details, see "1.7.2.12 Task (page 49)".

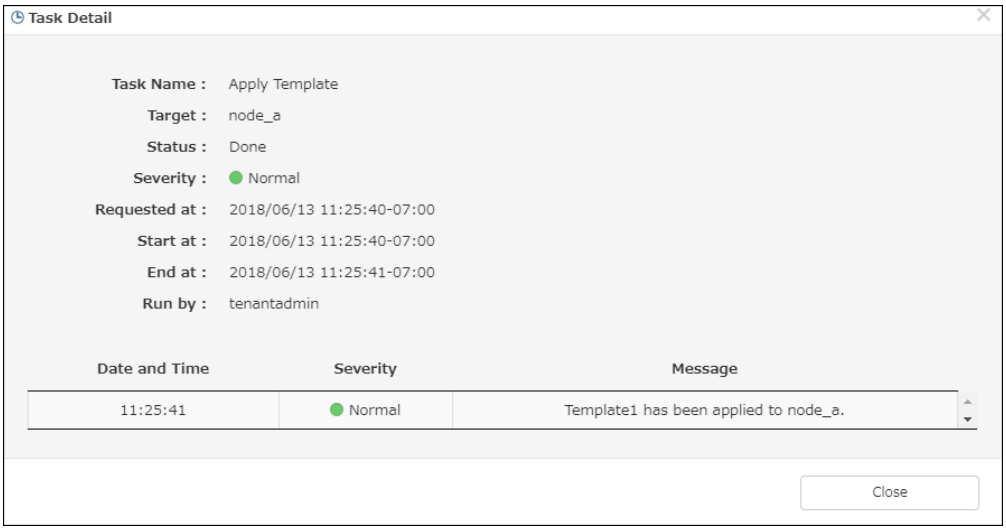

Figure 1-154 [Task Detail] dialog box

1.7.5.2 Setting up monitoring

This section describes the monitoring setup functions that you can execute from the [Monitoring Settings] tab of the [Node Monitoring] screen or the monitoring template details of the [Monitoring template] screen.

Note that the authority to view the individual monitoring setup panels is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

Note that the authority to change the individual monitoring settings is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Windows service monitoring

If you click [Windows Service Monitoring] in the [Monitoring Settings] tab of the [Node Monitoring] screen or the monitoring template details of the [Monitoring template] screen, the [Windows Service Monitoring] setting panel is displayed. The [Windows Service Monitoring] setting panel lets you check the monitoring states of Windows services.

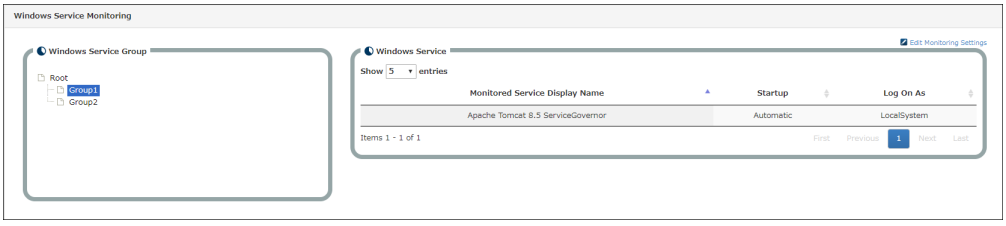

Figure 1-155 Windows service monitoring

This panel displays the tree of Windows service groups on the left. If you select a Windows service group in the tree, the services belonging to the selected group are listed on the right. This list contains the following items.

Table 1-78 Item list (Windows Service)

Item name	Description
Monitored service display name	Displays the display name of the monitored service.
Startup	Displays the startup status of the monitored service. • System • Automatic • Manual • Disabled • Unknown
Log on as	Displays the logon name of the monitored service.

If you select a Windows service in the Windows service list, [Windows Service Detail] is displayed below.

Table 1-79 Item list (Windows Service Details)

Item name	Description
Monitored service display name	Displays the display name of the monitored service.
Monitored service name	Displays the service name of the monitored service.
Startup	Displays the startup status of the monitored service. • System • Automatic • Manual • Disabled • Unknown
Log on as	Displays the logon name of the monitored service.
Service description	Displays the description of the monitored service.

Changing the Windows service monitoring setting

If you click the [Edit Monitoring Settings] link in the [Windows Service Monitoring] panel, the [Windows Service Monitoring Settings] screen is displayed.

The [Windows Service Monitoring Settings] screen displays a Windows service group tree, Windows service list, and Windows service details as in the [Windows Service Monitoring] panel.

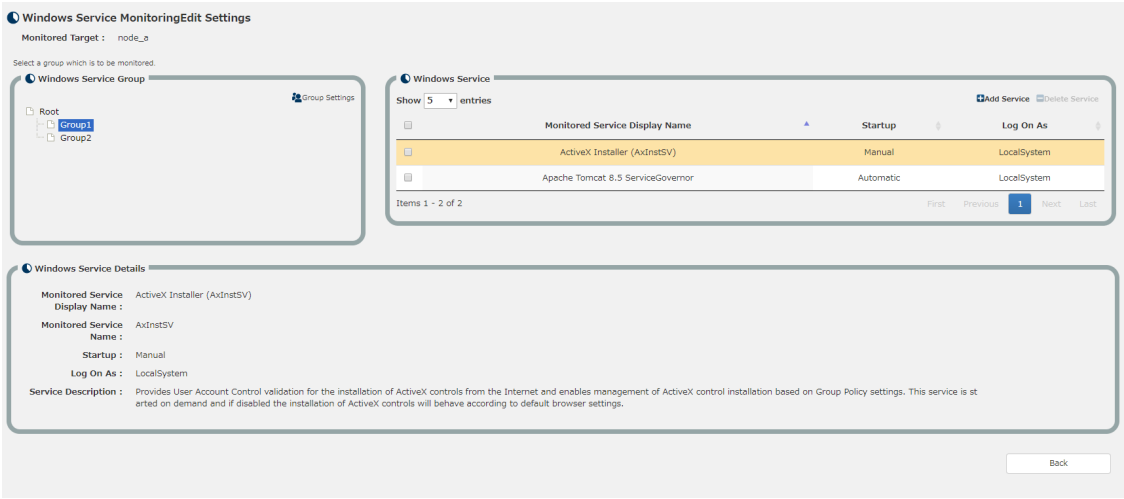

Figure 1-156 [Windows Service Monitoring Settings] screen

Adding, changing, and deleting a group

The Windows service group tree in the [Windows Service Monitoring Settings] screen contains the [Group Settings] link.

Clicking this link displays the following menu, which lets you add, change, and delete groups.

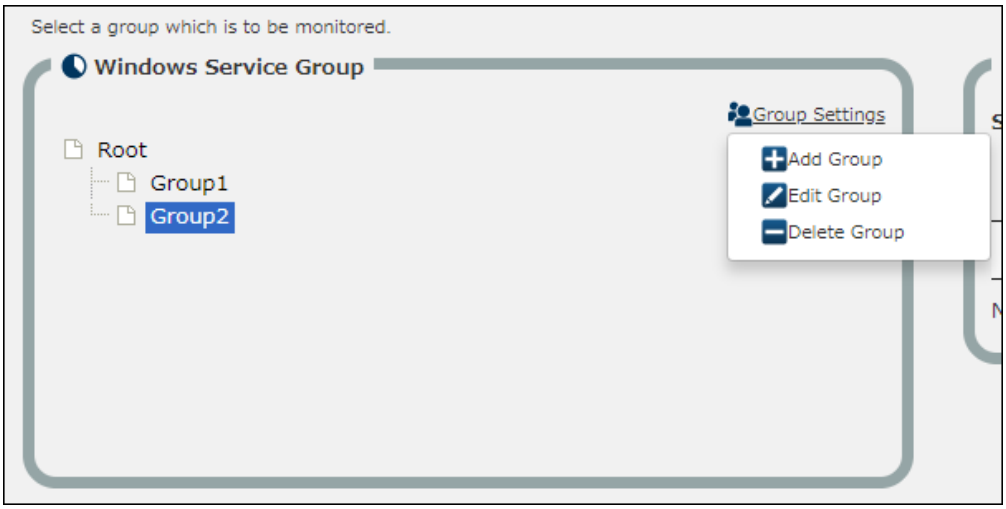

Figure 1-157 Pop-up menu

If you select [Add Group] from the pop-up menu, the [Add Group] dialog box shown below is displayed. By using this dialog box, you can add a group directly below the root or below the selected group. You can organize groups into a hierarchy. If the selected group has any service registered in it, you cannot add a child group to that group.

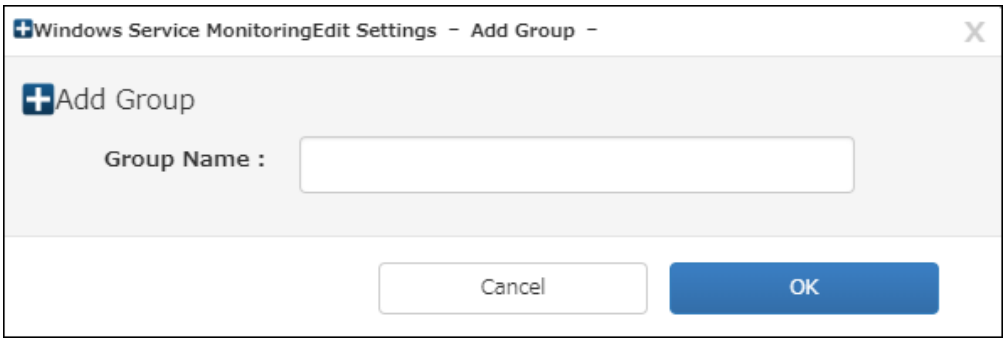

Figure 1-158 [Add Group] dialog box

Table 1-80 Item list ([Add Group] dialog box)

Item name	Description
Group name	Enter the name of the group to be added within 64 characters.
Cancel	Closes the dialog box without adding the group.
OK	Adds the group and then closes the dialog box.

If you select a group in the group tree and then [Edit Group] from the pop-up menu, the [Edit Group] dialog box shown below is displayed. By using this dialog box, you can rename the group selected in the tree.

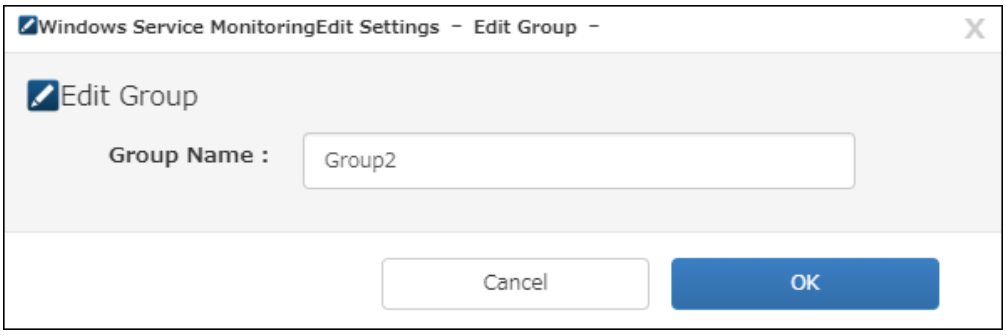

Figure 1-159 [Edit Group] dialog box

Table 1-81 Item list ([Edit Group] dialog box)

Item name	Description
Group name	Enter the name of the group to be changed within 64 characters.
Cancel	Closes the dialog box without changing the group.
OK	Changes the group and then closes the dialog box.

If you select a group in the group tree and then [Delete group] from the pop-up menu, the [Delete group] dialog box shown below is displayed. By using this dialog box, you can change the group selected in the tree. Once you delete a group, the groups and services below the deleted group are deleted as well.

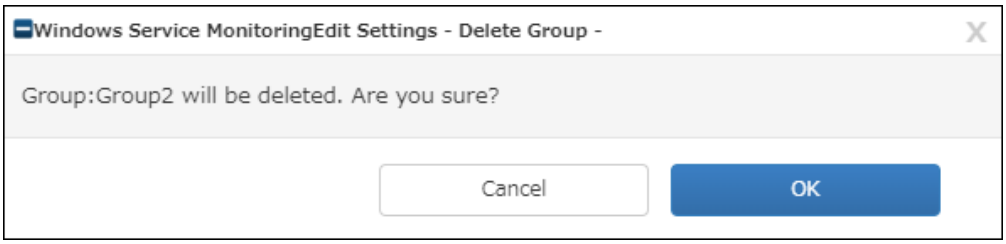

Figure 1-160 [Delete group] dialog box

Table 1-82 Item list ([Delete Group] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the group.
OK	Deletes the group and then closes the dialog box.

Adding and deleting a service

The [Windows Service] section in the [Windows Service Monitoring Settings] screen contains the [Add Service] link. If you click this link in the Windows service monitoring setting of the [Node Monitoring] screen, the [Windows Service List] dialog box shown below is displayed, which lets you add a selected Windows service to a Windows service group. A Windows service for which no check box is displayed has already been added.

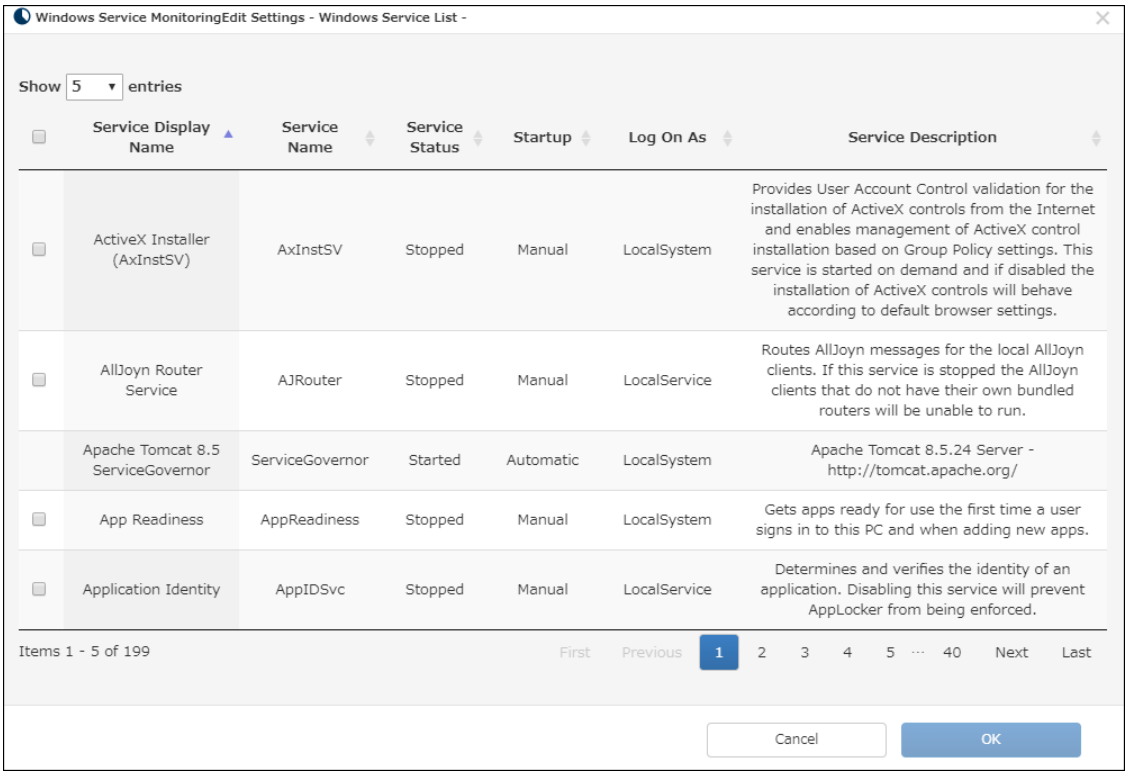

Figure 1-161 [Windows Service List] dialog box

Table 1-83 Item list ([Windows Service List] dialog box)

Item name	Description
Service display name	Displays the display name of the service.
Service name	Displays the name of the service.
Service status	Displays the status of the service.

Item name	Description
Startup	Displays the type of startup.
Log on as	Displays the name of the logon account.
Service description	Displays the description of the service.
Cancel	Closes the dialog box without adding the service.
OK	Adds the service and then closes the dialog box.

If you click the [Add Service] link in the Windows service monitoring setting of the [Monitoring template] screen, the [Add Windows Service Monitoring] dialog box shown below is displayed, which lets you add an entered Windows service to a Windows service group.

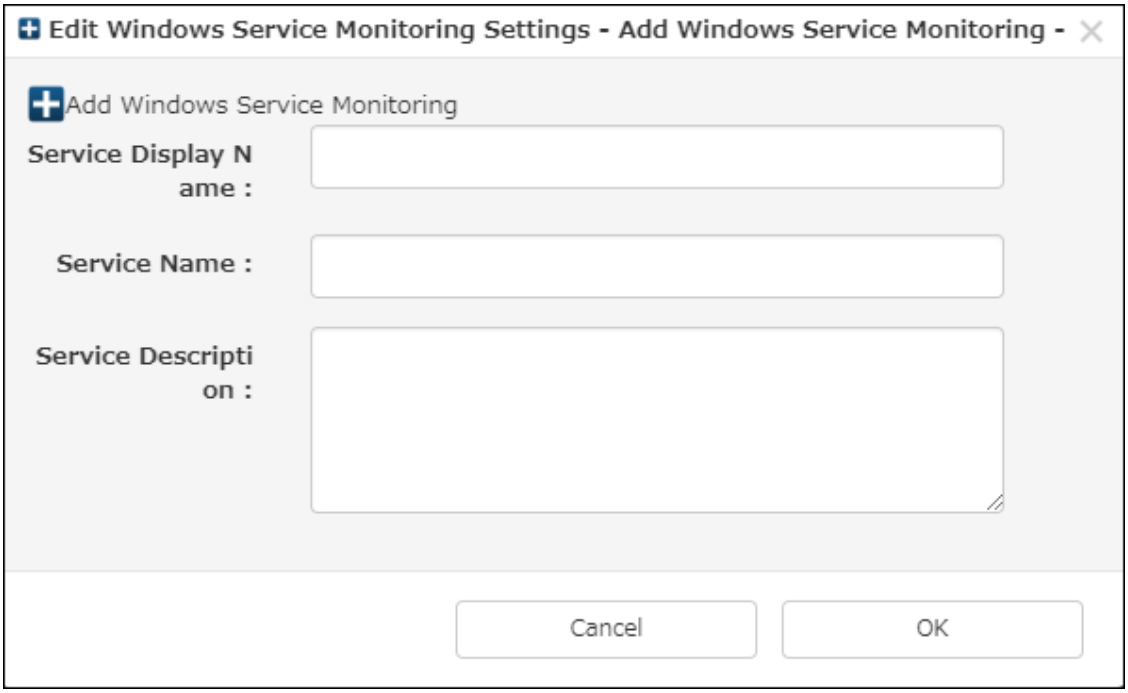

Figure 1-162 [Add Windows Service Monitoring] dialog box

Table 1-84 Item list ([Add Windows Service Monitoring] dialog box)

Item name	Required	Description
Service display name	Y	Enter the display name of the Windows service within 256 characters.
Service name	Y	Enter the service name of the Windows service within 256 characters.
Service description		Enter the description of the Windows service within 512 characters.

Also, the Windows service monitoring setting of the [Monitoring template] screen contains the [Edit Service] link. If you select the service you want to change and click the [Edit Service] link, the [Edit Windows Service Monitoring] dialog box shown below is displayed, which lets you change the Windows service. The items of the [Edit Windows Service Monitoring] dialog box are the same as those of the [Add Windows Service Monitoring] dialog box.

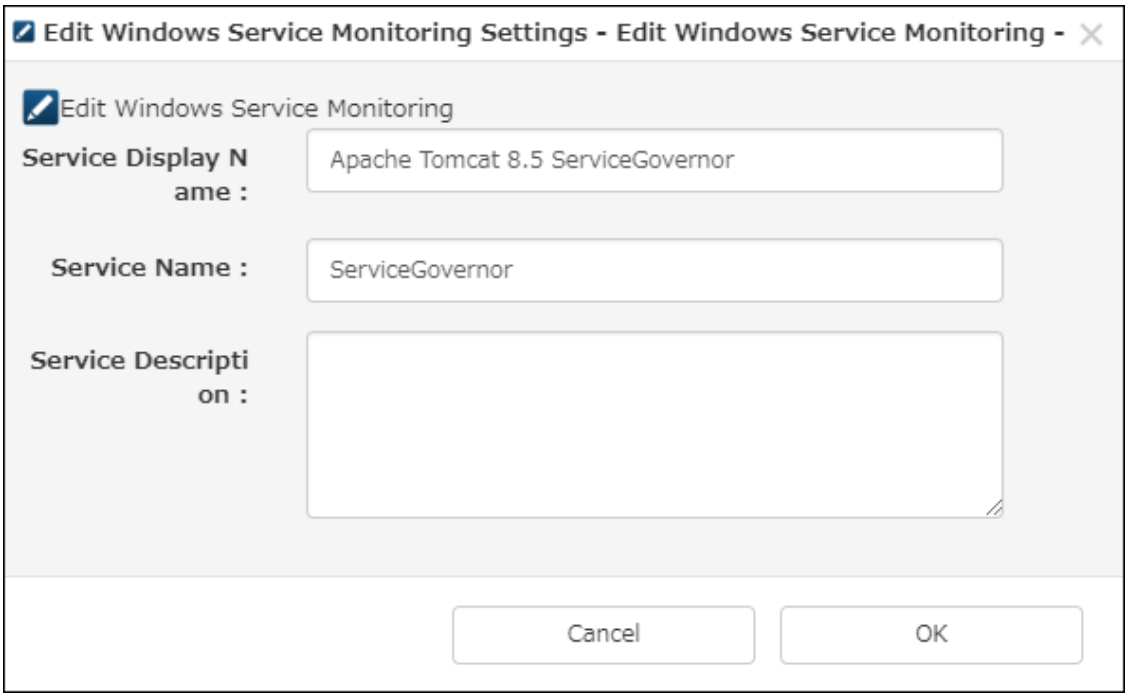

Figure 1-163 [Edit Windows Service Monitoring] dialog box

The [Windows Service] section in the [Windows Service Monitoring Settings] screen contains the [Delete Service] link. If you select the check box of the service you want to delete and click this link, the [Windows Service Monitoring Delete] dialog box shown below is displayed, which lets you delete the service from the group.

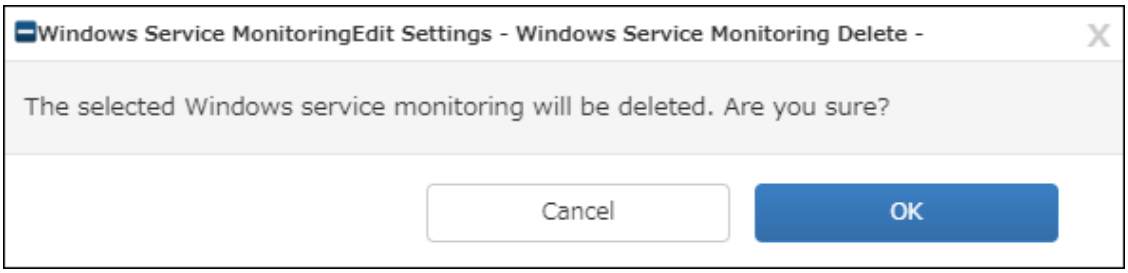

Figure 1-164 [Windows Service Monitoring Delete] dialog box

Table 1-85 Item list ([Delete Windows Service] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the service.
OK	Deletes the service and then closes the dialog box.

Process monitoring

If you click [Process Monitoring] in the [Monitoring Settings] tab of the [Node Monitoring] screen or the monitoring template details of the [Monitoring template] screen, the [Process Monitoring] setting panel is displayed. The [Process Monitoring] setting panel lets you check the monitoring states of processes.

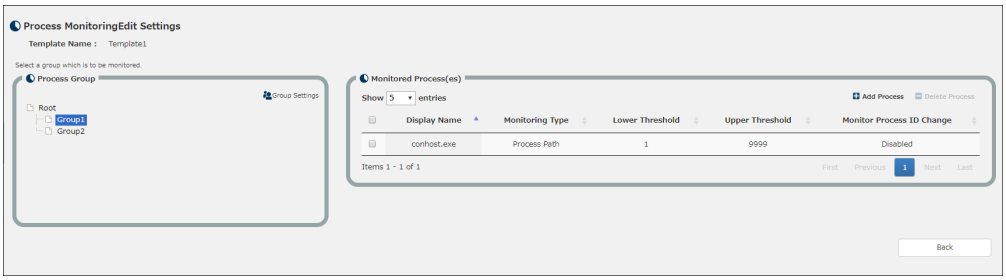

Figure 1-165 Process monitoring

This panel displays the tree of process groups on the left. If you select a process group in the tree, the monitoring services belonging to the selected group are listed on the right. This list contains the following items.

Table 1-86 Item list (Monitoring Process)

Item name	Description
Display name	Displays the display name of the monitored process.
Monitoring type	Displays the monitoring method. One of the following is displayed: • Process path • Command line
Lower threshold	Displays the lower limit of the process count.
Upper threshold	Displays the upper limit of the process count.
Monitor process ID change	Displays whether process ID change monitoring is specified. One of the following is displayed: • Enabled • Disabled

If you select a monitoring process in the monitoring process list, [Monitored Process Detail] is displayed below.

[Monitored Process Detail] contains the following items.

Table 1-87 Item list (Monitoring Process Details)

Item name	Description
Display name	Displays the display name of the monitored process.
Monitoring type	Displays the monitoring method. One of the following is displayed: • Process path • Command line
Process path	When [Monitoring type] is [Process path], the process path is displayed.
Command path	When [Monitoring type] is [Command line], the command line is displayed.
Lower threshold	Displays the lower limit of the process count.
Upper threshold	Displays the upper limit of the process count.
Monitor process ID change	Displays whether process ID change monitoring is specified. One of the following is displayed: • Enabled • Disabled
Start command	Displays the application of the start command.
Start command directory	Displays the work directory for the start command.

Item name	Description
Start command option	Displays the option of the start command.
Stop command	Displays the application of the stop command.
Stop command directory	Displays the work directory for the stop command.
Stop command option	Displays the option of the stop command.

Changing the process monitoring setting

If you click the [Edit Monitoring Settings] link in the [Process Monitoring] panel, the [Process Monitoring Settings] screen is displayed.

The [Process Monitoring Settings] screen displays a process group tree, monitoring process list, and monitoring process details as in the [Process Monitoring] panel.

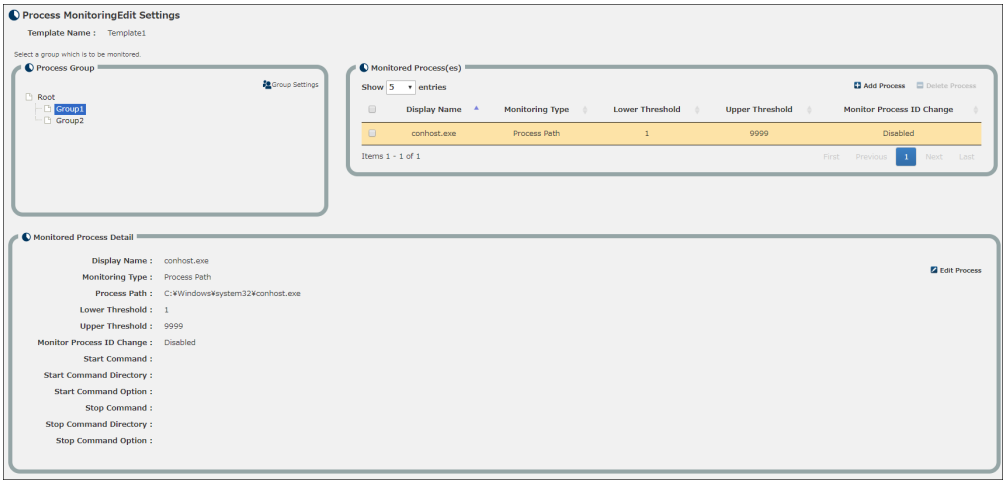

Figure 1-166 [Process Monitoring Settings] screen

Adding, changing, and deleting a group

The process group tree in the [Process Monitoring Settings] screen contains the [Group Settings] link.

Clicking this link displays the following menu, which lets you add, change, and delete groups.

Figure 1-167 Pop-up menu

If you select [Add Group] from the pop-up menu, the [Add Group] dialog box shown below is displayed. By using this dialog box, you can add a group directly below the root or below the selected group. You can organize groups into a hierarchy. If the selected group has any process registered in it, you cannot add a child group to that group.

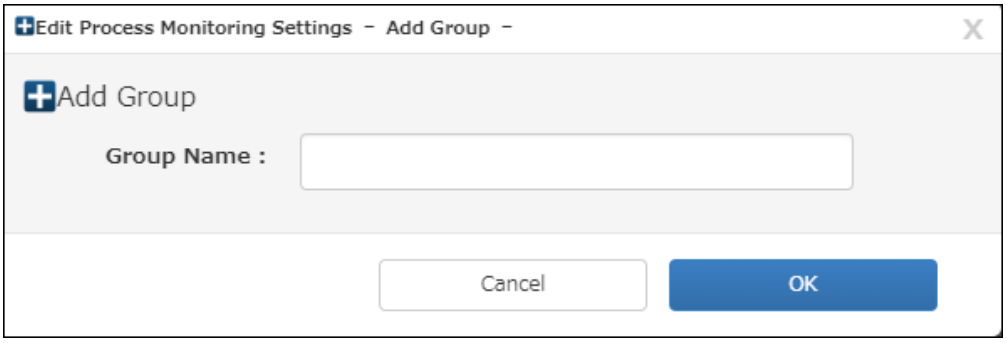

Figure 1-168 [Add Group] dialog box

Table 1-88 Item list ([Add Group] dialog box)

Item name	Description
Group name	Enter the name of the group to be added within 64 characters.
Cancel	Closes the dialog box without adding the group.
OK	Adds the group and then closes the dialog box.

If you select a group in the group tree and then [Edit Group] from the pop-up menu, the [Edit Group] dialog box shown below is displayed. By using this dialog box, you can rename the group selected in the tree.

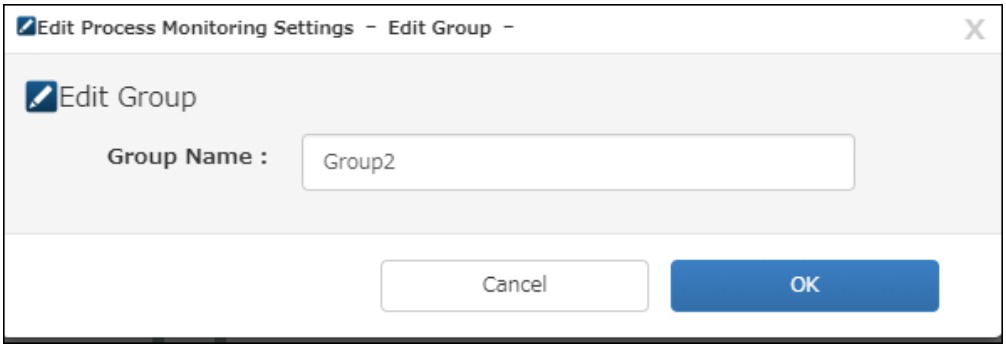

Figure 1-169 [Edit Group] dialog box

Table 1-89 Item list ([Edit Group] dialog box)

Item name	Description
Group name	Enter the name of the group to be changed within 64 characters.
Cancel	Closes the dialog box without changing the group.
OK	Changes the group and then closes the dialog box.

If you select a group in the group tree and then [Delete group] from the pop-up menu, the [Delete group] dialog box shown below is displayed. By using this dialog box, you can change the group selected in the tree. Once you delete a group, the groups and processes below the deleted group are deleted as well.

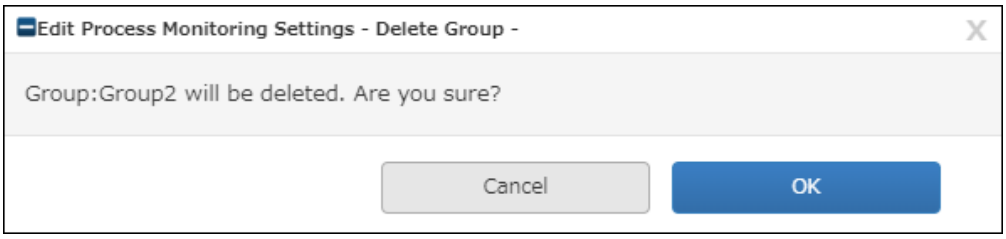

Figure 1-170 [Delete group] dialog box

Table 1-90 Item list ([Delete group] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the group.
OK	Deletes the group and then closes the dialog box.

Adding and deleting a process

[Process Monitoring] in the [Process Monitoring Settings] screen contains the [Add Process] link. Clicking this link displays the [Add Process(Form)] screen shown below, which lets you add processes to an process group.

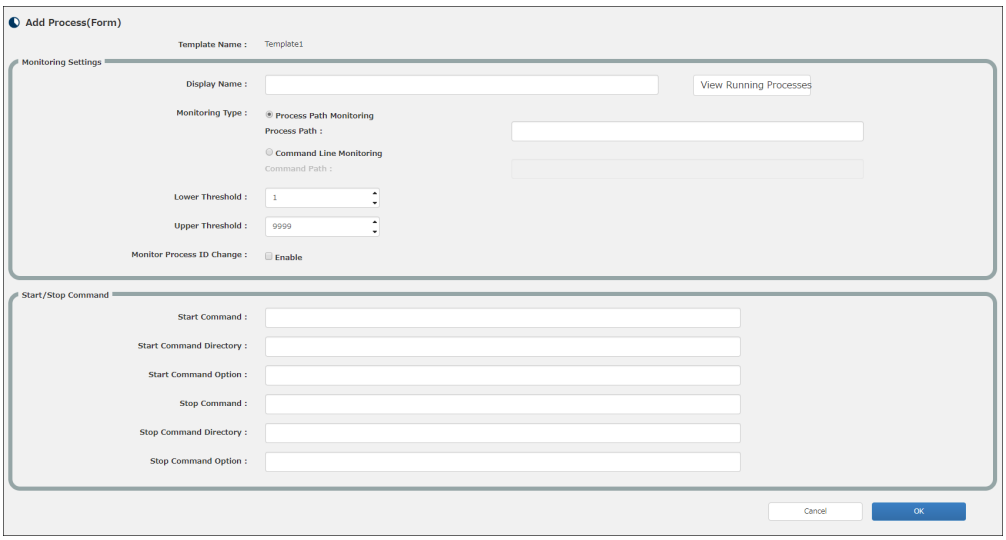

Figure 1-171 [Add Process(Form)] screen

Table 1-91 Item list ([Add Process(Form)] screen)

Item name	Description
Display name	Enter the display name of the process within 64 characters. Enter a process directly, or select one from the running process list.
View running processes	Displays the [Running Processes List] dialog box. The process monitoring setting of the [Monitoring template] screen does not display this item.
Monitoring type: Process path monitoring	To perform process path monitoring, select this item.
Monitoring type: Process path	If you select [Process path monitoring], specify the process path within 256 characters. Enter a process directly, or select one from the running process list.
Monitoring type: Command line monitoring	To perform command line monitoring, select this item.

Item name	Description
Monitoring type: Command path	If you select [Command line monitoring], specify the command line within 256 characters. Enter a process directly, or select one from the running process list.
Lower threshold	Specify the lower limit of the process count in the range of 1 to 9999. A value smaller than the upper limit of the process count must be specified.
Upper threshold	Specify the upper limit of the process count in the range of 1 to 9999. A value larger than the lower limit of the process count must be specified.
Monitor process ID change	Select this item to monitor not only whether the process exists but also for a change of the process ID.
Start command	Specify the command to start the process within 256 characters.
Start command directory	Specify the directory for executing the start command within 256 characters.
Start command option	Specify the option to be passed to the start command within 256 characters.
Stop command	Specify the command to stop the process within 256 characters.
Stop command directory	Specify the directory for executing the stop command within 256 characters.
Stop command option	Specify the option to be passed to the stop command within 256 characters.
Cancel	Returns you to the previous screen without adding the process.
OK	Adds the process and returns you to the previous screen.

Clicking the [View Running Processes] button in the [Add Process(Form)] screen displays the [Running Process List] dialog box. By selecting the process to be monitored from the [Running Process List] dialog box, you can have values automatically entered in some of the input fields of the [Add Process(Form)] screen.

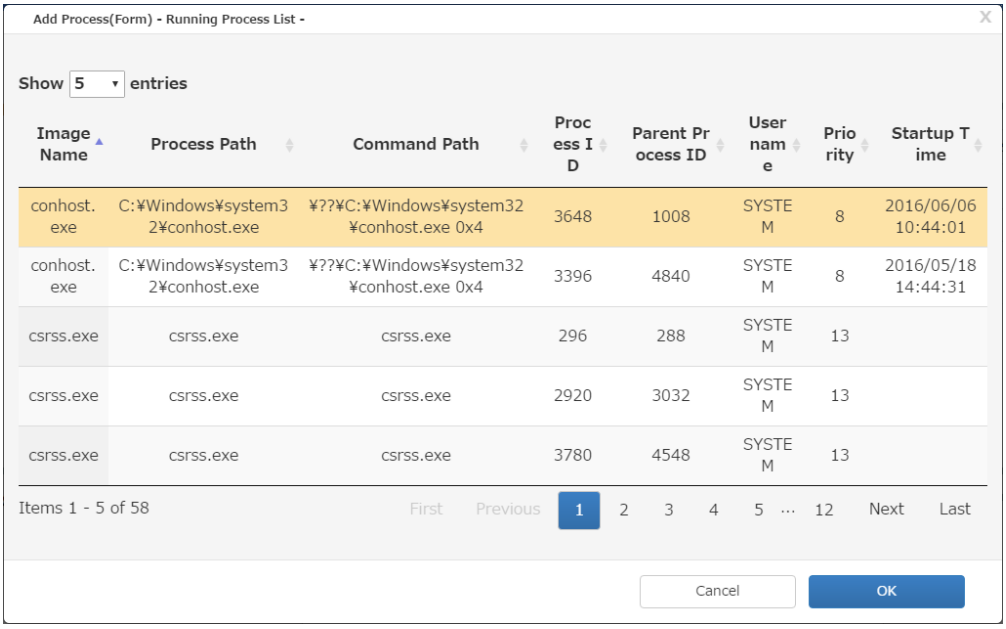

Figure 1-172 [Running Process List] dialog box

Table 1-92 Item list ([Start Process List] dialog box)

Item name	Description
Image name	Displays the image name of the process..
Process path	Displays the path of the process.
Command path	Displays the command line of the process.

Item name	Description
Process ID	Displays the process ID.
Parent process ID	Displays the parent process ID.
User name	Displays the name of the user who executes the process.
Priority	Displays the priority of the process.
Startup time	Displays the start time of the process.
Cancel	Closes the dialog box without selecting the process.
OK	Selects the process and then closes the dialog box.

[Process Monitoring] in the [Process Monitoring Settings] screen contains the [Delete Process] link. If you select the check box of the process you want to delete and click the [Delete Process] link, the [Delete Process] dialog box shown below is displayed, which lets you delete the process from the group.

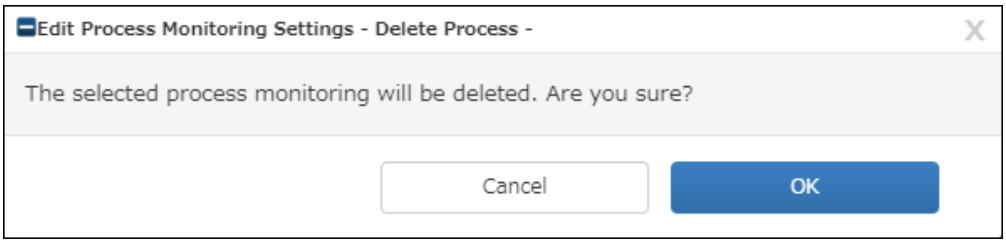

Figure 1-173 [Delete Process] dialog box

Table 1-93 Item list ([Delete Process] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the process.
OK	Deletes the process and then closes the dialog box.

Performance monitor

If you click [Performance Monitor] in the [Monitoring Settings] tab of the [Node Monitoring] screen or the monitoring template details of the [Monitoring template] screen, the [Performance Monitor] setting panel is displayed. The [Performance Monitor] setting panel lets you check the monitoring states of performance information.

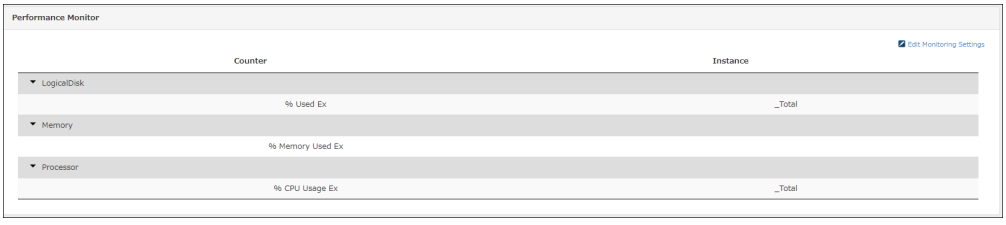

Figure 1-174 Performance monitor list

Table 1-94 Item list (Performance Monitor)

Item name	Description
Counter	Displays the item to be monitored.
Instance	Displays the instance to be monitored.

Clicking a counter displays the monitoring counter details shown below.

Figure 1-175 Monitoring counter details

Table 1-95 Item list (Monitoring Counter Details)

Item name	Description
Counter	Displays the item to be monitored.
Monitor type	One of the following is displayed. • Sequential • Continuous • Average
Number of times	This is displayed only when [Continuous] or [Average] is selected. When [Continuous] is selected, the count indicates how many times the threshold value is allowed to be exceeded before a change is reported. When [Average] is selected, it indicates how many sets of previous performance information are used to calculate the average value.
Upper error monitor	Displays the upper limit error threshold value. This item is blank when upper limit error monitoring is not performed.
Upper warning monitor	Displays the upper limit warning threshold value. This item is blank when upper limit warning monitoring is not performed.
Lower error monitor	Displays the lower limit error threshold value. This item is blank when lower limit error monitoring is not performed.
Lower warning monitor	Displays the lower limit warning threshold value. This item is blank when lower limit warning monitoring is not performed.

Changing the performance monitor setting

If you click the [Edit Monitoring Settings] link in the [Performance Monitor] panel, the [Performance Monitor Settings] screen is displayed. The [Performance Monitor Settings] screen displays the [Performance Monitor] panel, performance counter list, and performance counter details.

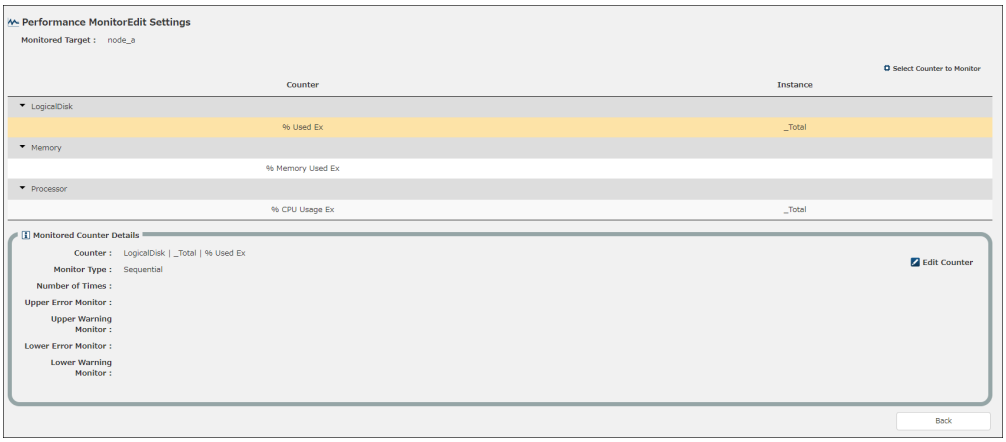

Figure 1-176 [Performance Monitor Settings] screen

Clicking [Select Counter to Monitor] in the performance monitoring setting of the [Node Monitoring] screen displays the [Select Counter to Monitor] screen shown below, which lets you select a resource, instance, and counter and add a counter to be monitored.

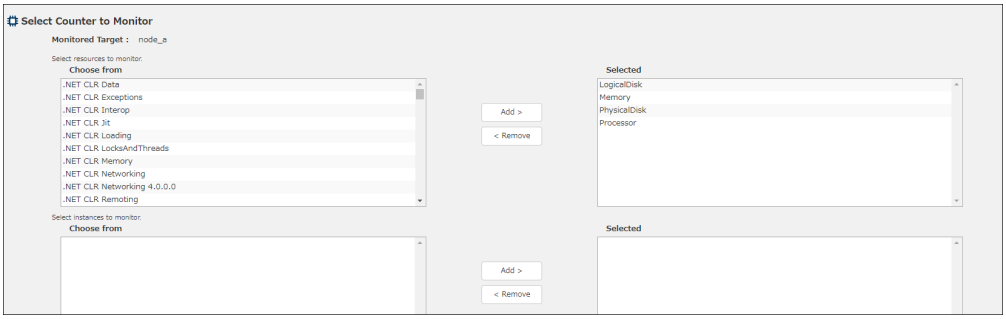

Figure 1-177 [Select Counter to Monitor] screen

In the performance monitoring setting of the [Monitoring template] screen, the performance counter list displays the following links.

- Add Monitored Counter
- Edit Monitored Counter
- Delete Monitored Counter

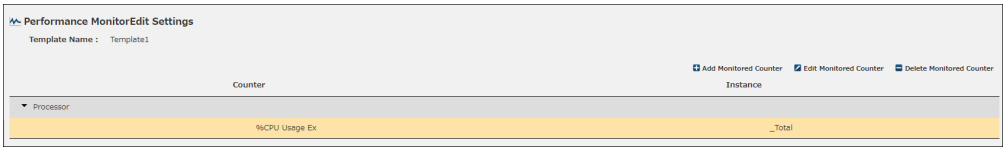

Figure 1-178 [Performance Monitor Settings] screen (Monitoring template)

Clicking [Add Monitored Counter] displays the [Add Monitored Counter] dialog box shown below, which lets you add an entered monitoring counter.

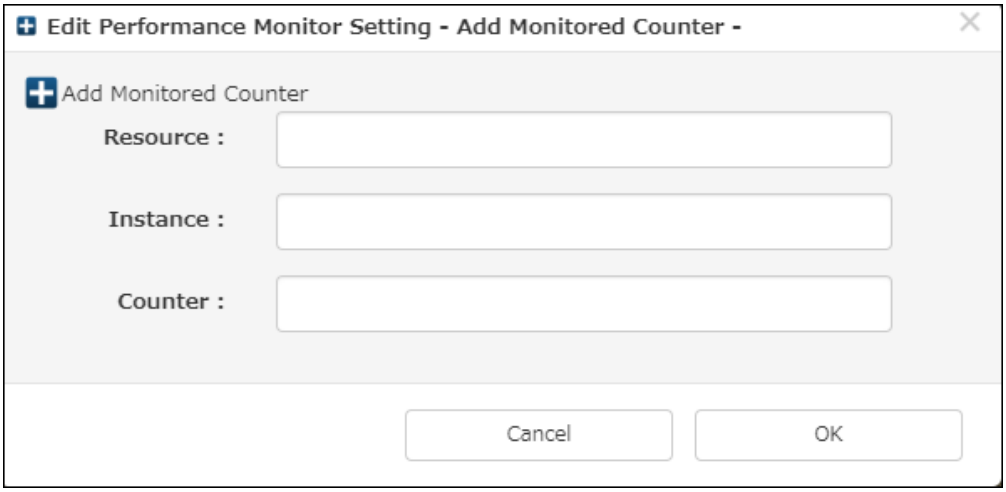

Figure 1-179 [Add Monitored Counter] dialog box

Table 1-96 Item list ([Add Monitored Counter] dialog box)

Item name	Required	Description
Resource	Y	Enter the resource of the monitoring counter within 128 characters.
Instance		Enter the instance of the monitoring counter within 128 characters.
Counter	Y	Enter the counter of the monitoring counter within 128 characters.

If you select the monitoring counter you want to change and click [Edit Monitored Counter], the [Edit Monitored Counter] dialog box shown below is displayed, which lets you change the monitoring counter.

The items of the [Edit Monitored Counter] dialog box are the same as those of the [Add Monitored Counter] dialog box.

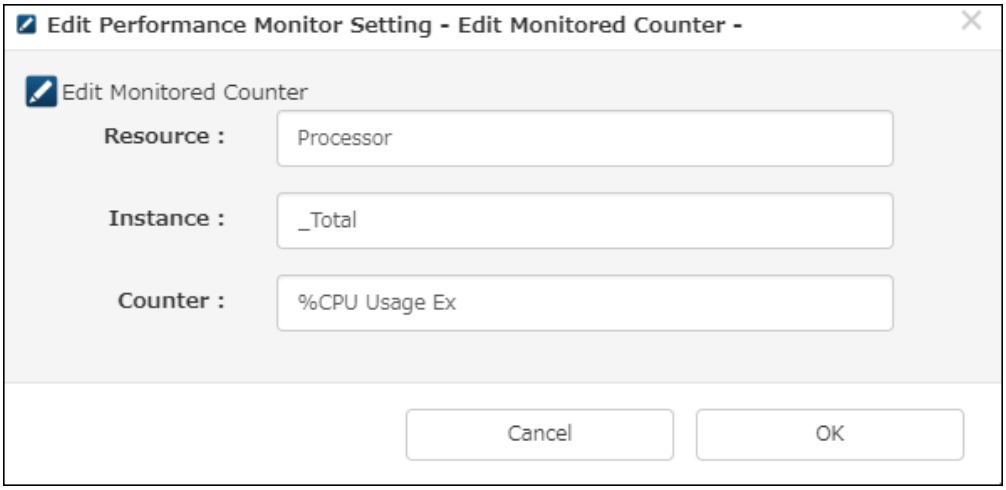

Figure 1-180 [Edit Monitored Counter] dialog box

If you select the monitoring counter you want to delete and click [Delete Monitored Counter], the [Delete Monitored Counter] dialog box shown below is displayed, which lets you delete the monitoring counter.

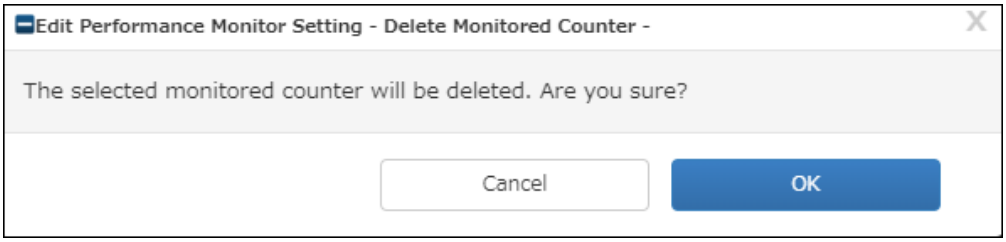

Figure 1-181 [Delete Monitored Counter] dialog box

Clicking the [Edit Counter] link in the monitoring counter details displays the [Edit Monitored Counter(Form)] screen shown below, which lets you change the monitoring setting of the counter.

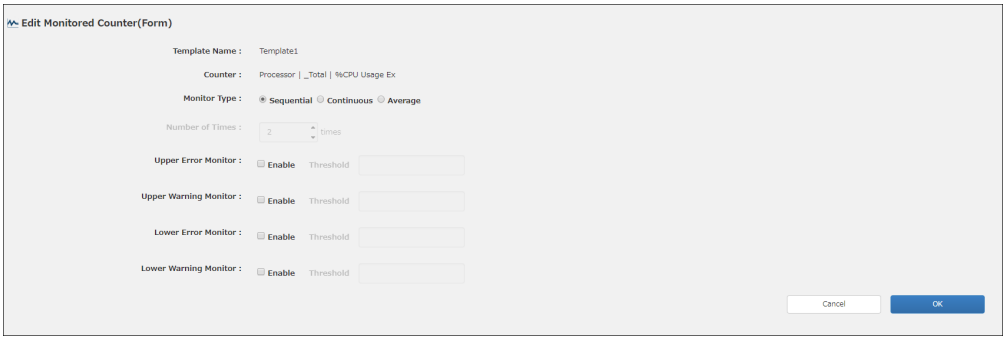

Figure 1-182 [Edit Monitored Counter(Form)] screen

Table 1-97 Item list ([Edit Monitored Counter(Form)] screen)

Item name	Description
Counter	Displays the counter name.
Monitor Type	Select one of the following.

Item name	Description
	• Sequential: A state change is reported every time the acquired performance information exceeds (matches) the threshold value. • Continuous: A state change is reported if the acquired performance information has exceeded (matched) the threshold value multiple consecutive times. To specify how many times the threshold value is allowed to be exceeded before a change is reported, use [Judgment count]. • Average: A state change is reported if the average of the acquired performance information exceeds (matches) the threshold value. The average value is calculated by using the multiple sets of previous performance information specified in [Judgment count], starting from the most recently acquired information.
Number of times	This is displayed only when [Continuous] or [Average] is selected. When [Continuous] is selected, the count indicates how many times the threshold value is allowed to be exceeded before a change is reported. When [Average] is selected, it indicates how many sets of previous performance information are used to calculate the average value. The specifiable value range is 2 to 16.
Upper error monitor	To enable upper limit error monitoring, select the check box and specify the threshold value. The specifiable value range is -99999999999999 to 999999999999999.
Upper warning monitor	To enable upper limit warning monitoring, select the check box and specify the threshold value. The specifiable value range is -99999999999999 to 999999999999999.
Lower error monitor	To enable lower limit error monitoring, select the check box and specify the threshold value. The specifiable value range is -99999999999999 to 999999999999999.
Lower warning monitor	To enable lower limit warning monitoring, select the check box and specify the threshold value. The specifiable value range is -99999999999999 to 999999999999999.
Cancel	Discards the entered data and returns you to the previous screen.
OK	Applies the entered data and returns you to the previous screen.

Service port monitoring

If you click [Service Port Monitoring] in the [Monitoring Settings] tab of the [Node Monitoring] screen or the monitoring template details of the [Monitoring template] screen, the [Service Port Monitoring] setting panel is displayed. The [Service Port Monitoring] setting panel lets you check the monitoring states of service ports.

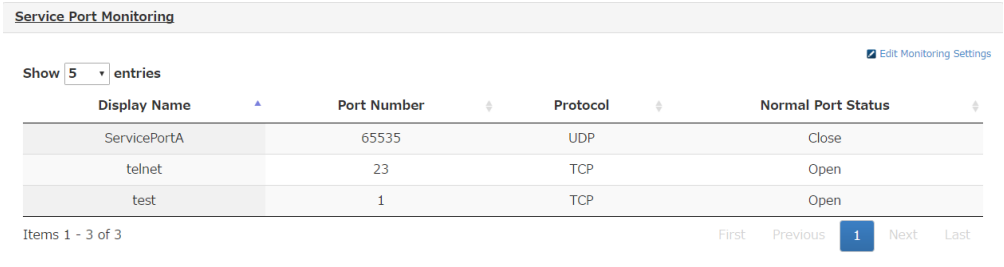

Figure 1-183 Service port monitoring

Table 1-98 Item list (Service Port Monitoring)

Item name	Description
Display name	Displays the display name of the service port.
Port number	Displays the port number of the service port.
Protocol	Either of the following is displayed. • TCP • UDP
Normal port status	Either of the following is displayed. • Open • Close

Selecting a service port from the list in [Service Port Monitoring] displays [Service Port Monitoring Detail Settings] shown below.

Figure 1-184 Service port details

Table 1-99 Item list (Service Port Details)

Item name	Description
Display name	Displays the display name of the service port.
Port number	Displays the port number of the service port.
Protocol	Either of the following is displayed. • TCP • UDP
Normal port status	Either of the following is displayed. • Open • Close
Interval	Displays the port monitoring interval (seconds).
Connect timeout	Displays the time (seconds) allowed to elapse before a connection timeout is detected.
Retry count	Displays the number of retries to be made at a connection timeout.
Monitoring address	Displays the address to be monitored. Either an IP address (IPv4/IPv6) or localhost is displayed.

Changing the service port monitoring setting

If you click the [Edit Monitoring Settings] link in the [Service Port Monitoring] panel, the [Service Port Monitoring Settings Change] screen is displayed.

The [Service Port Monitoring Settings Change] screen displays a service port list and [Service Port Monitoring Detail Settings] as in the [Service Port Monitoring] panel.

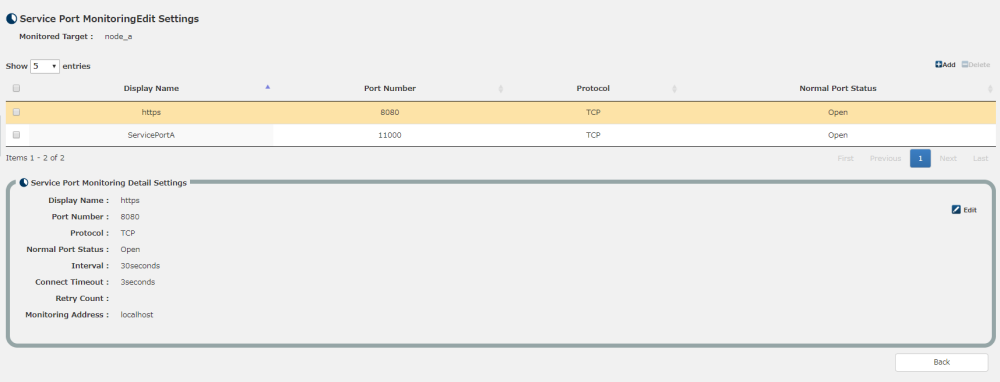

Figure 1-185 [Service Port Monitoring Settings] screen

Table 1-100 Item list ([Edit Service Port Monitoring Settings] screen)

Item name	Description
Add	Displays the [Add Service Port (Form)] screen.
Delete	Displays the [Delete Service Port Monitoring Settings] dialog box.
Edit	Displays the [Edit Service Port (Form)] screen.
Back	Returns you to the previous screen.

Adding, changing, and deleting a service port

Clicking the [Add] link in the [Service Port Monitoring Settings] screen displays the [Add Service Port(Form)] screen shown below, which lets you add a service port monitoring setting.

Figure 1-186 [Add Service Port(Form)] screen

Table 1-101 Item list ([Add Service Port(Form)] screen)

Item name	Description
Display name	Enter the display name of the service port within 64 characters.
Port number	Enter the port number of the service port in the range of 1 to 65535.
Protocol	Either of the following is displayed. • TCP • UDP
Normal port status	Either of the following is displayed. • Open • Close
Interval (seconds)	Specify the port monitoring interval (seconds) in the range of 10 to 86400.

Item name	Description
Connect timeout (seconds)	Specify the time (seconds) allowed to elapse before a connection timeout is detected in the range of 1 to 60.
Retry count	Specify the number of retries to be made at a connection timeout in the range of 0 to 10. Required only when the protocol is UDP.
Monitoring address	When [Enable] is selected, specify whether to use an IP address (IPv4/IPv6) or localhost as the monitoring target address. If you do not specify this item, localhost is assumed.
Cancel	Returns you to the previous screen without adding the service.
OK	Adds the service port and returns you to the previous screen.

Clicking the [Edit] link in the [Service Port Monitoring Settings] screen displays the [Edit Service Port(Form)] screen shown below, which lets you change a service port monitoring setting.

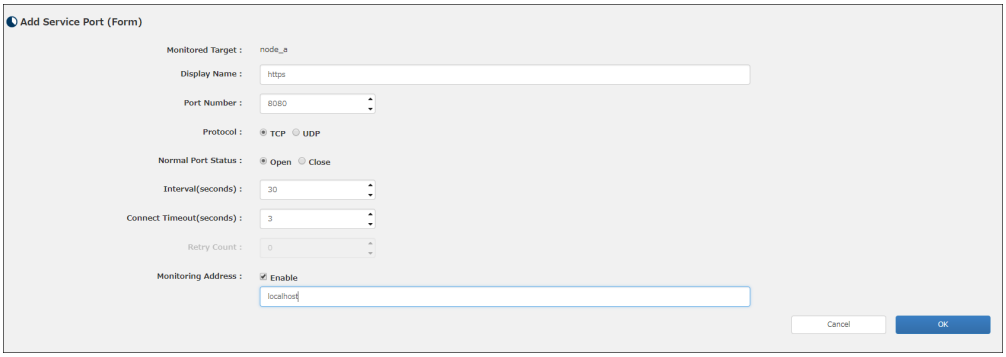

Figure 1-187 [Edit Service Port(Form)] screen

The input items are the same as those of the [Add Service Port(Form)] screen.

Clicking the [Delete] link in the [Service Port Monitoring Settings] screen displays the [Delete Service Port Monitoring Settings] dialog box shown below, which lets you delete a selected service port monitoring setting.

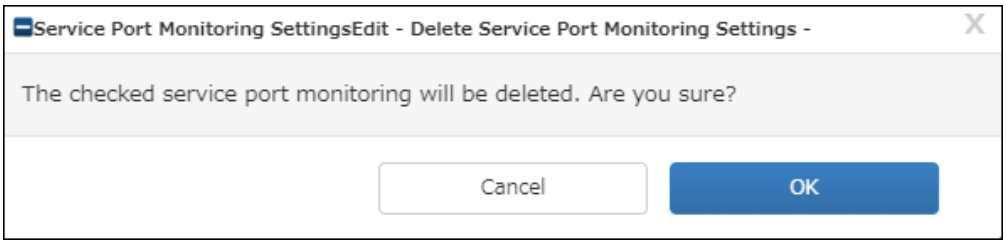

Figure 1-188 [Delete Service Port Monitoring Settings] dialog box

Table 1-102 Item list ([Delete Service Port Monitoring Settings] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the service port.
OK	Deletes the service port and then closes the dialog box.

Event log monitoring

If you click [Event Log Monitoring] in the [Monitoring Settings] tab of the [Node Monitoring] screen or the monitoring template details of the [Monitoring template] screen, the [Event Log Monitoring] setting panel is displayed. The [Event Log Monitoring] setting panel lets you check the monitoring states of event logs.

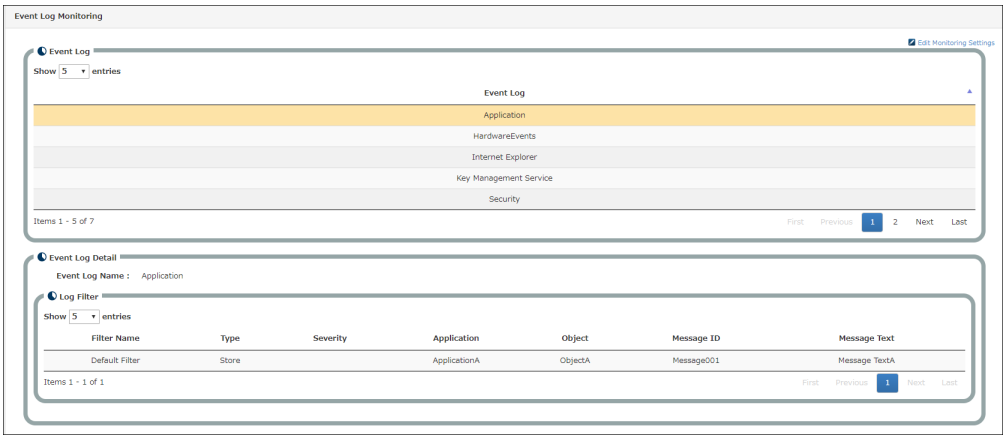

Figure 1-189 Event log monitoring

If you select an event log in the event log list, [Event Log Detail] is displayed below. [Event Log Detail] contains the following items.

Table 1-103 Item list (Event Log Details)

Item name	Description
Event log name	Displays the name of the event log.
Log filter	Displays the list of log filters.

Table 1-104 Item list (Log Filter)

Item name	Description
Filter name	Displays the log filter name.
Type	Displays one of the following filter types. • Store • Ignore When [Store] is selected, a message is reported for a log matching this filter. When [Ignore] is selected, no message is reported for a log matching this filter, and the filtering processing of the subsequent filters is not performed.
Severity	Displays the filter condition for the event log type.
Application	Displays the filter condition for the event log source.
Object	Displays the filter condition for the task category or classification in the event log.
Message ID	Displays the filter condition for the event ID of the event log.
Message text	Displays the filter condition for the message text.

Changing the event log monitoring setting

If you click the [Edit Monitoring Settings] link in the [Event Log Monitoring] panel, the [Event Log Monitoring Settings] screen is displayed. The [Event Log Monitoring Settings] screen displays an event log list and event log details as in the [Event Log Monitoring] panel.

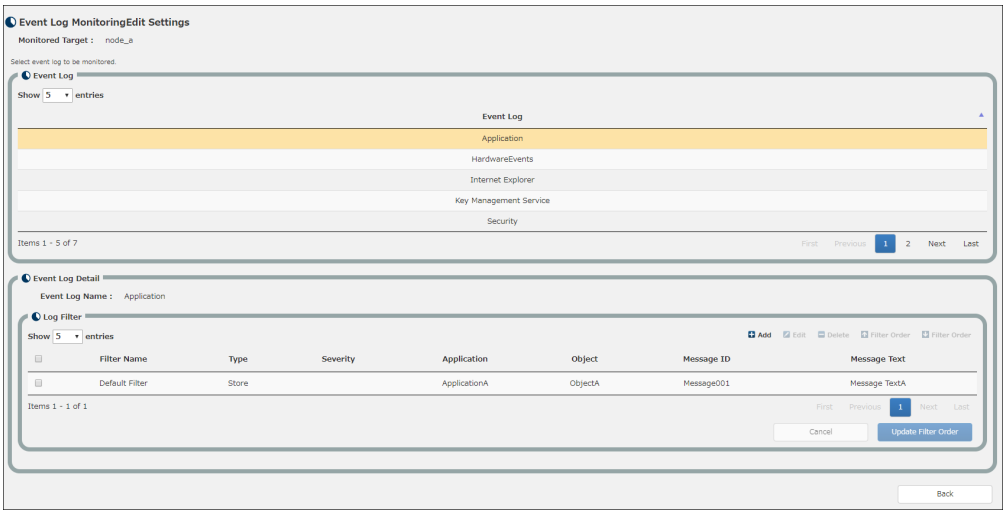

Figure 1-190 [Event Log Monitoring Settings] screen

The event log monitoring setting of the [Monitoring template] screen displays the following links.

- Add Event Log
- Edit Event Log
- Delete Event Log

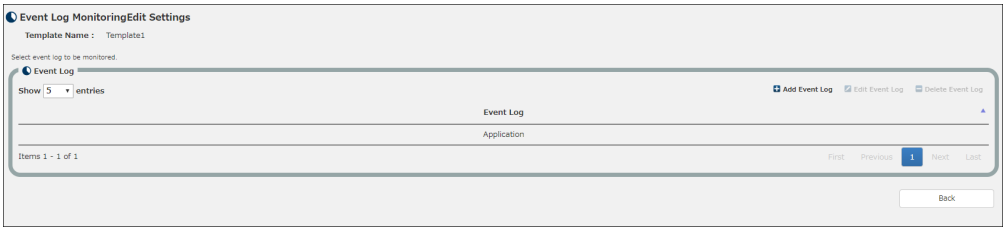

Figure 1-191 [Event Log Monitoring Settings] screen (Monitoring template)

Clicking [Add Event Log] displays the [Add Event Log] dialog box shown below, which lets you add an entered event log.

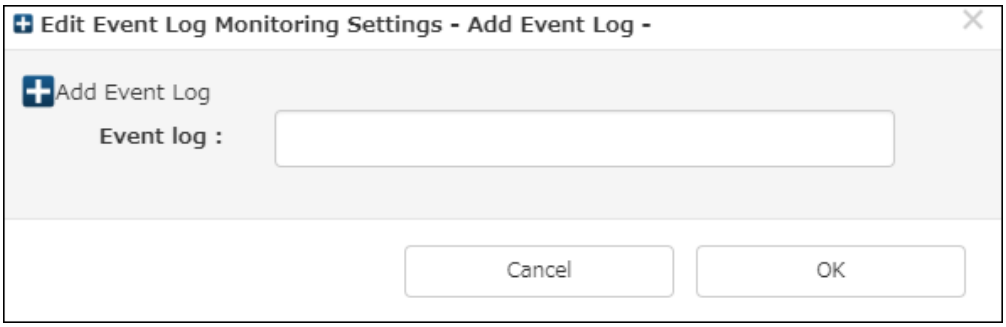

Figure 1-192 [Add Event Log] dialog box

Table 1-105 Item list ([Add Event Log] dialog box)

Item name	Required	Description
Event log	Y	Enter an event log within 64 characters.

If you select the event log you want to change and click [Edit Event Log], the [Edit Event Log] dialog box shown below is displayed, which lets you change the event log.

The items of the [Edit Event Log] dialog box are the same as those of the [Add Event Log] dialog box.

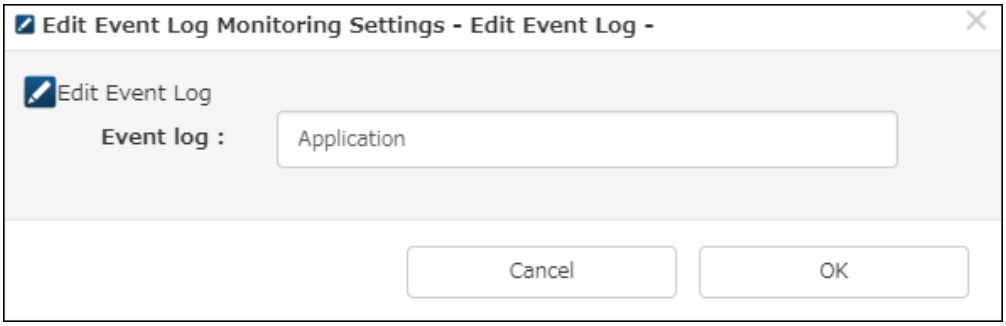

Figure 1-193 [Edit Event Log] dialog box

If you select the event log you want to delete and click [Delete Event Log], the [Delete Event Log] dialog box shown below is displayed, which lets you delete the event log.

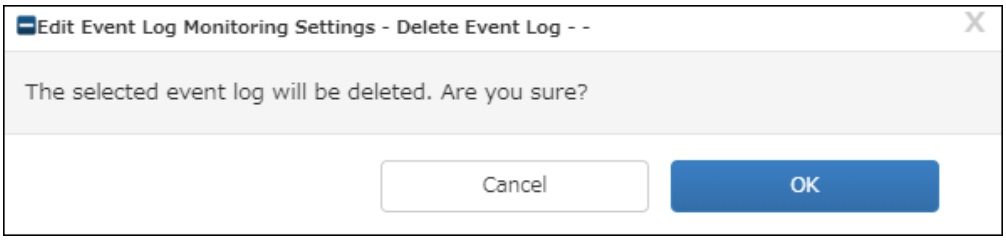

Figure 1-194 [Delete Event Log] dialog box

Adding, changing, and deleting a log filter

The [Log Filter] section in the [Event Log Monitoring Settings] screen contains the [Add] link. Clicking the [Add] link displays the [Add Log Filter(Form)] screen shown below. By using this screen, you can add a filter definition.

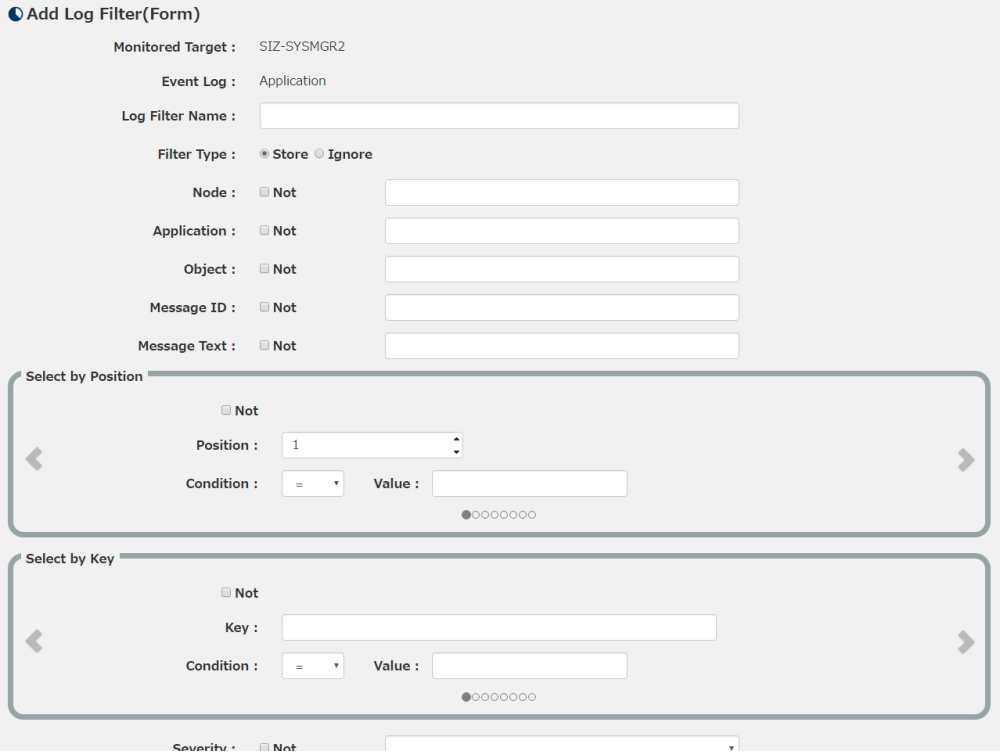

Figure 1-195 [Add Log Filter (Form)] screen

Table 1-106 Item list ([Add Log Filter(Form)] screen)

Item name	Description
Log filter name	Enter the log filter name within 256 characters.
Filter type	Displays one of the following filter types. • Store • Ignore When [Store] is selected, a message is reported for a log matching this filter. When [Ignore] is selected, no message is reported for a log matching this filter, and the filtering processing of the subsequent filters is not performed.
Node	Specify the filter condition to the node name within 256 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.
Application	Specify the item corresponding to the event log source as the filter condition, within 128 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.
Object	Specify the item corresponding to the task category or classification in the event log as the filter condition, within 128 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.
Message ID	Specify the item corresponding to the event ID of the event log as the filter condition, within 128 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.
Message text	Specify the message text within 1024 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.
Select by position	Specify the position specification information.
Select by key	Specify the key information.

Item name	Description
Severity	Select a search condition for an item corresponding to the item of event log type. If a negative condition is specified, messages that do not match the selected condition are targeted.
Display setting	Specify the definition related to the message display.
Option setting	Specify the option definition of the filter.
Cancel	Discards the setting and returns you to the previous screen.
OK	Applies the setting and returns you to the previous screen.

[Select by Position] specifies up to 8 search conditions using the position specification in the message text. If a negative condition is specified, messages that do not match the condition are selected.

Figure 1-196 [Add Log Filter (Form)] screen - Select by Position

Table 1-107 Item list ([Add Log Filter(Form)] screen - Select by Position)

Item name	Description
Not	If this is selected, messages that do not match the condition are selected.
Position	Specify the position in the message text.
Condition	Select from =, <>, >=, >, <=, and <.
Value	Specify the value to compare within 64 characters. No regular expression can be specified.

[Select by Key] specifies up to 8 search conditions using the key specification in the log content. If a negative condition is specified, messages that do not match the condition are selected.

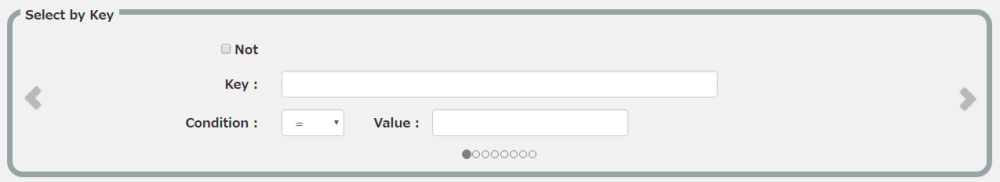

Figure 1-197 [Add Log Filter (Form)] screen - Select by Key

Table 1-108 Item list ([Add Log Filter(Form)] screen - Select by Key)

Item name	Description
Not	If this is selected, messages that do not match the condition are selected.
Key	Specify the key in the log content within 64 characters.
Condition	Select from =, <>, >=, >, <=, and <.
Value	Specify the value to compare. When [=] is specified for [Condition], specify [Comparison value] using a regular expression.

Define the information to add when reporting a message for the extracted log.

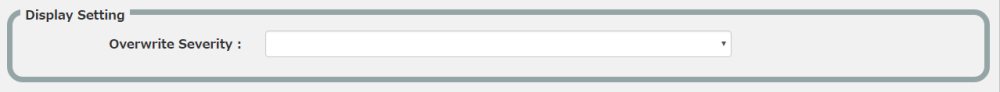

Figure 1-198 [Add Log Filter (Form)] screen - Display Setting

Table 1-109 Item list ([Add Log Filter(Form)] screen - Display Setting)

Item name	Description
Overwrite Severity	Changes the severity of the message matching the filter condition to the specified severity.

In [Option Setting], define extended settings for extracted logs.

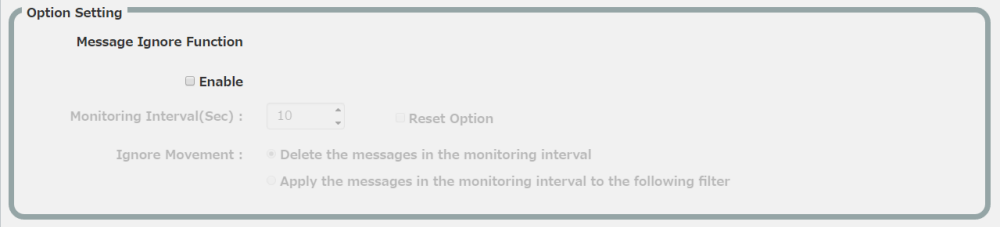

Figure 1-199 [Add Log Filter (Form)] screen - Option Setting

Table 1-110 Item list ([Add Log Filter(Form)] screen - Option Setting)

Item name	Description
Enable	Select this to use the message suppression function.
Monitoring interval (sec)	Specify the period during which no message is reported from the first extracted log in the range of 1 to 3600 seconds. When a log is extracted after this interval, a message is reported and the no-reporting period starts again.
Reset Option	Select this item to reset the monitoring interval when message reporting is suppressed by extracting logs within the no-reporting period. Use it to keep extracted logs suppressed continuously.
Ignore movement	Specify the behavior of message suppression. [Delete the messages in the monitoring interval] When multiple logs that match the filter are detected during the monitoring interval, a message is output for the first detected log and the subsequent logs are deleted without being reported. The logs that match the filter during the monitoring interval are disabled even if a filter whose priority is lower than this filter is set. [Apply the messages in the monitoring interval to the following filter]When multiple logs that match the filter are detected during the monitoring interval, a message is output for the first detected log and the filter is disabled for the subsequent logs. If a filter whose priority is lower than the filter exists, the logs that match the filter during the monitoring interval are sequentially checked for this filter and a message is output when they match.

The [Log Filter] section in the [Event Log Monitoring Settings] screen contains the [Edit] link. If you select the filter you want to change and click the [Edit] link, the [Edit Log Filter(Form)] screen shown below is displayed. By using this screen, you can change the filter definition.

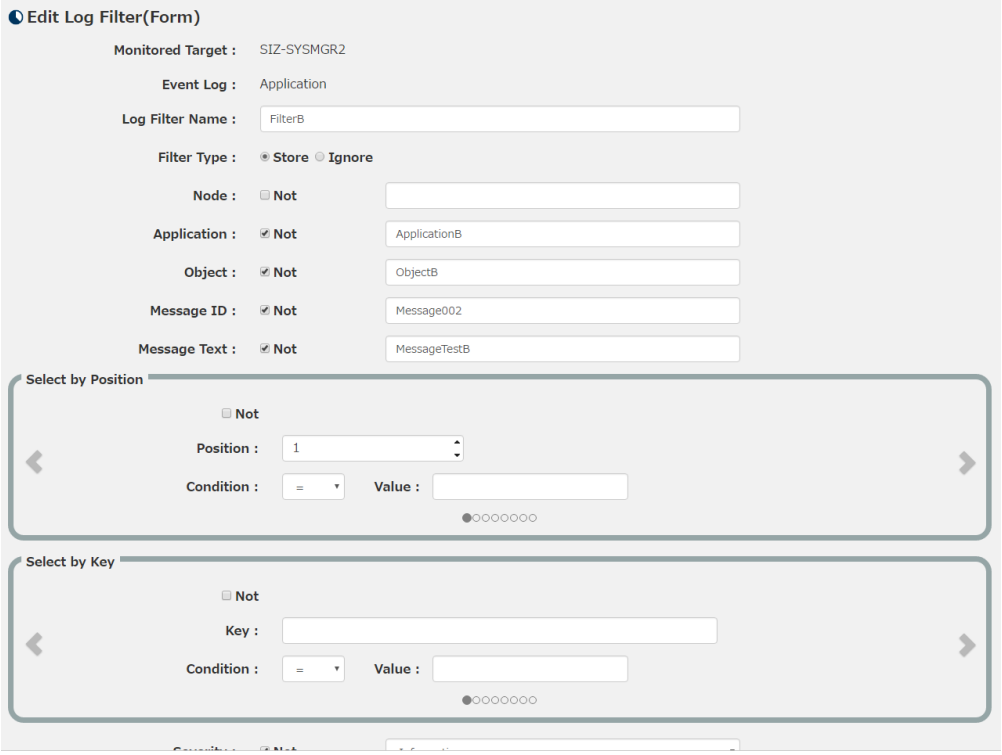

Figure 1-200 [Edit Log Filter (Form)] screen

The input items are the same as those of the [Add Log Filter(Form)] screen. The [Log Filter] section in the [Event Log Monitoring Settings] screen contains the [Delete] link. If you select the filter you want to delete and click the [Delete] link, the [Delete Log Filter] dialog box shown below is displayed. By using this dialog box, you can delete the filter definition.

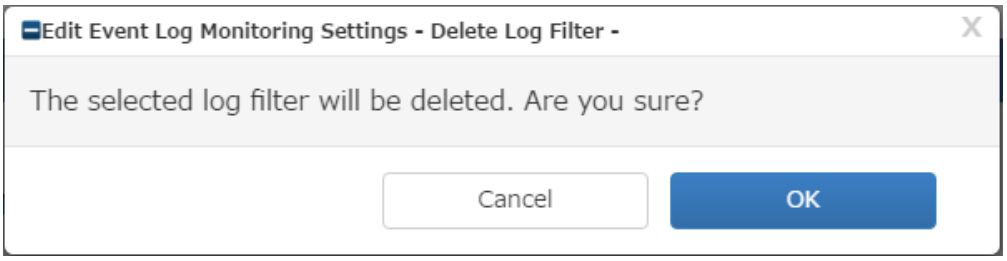

Figure 1-201 [Delete Filter] dialog box

Table 1-111 Item list ([Delete Log Filter] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the filter.
OK	Deletes the filter and then closes the dialog box.

Changing the order of log filters

The [Log Filter] section in the [Event Log Monitoring Settings] screen contains the [Edit Order] link. Clicking the [Edit Order] link moves the selected log up and down in the order.

System log monitoring

If you click [System Log Monitoring] in the [Monitoring Settings] tab of the [Node Monitoring] screen or the monitoring template details of the [Monitoring template] screen, the [System Log

Monitoring] setting panel is displayed. The [System Log Monitoring] setting panel lets you check the monitoring states of system logs.

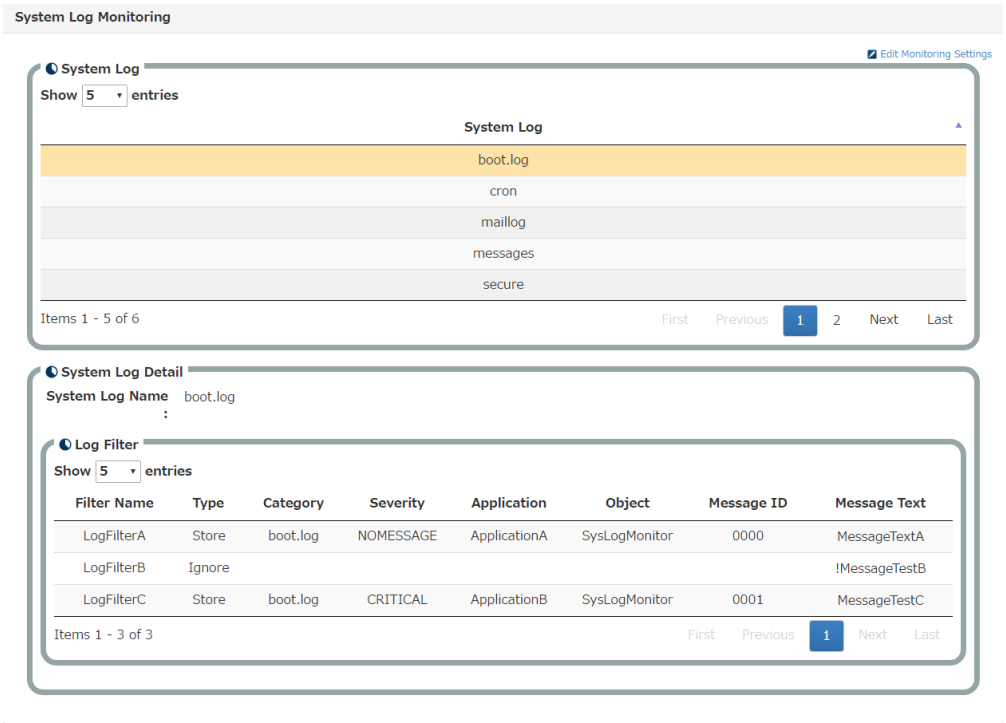

Figure 1-202 System log monitoring

If you select a system log in the system log list, [System Log Detail] is displayed below. [System Log Detail] contains the following items.

Table 1-112 Item list (System Log Details)

Item name	Description
System log name	Displays the name of the system log.
Log filter	Displays the list of log filters.

Table 1-113 Item list (Log Filter)

Item name	Description
Filter name	Displays the log filter name.
Type	Displays one of the following filter types. • Store • Ignore When [Store] is selected, a message is reported for a log matching this filter. When [Ignore] is selected, no message is reported for a log matching this filter, and the filtering processing of the subsequent filters is not performed.
Category	Displays the category of the system log.
Severity	Displays the severity assigned when the log is reported as a message.
Application	Displays the application name assigned when the log is reported as a message.
Object	Displays the object name assigned when the log is reported as a message.
Message ID	Displays the message ID assigned when the log is reported as a message.
Message text	Displays the filter condition for the message text.

Changing the system log monitoring setting

If you click the [Edit Monitoring Settings] link in the [System Log Monitoring] panel, the [System Log Monitoring Settings] screen is displayed. The [System Log Monitoring Settings] screen displays a system log list and system log details as in the [System Log Monitoring] panel.

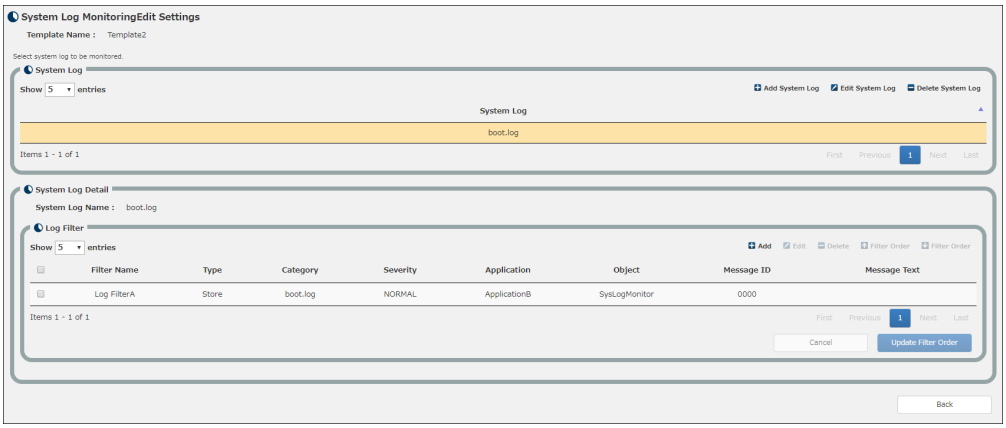

Figure 1-203 [System Log Monitoring Settings] screen

The monitoring setting of the [Monitoring template] screen displays the following links.

- Add System Log
- Edit System Log
- Delete System Log

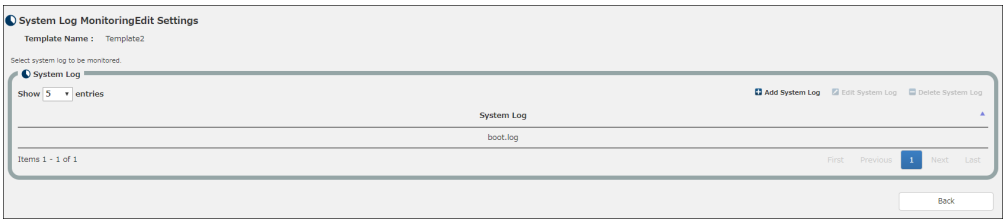

Figure 1-204 [System Log Monitoring Settings] screen (Monitoring template)

Clicking [Add System Log] displays the [Add System Log] dialog box shown below, which lets you add an entered system log.

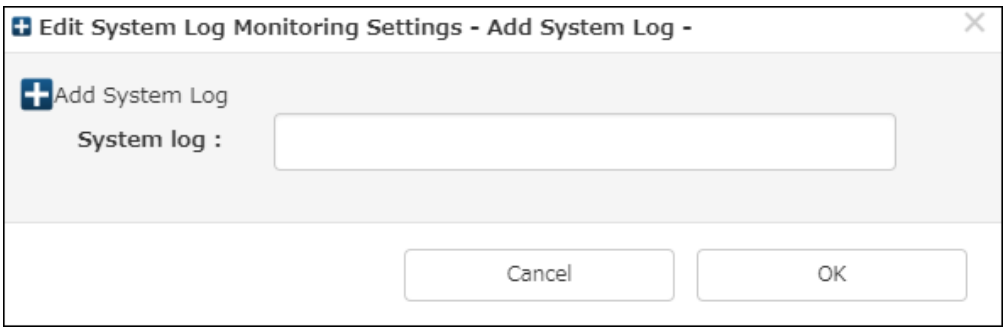

Figure 1-205 [Add System Log] dialog box

Table 1-114 Item list ([Add System Log] dialog box)

Item name	Required	Description
System log	Y	Enter a system log within 256 characters.

If you select the system log you want to change and click [Edit System Log], the [Edit System Log] dialog box shown below is displayed, which lets you change the system log.

The items of the [Edit System Log] dialog box are the same as those of the [Add System Log] dialog box.

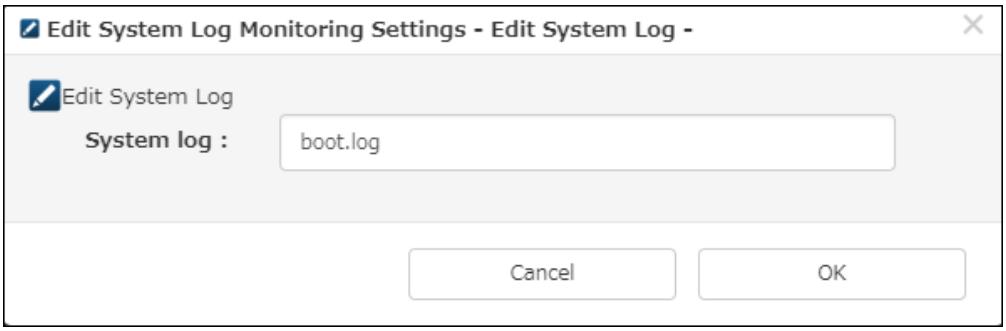

Figure 1-206 [Edit System Log] dialog box

If you select the system log you want to delete and click [Delete System Log], the [Delete System Log] dialog box shown below is displayed, which lets you delete the system log.

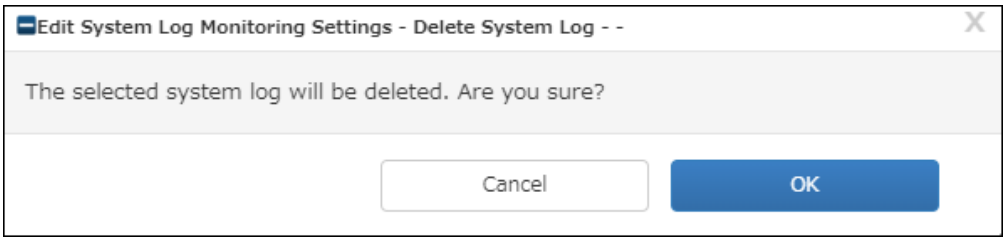

Figure 1-207 [Delete System Log] dialog box

Adding, changing, and deleting a log filter

The [Log Filter] section in the [Event Log Monitoring Settings] screen contains the [Add] link. Clicking the [Add] link displays the [Add Log Filter(Form)] screen shown below. By using this screen, you can add a filter definition.

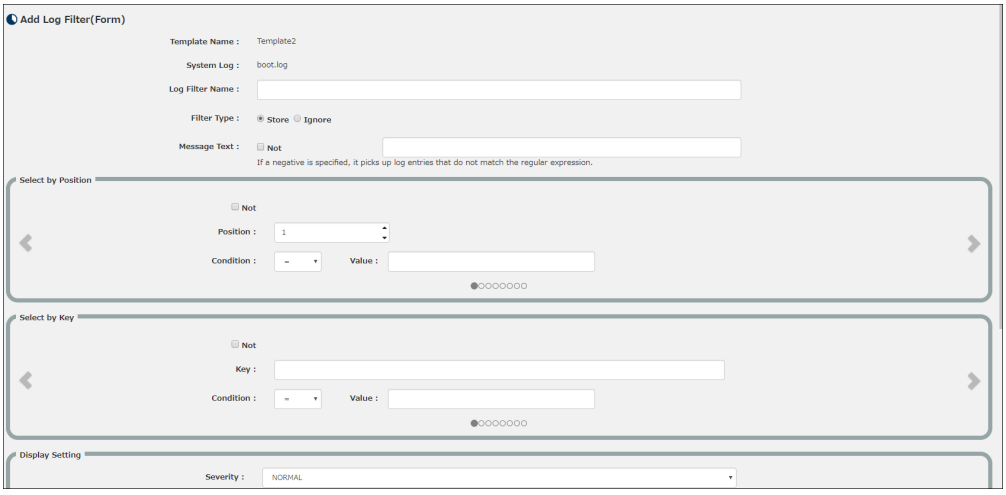

Figure 1-208 [Add Log Filter (Form)] screen

Table 1-115 Item list ([Add Log Filter(Form)] screen)

Item name	Description
Log filter name	Displays the log filter name.

Item name	Description
Filter type	Displays one of the following filter types. • Store • Ignore When [Store] is selected, a message is reported for a log matching this filter. When [Ignore] is selected, no message is reported for a log matching this filter, and the filtering processing of the subsequent filters is not performed.
Message text	Specify the message text within 1024 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.
Select by position	Specify the position specification information.
Select by key	Specify the key information.
Display setting	Specify the definition related to the message display.
Option setting	Specify the option definition of the filter.
Cancel	Discards the setting and returns you to the previous screen.
OK	Applies the setting and returns you to the previous screen.

[Select by Position] specifies up to 8 search conditions using the position specification in the message text. If a negative condition is specified, messages that do not match the condition are selected.

Figure 1-209 [Add Log Filter (Form)] screen - Select by Position

Table 1-116 Item list ([Add Log Filter(Form)] screen - Select by Position)

Item name	Description
Not	If this is selected, messages that do not match the condition are selected.
Position	Specify the position in the message text.
Condition	Select from =, <>, >=, >, <=, and <.
Value	Specify the value to compare within 64 characters. No regular expression can be specified.

[Select by Key] specifies up to 8 search conditions using the key specification in the log content. If a negative condition is specified, messages that do not match the condition are selected.

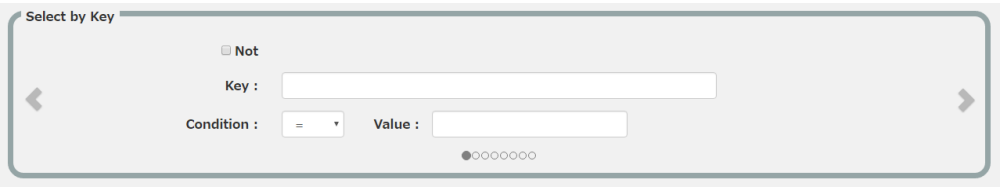

Figure 1-210 [Add Log Filter (Form)] screen - Select by Key

Table 1-117 Item list ([Add Log Filter(Form)] screen - Select by Key)

Item name	Description
Not	If this is selected, messages that do not match the condition are selected.
Key	Specify the key in the log content within 64 characters.
Condition	Select from =, <>, >=, >, <=, and <.
Value	Specify the value to compare. When [=] is specified for [Condition], specify [Comparison value] using a regular expression.

Define the information to add when reporting a message for the extracted log.

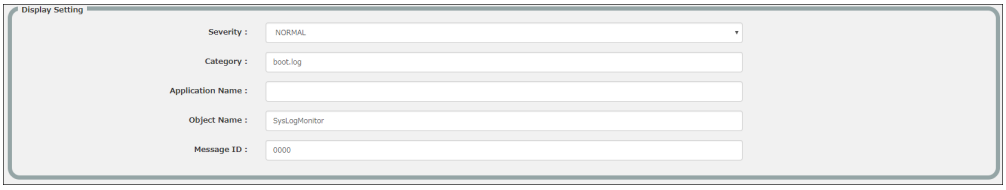

Figure 1-211 [Add Log Filter (Form)] screen - Display Setting

Table 1-118 Item list ([Add Log Filter(Form)] screen - Display Setting)

Item name	Description
Overwrite Severity	Select the severity to be assigned when the log is reported as a message.
Category	Specify the information about the category assigned when the log is reported as a message within 32 characters, or select a category from the monitored system log names.
Application name	Specify the information about the application assigned when the log is reported as a message within 32 characters.
Object name	Specify the information about the object assigned when the log is reported as a message within 32 characters.
Message ID	Specify the message ID assigned when the log is reported as a message within 32 characters.

In [Option Setting], define extended settings for extracted logs.

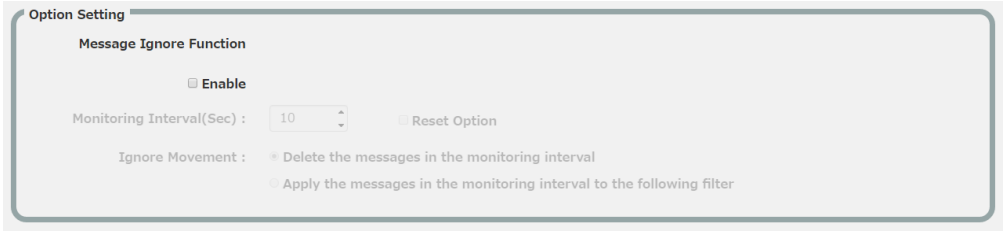

Figure 1-212 [Add Log Filter (Form)] screen - Option Setting

Table 1-119 Item list ([Add Log Filter(Form)] screen - Option Setting)

Item name	Description
Enable	Select this to use the message suppression function.
Interval (seconds)	Specify the period during which no message is reported from the first extracted log in the range of 1 to 3600 seconds. When a log is extracted after this interval, a message is reported and the no-reporting period starts again.
Reset Option	Select this item to reset the monitoring interval when message reporting is suppressed by extracting logs within the no-reporting period. Use it to keep extracted logs suppressed continuously.

Item name	Description
Ignore movement	Specify the behavior of message suppression. [Delete the messages in the monitoring interval] When multiple logs that match the filter are detected during the monitoring interval, a message is output for the first detected log and the subsequent logs are deleted without being reported. The logs that match the filter during the monitoring interval are disabled even if a filter whose priority is lower than this filter is set. [Apply the messages in the monitoring interval to the following filter]When multiple logs that match the filter are detected during the monitoring interval, a message is output for the first detected log and the filter is disabled for the subsequent logs. If a filter whose priority is lower than the filter exists, the logs that match the filter during the monitoring interval are sequentially checked for this filter and a message is output when they match.

The [Log Filter] section in the [System Log Monitoring Settings] screen contains the [Edit] link. If you select the filter you want to change and click the [Edit] link, the [Edit Log Filter(Form)] screen shown below is displayed. By using this screen, you can change the filter definition.

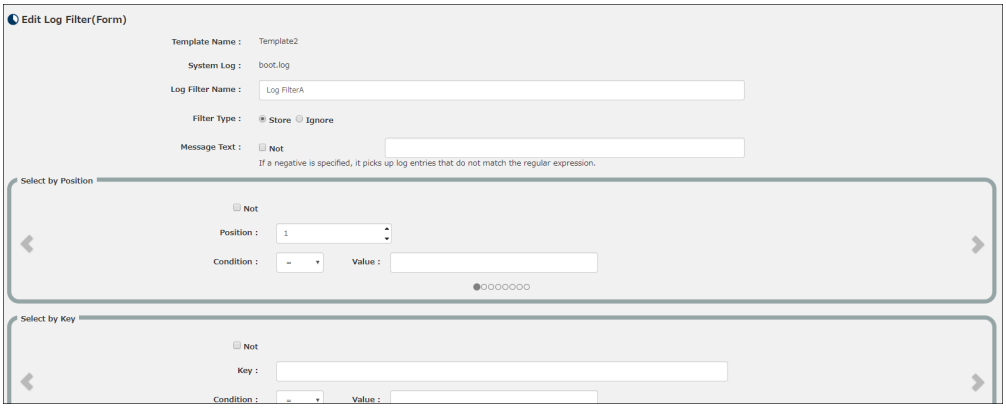

Figure 1-213 [Edit Log Filter (Form)] screen

The input items are the same as those of the [Add Log Filter(Form)] screen. The [Log Filter] section in the [System Log Monitoring Settings] screen contains the [Delete] link. If you select the filter you want to delete and click the [Delete] link, the [Delete Log Filter] dialog box shown below is displayed. By using this dialog box, you can delete the filter definition.

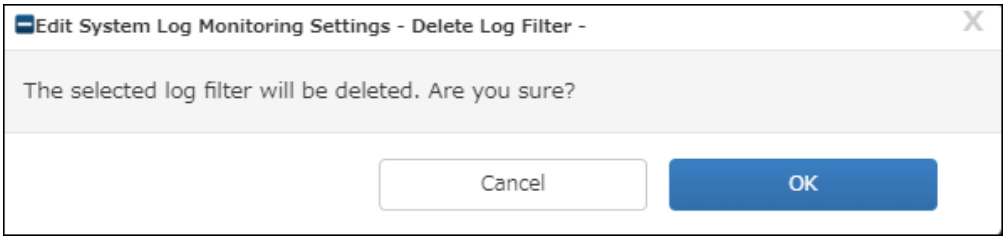

Figure 1-214 [Delete Filter] dialog box

Table 1-120 Item list ([Delete Log Filter] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the filter.
OK	Deletes the filter and then closes the dialog box.

Changing the order of log filters

The [Log Filter] section in the [System Log Monitoring Settings] screen contains the [Edit Order] link. Clicking the [Edit Order] link moves the selected log up and down in the order.

Application log monitoring

If you click [Application Log Monitoring] in the [Monitoring Settings] tab of the [Node Monitoring] screen or the monitoring template details of the [Monitoring template] screen, the [Application Log Monitoring] setting panel is displayed. The [Application Log Monitoring] setting panel lets you check the monitoring states of application logs.

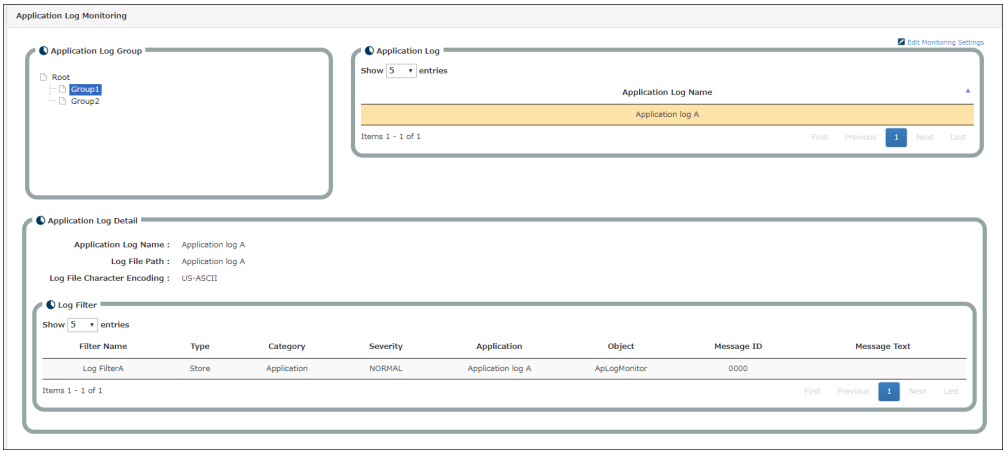

Figure 1-215 Application log monitoring

Table 1-121 Item list (Application Log Details)

Item name	Description
Application log name	Displays the application log name.
Log file path	Displays the file path of the application log.
Log file character encoding	This is the character code of the application log. • US-ASCII • Unicode (UTF-8) • Unicode (Big-Endian) • Unicode • Japanese (Shift-JIS) • Japanese (JIS) • Japanese (JIS 0208-1990 and 0212-1990) • Chinese Traditional (Big5) • Chinese Simplified (GB2312) • Chinese Simplified (GB18030)
Log filter	Displays the list of log filters.

This panel displays the tree of application log groups on the left. If you select an application log group in the tree, the application logs belonging to the selected group are listed on the right. If you select an application log in the application log list, [Application Log Detail] is displayed below. [Application Log Detail] contains the following items.

Table 1-122 Item list (Log Filter)

Item name	Description
Filter name	Displays the log filter name.
Type	Displays one of the following filter types. • Store • Ignore

Item name	Description
	When [Store] is selected, a message is reported for a log matching this filter. When [Ignore] is selected, no message is reported for a log matching this filter, and the filtering processing of the subsequent filters is not performed.
Category	Displays the category assigned when the log is reported as a message.
Severity	Displays the severity assigned when the log is reported as a message.
Application	Displays the application name assigned when the log is reported as a message.
Object	Displays the object name assigned when the log is reported as a message.
Message ID	Displays the message ID assigned when the log is reported as a message.
Message text	Displays the filter condition for the message text.

Changing the application log monitoring setting

If you click the [Edit Monitoring Settings] link in the [Application Log Monitoring] panel, the [Application Log Monitoring Settings] screen is displayed. Like the [Application Log Monitoring] panel, the [Application Log Monitoring Settings] screen consists of an application log group tree, an application log list, and details of an application log.

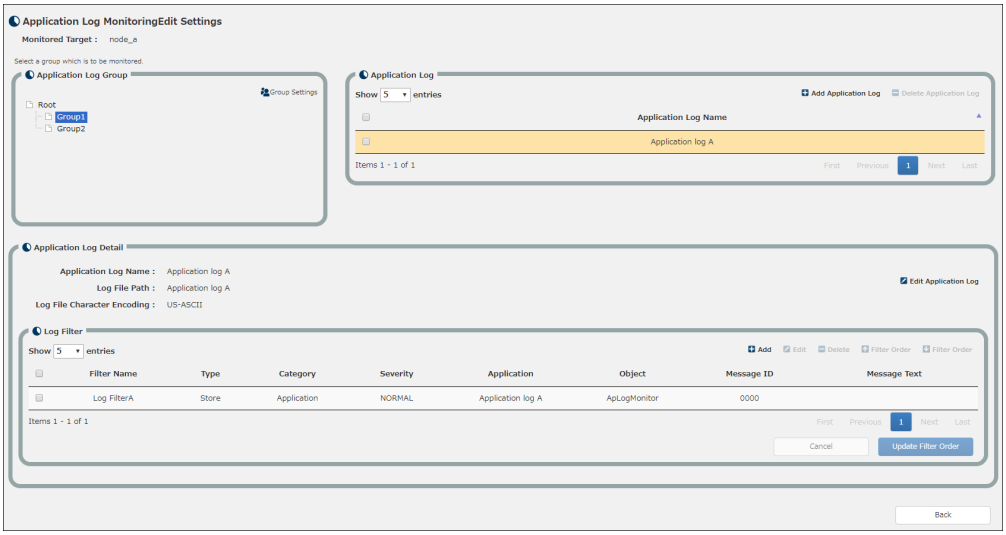

Figure 1-216 [Application Log Monitoring Settings] screen

Adding, changing, and deleting a group

The application log group tree in the [Application Log Monitoring Settings] screen contains the [Group Settings] link. Clicking this link displays the following menu, which lets you add, change, and delete groups.

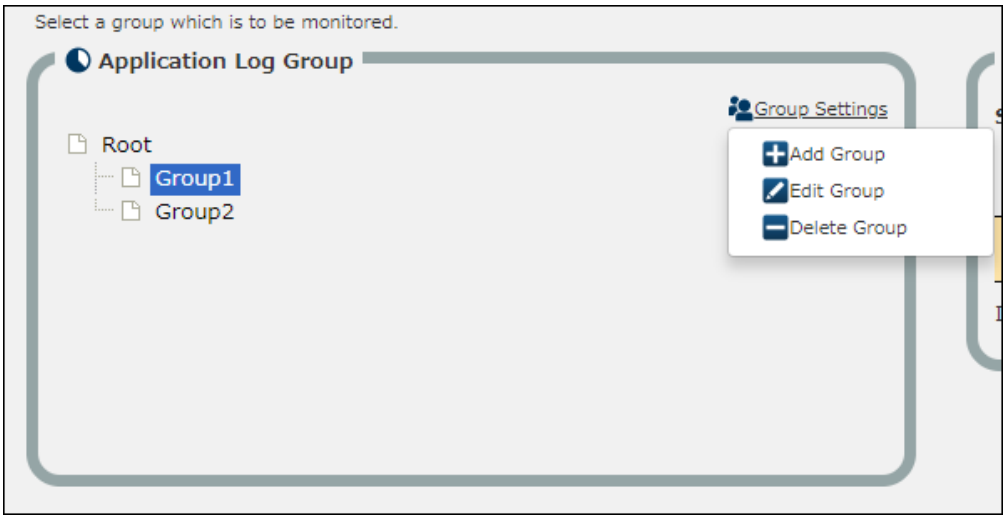

Figure 1-217 Pop-up menu

If you select [Add Group] from the pop-up menu, the [Add Group] dialog box shown below is displayed. By using this dialog box, you can add a group directly below the root or below the selected group. You can organize groups into a hierarchy.

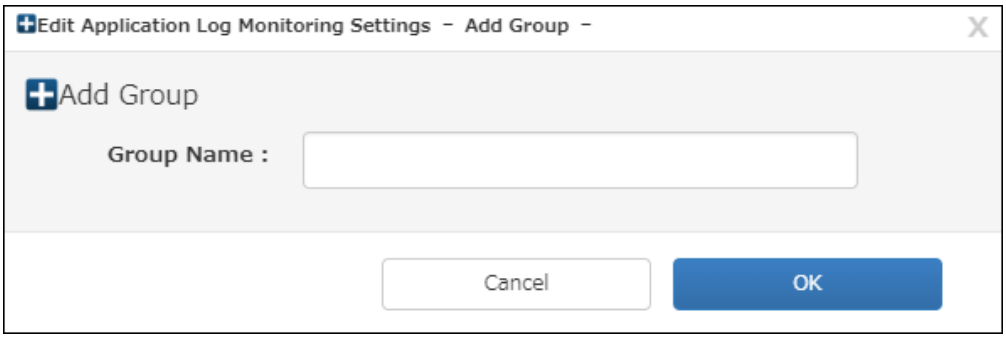

Figure 1-218 [Add Group] dialog box

Table 1-123 Item list ([Add Group] dialog box)

Item name	Description
Group name	Enter the name of the group to be added within 64 characters.
Cancel	Closes the dialog box without adding the group.
OK	Adds the group and then closes the dialog box.

If you select a group in the group tree and then [Edit Group] from the pop-up menu, the [Edit Group] dialog box shown below is displayed. By using this dialog box, you can rename the group selected in the tree.

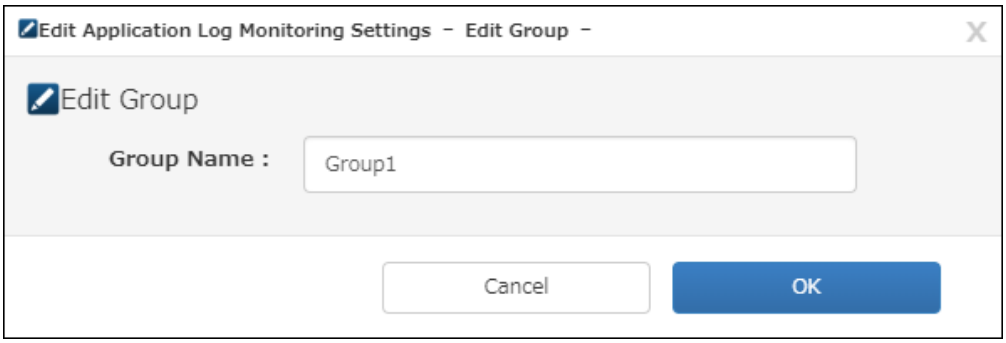

Figure 1-219 [Edit Group] dialog box

Table 1-124 Item list ([Edit Group] dialog box)

Item name	Description
Group name	Enter the name of the group to be changed within 64 characters.
Cancel	Closes the dialog box without changing the group.
OK	Changes the group and then closes the dialog box.

If you select a group in the group tree and then [Delete group] from the pop-up menu, the [Delete group] dialog box shown below is displayed. By using this dialog box, you can change the group selected in the tree. Once you delete a group, the groups, application logs, and application log filters below the deleted group are deleted as well.

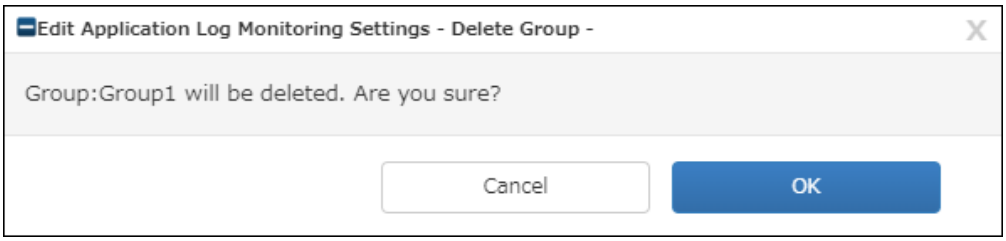

Figure 1-220 [Delete group] dialog box

Table 1-125 Item list ([Delete Group] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the group.
OK	Deletes the group and then closes the dialog box.

Adding, changing, and deleting an application log

The [Application Log] section in the [Application Log Monitoring Settings] screen contains the [Add application log] link. Clicking this link displays [Edit application log(Form)] shown below, which lets you add application logs to an application log group.

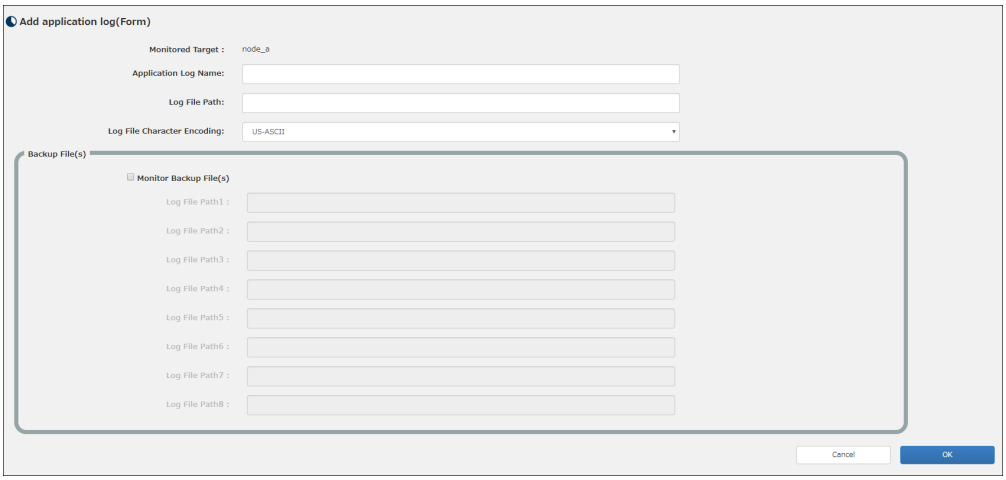

Figure 1-221 [Add Application Log (Form)] screen

Table 1-126 Item list ([Add Application Log(Form)] screen)

Item name	Description
Application log name	Enter the name of the application log within 32 characters.
Log file path	Enter the file path of the application log within 256 characters.
Log file character encoding	This is the character code of the application log. • US-ASCII • Unicode (UTF-8) • Unicode (Big-Endian) • Unicode • Japanese (Shift-JIS) • Japanese (JIS) • Japanese (JIS 0208-1990 and 0212-1990) • Chinese Traditional (Big5) • Chinese Simplified (GB2312) • Chinese Simplified (GB18030)
Backup file(s)	Specify whether to monitor backup files.
Cancel	Returns you to the previous screen without applying the setting.
OK	Applies the setting and returns you to the previous screen.

Table 1-127 Item list (Backup File)

Item name	Description
Monitor backup file(s)	Select this to monitor backup files.
Log file path 1 to 8	Enter the path of the backup files within 256 characters.

[Application Log Detail] contains the [Edit Application Log] link. Clicking the [Edit Application Log] link displays the [Edit application log(Form)] screen shown below. This screen lets you change the monitoring settings of an application log.

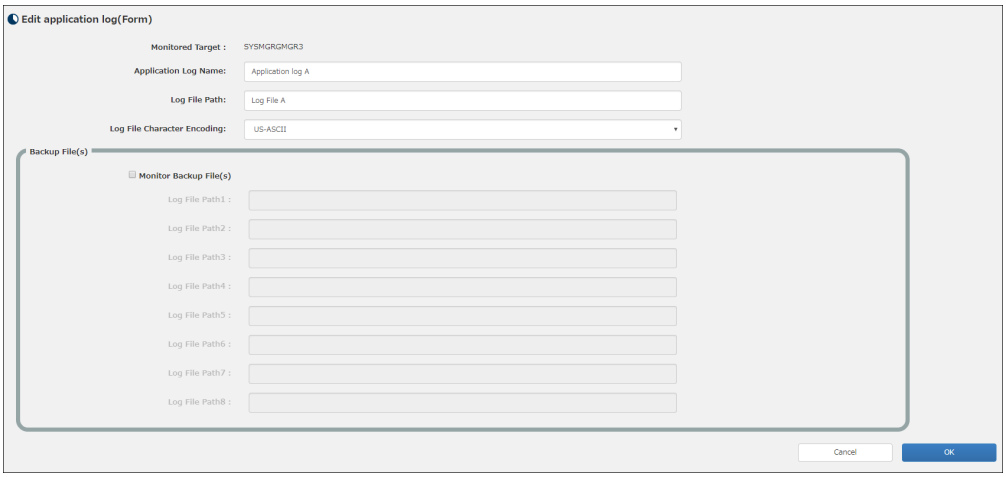

Figure 1-222 [Change Application Log (Form)] screen

The input items of the [Edit application log(Form)] screen are the same as those of the [Edit application log(Form)] screen. See the description about this screen.

The [Application Log] section in the [Application Log Monitoring Settings] screen contains the [Delete Application Log] link. If you select the check box of the application log you want to delete and click this link, the [Delete Application Log] dialog box shown below is displayed, which lets you delete the application log from the group. Once you delete an application log, the application log filters below the deleted application log are deleted as well.

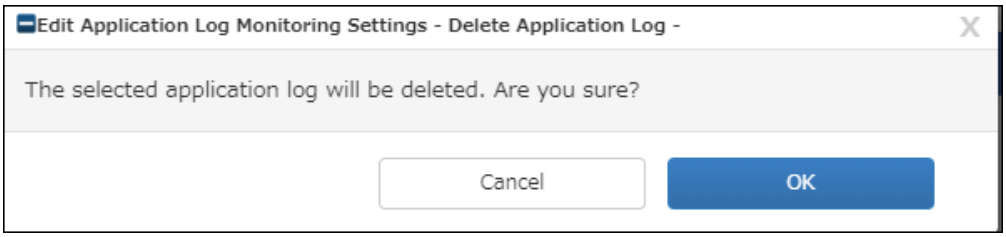

Figure 1-223 [Delete Application Log] dialog box

Table 1-128 Item list ([Delete Application Log] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the application log.
OK	Deletes the application log and then closes the dialog box.

Adding, changing, and deleting a log filter

The [Log Filter] section in the [Application Log Monitoring Settings] screen contains the [Add] link. Clicking the [Add] link displays the [Add Log Filter(Form)] screen shown below. By using this screen, you can add a filter definition.

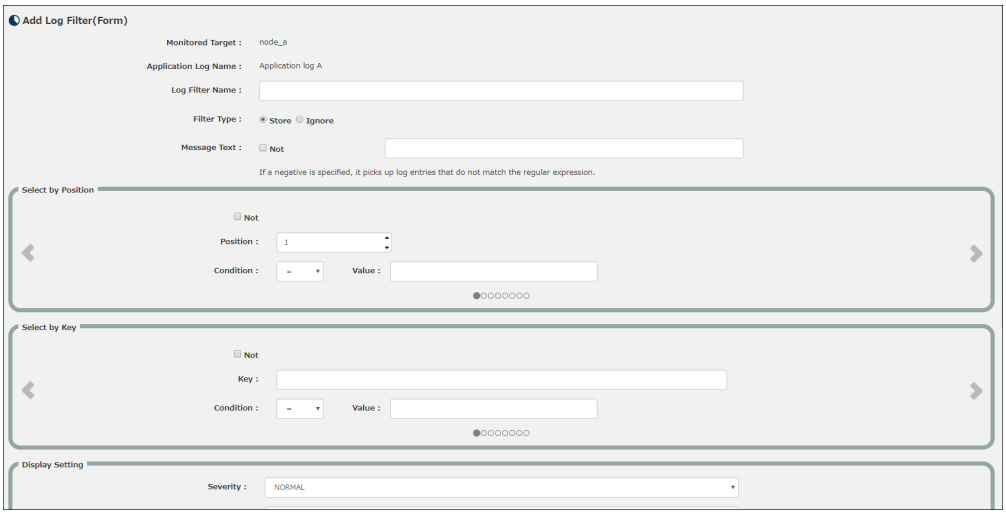

Figure 1-224 [Add Log Filter (Form)] screen

Table 1-129 Item list ([Add Log Filter(Form)] screen)

Item name	Description
Log filter name	Displays the log filter name.
Filter type	Displays one of the following filter types. • Store • Ignore When [Store] is selected, a message is reported for a log matching this filter. When [Ignore] is selected, no message is reported for a log matching this filter, and the filtering processing of the subsequent filters is not performed.
Message text	Specify the message text within 1024 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.
Select by position	Specify the position specification information.
Select by key	Specify the key information.
Display setting	Specify the definition related to the message display.
Option setting	Specify the option definition of the filter.
Cancel	Discards the setting and returns you to the previous screen.
OK	Applies the setting and returns you to the previous screen.

In [Select by Position], specify up to 8 search conditions using the position specification in the message text. If a negative condition is specified, messages that do not match the condition are selected.

Figure 1-225 [Add Log Filter (Form)] screen - Select by Position

[Select by Key] specifies up to 8 search conditions using the key specification in the log content. If a negative condition is specified, messages that do not match the condition are selected.

Figure 1-226 [Add Log Filter (Form)] screen - Select by Key

Table 1-130 Item list ([Add Log Filter(Form)] screen - Select by Key)

Item name	Description
Not	If this is selected, messages that do not match the condition are selected.
Key	Specify the key in the log content within 64 characters.
Condition	Specify the value to compare. When [=] is specified for [Condition], specify [Comparison value] using a regular expression.
Value	Specify the value to compare within 64 characters. No regular expression can be specified.

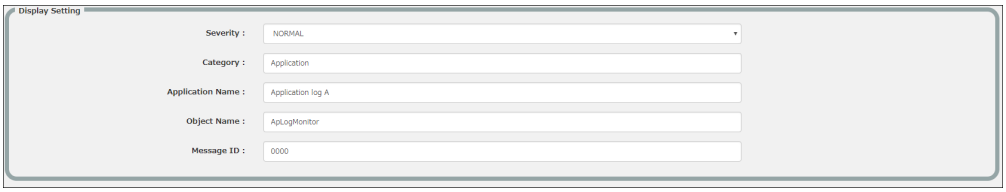

Figure 1-227 [Add Log Filter (Form)] screen - Display Setting

Table 1-131 Item list (Add Log Filter(Form) screen - Display Setting)

Item name	Description
Severity	Select the severity to be assigned when the log is reported as a message.
Category	Select a category from Application, Security, or System, or enter a category within 32 characters.
Application name	Specify the information about the application assigned when the log is reported as a message within 32 characters.
Object name	Specify the information about the object assigned when the log is reported as a message within 32 characters.
Message ID	Specify the message ID assigned when the log is reported as a message within 32 characters.

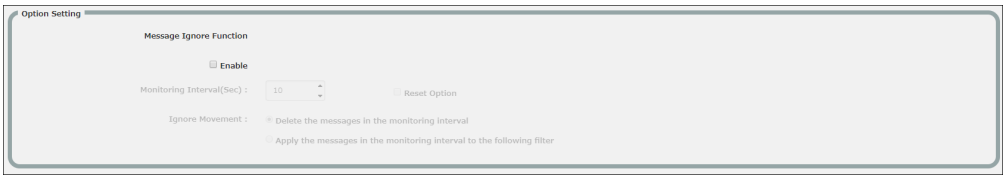

Figure 1-228 [Add Log Filter (Form)] screen - Option Setting

Table 1-132 Item list ([Add Log Filter(Form)] screen - Option Setting)

Item name	Description
Enable	Select this to use the message suppression function.
Monitoring interval (sec)	Specify the period during which no message is reported from the first extracted log in the range of 1 to 3600 seconds. When a log is extracted after this interval, a message is reported and the no-reporting period starts again.

Item name	Description
Reset Option	Select this item to reset the monitoring interval when message reporting is suppressed by extracting logs within the no-reporting period. Use it to keep extracted logs suppressed continuously.
Ignore movement	Specify the behavior of message suppression. [Delete the messages in the monitoring interval] When multiple logs that match the filter are detected during the monitoring interval, a message is output for the first detected log and the subsequent logs are deleted without being reported. The logs that match the filter during the monitoring interval are disabled even if a filter whose priority is lower than this filter is set. [Apply the messages in the monitoring interval to the following filter]When multiple logs that match the filter are detected during the monitoring interval, a message is output for the first detected log and the filter is disabled for the subsequent logs. If a filter whose priority is lower than the filter exists, the logs that match the filter during the monitoring interval are sequentially checked for this filter and a message is output when they match.

The [Log Filter] section in the [Application Log Monitoring Settings] screen contains the [Edit] link. If you select the filter you want to change and click the [Edit] link, the [Edit Log Filter(Form)] screen shown below is displayed. By using this screen, you can change the filter definition.

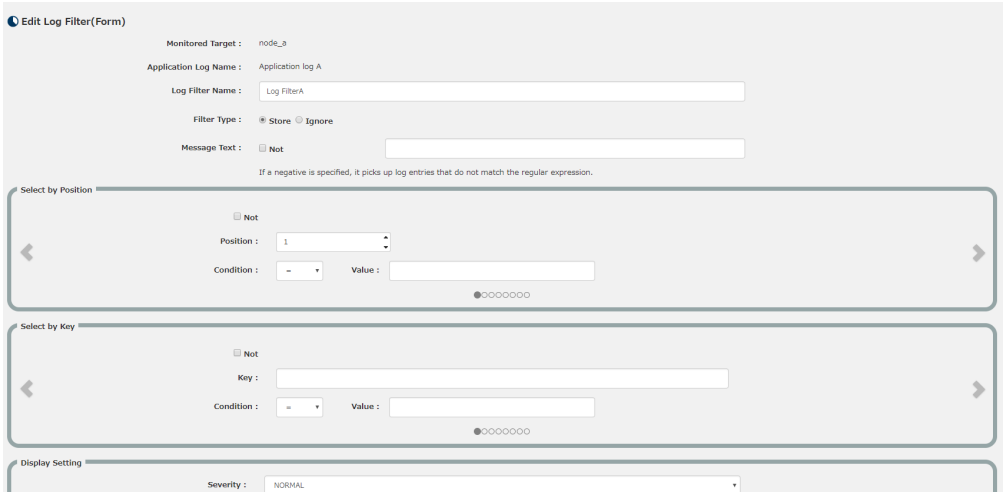

Figure 1-229 [Edit Log Filter (Form)] screen

The input items are the same as those of the [Add Log Filter(Form)] screen. The [Log Filter] section in the [Application Log Monitoring Settings] screen contains the [Delete] link. If you select the filter you want to delete and click the [Delete] link, the [Delete Log Filter] dialog box shown below is displayed. By using this dialog box, you can delete the filter definition.

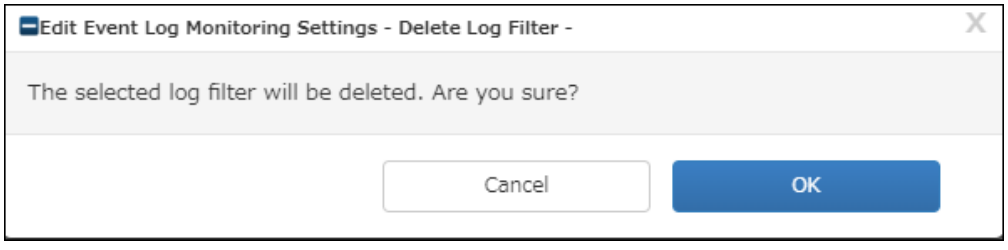

Figure 1-230 [Delete Filter] dialog box

Table 1-133 Item list ([Delete Log Filter] dialog box)

Item name	Description
Cancel	Closes the dialog box without deleting the filter.
OK	Deletes the filter and then closes the dialog box.

Changing the order of log filters

The [Log Filter] section in the [Application Log Monitoring Settings] screen contains the [Edit Order] link. Clicking the [Edit Order] link moves the selected log up and down in the order.

1.7.5.3 Monitoring template

This section describes the [Monitoring template] screen that displays monitoring templates.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	Y	Y

From the menu, click [Monitoring], [Configuration], and then [Monitoring template] tab, and the [Monitoring template] screen is displayed.

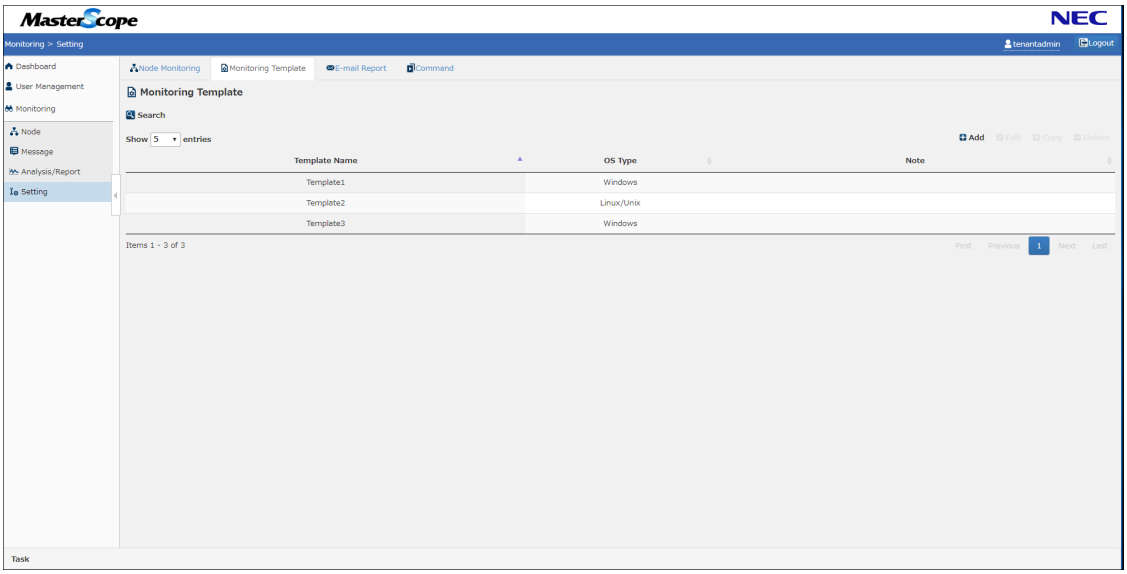

Figure 1-231 [Monitoring template] screen

Table 1-135 Item list ([Monitoring template] screen)

Item name	Description
[Search] button	This button displays the [Search] screen used to search for monitoring templates that match the specified conditions.
Show [ ] entries	The number of monitoring templates to be displayed in the list per page. You can select the number of email report settings to be displayed from 5, 10, 50, and 100.
[Add] button	Adds a monitoring template. For details, see "1.7.5.3.1 Adding a monitoring template (page 146)".
[Edit] button	Edits a monitoring template. For details, see "1.7.5.3.2 Changing a monitoring template (page 147)".
[Copy] button	Copies a monitoring template. For details, see "1.7.5.3.3 Copying a monitoring template (page 148)".
[Delete] button	Deletes a monitoring template. For details, see "1.7.5.3.4 Deleting a monitoring template (page 149)".
Monitoring template list	List of monitoring templates

The monitoring template list displays the following items.

Table 1-136 Item list ([Monitoring template] screen - Monitoring template list)

Item name	Description
Template name	Name of the monitoring template
OS type	OS type of the monitoring template. Either of the following OS types is displayed. • Windows: Indicates that the monitoring template can be applied to nodes whose OS type is Windows. • Linux/Unix: Indicates that the monitoring template can be applied to nodes whose OS type is Linux or Unix.
Note	Note on the monitoring template

To search for a monitoring template, click the [Search] button to display the [Search] screen, enter search conditions, and then execute the search.

The [Search] screen displays the items and buttons shown below. A string search is a partial match search.

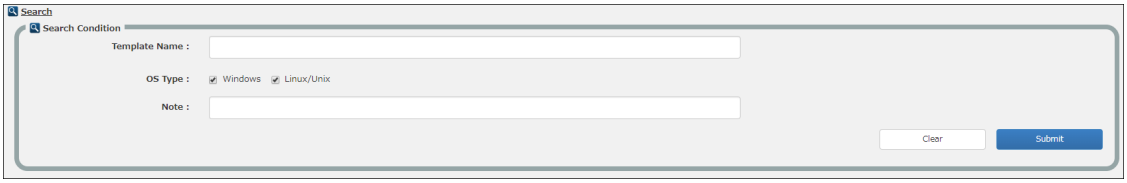

Figure 1-232 [Monitoring template] screen - Search

Table 1-137 Item list ([Monitoring template] screen - Search)

Item name	Input rule	Description
Template name	Up to 256 characters	Searches for the entered template name.
OS type	At least one	Searches for the selected OS type. You can also select the OS type from the following. • Windows • Linux/Unix
Note	Up to 256 characters	Searches for the entered note.

If you select a monitoring template shown in the monitoring template list in the [Monitoring template] screen, monitoring template details are displayed.

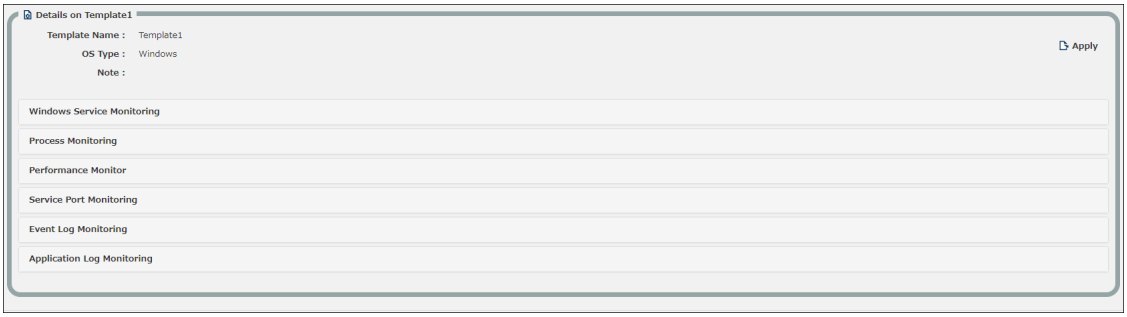

Figure 1-233 [Monitoring template] screen - Details

Table 1-138 Item list ([Monitoring template] screen - Details)

Item name	Description
Template name	Displays the name of the monitoring template.
OS type	Displays the OS type of the monitoring template. Either of the following OS types is displayed. • Windows: Indicates that the monitoring template can be applied to nodes whose OS type is Windows. • Linux/Unix: Indicates that the monitoring template can be applied to nodes whose OS type is Linux or Unix.
Note	Displays the note on the monitoring template.
Windows service monitoring panel	Displays the Windows service monitoring setting of the monitoring template. This is displayed only when the OS type is Windows. For details, see "1.7.5.2.1 Windows service monitoring (page 102)".
Process monitoring panel	Displays the process monitoring setting of the monitoring template. For details, see "1.7.5.2.2 Process monitoring (page 108)".
Performance monitoring panel	Displays the performance monitoring setting of the monitoring template. For details, see "1.7.5.2.3 Performance monitor (page 114)".
Service port monitoring panel	Displays the service port monitoring setting of the monitoring template. For details, see "1.7.5.2.4 Service port monitoring (page 118)".
Event log monitoring panel	Displays the event log monitoring setting of the monitoring template. This is displayed only when the OS type is Windows. For details, see "1.7.5.2.5 Event log monitoring (page 121)".
System log monitoring panel	Displays the syslog monitoring setting of the monitoring template. This is displayed only when the OS type is Linux/Unix. For details, see "1.7.5.2.6 System log monitoring (page 128)".
Application log monitoring panel	Displays the application log monitoring setting of the monitoring template. For details, see "1.7.5.2.7 Application log monitoring (page 135)".
[Apply] button	Applies the monitoring template to nodes. For details, see "1.7.5.3.5 Applying a monitoring template (page 150)".

Adding a monitoring template

This section describes how to add a monitoring template.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Click the [Add] button in the [Monitoring template] screen to display the [Add Template] dialog box.

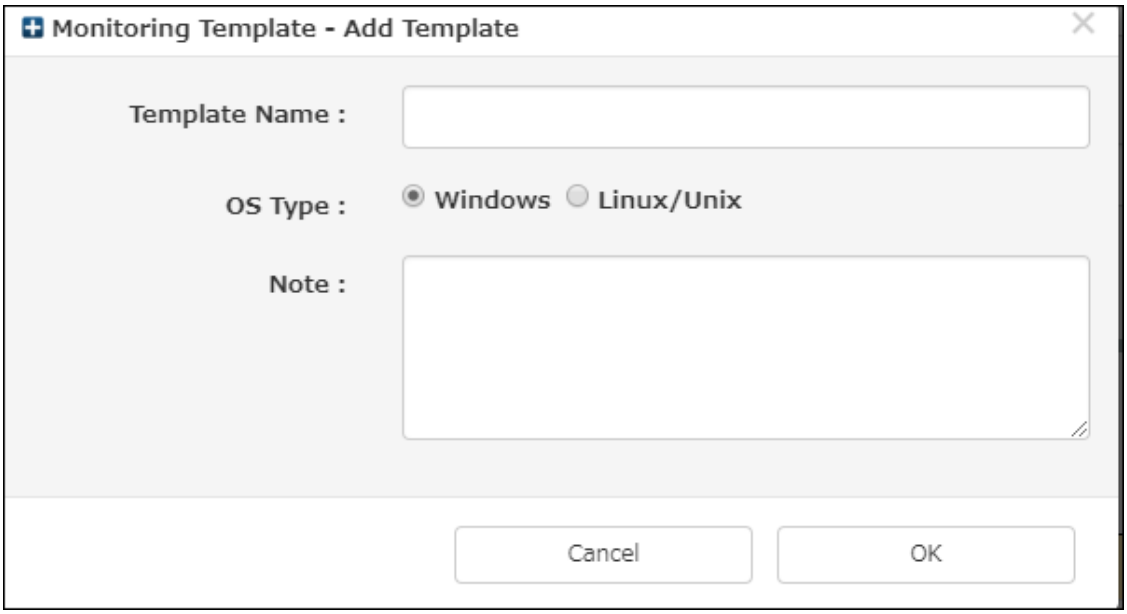

Figure 1-234 [Add Template] dialog box

Table 1-139 Item list ([Add Template] dialog box)

Item name	Required	Description
Template name	Y	Enter the name of the monitoring template within 256 characters.
OS type	Y	Select the OS type of the monitoring template. The monitoring settings you can configure differ depending on the OS type you select. • Windows: You can configure monitoring settings for nodes whose OS type is Windows. • Linux/Unix: You can configure monitoring settings for nodes whose OS type is Linux or Unix.
Note		Enter the note on the monitoring template within 1024 characters.

When you have entered all necessary items, click the [OK] button to add the monitoring template.

Clicking the [Cancel] button discards the data entered in the fields and returns you to the [Monitoring template] screen.

Changing a monitoring template

This section describes how to change a monitoring template.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

In the [Monitoring template] screen, select a monitoring template in the list and click the [Edit] button to display the [Edit Template] dialog box.

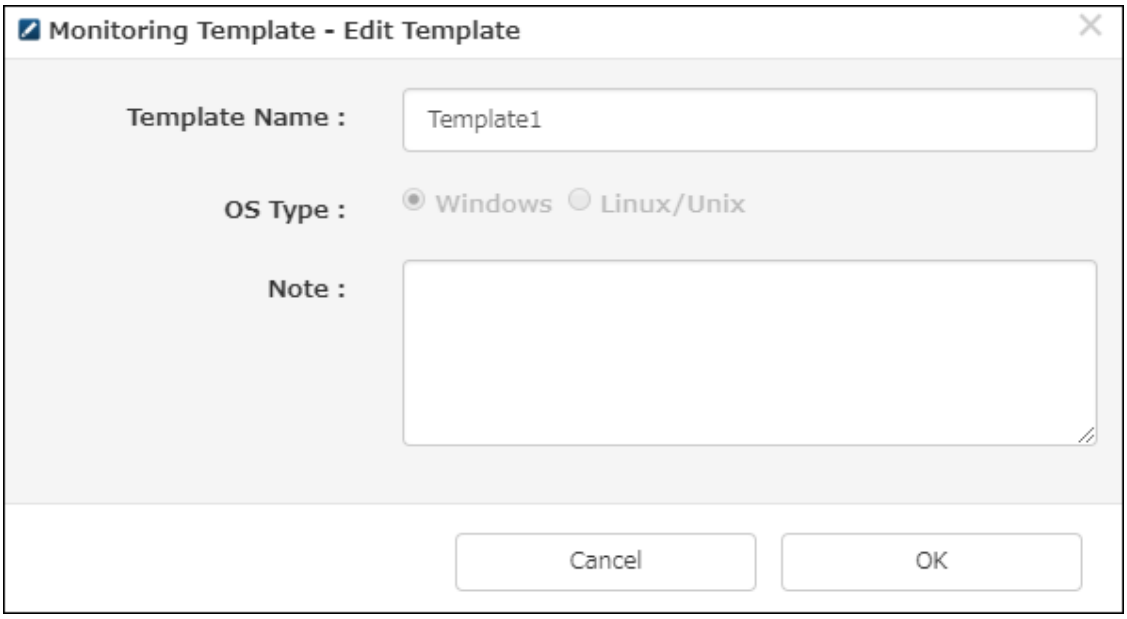

Figure 1-235 [Edit Template] dialog box

Table 1-140 Item list ([Edit Template] dialog box)

Item name	Required	Description
Template name	Y	Enter the name of the changed monitoring template within 256 characters. By default, the template name of the monitoring template to be changed is displayed.
OS type	Y	Selects the OS type of the monitoring template to be changed. The OS type cannot be changed.
Note		Enter the note on the changed monitoring template within 1024 characters. By default, the remark on the monitoring template to be changed is displayed.

When you have entered all necessary items, click the [OK] button to change the monitoring template.

Clicking the [Cancel] button discards the data entered in the fields and returns you to the [Monitoring template] screen.

Copying a monitoring template

This section describes how to copy a monitoring template.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

In the [Monitoring template] screen, select a monitoring template in the list and click the [Copy] button to display the [Copy Template] dialog box.

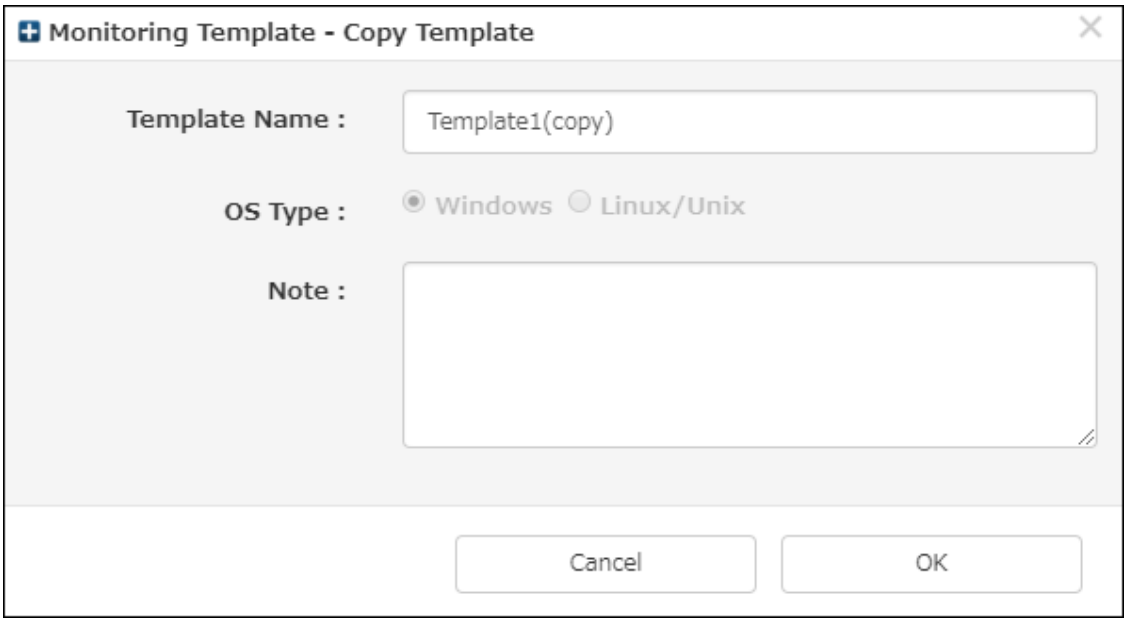

Figure 1-236 [Copy Template] dialog box

Table 1-141 Item list ([Copy Template] dialog box)

Item name	Required	Description
Template name	Y	Enter the name of the monitoring template within 256 characters. By default, the name of the copy source monitoring template is displayed with "(copy)" appended at the end.
OS type	Y	Selects the OS type of the copy source monitoring template. The OS type cannot be changed.
Note		Enter the note on the monitoring template within 1024 characters. By default, the remark on the copy source monitoring template is displayed.

When you have entered all necessary items, click the [OK] button to copy the monitoring template.

Clicking the [Cancel] button discards the data entered in the fields and returns you to the [Monitoring template] screen.

Deleting a monitoring template

This section describes how to delete a monitoring template.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

In the [Monitoring template] screen, select a monitoring template in the list and click the [Delete] button to display the [Delete Template] dialog box.

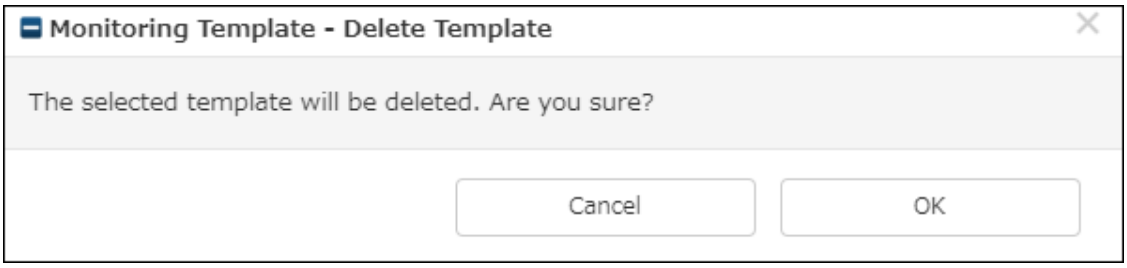

Figure 1-237 [Delete Template] dialog box

Click the [OK] button to delete the monitoring template.

Clicking the [Cancel] button returns you to the [Monitoring template] screen without deleting the monitoring template.

Applying a monitoring template

This section describes how to apply a monitoring template.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

In the [Monitoring template] screen, select a monitoring template in the list to display the monitoring template details.

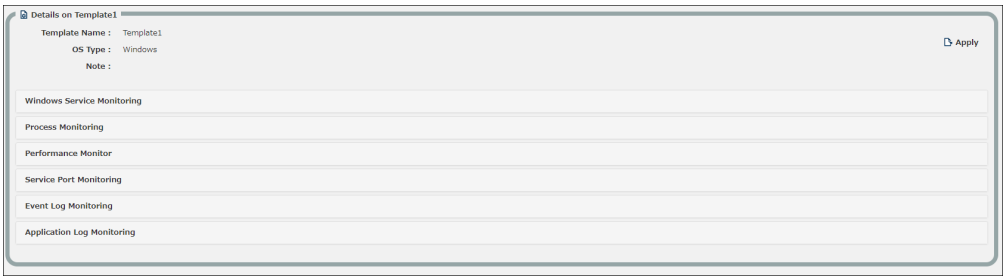

Figure 1-238 Applying a monitoring template

Click the [Apply] button in the monitoring template details to display the [Apply Template] dialog box.

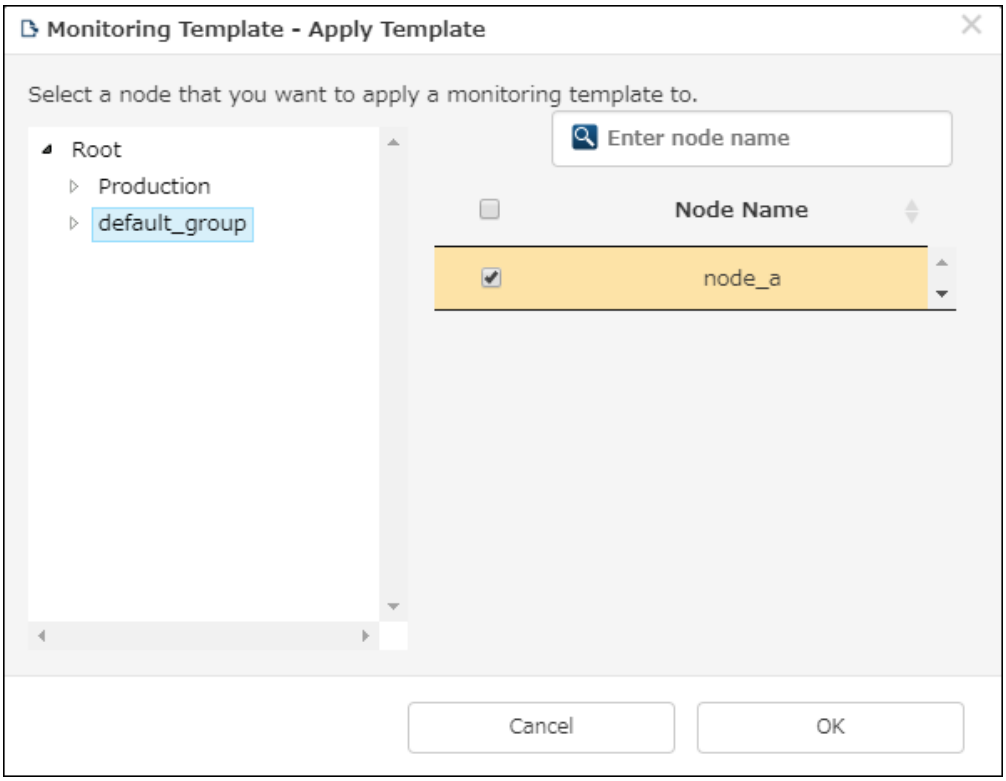

Figure 1-239 Applying a monitoring template

Table 1-142 Item list ([Apply Template] dialog box)

Item name	Description
Group tree	Displays the tree of groups set in the [Node] screen. If you select a group, the nodes in the selected group are listed.
List of nodes	Lists the nodes in the group selected in the group tree. You can select a node to which to apply the monitoring template, by selecting the corresponding check box. You can select more than one node to apply the monitoring template.
Search field	Searches the node name. Lines of the node names including the entered character string are extracted.

From the group tree in the [Apply Template] dialog box, select a group to display the list of nodes.

Select a node to which to apply the monitoring template, by selecting the corresponding check box in the list of nodes.

After selecting a node, click the [OK] button to apply the monitoring template.

A task list is displayed that shows the status of template application. For information about the items displayed in the task list, see "1.7.2.12 Task (page 49)".

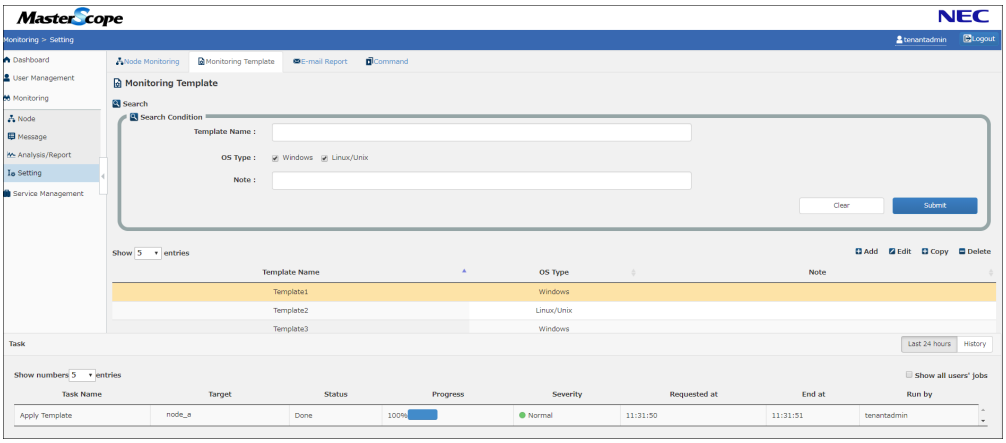

Figure 1-240 Task List

If you select a task in the task list, the [Task Detail] dialog box is displayed that lets you view the template application execution log. For information about the items displayed in [Task Detail], see "1.7.2.12 Task (page 49)".

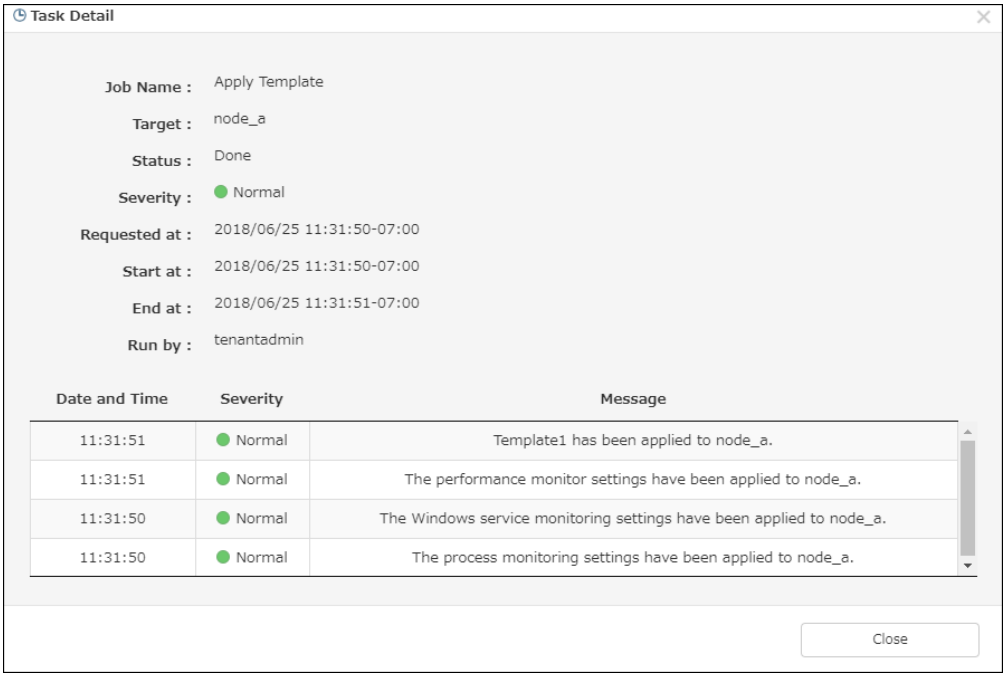

Figure 1-241 [Task Detail] dialog box

1.7.5.4 Email report

This section describes the [E-mail Report] screen that displays email report settings.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

From the menu, click [Monitoring], [Setting], and then the [E-mail Report] tab, and the [E-mail Report] screen is displayed.

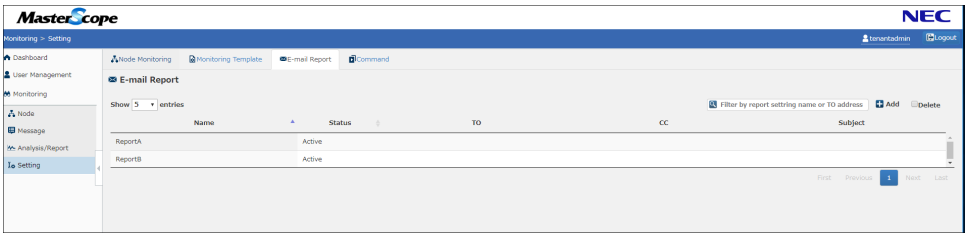

Figure 1-242 [E-mail Report] screen

Table 1-143 Item list ([E-mail Report] screen)

Item name	Description
Show [ ] entries	The number of email report settings to be displayed in the list per page. You can select the number of email report settings to be displayed from 5, 10, 50, and 100.
Search field	Searches for an email report setting name or receiver (TO). Only those lines whose email report setting name or receiver (TO) includes the entered character string are extracted.
[Add] button	Adds an email report setting. For details, see "1.7.5.4.1 Adding or changing an email report setting (page 154)".
[Delete] check box	Selecting this check box enables to delete the email report settings. For details, see "1.7.5.4.2 Deleting an email report setting (page 159)".

Selecting an email report setting shown in the action list in the [E-mail Report] screen displays Email report details.

Figure 1-243 [E-mail Report] screen - Email report details

Table 1-144 Item list ([E-mail Report] screen - Email report details)

Item name	Description
Name	Displays the definition name of Email report.
Status	Displays the status of the email report setting. Enable: Indicates that the email report setting is enabled. Disable: Indicates that the email report setting is disabled.
TO	Displays the email address of the receiver (TO) for Email report. When there are multiple email addresses that are set, each of them is separated by a comma (,).
CC	Displays the email address of the receiver (CC) for Email report.

Item name	Description
	When there are multiple email addresses that are set, each of them is separated by a comma (,).
BCC	Displays the email address of the receiver (BCC) for Email report. When there are multiple email addresses that are set, each of them is separated by a comma (,).
Subject	Displays the subject of the email to be sent.
Body	Displays the text of the email to be sent.
[Edit] button	Used to edit an email report setting. For details, see "1.7.5.4.1 Adding or changing an email report setting (page 154)".
[Copy] button	Adds an email report setting by citing the email report setting whose details are currently displayed. For details, see "1.7.5.4.1 Adding or changing an email report setting (page 154)". The added email report setting is inserted above the copied email report setting.

Adding or changing an email report setting

This section describes how to add an email report setting.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

If you click [Add] or select an action and then click [Copy] in the [E-mail Report] screen, the [Create E-mail Report] screen is displayed. If you click [Copy], the input fields are displayed with the corresponding items of the selected action shown in them.

If you select an action and then click [Edit] in the [E-mail Report] screen, the [Edit E-mail Report] screen is displayed.

To set Email report, you need to specify the information of the SMTP server to be used for Email report in advance.

See "Report mail server configuration file (msc_report_mail_server.properties)" in the "Environment Construction Guide," and set the information of the mail server to be used.

The mail server to be used must be set to the default (mail_server{n}.default=on).

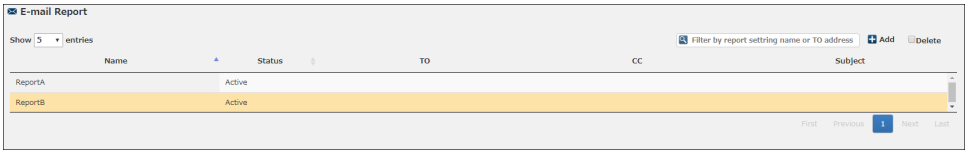

Figure 1-244 [E-mail Report] screen - [Add] button

Figure 1-245 [E-mail Report] screen - [Edit] and [Copy] buttons

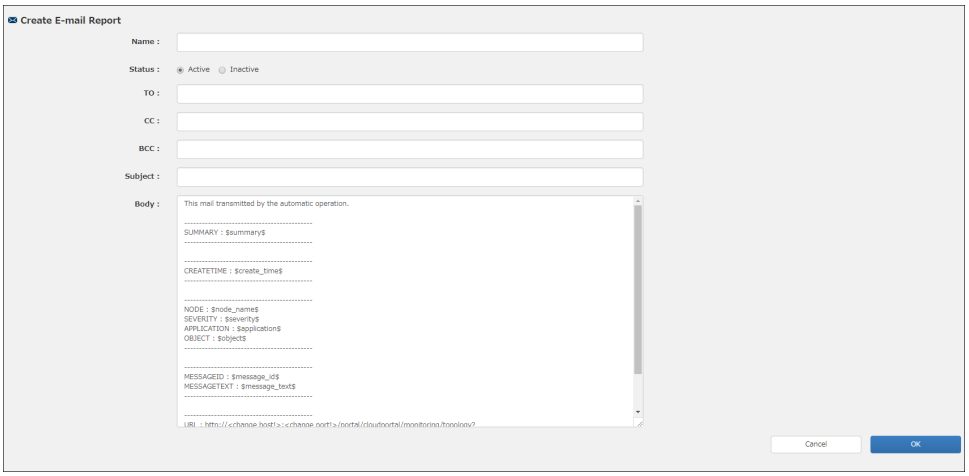

Figure 1-246 [Create E-mail Report] screen

Table 1-145 Item list ([Create E-mail Report] screen)

Item name	Required	Description
Name	Y	Enter the name of the email report setting within 64 characters.
Status	Y	When [Active] is specified, the status of the Email report is "Active". When [Inactive] is specified, the status of the Email report is "Inactive".
TO		Specify the email address of the receiver (TO). When specifying multiple receivers, separate each of them by a comma or a space character (single-byte space, line break, or tab). Make sure that the length of an email address is 256 characters or less and that the total length is 768 characters or less (the number of characters includes commas and space characters). The email address must be of the email address format (local-part@domain).
CC		Specify the email address of the receiver (CC). When specifying multiple receivers, separate each of them by a comma or a space character (single-byte space, line break, or tab). Make sure that the length of an email address is 256 characters or less and that the total length is 768 characters or less (the number of characters includes commas and space characters). The email address must be of the email address format (local-part@domain).
BCC		Specify the email address of the receiver (BCC). When specifying multiple receivers, separate each of them by a comma or a space character (single-byte space, line break, or tab). Make sure that the length of an email address is 256 characters or less and that the total length is 768 characters or less (the number of characters includes commas and space characters). The email address must be of the email address format (local-part@domain).
Subject		Specify the subject of the email within 128 characters. Replacement strings can be specified. When specifying any replacement string, take into account the number of characters to be actually displayed.
Body		Specify the text of the email within 8192 characters. Replacement strings shown in "Table 1-146 Item list (replacement strings) (page 156)" can be specified. When specifying any replacement string, take into account the number of characters to be actually displayed.

Item name	Required	Description

		From the text of the email sent by SystemManager G Manager, you can access the [Detail] page of the message that triggered the Email report. As the text of the email, specify the URL shown below. As for "<change host!>:<change port!>" in the setting examples, change them to the host name and port number (default: 12080) of SystemManager G Manager if appropriate.
		• Setting example 1: URL of [Message Details] of the [Node] screen
		`http://<change host!>:<change port!>/portal/cloudportal/monitoring/topology?view=detail&node=$node_id$&msg=$message_no$`
		For information about the parameters that can be specified in URL queries, see "1.7.2 Node (page 28)".
		• Setting example 2: URL of [Message Details] of the [Message] screen (A separate license is required.)
		`http://<change host!>:<change port!>/portal/cloudportal/monitoring/business?view=detail&category=$business_node_id$&msg=$message_no$`
		For information about the parameters that can be specified in URL queries, see "1.7.3 Message (page 52)".

Table 1-146 Item list (replacement strings)

Replacement string	Description
$message_id$	Message ID
$definition_code$	Message definition
$tenant_id$	Tenant ID
$severity$	Severity
$create_time$	Occurrence date and time
$system_name$	System name
$node_id$	Node ID
$node_type$	Node type
$node_name$	Node name
$object$	Object
$summary$	Description of the message
$message_no$	Message number
$receive_time$	Reception date and time
$message_text$	Message text
$business_node_id$	Business category node ID set in the filter that triggered the reporting. It cannot be specified for a reporting filter of a node.

The following table lists the URL parameters that you can use when specifying the URL of the [Node] or [Message] screen as the text of the email.

Table 1-147 [Node] screen - URL parameter

URL parameter	Valid values	Description
view	list detail status status_count status_list msg	Specify the panel to be displayed by default when the URL is accessed. If the view parameter is not specified or the specified view parameter is invalid, only the node list panel is displayed. • list: Displays the node list panel. • detail: Displays the status panel and message panel. It is required to specify group or node. (If no target node is specified, the specified view parameter becomes invalid.) • status: Displays only the status panel (displays the number of nodes of each severity level and the status list). It is required to specify group or node. (If no target node is specified, the specified view parameter becomes invalid.) • status_count: Displays only the status panel (displays only the number of nodes of each severity level). It is required to specify group or node. (If no target node is specified, the specified view parameter becomes invalid.) This parameter is valid only when you add a widget to the dashboard. • status_list: Displays only the status panel (displays only the status list). It is required to specify group or node. (If no target node is specified, the specified view parameter becomes invalid.) This parameter is valid only when you add a widget to the dashboard. • msg: Displays the message panel only. If group or node is not specified, all messages are displayed.
group	Group ID	Specify the group for which to display the status panel or message panel. This parameter is ignored when the node list panel is displayed.
node	Node ID	Specify the node for which to display the status panel or message panel. This parameter is ignored when the node list panel is displayed.
auto	on	Specify this parameter to enable automatic update. If the parameter is not specified or an invalid value other than on is specified, automatic update is disabled.

Shown below is an example of the [Node] screen that is displayed when the URL of the screen is specified with msg specified in the URL parameter of view and a node ID specified in the URL parameter of node.

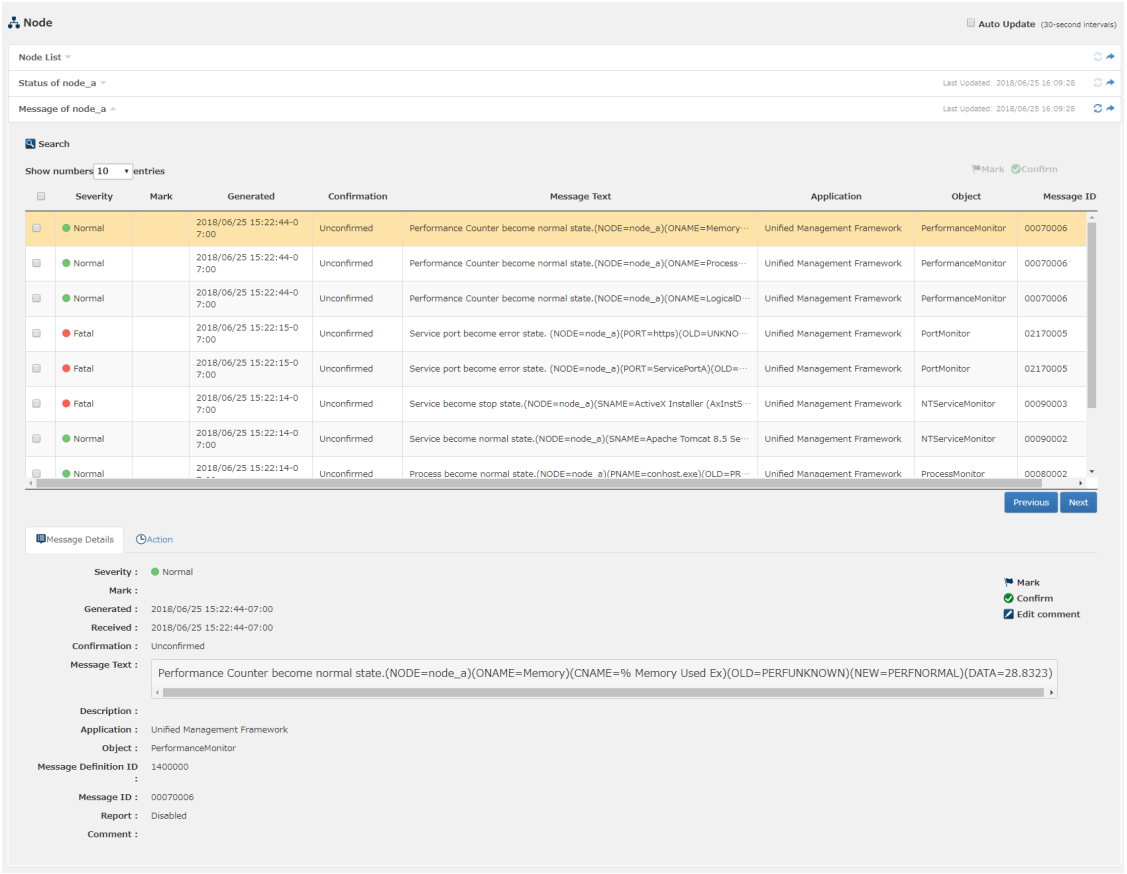

Figure 1-247 Example of the [Node] screen displayed when the URL parameters are used

Table 1-148 [Message] screen - URL parameter

URL parameter	Valid values	Description
view	list list_count list_list detail msg	Specify the panels to be displayed. If the view parameter is not specified or the specified view parameter is invalid, only the [Category list] panel is displayed. • list: Displays the [Category list] panel and [Number of Messages by Severity] panel. • list_count: Displays only the [Number of Messages by Severity] panel. It is required to specify category. (If no target node is specified, the specified view parameter becomes invalid.) This parameter is valid only when you add a widget to the dashboard. • list_list: Displays only [Category list]. This parameter is valid only when you add a widget to the dashboard. • detail: Displays the [Category list] panel, [Number of Messages by Severity] panel, and [Message List] panel. It is required to specify category. (If no target node is specified, the specified view parameter becomes invalid.) • msg: Displays the message list panel only. It is required to specify category. (If no target node is specified, the specified view parameter becomes invalid.)
category	Category	Specify the category ID for which to display the [Number of Messages by Severity] panel and [Message List] panel.
auto	on	Specify this parameter to enable automatic update. If the parameter is not specified or an invalid value other than on is specified, automatic update is disabled.

Shown below is an example of the [Message] screen that is displayed when the URL of the screen is specified with msg specified in the URL parameter of view and the replacement string of $business_node_id$ specified in the URL parameter of category.

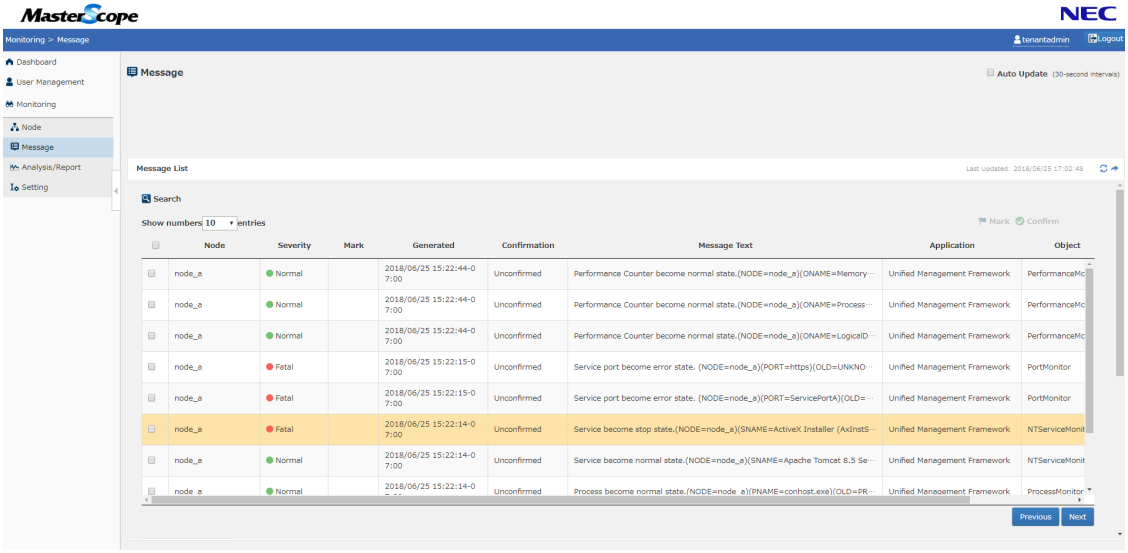

Figure 1-248 Example of the [Message] screen displayed when the URL parameters are used

Deleting an email report setting

This section describes how to delete an email report setting.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Selecting [Delete] on the [E-mail Report] screen enables to delete a filter.

If you select the check box of the email report setting you want to delete from the email report list and then click the [Delete] button, the [Delete E-mail Report] dialog box is displayed. Click [OK] to delete the email report setting.

Note

You can also delete an email report setting set for the action definition of a filter. Once you delete the email report setting, [Deleted] is displayed in the [Action definition] screen of the filter and Email report is not performed.

For information about action definitions of filters, see:

- "1.7.2.10 Setting a reporting filter (page 39)"
- "1.7.3.10 Adding or changing the filter (page 68)"

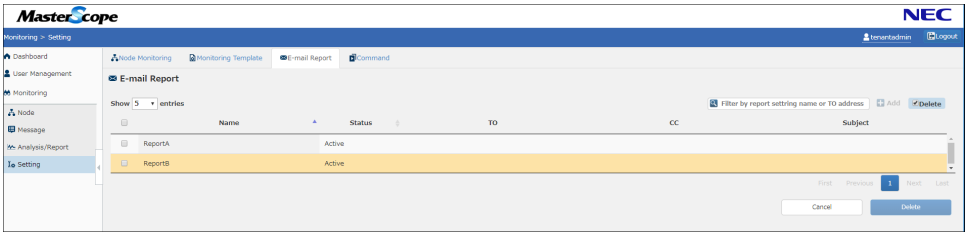

Figure 1-249 [E-mail Report] screen - [Delete] check box

Figure 1-250 [Delete E-mail Report] dialog box

1.7.5.5 Command

This section describes the [Command] screen that displays command settings.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

From the menu, click [Monitoring], [Setting], and then the [Command] tab, and the [Command] screen is displayed.

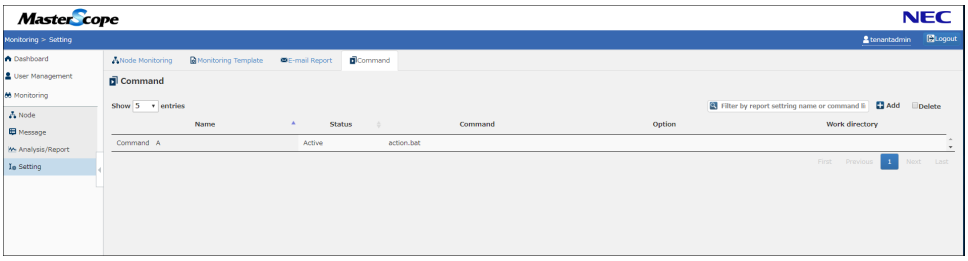

Figure 1-251 [Command] screen

Table 1-149 Item list ([Command] screen)

Item name	Description
[Show [ ] entries] button	The number of command settings to be displayed in the list per page. You can select the number of command settings to be displayed from 5, 10, 50, and 100.
Search field	Searches for a command report setting or command. Only those lines whose command report setting or command includes the entered character string are extracted.
[Add] button	Adds a command setting. For details, see "1.7.5.5.1 Adding or changing a command setting (page 161)".
[Delete] check box	Selecting this check box enables to delete the command settings. For details, see "1.7.5.5.2 Deleting a command setting (page 163)".

Selecting a command setting shown in the command list in the [Command] screen displays command setting details.

Figure 1-252 [Command] screen - Command setting details

Table 1-150 Item list ([Command] screen - Command setting details)

Item name	Description
Name	Displays the report setting name.
Status	Displays the status of the command setting. Active: Indicates that the command setting is Active. Inactive: Indicates that the command setting is Inactive.
Command	Displays the command registered as the command setting.
Option	Displays the option registered as the command setting.
Work directory	Displays the working directory registered as the command setting.
[Edit] button	Edits a command setting. For details, see "1.7.5.5.1 Adding or changing a command setting (page 161)".
[Copy] button	Adds a command setting by citing the command setting whose details are currently displayed. For details, see "1.7.5.5.1 Adding or changing a command setting (page 161)". The added command setting is inserted above the copied command setting.

Adding or changing a command setting

This section describes how to add a command setting.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

If you click [Add] or select a command setting and then click [Copy] in the [Command] screen, the [Create Command] screen is displayed. If you click [Copy], the input fields are displayed with the corresponding items of the selected command setting shown in them.

If you select a command setting and then click [Edit] in the [Commands] screen, the [Edit Command] screen is displayed.

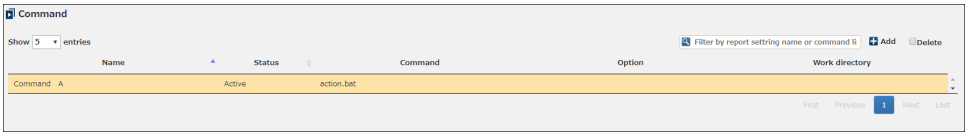

Figure 1-253 [Commands] screen - [Add] button

Figure 1-254 [Commands] screen - [Edit] and [Copy] buttons

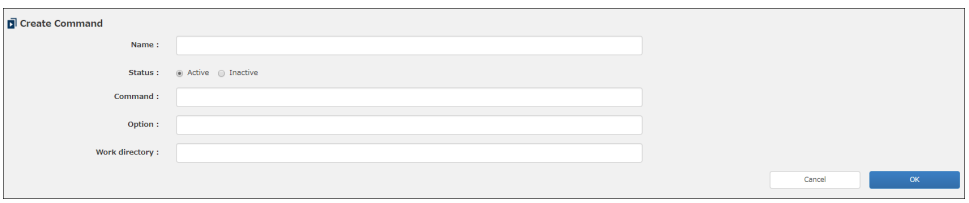

Figure 1-255 [Create Command] screen

Table 1-151 Item list ([Create Command] screen)

Item name	Required	Description
Name	Y	Enter the name of the command setting within 64 characters.
Status	Y	When [Active] is specified, the status of the command is "Active". When [Inactive] is specified, the status of the command is "Inactive".
Command	Y	Specify the command to be executed, by using an absolute path or relative path. Specify this value within 256 characters. When specifying a relative path, make sure it starts from the working directory. The command must reside in the machine in which the WebConsole Option is installed. If the path contains any space, do not enclose it in double quotation marks ("). Replacement strings can be specified. When specifying any replacement string, take into account the number of characters to be actually displayed. Note that the character code for the standard output and error output of the command to be started must be UTF-8. If the character code for the standard output and error output of the command is not UTF-8, the output results of the command cannot be acquired.
Option		Specify the argument to be used when the command is executed. Specify this value within 2048 characters. Replacement strings can be specified. When specifying any replacement string, take into account the number of characters to be actually displayed.
Work directory		Specify the absolute path of the working directory for executing the command. Specify this value within 256 characters. If the path contains any space, do not enclose it in double quotation marks ("). Replacement strings can be specified. When specifying any replacement string, take into account the number of characters to be actually displayed. If this item is not specified, the following directory is used as the working directory. <WebConsole-install-path>\bin

Table 1-152 Item list (Replacement string)

Replacement string	Description
$message_id$	Message ID
$definition_code$	Message definition
$tenant_id$	Tenant ID
$severity$	Severity
$create_time$	Occurrence date and time
$system_name$	System name
$node_id$	Node ID
$node_type$	Node type
$node_name$	Node name
$object$	Object

Replacement string	Description
$summary$	Description of the message
$message_no$	Message number
$receive_time$	Reception date and time
$message_text$	Message text
$business_node_id$	Business category node ID set in the filter that triggered the reporting. It cannot be specified for a reporting filter of a node.

In the example shown below, the following command is executed on Windows with C:\tmp as the execution directory.

```
C:\Program Files\Scripts\Action.bat Error Recovery
```

Table 1-153 Item list ([Create Command] screen: Example of Windows)

Item name	Description
Name	Windows action
Status	Enabled
Command	C:\Program Files\Scripts\Action.bat
Option	Error Recovery
Work directory	C:\tmp

In the example shown below, the following command is executed on UNIX with /tmp as the execution directory.

```
/usr/local/bin/action.sh -s error -m recovery
```

Table 1-154 Item list ([Create Command] screen: Example of UNIX)

Item name	Description
Name	UNIX action
Status	Enabled
Command	/usr/local/bin/action.sh
Option	-s error -m recovery
Work directory	/tmp

When you have entered all necessary items, click [OK] to register them.

Clicking the [Cancel] button discards the data in the fields and returns you to the [Commands] screen.

Note

To perform patrol lamp reporting, register the patrol lamp command. For details of the command, see "2.3 PATLITE command (msc_patlite_cmd) (page 172)".

Deleting a command setting

This section describes how to delete a command setting.

Note that the authority to perform the operations described in this section is controlled according to the role, and these operations are available to the following users.

MONITORING ADMINISTRATOR	MONITORING OPERATOR	MONITORING USER
Y	N	N

Selecting [Delete] on the [Command] screen enables to delete a filter.

If you select the check box of the command setting you want to delete from the command list and then click the [Delete] button, the [Command Delete] dialog box is displayed. Click [OK] to delete the command setting.

Note

You can also delete a command setting set for the action definition of a filter. Once you delete the command setting, [Deleted] is displayed in the [Action definition] screen of the filter and the command is not executed.

For information about action definitions of filters, see:

- "1.7.2.10 Setting a reporting filter (page 39)"
- "1.7.3.10 Adding or changing the filter (page 68)"

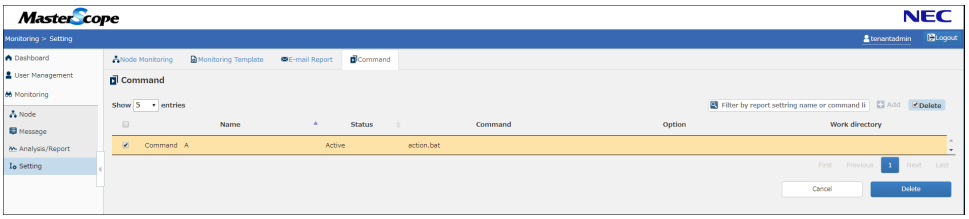

Figure 1-256 [Command] screen - [Delete] check box

Figure 1-257 [Command Delete] dialog box

Chapter 2. Command Reference

This chapter describes the commands of SystemManager G.

Contents

2.1 API gateway operation command (msc_apigateway_cmd)

2.1.1 Path

<WebConsole-install-path>\bin\msc_apigateway_cmd

2.1.2 Format

msc_apigateway_cmd --token [--address=*ip_address*] [--port=*port_num*] [--pass=*password*] [--file[=*file_path*]]

2.1.3 Functional description

The authentication token that is required when token authentication is performed by the API gateway component is displayed on the standard output.

When establishing connection to the API gateway, specify the HTTP header with the output authentication token in the format of "Authorization: Bearer *token*", as shown in the following example.

```
Authorization: Bearer d51398e8-d43b-3cc8-9e04-b6fde97eabe4
```

With the default settings, the token authentication by the API gateway component is disabled. It can be enabled by setting the apigateway.authentication parameter of msc_apigateway.properties to token.

2.1.4 Options

--token

This option is used to output the authentication token that is required to establish a connection to the API gateway.

--address=*ip_address*

-a*ip_address*

This option is used to specify an API gateway for which the authentication token is to be output. Specify *ip_address* with the IP address of the API gateway or a host name. If this option is not specified, it will be regarded as being specified with "localhost".

--port=*port_num*

-o*port_num*

This option is used to specify the port number of an API gateway for which the authentication token is to be output. Specify *port_num* with the management HTTP port number of the API gateway. If this option is not specified, it will be regarded as being specified with "9763".

--file[=*file_path*]
-f[*file_path*]

This option is used to output the authentication token to a file. When this option is specified, the authentication token will be output to both the specified file and the standard output. If this option is not specified, the authentication token will be output only to the standard output.
Specify *file_path* with the file name of the output destination. If *file_path* is not specified when this option is specified, a file named "api_token" will be output to the directory that is the current directory when the command is run.

2.1.5 Return values

Return value	Description	Action
0	Normal end	Command execution was completed normally. No action is required.
70	Internal software error	Contact the support center if this error occurs.
73	File output error	File output to the path specified by the --file option failed. Run the command again after checking for the access authority over the output destination directory, the disk capacity, and other conditions that are required to allow the file to be output.

2.1.6 Cautions

- The common library (msc_common_library) must be installed to run this command.

2.2 License command (msc_license_cmd)

This section describes the command (msc_license_cmd) for performing the following license-related operations.

- Registering a license key
- Registering a codeword
- Deleting a license
- Checking a license

2.2.1 Registering a license (msc_license_cmd --add)

2.2.1.1 Path

<WebConsole-install-path>\bin\msc_license_cmd

2.2.1.2 Format

msc_license_cmd --add {--key=*license-key*|--File=*license-file-path*} [--outpath=*output-file-path*]

2.2.1.3 Functional description

This command registers the license key attached to the purchased product and produces the file output of a code (codeword application code) used to apply for the issue of a codeword.

Send the file created by this command to NEC Corporation to obtain the codeword.

2.2.1.4 Options

--add

--a

This option is used to register a license key. When this option is used, also specify the --key or --File option.

--key=*license-key*

-k*license-key*

This option is used to register the license key by directly specifying its character string. Specify *license-key* with the character string of the license key.

--File=*license-file-path*

-F*license-file-path*

This option is used to register the license key by specifying a file that describes the license key. Specify *license-file-path* with either the full or relative path to a file containing the license key. If the path contains a space, enclose it in double quotation marks (").

--outpath=*output-file-path*

-o*output-file-path*

This option is used to specify the output file of the codeword application file. If this option is not specified, the file will be output to the current directory as a file with the following file name.

codeword_*
(An undefined string will be set in *.)

2.2.1.5 Return values

Return value	Description	Action
0	Normal end	Command execution was completed normally. No action is required.
64	Syntax error in the argument	Check for an error in the argument and run the command again using the correct syntax.
70	Internal software error An error occurred within the command.	Check whether the license management (License Component) is operating. If this error occurs while the license management is operating, contact the support center.

2.2.1.6 Cautions

- The Administrators authority is required to run this command.
- The license management component (msc_license) must be installed to run this command.

2.2.2 Registering a codeword (msc_license_cmd --register)

2.2.2.1 Path

<WebConsole-install-path>\bin\msc_license_cmd

2.2.2.2 Format

msc_license_cmd --register=*codeword-file-path*

2.2.2.3 Functional description

This command registers the codeword returned from NEC Corporation, and thereby updates the expiration date of the relevant license.

2.2.2.4 Options

--register=*codeword-file-path*

-r*codeword-file-path*

Specify this option to register a codeword of the specified file. Specify *codeword-file-path* with the full or relative path to the codeword file returned from NEC Corporation. If the path contains a space, enclose it in double quotation marks (").

2.2.2.5 Return values

Return value	Description	Action
0	Normal end	Command execution was completed normally. No action is required.
64	Syntax error in the argument	Check for an error in the argument and run the command again using the correct syntax.
70	Internal software error An error occurred within the command.	Check whether the license management (License Component) is operating. If this error occurs while the license management is operating, contact the support center.

2.2.2.6 Cautions

- The Administrators authority is required to run this command.
- The license management component (msc_license) must be installed to run this command.

2.2.3 Deleting a license (msc_license_cmd --delete)

2.2.3.1 Path

<WebConsole-install-path>\bin\msc_license_cmd

2.2.3.2 Format

msc_license_cmd --delete

2.2.3.3 Functional description

This command deletes a registered license.

In the process of the execution of this command, registered licenses are displayed as follows. Select the index (number displayed at the beginning of each line) of the license to be deleted, and then press the Enter key.

The deletion window can be terminated by entering 'quit' or 'q' and then pressing the Enter key.

```
Index,LicenseName(Licensekey),ProductID,LicenseID,LicenseNum,ExpireDate,Sta
tus
1,SystemManager G BusinessView Option(ABC-0123),103,4,1,99991231,enable
2,SystemManager G External Linker Option(ABC-1123),103,5,1,99991231,enable
3,SystemManager G WebConsole Option(ABC-2123),103,3,1,99991231,enable
4,SystemManager G Manager(ABC-3123),103,1,1,99991231,enable
Please input Index of an delete license. (It ends at quit or q.)
ex:1
  :1,3
  :1-3
```

Tip

Multiple indexes can be specified at one time by separating them with commas. In addition, consecutive indexes can be specified by using a hyphen.

2.2.3.4 Options

--delete

-d

Specify this option to delete a registered license.

2.2.3.5 Return values

Return value	Description	Action
0	Normal end	Command execution was completed normally. No action is required.
64	Syntax error in the argument	Check for an error in the argument and run the command again using the correct syntax.
70	Internal software error An error occurred within the command.	Check whether the license management (License Component) is operating. If this error occurs while the license management is operating, contact the support center.

2.2.3.6 Cautions

- The Administrators authority is required to run this command.
- The license management component (msc_license) must be installed to run this command.

2.2.4 Checking a license (msc_license_cmd --list)

2.2.4.1 Path

<WebConsole-install-path>\bin\msc_license_cmd

2.2.4.2 Format

msc_license_cmd --list

2.2.4.3 Functional description

The command outputs a list of information about registered licenses.

```
Index,LicenseName(Licensekey),LicenseNum,ExpireDate,Status
1,SystemManager G BusinessView Option(ABC-0123),1,99991231,enable
2,SystemManager G External Linker Option(ABC-1123),1,99991231,enable
3,SystemManager G WebConsole Option(ABC-2123),1,99991231,enable
4,SystemManager G Manager(ABC-3123),1,99991231,enable
```

For details on the meaning of each item, see the following.

Item name	Meaning
Index	Number (index) for uniquely identifying each license.
LicenseName	Name of the license.
Licensekey	Character string of the license key.
LicenseNum	Number of registered licenses.
ExpireDate	Expiration date of the license. Described in the YYYYMMDD format.
Status	Validity/invalidity of the license. When the license is valid, `enable` is displayed. When the license is invalid, `disable` is displayed.

2.2.4.4 Options

--list

-l

Specify this option to display a list of licenses registered in a system.

2.2.4.5 Return values

Return value	Description	Action
0	Normal end	Command execution was completed normally. No action is required.
64	Syntax error in the argument	Check for an error in the argument and run the command again using the correct syntax.
70	Internal software error An error occurred within the command.	Check whether the license management (License Component) is operating. If this error occurs while the license management is operating, contact the support center.

2.2.4.6 Cautions

- The Administrators authority is required to run this command.
- The license management component (msc_license) must be installed to run this command.

2.3 PATLITE command (msc_patlite_cmd)

This section describes the command (msc_patlite_cmd) for performing operations on Patlite of the following types.

- Serial connection type
- LAN connection type

2.3.1 Serial connection type (msc_patlite_cmd --serial)

2.3.1.1 Path

<WebConsole-install-path>\bin\msc_patlite_cmd

2.3.1.2 Format

msc_patlite_cmd --serial --host *hostname* --port *port_num* --level *level_num*

2.3.1.3 Functional description

This command cooperates with PATLITE service to operate PATLITE of the serial connection type.

Use of this command requires installation of PATLITE service bundled with the MasterScope Media.

For details about the installation method, see the manual of PATLITE service (<Media Root>\tools \Patlite\PatliteManual.pdf).

This command establishes a connection to PATLITE service. The following communication ports are used.

msc_patlite_cmd	ANY(*1)/TCP	→	PATLITE service	1 to 32767/TCP

*1 ANY indicates a port number between 1024 and 65535.

2.3.1.4 Options

--serial

This option is used to operate PATLITE of the serial connection type.

--host *host_name*

This option is used to specify the Patlite service for operating PATLITE. Specify *host_name* with the IP address or host name of a host on which PATLITE service has been installed.

--port *port_num*

This option is used to specify the port number of PATLITE service for operating PATLITE. Specify *port_num* with the communication port that was specified forPATLITE service.

--level *level_num*

This option is used to operate PATLITE. Specify level_num with the level that was set in the relay definition for PATLITE service. For details on the setup of PATLITE service, see the manual of PATLITE service (<MasterScope Root>\tools\Patlite\PatliteManual.pdf) bundled with the MasterScope Media. For PATLITE service, "0" means that PATLITE is turned off. When 012 is set, PATLITE will be turned off and then turned on at Level 1, and finally transition to Level 2.

2.3.1.5 Return values

Return value	Description	Action
0	Normal end	Command execution was completed normally. No action is required.
64	Syntax error in the argument	Check for an error in the argument and run the command again using the correct syntax.
70	Communication error	Establishment of communication with PATLITE service failed. Confirm that the system is in a state that allows it to establish communication using the specified host name and port number, and then run the command again.

2.3.1.6 Cautions

- For this command, an IPv6 address cannot be specified for host_name.
- If a problem occurs between PATLITE service of the connection destination and PATLITE, this command will terminate with a return value of "0".

2.3.2 LAN connection type (msc_patlite_cmd --lan)

2.3.2.1 Path

<WebConsole-install-path>\bin\msc_patlite_cmd

2.3.2.2 Format

msc_patlite_cmd --lan --host *hostname* --loginname *user_name*--level *level_num*

2.3.2.3 Functional description

This command uses a remote shell to operate PATLITE of the LAN connection type.

This command uses the following communication ports.

Patlite	ANY(*1)/TCP	→	msc_patlite_cmd	1022(*1)/TCP
msc_patlite_cmd	1023(*2)/TCP	→	PATLITE	514/TCP

*1 Use a port number between 512 and 1022 when a remote shell has been started and port number 1022 is used.

*2 Use a port number between 513 and 1023 when a remote shell has been started and port number 1023 is used.

2.3.2.4 Options

--lan

This option is used to operate PATLITE of the LAN connection type.

--host *host_name*

This option is used to specify PATLITE. Specify *hostname* with the IP address or host name of PATLITE.

--loginname *user_name*

This option is used to specify a user who executes the remote shell. Specify *user_name* with the login name of a user who is registered for PATLITE as a person having the execution authority over the remote shell.

--level *level_num*

This option is used to operate PATLITE. Specify level_num with a lighting type. For details about the lighting type, see the manual of PATLITE. When Model No. PHE-3FB-RYG is to be used with the default settings, the red lamp can be turned on by specifying100000.

2.3.2.5 Return values

Return value	Description	Action
0	Normal end	Command execution was completed normally. No action is required.
64	Syntax error in the argument	Check for an error in the argument and run the command again using the correct syntax.
70	Internal software error In the event of an error occurring within the command.	Contact the support center if this error occurs.

2.3.2.6 Cautions

- For this command, an IPv6 address cannot be specified for host_name.
- An OS package (rsh) is required to run this command on Linux.
- If an invalid value is set as the report level, this command will terminate with a return value of "0".

Chapter 3. WebAPI Reference

This chapter describes the API of SystemManager G.

Contents

3.1 API common specifications

3.1.1 HTTHTTP method

In APIs, the following HTTP methods are used according to the purpose.

HTTP method	Usage
GET	Obtains the existing resource information.
POST	Creates a new resource.
PET	Edits the existing resource.
DELETE	Deletes the existing resource.

3.1.2 JSOJSON

The API supports the JSON format.

- JSON specifications
  The JSON specifications conform to RFC4627.
- Character encoding
  UTF-8 is used for encoding of all character strings.

3.1.3 Request format

- URL
  The URL and query character strings are case-sensitive.
- HTTP message body
  The HTTP message body is case-sensitive.

3.1.4 RESTful API authentication method

When API gateway token authentication is enabled, check the API gateway authentication key.

1. Log in to the manager with root privileges.
2. Execute the following msc_apigateway_cmd command to retrieve the access key.

```
> cd <installation directory>/bin
> export LD_LIBRARY_PATH=<installation directory>>/lib/common:<install
ation directory>>/lib/poco
> ./msc_apigateway_cmd -t
```

   Confirm that the following is displayed in the standard output.

```
d1315acf-ed02-3a18-b624-5903908ed959
```

   Caution

   - A different value is displayed for each server on which an API gateway is installed.

3. Use the RESTful API for user authentication.

   Use the following API for user authentication.
   "3.2.1 User Authentication (page 178)"

When using the WebAPI, create the HTTP request header, as follows.

Use the following HTTP request header for authentication.

HTTP header name	Procedure	Example of a created value
X-Authorization	Specify in token XXXX format. Change XXXX to the value retrieved in "3.2.1 User Authentication (page 178)".	X-Authorization: token EBE01AC699A00496D6F5B699ED322B25
Authorization	Specify in Bearer XXXX format. Change XXXX to the id retrieved with msc_apigateway_cmd.	Authorization: Bearer d1315acf-ed02-3a18-b624-5903908ed959

3.1.5 Response format

3.1.5.1 Common HTTP status codes

The success or failure of the API is reported as an HTTP status code. HTTP status codes common to all APIs are as follows.

Code	Meaning	Description
4xx system	Client Error	Returned if a client request contains an error. Correct the client request and then make the request again.
400	Bad Request	Returned if the syntax of an HTTP request, such as a request JSON and a query character string, contains an error. Also returned if a specified parameter value is outside its allowable range even when the relevant request is written in correct syntax. Correct the HTTP request in syntax, correct the specified parameter value, and then make the request again.
404	Not Found	Returned if a specified resource is not found.
405	Method Not Allowed	Returned if an HTTP method that is not supported by the requested resource is used.
5xx system	Server Error	Returned if an error occurs within the server. Whether the request can be made again differs depending on HTTP status codes. Check the specifications of the relevant WebAPI.
500	Internal Server Error	Returned if an unexpected error occurs during the API execution. The request cannot be made again before the problem has been corrected.
503	Service Unavailable	Returned if a service is temporarily unavailable due to an overload. The request can be made again when the load is reduced some time later.

⚠ Caution

HTTP status codes other than the above are also defined for each API. For details on API-unique errors, see the specifications of the relevant API.

3.2 User authentication infrastructure

3.2.1 User Authentication

1. Process overview
   Perform user authentication to dispense an authentication token.
2. HTTP method

```
POST
```

3. URL

```
/session/new
```

4. Parameter

Parameter	Type	Description	Required	Valid values
UserID	string	User ID of the user to be authenticated	Required	-
Password	string	Password of the user to be authenticated	Required	-

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	User authentication succeeded. The combination of UserID and Password is valid.
401	Unauthorized	User authentication failed. The combination of UserID and Password is not valid.

6. Response (HTTP header)

HTTP header	Meaning	Valid values
X-Authorization	Authentication token	token authentication-token
Set-Cookie	Cookie	JSESSIONID=Authentication token

7. Response (HTTP body)

Parameter	Type	Description	Valid values
user	object	Login user information	-
user.id	string	ID of the login user	-
user.displayName	string	Display name of the login user	-
user.mailAddress	string	Email address of the login user	-

Parameter	Type	Description	Valid values
user.tenant	object	Information on the tenant to which the login user belongs.	If a user does not belong to any tenant, null is set.
user.tenant.id	string	Tenant ID	-
user.tenant.displayName	string	Tenant display name	-
user.auths	string[]	List of the authority that the login user has.	Only the authority that the login user has is selected from the following list and set. 1. MSC_USER_LIST: User list display 2. MSC_USER_DETAIL: User detail display 3. MSC_USER_CREATE: User registration 4. MSC_USER_EDIT: User change 5. MSC_USER_DELETE: User deletion 6. MSC_TENANT_LIST_SHOW: Tenant list display 7. MSC_TENANT_DETAIL_SHOW : Tenant detail display 8. MSC_TENANT_CREATE: Tenant registration 9. MSC_TENANT_EDIT: Tenant change 10. MSC_TENANT_DELETE: Tenant deletion

8. Change history
   - Version: 7.0.0
     - Newly added.
9. Example
   Example: Perform authentication for a user with user ID "UserA" and password "Password".

   [Request]

```
POST /session/new HTTP/1.1
Host: 192.168.226.215:38080
User-Agent: curl/7.53.1
Accept: */*
Content-type: application/json
Content-Length: 44

{
    "UserID": "UserA",
    "Password": "Password"
}
```

   [Response]

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=98376C0C259B6FB6C109EE1B8D564524
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
X-Authorization: token 98376C0C259B6FB6C109EE1B8D564524
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 21 Mar 2017 10:02:57 GMT

{
    "user": {
        "auths": [
            "MSC_TENANT_EDIT",
            "MSC_USER_CREATE",
            "MSC_USER_LIST",
            "MSC_TENANT_LIST_SHOW",
            "MSC_USER_DETAIL",
            "MSC_USER_EDIT",
            "MSC_TENANT_DETAIL_SHOW",
            "MSC_USER_DELETE"
        ],
        "displayName": "UserA",
        "id": "UserA",
        "mailAddress": "usera@nec.com",
        "tenant": {
            "displayName": "Tenant A",
            "id": "tenantA"
        }
    }
}
```

3.2.2 Verifying the authentication token

1. Process overview
   Judge the validity of the authentication token.
2. HTTP method

```
GET
```

3. URL

```
/session/validate
```

4. Request (HTTP header)

HTTP header	Meaning	Valid values
X-Authorization	Authentication token	token authentication-token

5. Parameter

   None

6. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The authentication token is valid.
401	Unauthorized	The authentication token is not valid.

7.

Parameter	Type	Description	Valid values
user	object	Login user information	-
user.id	string	ID of the login user	-
user.displayName	string	Display name of the login user	-
user.mailAddress	string	Email address of the login user	-
user.tenant	object	Information on the tenant to which the login user belongs.	If a user does not belong to any tenant, null is set.
user.tenant.id	string	Tenant ID	-
user.tenant.displayName	string	Tenant display name	-
user.auths	string[]	List of the authority that the login user has.	Only the authority that the login user has is selected from the following list and set. 1. MSC_USER_LIST: User list display 2. MSC_USER_DETAIL: User detail display 3. MSC_USER_CREATE: User registration 4. MSC_USER_EDIT: User change 5. MSC_USER_DELETE: User deletion 6. MSC_TENANT_LIST_SHOW: Tenant list display 7. MSC_TENANT_DETAIL_SHOW : Tenant detail display 8. MSC_TENANT_CREATE: Tenant registration 9. MSC_TENANT_EDIT: Tenant change 10. MSC_TENANT_DELETE: Tenant deletion

8. Change history
   - Version: 7.0.0
     - Newly added.
9. Example
   Example: Verify the "98376C0C259B6FB6C109EE1B8D564524" authentication token.

   [Request]

```
GET /session/validate HTTP/1.1
Host: 192.168.226.215:38080
User-Agent: curl/7.53.1
Accept: */*
X-Authorization: token 98376C0C259B6FB6C109EE1B8D564524
```

[Response]

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=4719050F8209FE02769470D5CE9BDC81; Path=/portal;
 HttpOnly
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: application/json;charset=UTF-8
Content-Length: 288
Date: Tue, 21 Mar 2017 10:08:34 GMT

{
    "user": {
        "auths": [
            "MSC_TENANT_EDIT",
            "MSC_USER_CREATE",
            "MSC_USER_LIST",
            "MSC_TENANT_LIST_SHOW",
            "MSC_USER_DETAIL",
            "MSC_USER_EDIT",
            "MSC_TENANT_DETAIL_SHOW",
            "MSC_USER_DELETE"
        ],
        "displayName": "UserA",
        "id": "UserA",
        "mailAddress": "usera@nec.com",
        "tenant": {
            "displayName": "Tenant A",
            "id": "tenantA"
        }
    }
}
```

3.2.3 Discarding the authentication token

1. Process overview
   Discard the authentication token.
2. HTTP method

```
DELETE
```

3. URL

```
/session/invalidate
```

4. Request (HTTP header)

HTTP header	Meaning	Valid values
X-Authorization	Authentication token	token authentication-token

5. Parameter

   None

6. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The authentication token was successfully discarded.

7. None

8. Change history

   - Version: 7.0.0
     - Newly added.

9. Example
   Example: Discard the "98376C0C259B6FB6C109EE1B8D564524" authentication token.

   [Request]

```
DELETE /session/invalidate HTTP/1.1
Host: 192.168.226.215:38080
User-Agent: curl/7.53.1
Accept: */*
X-Authorization: token 98376C0C259B6FB6C109EE1B8D564524
```

   [Response]

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=E15865983C32BAD72AB4539D46154EEA; Path=/portal;
 HttpOnly
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Length: 0
Date: Tue, 21 Mar 2017 10:11:58 GMT
```

3.3 Role administration

3.3.1 Getting user information

1. Process overview

   Retrieve the role set to the specified user. This is used to retrieve the current status when changing the role setting on the Web GUI.

2. HTTP method

```
GET
```

3. URL

```
/v1/auth/authorities
```

4. Parameter

None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The user information was successfully retrieved.
400	Bad Request	The request is incorrect. The parameter is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Forbidden	The resource specified in the URI does not exist. Deleted
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
user	object	User information	-
user.id	string	ID of the login user	-
user.display_name	string	Display name of the login user	-
user.mail_address	string	Email address of the login user	-
user.tenant	object	Tenant information	-
user.tenant.id	string	Tenant ID	-
user.tenant.display_name	string	Tenant display name	-
user.tenant.auths[]	string[]	Authority list	-
authority_list[]	string[]	Authority list of the SysMgrG/IoT platform	-

7. Change history

- Version: 7.0.0
  - Newly added.

8. Example

[Request]

```
GET /v1/auth/authorities HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token AF476CAB624DBB0EAC08919889BEAC36
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
```

```
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/octet-stream
Date: Wed, 22 Mar 2017 18:59:46 GMT
Transfer-Encoding: chunked
Connection: keep-alive

1ec
{"user":{
  "auths" : [
    "MSC_TENANT_EDIT",
    "MSC_USER_CREATE",
    "MSC_USER_LIST",
    "MSC_TENANT_LIST_SHOW",
    "MSC_USER_DETAIL",
    "MSC_USER_EDIT",
    "MSC_TENANT_DETAIL_SHOW",
    "MSC_USER_DELETE"
  ],
  "displayName" : "",
  "id" : "nec user",
  "mailAddress" : "nsc-user@nec.com",
  "tenant" : {
    "displayName" : "tenantA",
    "id" : "tenantA"
  }
},"authority_list":["MSC_GENERAL_REFERENCE","MSC_GENERAL_OPERATION","M
SC_GENERAL_DEFINITION"]}
0
```

3.3.2 Checking a role

1. Process overview

   Retrieve roles linked to the specified user in a list form. This is used to retrieve the current status when changing the role setting on the Web GUI.

2. HTTP method

   ```
   GET
   ```

3. URL

   ```
   /v1/auth/roles/user_id
   ```

   Specify the target user ID in ***user_id***.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Success
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
403	Forbidden	There is no access privilege.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
[n] (Array without a key)	string	Array of role names	-

7. Change history
   - Version: 7.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/auth/roles/nec-user HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 9011F0BF1A3D76787ED09F886386245F
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST,GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/octet-stream
Date: Wed, 22 Mar 2017 19:31:21 GMT
Transfer-Encoding: chunked
Connection: keep-alive

1a
["MSC_ROLE_ADMINISTRATOR","MSC_ROLE_USER","MSC_ROLE_OPERATOR"]
0
```

3.3.3 Setting a role

1. Process overview

   Set a role for a user. Set a link between the specified user and the role. If a previously configured user is selected, its role is replaced with the specified role. This is used from the Web GUI, working with the user management.

2. HTTP method

```
POST
```

3. URL

```
/v1/auth/roles/user_id
```

   Specify the target user ID in ***user_id***.

4. Parameter

Parameter	Type	Description	Required	Valid values
[n] (Array without a key)	string	Array of role names	Required	-

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Success
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
403	Forbidden	There is no access privilege.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

   None

7. Change history

   - Version: 7.0.0
     - Newly added.

8. Example

   [Request]

```
POST /v1/auth/roles/nsc-user HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 9011F0BF1A3D76787ED09F886386245F
Content-Type: application/json;charset=utf-8
```

```
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 62

["MSC_ROLE_ADMINISTRATOR","MSC_ROLE_USER","MSC_ROLE_OPERATOR"]
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST,GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/octet-stream
Date: Wed, 22 Mar 2017 19:32:06 GMT
Transfer-Encoding: chunked
Connection: keep-alive

0
```

3.4 Tenant administration

3.4.1 Deleting all tenant information simultaneously

1. Process overview

   Receive a tenant deletion notification. When this notification is received, it is forwarded to the component for which the tenant deletion notification URI is registered.

2. HTTP method

   ```
   DELETE
   ```

3. URL

   ```
   /v1/auth/tenants/tenant_id
   ```

   In ***tenant_id***, specify the deleted tenant ID.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
204	No Content	The resources of all components were successfully deleted.
404	Not Found	The resources of all components were successfully deleted (including components whose resources have already been deleted).

HTTP status code	Meaning	Description
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

   None

7. Change history

   - Version: 7.0.0
     - Newly added.

8. Example

   [Request]

```
DELETE /v1/auth/tenants/tenantB HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token AF476CAB624DBB0EAC08919889BEAC36
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 204 OK
```

3.5 Status management

3.5.1 Getting the monitoring node name list

1. Process overview

   Retrieve the node name list provided by the monitoring status management.

2. HTTP method

```
GET
```

3. URL

```
/v1/status/nodes?tenant_id=tenant_id&parent_id=parent_id&node_type=node_type
```

   In ***tenant_id***, specify the tenant ID. If omitted, the tenant ID owned by the user ID is set.

   In ***parent_id***, specify the parent group ID. For the root, specify "0". This is required.

   In ***node_type***, specify the node type under the target parent group. This is required.

   - "AGENTGROUP": Agent group

- "AGENT": Agent
- "EXLINKGROUP": External interface group
- "EXTLINKAGENT": External interface agent

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Success
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
403	Forbidden	There is no access privilege.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

   HTTP status code: When 200 - OK is returned

Parameter	Type	Description	Return value
tenant_id	string	Stores the tenant ID to which the user registering the message belongs or the tenant ID reported from the agent.	-
parent_id	string	Parent group ID of the organization node	-
node_type	string	Organization node type	"AGENT": Agent "AGENTGROUP": Agent group "EXTLINKAGENT": External interface agent "EXLINKGROUP": External interface group
severity	number	Severity used to display the icon. (Highest severity under the organization node)	Integer between 0 to 255
nodes[n]	object	A list of organization groups immediately under the node or a list of all organization agents under the node.	Set ascending order of node ID.
nodes[n].node_id	string	Organization node ID	-
nodes[n].node_type	string	Organization node ID type	"AGENT": Agent "AGENTGROUP": Agent group "EXTLINKAGENT": External interface agent

Parameter	Type	Description	Return value
			"EXLINKGROUP": External interface group
nodes[n].node_name	string	Organization node name * The setting node name varies depending on node_type. • node_type="AGENT": Agent name • node_type="AGENTGROUP": Agent group name • node_type="EXTLINKAGENT": Agent name of the external interface • node_type="EXTLINKGROUP": Group name of the external interface	-
nodes[n].severity	number	Severity used to display the organization node icon. (Highest severity in the node ID type)	Integer between 0 to 255

*Node

HTTP status code: When a status code other than 200 - OK is returned

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 7.1.0
     - The external interface types have been added to node_type.
   - Version: 7.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/status/nodes?parent_id=0&node_type=AGENTGROUP HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/octet-stream
Date: Wed, 22 Mar 2017 19:33:29 GMT
Transfer-Encoding: chunked
Connection: keep-alive

105
{
  "node_type" : "AGENTGROUP",
  "nodes" : [
    {
      "node_id" : "0000000000",
      "node_name" : "default_group",
      "node_type" : "AGENTGROUP",
      "severity" : "200"
    }
  ],
  "parent_id" : "0",
  "severity" : "200",
  "tenant_id" : "tenantA"
}
0
```

3.5.2 Getting the monitoring status list by group

1. Process overview

   Retrieve the severity list by group provided by the monitoring status management.

2. HTTP method

   ```
   GET
   ```

3. URL

   ```
   /v1/status/groups?tenant_id=tenant_id&group_id=group_id&order=order&ordered=or
   dered&group_type=group_type
   ```

   In ***tenant_id***, specify the tenant ID. If omitted, the tenant ID owned by the user ID is set.

   In ***group_id***, specify the group ID. This is required.

   In ***order***, specify ascending or descending order. If omitted, "descend" is set.

   - "ascend": Ascending
   - "descend": Descending

   In ***ordered***, specify the item name to which order is applied. If omitted, "severity" is set. In this version, only "severity" can be specified.

   In ***group_type***, specify the type to identify the group ID. If omitted, "AGENTGROUP" is set.

   - "AGENTGROUP": Agent group

- "EXLINKGROUP": External interface group

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Success
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
403	Forbidden	There is no access privilege.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

   HTTP status code: When 200 - OK is returned

Parameter	Type	Description	Return value
tenant_id	string	Tenant ID	-
group_id	string	Group ID	-
group_type	string	Group type	"AGENTGROUP": Agent group "EXLINKGROUP": External interface group
severity	number	Severity with the highest level of emergency. Highest severity in total	Integer between 0 to 255
total[n]	object	Number of nodes by monitoring severity under the group ID. Sorted in descending order by severity.	-
total[n].count	number	Number of records. Always paired with "severity".	-
total[n].severity	number	Severity. Always paired with "count".	Integer between 0 to 255
messages[n]	object	Node list in order of severity, starting from the highest	-
messages[n].node_id	string	Node ID. Unique value used to identify node.	-
messages[n].node_type	string	Node type	"AGENT": Agent "EXLINKAGENT": External interface agent
messages[n].node_name	string	Node name. This setting varies depending on node_type.	-

Parameter	Type	Description	Return value
		node_type="AGENT": Agent name node_type="EXLINKAGENT": Agent name of the external interface	
statuses	object	Message information. Set only the message with the highest severity and latest occurrence time.	-
statuses.target	string	Target Unique string in the monitoring target.	-
statuses.message_text	string	Message text	-
statuses.occurrence_time	string	Occurrence date and time	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
statuses.severity	number	Severity	Integer between 0 to 255
statuses.type	string	Type	"Agent Status": Agent status "ProcessMonitor": Process monitoring "FileMonitor": File monitoring "PortMonitor": Port monitoring "NTServiceMonitor": Service monitoring "PerformanceMonitor": Performance monitoring
statuses.state	string	Status	"running": Running "stop": Stopped "disconnect": Disconnected "disable": Disabled "unknown": Unknown "function stop": Process stopped "upper error": Upper limit error "lower error": Lower limit error "upper warning": Upper limit warning "lower warning": Lower limit warning "unmanaged": Not managed "normal": Normal "warning": Warning "fatal": Fatal error "open": Open "close": Closed
statuses.message_no	number	Message number managed by the message store	-
statuses.recoveries[]	object	Array for recovery.	-
statuses.recoveries[n].operation_type	number	Operation type when recovery is selected.	[For process monitoring] 1: Execute the start command 2: Execute the stop command

Parameter	Type	Description	Return value
			[For Windows service monitoring] 1: Start the service 2: Stop the service 3: Pause the service 4: Resume the service 5: Restart the service
statuses.display_name	string	Display name. The display name will be "target" if this item does not exist.	-

HTTP status code: When a status code other than 200 - OK is returned

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 8.0.0
     - statuses.latest_flag has been added to the response parameters.
   - Version: 7.1.0
     - group_type has been added to the query parameters.
     - recoveries[], recoveries[k].operation_type, and display_name have been added to the response parameters.
     - The external interface types have been added to node_type and node_name in the response parameters.
     - The file monitoring, port monitoring, service monitoring, and performance monitoring types have been added to statuses.type in the response parameters.
     - The targets by statuses.type have been added to statuses.target in the response parameters.
     - The statuses added in statuses.type have been added to statuses.state in the response parameters.
   - Version: 7.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/status/groups?group_id=0000000000&order=descend&ordered=severi
ty HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
```

```
Connection: keep-alive
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/octet-stream
Date: Wed, 22 Mar 2017 19:34:53 GMT
Transfer-Encoding: chunked
Connection: keep-alive

4c7
{
  "group_id" : "0000000000",
  "group_type" : "AGENTGROUP",
  "messages" : [
    {
      "node_id" : "SystemA0000000001",
      "node_name" : "Edge1",
      "node_type" : "AGENT",
      "statuses" : {
        "message_no" : "3252",
        "message_text" : "(NODE=EdgeTest)(PNAME=\/bin\/sleep1)(OLD=)(N
EW=stop)(COUNT=0)(LOWER=1)(UPPER=3)",
        "occurrence_time" : "2017-03-17T03:19:38+09:00",
        "severity" : "200",
        "state" : "stop",
        "target" : "\/bin\/sleep1",
        "type" : "ProcessMonitor",
        "latest_flag":"0"
      }
    },
    {
      "node_id" : "SystemA0000000002",
      "node_name" : "Edge2",
      "node_type" : "AGENT",
      "statuses" : {
        "message_no" : "5731",
        "message_text" : "(NODE=EdgeTest1)(PNAME=\/bin\/sleep)(OLD=)(N
EW=stop)(COUNT=0)(LOWER=1)(UPPER=3)",
        "occurrence_time" : "2017-03-17T03:52:33+09:00",
        "severity" : "200",
        "state" : "stop",
        "target" : "\/bin\/sleep",
        "type" : "ProcessMonitor",
        "latest_flag":"0"
       }
    },
    {
      "node_id" : "SystemA0000000003",
      "node_name" : "Edge3",
      "node_type" : "AGENT",
      "statuses" : {
        "message_no" : "5731",
```

```
        "message_text" : "(NODE=EdgeTest1)(PNAME=\/bin\/sleep)(OLD=)(N
EW=stop)(COUNT=0)(LOWER=1)(UPPER=3)",
        "occurrence_time" : "2017-03-18T03:52:33+09:00",
        "severity" : "50",
        "state" : "running",
        "target" : "\/bin\/sleep",
        "type" : "ProcessMonitor",
        "latest_flag":"0"
      }
    }
  ],
  "severity" : 200,
  "tenant_id" : "tenantA",
  "total" : [
    {
      "count" : 2,
      "severity" : 200
    },
    {
      "count" : 1,
      "severity" : 50
    }
  ]
}
0
```

3.5.3 Getting the monitoring status list by agent

1. Process overview

   Retrieve the monitoring status list by agent provided by the monitoring status management.

2. HTTP method

   ```
   GET
   ```

3. URL

   ```
   /v1/status/agents?tenant_id=tenant_id&group_id=group_id&agent_id=agent_id&type
   =type&order=order&ordered=ordered&group_type=group_type&target=target
   ```

   In ***tenant_id***, specify the tenant ID. If omitted, the tenant ID owned by the user ID is set.

   In ***group_id***, specify the group ID. This is required.

   In ***agent_id***, specify the agent ID. This is required.

   In ***type***, specify the monitoring type. This is required when performing extraction for each monitoring type. If omitted, all types are selected.

   - "Agent Status": Agent status
   - "ProcessMonitor": Process monitoring
   - "FileMonitor": File monitoring
   - "PortMonitor": Port monitoring
   - "NTServiceMonitor": Service monitoring
   - "PerformanceMonitor": Performance monitoring

In ***order***, specify ascending or descending order. If omitted, "descend" is set.

- "ascend": Ascending
- "descend": Descending

In ***ordered***, specify the item name to which order is applied. If omitted, "severity" is set. In this version, only "severity" can be specified.

In ***group_type***, specify the type to identify the group ID. If omitted, "AGENTGROUP" is set.

- "AGENTGROUP": Agent group
- "EXLINKGROUP": External interface group

In ***target***, specify the target. If omitted, all targets are selected. If the target is specified, type (monitoring type) is required.

- If group_type is "AGENTGROUP" with type="Agent Status", specify "Agent".
- If group_type is "AGENTGROUP" with type="ProcessMonitor", specify the process name.
- If group_type is "EXTLINKGROUP", specify the node ID of MasterScope.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Success
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
403	Forbidden	There is no access privilege.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

   HTTP status code: When 200 - OK is returned

Parameter	Type	Description	Return value
tenant_id	string	Tenant ID	-
group_id	string	Group ID	-
group_type	string	Group type	"AGENT": Agent "EXLINKAGENT": External interface agent
agent_id	string	Agent ID	-
statuses[n]	object	Message information. Set only the message with the	-

Parameter	Type	Description	Return value
		highest severity and latest occurrence time.	
statuses[n].target	string	Target Unique string in the monitoring target.	-
statuses[n].message_text	string	Message text	-
statuses[n].occurrence_time	string	Occurrence date and time	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
statuses[n].severity	number	Severity	Integer between 0 to 255
statuses[n].type	string	Type	"Agent Status": Agent status "ProcessMonitor": Process monitoring "FileMonitor": File monitoring "PortMonitor": Port monitoring "NTServiceMonitor": Service monitoring "PerformanceMonitor": Performance monitoring
statuses[n].state	string	Status	"running": Running "stop": Stopped "disconnect": Disconnected "disable": Disabled "unknown": Unknown "function stop": Process stopped "upper error": Upper limit error "lower error": Lower limit error "upper warning": Upper limit warning "lower warning": Lower limit warning "unmanaged": Not managed "normal": Normal "warning": Warning "fatal": Fatal error "open": Open "close": Closed
statuses[n].message_no	number	Message number managed by the message store	-
statuses.recoveries[]	object	Array for recovery.	-
statuses.recoveries[n].operation_type	number	Operation type when recovery is selected.	[For process monitoring] 1: Execute the start command 2: Execute the stop command [For Windows service monitoring] 1: Start the service 2: Stop the service 3: Pause the service 4: Resume the service 5: Restart the service

Parameter	Type	Description	Return value
statuses.display_name	string	Display name. The display name will be "target" if this item does not exist.	-

HTTP status code: When a status code other than 200 - OK is returned

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 8.0.0
     - statuses[n].latest_flag has been added to the response parameters.
   - Version: 7.1.0
     - group_type and target have been added to the query parameters.
     - recoveries[], recoveries[k].operation_type, and display_name have been added to the response parameters.
     - The file monitoring, port monitoring, service monitoring, and performance monitoring types have been added to statuses[n].type in the response parameters.
     - The targets by statuses.type have been added to statuses[n].target in the response parameters.
     - The statuses added in statuses.type have been added to statuses[n].state in the response parameters.
   - Version: 7.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/status/agents?group_id=0000000000&agent_id=SystemA0000000002&o
rder=descend&ordered=severity HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/octet-stream
```

```
Date: Wed, 22 Mar 2017 19:33:38 GMT
Transfer-Encoding: chunked
Connection: keep-alive

200
{
  "agent_id" : "SystemA0000000002",
  "group_id" : "0000000000",
  "group_type" : "AGENTGROUP",
  "statuses" : [
    {
      "message_no" : "5731",
      "message_text" : "(NODE=Edge1)(PNAME=\/bin\/sleep)(OLD=)(NEW=sto
p)(COUNT=0)(LOWER=1)(UPPER=3)",
      "occurrence_time" : "2017-03-17T03:52:33+09:00",
      "severity" : "200",
      "state" : "stop",
      "target" : "\/bin\/sleep",
      "type" : "ProcessMonitor",
      "latest_flag":"0"
    }
  ],
  "tenant_id" : "tenantA"
}
0
```

3.5.4 Recovery request

1. Process overview

   Request the execution of a recovery operation (service start/stop/pause/resume/restart, process start/stop).

2. HTTP method

```
PUT
```

3. URL

```
/v1/status/recoveries
```

4. Parameter

Parameter	Type	Description	Required	Valid values
tenant_id	string	Tenant ID If omitted, the tenant ID owned by the user ID for authentication is set.	Possible	-
group_id	string	Group ID	Required	-
group_type	string	Type of the specified group ID	Required	"AGENTGROUP": Agent management group "EXLINKGROUP": External interface group
agent_id	string	Agent ID	Required	-

Parameter	Type	Description	Required	Valid values
type	string	Monitoring type	Required	"ProcessMonitor": Process monitoring "NTServiceMonitor": Windows service monitoring
target	string	Target	Required	-
operation_type	number	Operation type selected for recovery	Required	[For process monitoring] 1: Execute the start command 2: Execute the stop command [For Windows service monitoring] 1: Start the service 2: Stop the service 3: Pause the service 4: Resume the service 5: Restart the service
force	string	Forcible stop (valid only for service stop/restart). If omitted, it is treated as 0 (Not forcibly stopped). This item is required to enable a recovery request again when 412 is returned after a recovery request. (The monitoring status management does not determine whether it is the first time or the second or subsequent time.)	Possible	"1": Forcibly stopped "0": Not forcibly stopped

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Success
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
403	Forbidden	There is no access privilege.
404	Not Found	The specified target was not found.
412	Precondition Failed	Precondition error: Recovery failed because a dependent service exists.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

HTTP status code: When a status code other than 200 - OK /412 - Precondition Failed is returned

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

HTTP status code: When 412 - Precondition Failed is returned

Parameter	Type	Description	Return value
message	string	Error message	"Precondition Failed": The precondition failed.
display_name	string	Windows service display name	-
target_id	string	Windows service name	-
depend_count	number	Number of dependent Windows services	-
depend	object[]	Dependent service array	-
depend[i].display_name	string	Dependent Windows service display name	-
depend[i].target_id	string	Dependent Windows service name	-

7. Change history
   - Version: 7.1.0
     - Newly added.
8. Example

   [Request]

```
PUT /v1/status/recoveries HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 1EFECD7965F72E48D98CF58078EBAE28
Content-Type: application/json;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 48

{
     "tenant_id":"tenantA",
     "group_id":"msc_extlink_0000000000",
     "group_type":"EXTLINKGROUP",
     "agent_id":"msc_extlink_TESTMGR~TESTAGENT",
     "type":"ProcessMonitor",
     "target":"18a1111f",
     "operation_type":2
}
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: PUT
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 20:46:34 GMT
Transfer-Encoding: chunked
Connection: keep-alive

0
```

3.5.5 Getting the status rate

1. Process overview

   Calculate the "status rate" by node, monitoring function type, and target from the specified condition parameters and provide the status rate.

   The status rate represents the proportion of "status" during the specified period to the history information owned by the monitoring status management.

   If the specified period is outside the range of history information owned by the monitoring status management, the correct rate may not be returned.

2. HTTP method

   ```
   POST
   ```

3. URL

   ```
   /v1/status/ratios
   ```

4. Parameter

Parameter	Type	Description	Required	Valid values
start_time	string	Start date. If omitted, the oldest data is set.	Possible	YYYY-MM-DDTHH:MM:SS ±HH:MM YYYY-MM-DDTHH:MM:SSZ Example: 2016-11-16T20:00:00+09:00
end_time	string	End date. If omitted, the reception date and time is set.	Possible	YYYY-MM-DDTHH:MM:SS ±HH:MM YYYY-MM-DDTHH:MM:SSZ Example: 2016-11-16T20:00:00+09:00
list[]	object	Condition list	Possible	-
list[i].tenant_id	string	Tenant ID If omitted, the tenant ID of the user ID is set.	Possible	-

Parameter	Type	Description	Required	Valid values
list[i].node_id	string	Node ID. Agent ID or group ID by node type. If omitted, all the agents in the tenant of the node type are selected. Reference privilege at that instant is required.	Possible	If the group ID is specified, the agent ID under the latest group ID at that instant is extracted.
list[i].node_type	string	Node type. Specify the node ID type. If omitted, "AGENT" is set.	Possible	"AGENT": Agent "EXTLINKAGENT": External interface agent "AGENTGROUP": Agent group "EXLINKGROUP": External interface group
list[i].type	string	Monitoring function type. If omitted, "Agent Status" is set.	Possible	"Agent Status": Agent status "ProcessMonitor": Process monitoring "FileMonitor": File monitoring "PortMonitor": Port monitoring "NTServiceMonitor": Service monitoring "PerformanceMonitor": Performance monitoring
list[i].statuses[]	object[]	Target array	Possible	-
list[i].statuses[j].target	string	Target If omitted, this extraction condition is not used.	Possible	Target Unique string in the monitoring target.
list[i].statuses[j].status	string	Status If omitted, the first item name (indicated by ◎) of the specified "type" is set. Example: "running" for "Agent Status"	Possible	Valid character strings differ according to the function type (type). [type="Agent Status": Agent status notification] • "running": Running ◎ • "stop": Stopped • "disconnect": Disconnected • "disable": Disabled • "unknown": Unknown

Parameter	Type	Description	Required	Valid values
				• "function stop": Process stopped [type="ProcessMonitor": Process monitoring] • "running": Running ◎ • "stop": Stopped • "upper error": Upper limit error • "unknown": Unknown • "lower error": Lower limit error • "unmanaged": Not managed [type="FileMonitor": File monitoring] • "normal": Normal ◎ • "unknown": Unknown • "warning": Warning • "fatal": Fatal error [type="PortMonitor": Port monitoring] • "open": Open ◎ • "close": Closed • "unknown": Unknown [type="NTServiceMonitor": Service monitoring] • "running": Running ◎ • "stop": Stopped • "unknown": Unknown [type="PerformanceMonitor": Performance monitoring]

Parameter	Type	Description	Required	Valid values
				• "normal": Normal ◎ • "unknown": Unknown • "upper error": Upper limit error • "lower error": Lower limit error • "upper warning": Upper limit warning • "lower warning": Lower limit warning
list[i].statuses[j].display_name	string	Display name. If omitted, this extraction condition is not used.	Possible	-

* In this version, sort order cannot be specified.

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Success
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
403	Forbidden	There is no access privilege.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Status: When 200 - OK is returned

Parameter	Type	Description	Valid values
start_time	string	Request start date. If omitted from the request, the oldest data occurrence date and time in the list[] is set.	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
end_time	string	Request end date. If omitted from the request, the receiving date and time is set.	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
list[]	object	Result list	Listed in ascending order of node ID/ monitoring function type.

Parameter	Type	Description	Valid values
list[i].tenant_id	string	Tenant ID	
list[i].node_id	string	Node ID.	
list[i].node_name	string	Node name.	
list[i].node_type	string	Node type	"AGENT": Agent "EXTLINKAGENT": External interface agent
list[i].type	string	Monitoring function type.	"Agent Status": Agent status "ProcessMonitor": Process monitoring "FileMonitor": File monitoring "PortMonitor": Port monitoring "NTServiceMonitor": Service monitoring "PerformanceMonitor": Performance monitoring
list[i].statuses[]	object[]	Target array.	Listed in ascending order of value.
list[i].statuses[j].target	string	Target	Target Unique string in the monitoring target.
list[i].statuses[j].status	string	Status	
list[i].statuses[j].display_name	string	Display name	-
list[i].statuses[j].time	string	The ratio calculation date and time	SO8601 format
list[i].statuses[j].value	number	Rate	Integer between 0 to 100

Status: When a status code other than 200 - OK is returned

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
POST /v1/status/ratios HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 9011F0BF1A3D76787ED09F886386245F
Content-Type: application/json;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

```
Content-Length:

{
"start_time":"2016-10-01T00:00:00+9:00",
"list":[
  {
    "tenant_id":"DefaultTenant",
    "node_id":"msc_extlink_WIN01~WIN01",
    "node_type":"EXTLINKAGENT",
    "type":"Agent Status",
    "statuses":[
      {
        "status":"running"
      },
      {
        "status":"stop"
      },
      {
        "status":"unknown"
      }
    ]
  },
  {
    "tenant_id":"DefaultTenant",
    "node_id":"msc_extlink_WIN01~WIN01",
    "node_type":"EXTLINKAGENT",
    "type":"ProcessMonitor",
    "statuses":[
      {
        "status":"running"
      },
      {
        "status":"stop"
      },
      {
        "status":"unknown"
      }
    ]
  }
]
}
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/octet-stream
Date: Tue, 31 Oct 2017 21:16:24 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
 "start_time":"2016-10-01T00:00:00+9:00",
 "end_time":"2016-10-31T21:16:24+9:00",
```

```
"list":[
 {
   "tenant_id":"DefaultTenant",
   "node_id":"msc_extlink_WIN01~WIN01",
   "node_name":"WIN01",
   "node_type":"EXTLINKAGENT",
   "type":"Agent Status",
   "statuses":[
     {
       "target":"1a2b3c4d",
       "status":"running",
       "display_name":"",
       "time":"2016-10-31T21:16:24+9:00",
       "value":"80.8685423"
     },
     {
       "target":"1a2b3c4d",
       "status":"stop",
       "display_name":"",
       "time":"2016-10-31T21:16:24+9:00",
       "value":"13.4733377"
     },
     {
       "target":"1a2b3c4d",
       "status":"unknown",
       "display_name":"",
       "time":"2016-10-31T21:16:24+9:00",
       "value":"5.65812"
     }
   ]
 },
 {
   "tenant_id":"DefaultTenant",
   "node_id":"msc_extlink_WIN01~WIN01",
   "node_name":"WIN01",
   "node_type":"EXTLINKAGENT",
   "type":"ProcessMonitor",
   "statuses":[
     {
       "target":"8145f578",
       "status":"running",
       "display_name":"Proc1|notepad",
       "time":"2016-10-31T21:16:24+9:00",
       "value":"50.25"
     },
     {
       "target":"8145f578",
       "status":"stop",
       "display_name":"Proc1|notepad",
       "time":"2016-10-31T21:16:24+9:00",
       "value":"49.75"
     },
     {
       "target":"8145f578",
       "status":"unknown",
       "display_name":"Proc1|notepad",
       "time":"2016-10-31T21:16:24+9:00",
       "value":"0"
```

```
        }
      ]
    }
  ]
}
```

3.5.6 Getting the monitoring status list by agent at the specified date and time

1. Process overview

   Retrieve the "monitoring status list by agent" at the specified date and time.

2. HTTP method

```
GET
```

3. URL

```
/v1/status/histories?tenant_id=tenant_id&node_id=node_id&node_type=node_type
                &time=time&type=type
                &order=order&ordered=ordered&target=target
```

In ***tenant_id***, specify the tenant ID. If omitted, the tenant ID owned by the user ID is set.

In ***node_id***, specify the group ID or agent ID. This is required. If the group ID is specified, nodes under the current group ID are selected.

In ***node_type***, specify the type to identify the node ID. If omitted, "AGENT" is set.

- "AGENTGROUP": Agent group
- "EXLINKGROUP": External interface group
- "AGENT": Agent
- "EXTLINKAGENT": External interface agent

In ***time***, specify the specified date and time. This is required.

In ***type***, specify the monitoring type. This is required when performing extraction for each monitoring type. If omitted, all types are selected.

- "Agent Status": Agent status
- "ProcessMonitor": Process monitoring
- "FileMonitor": File monitoring
- "PortMonitor": Port monitoring
- "NTServiceMonitor": Service monitoring
- "PerformanceMonitor": Performance monitoring

In ***order***, specify ascending or descending order. If omitted, "descend" is set.

- "ascend": Ascending
- "descend": Descending

In ***ordered***, specify the item name to which order is applied. If omitted, "severity" is set.

- Item name: Set the item name under response parameter "list[m].statuses[n]". Example: occurrence_time
- Multiple item names cannot be specified. For response, the order is item name + occurrence date and time + severity. (For occurrence date and time, the order is occurrence date and time + severity. For severity, the order is severity + occurrence date and time.)

In ***target***, specify the target. If omitted, all targets are selected. If the target is specified, type (monitoring type) is required.

- If group_type is "AGENTGROUP" with type="Agent Status", specify "Agent".
- If group_type is "AGENTGROUP" with type="ProcessMonitor", specify the process name.
- If group_type is "EXTLINKGROUP", specify the node ID of MasterScope.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Success
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
403	Forbidden	There is no access privilege.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

   HTTP status code: When 200 - OK is returned

Parameter	Type	Description	Valid values
list[m]	object	Node list array	-
list[m].tenant_id	string	Tenant ID	-
list[m].group_id	string	Group ID	-
list[m].group_type	string	Group type	"AGENTGROUP": Agent group "EXLINKGROUP": External interface group
list[m].agent_id	string	Agent ID	Specific string of at least one byte. Unique value used to identify the agent.
list[m].statuses[n]	object	Message information.	Set only the message with the highest severity and latest occurrence date and time.
list[m].statuses[n].target	string	Target Unique string in the monitoring target.	-

Parameter	Type	Description	Valid values
list[m].statuses[n].message_text	string	Message text	
list[m].statuses[n].occurrence_time	string	Occurrence date and time	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
list[m].statuses[n].severity	number	Severity	
list[m].statuses[n].type	string	Type	"Agent Status": Agent status "ProcessMonitor": Process monitoring "FileMonitor": File monitoring "PortMonitor": Port monitoring "NTServiceMonitor": Service monitoring "PerformanceMonitor": Performance monitoring
list[m].statuses[n].state	string	Status	• "running": Running • "stop": Stopped • "disconnect": Disconnected • "disable": Disabled • "unknown": Unknown • "function stop": Process stopped • "upper error": Upper limit error • "lower error": Lower limit error • "upper warning": Upper limit warning • "lower warning": Lower limit warning • "unmanaged": Not managed • "normal": Normal • "warning": Warning • "fatal": Fatal error • "open": Open • "close": Closed
list[m].statuses[n].message_no	number	Message number managed by the message store	
list[m].statuses[n].display_name	string	Display name	The display name will be target if this item does not exist.

HTTP status code: When a status code other than 200 - OK is returned

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 8.0.0
     - Newly added.

8. Example

[Request]

```
GET /v1/status/histories?tenant_id=DefaultTenant&node_id=msc_extlink_W
IN01~WIN01&node_type=EXTLINKAGENT
                &time=2017-11-02T23:59:59+09:0&order=ascend&ordered=oc
currence_time  HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/octet-stream
Date: Wed, 08 Nov 2017 19:33:38 GMT
Transfer-Encoding: chunked
Connection: keep-alive

200
{
  "list":[
  {
    "agent_id" : "msc_extlink_WIN01~WIN01",
    "group_id" : "0000000000",
    "group_type" : "EXTLINKAGENT",
    "statuses" : [
      {
        "message_no" : "",
        "message_text" : "",
        "occurrence_time" : "2017-10-01T15:25:00+09:00",
        "severity" : "50",
        "state" : "running",
        "target" : "WIN01",
        "type" : "Agent Status",
      },
      {
        "message_no" : "",
        "message_text" : "",
        "occurrence_time" : "2017-11-02T08:36:58+09:00",
        "severity" : "50",
        "state" : "running",
        "target" : "59df1a20",
        "type" : "ProcessMonitor",
        "display_name":"procG1|Notepad"
      }
      {
```

```
        "message_no" : "",
        "message_text" : "",
        "occurrence_time" : "2017-11-02T10:15:20+09:00",
        "severity" : "50",
        "state" : "close",
        "target" : "59df188b",
        "type" : "PortMonitor",
        "display_name":"http"
      }
    ],
    "tenant_id" : "DefaultTenant"
   }
 ]
}0
```

3.5.7 Getting the monitoring status notification list during the specified period

1. Process overview

   Retrieve the monitoring status notification list reported during the specified period. If not reported, the array of status information is 0.

2. HTTP method

   ```
   GET
   ```

3. URL

   ```
   /v1/status/histories?tenant_id=tenant_id&node_id=node_id&node_type=node_type
                  &start_time=start_time&end_time=end_time&type=type
                  &order=order&ordered=ordered&target=target
   ```

   In ***tenant_id***, specify the tenant ID. If omitted, the tenant ID owned by the user ID is set.

   In ***node_id***, specify the group ID or agent ID. This is required. If the group ID is specified, nodes under the current group ID are selected.

   In ***node_type***, specify the type to identify the node ID. If omitted, "AGENT" is set.

   - "AGENTGROUP": Agent group
   - "EXLINKGROUP": External interface group
   - "AGENT": Agent
   - "EXTLINKAGENT": External interface agent

   In ***start_time***, specify the start date and time. If omitted, the oldest date and time in the history is set.

   In ***end_time***, specify the end date and time. If omitted, the receiving date and time is set.

   In ***type***, specify the monitoring type. This is required when performing extraction for each monitoring type. If omitted, all types are selected.

   - "Agent Status": Agent status
   - "ProcessMonitor": Process monitoring

- "FileMonitor": File monitoring
- "PortMonitor": Port monitoring
- "NTServiceMonitor": Service monitoring
- "PerformanceMonitor": Performance monitoring

In ***order***, specify ascending or descending order. If omitted, "descend" is set.

- "ascend": Ascending
- "descend": Descending

In ***ordered***, specify the item name to which order is applied. If omitted, "severity" is set.

- Item name: Set the item name under response parameter "list[m].statuses[n]". Example: occurrence_time
- Multiple item names cannot be specified. For response, the order is item name + occurrence date and time + severity. (For occurrence date and time, the order is occurrence date and time + severity. For severity, the order is severity + occurrence date and time.)

In ***target***, specify the target. If omitted, all targets are selected. If the target is specified, type (monitoring type) is required.

- If group_type is "AGENTGROUP" with type="Agent Status", specify "Agent".
- If group_type is "AGENTGROUP" with type="ProcessMonitor", specify the process name.
- If group_type is "EXTLINKGROUP", specify the node ID of MasterScope.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Success
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
403	Forbidden	There is no access privilege.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

   HTTP status code: When 200 - OK is returned

Parameter	Type	Description	Valid values
list[m]	object	Node list array	Node ID ascending order
list[m].tenant_id	string	Tenant ID	-
list[m].group_id	string	Group ID	-

Parameter	Type	Description	Valid values
list[m].group_type	string	Group type	"AGENTGROUP": Agent group "EXLINKGROUP": External interface group
list[m].agent_id	string	Agent ID	Specific string of at least one byte. Unique value used to identify the agent.
list[m].statuses[n]	object	Array of status information The array is 0 if there is no status notification.	Order setting order
list[m].statuses[n].target	string	Target Unique string in the monitoring target.	-
list[m].statuses[n].message_text	string	Message text	-
list[m].statuses[n].occurrence_time	string	Occurrence date and time	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
list[m].statuses[n].severity	number	Severity	
list[m].statuses[n].type	string	Type	"Agent Status": Agent status "ProcessMonitor": Process monitoring "FileMonitor": File monitoring "PortMonitor": Port monitoring "NTServiceMonitor": Service monitoring "PerformanceMonitor": Performance monitoring
list[m].statuses[n].state	string	Status	• "running": Running • "stop": Stopped • "disconnect": Disconnected • "disable": Disabled • "unknown": Unknown • "function stop": Process stopped • "upper error": Upper limit error • "lower error": Lower limit error • "upper warning": Upper limit warning • "lower warning": Lower limit warning • "unmanaged": Not managed • "normal": Normal • "warning": Warning • "fatal": Fatal error • "open": Open • "close": Closed
list[m].statuses[n].message_no	number	Message number managed by the message store	

Parameter	Type	Description	Valid values
list[m].statuses[n].display_name	string	Display name	The display name will be target if this item does not exist.

HTTP status code: When a status code other than 200 - OK is returned

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/status/histories?tenant_id=DefaultTenant&node_id=msc_extlink_W
IN01~WIN01&node_type=EXTLINKAGENT
                &start_time=2017-11-02T00:00:00+09:0&end_time=2017-11-
02T23:59:59+09:0
                &order=ascend&ordered=occurrence_time HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/octet-stream
Date: Wed, 22 Mar 2017 19:33:38 GMT
Transfer-Encoding: chunked
Connection: keep-alive

200
{
  "list":[
  {
    "agent_id" : "msc_extlink_WIN01~WIN01",
    "group_id" : "0000000000",
    "group_type" : "EXTLINKAGENT",
    "statuses" : [
      {
        "message_no" : "",
        "message_text" : "",
        "occurrence_time" : "2017-11-02T03:52:33+09:00",
```

```
        "severity" : "100",
        "state" : "unknown",
        "target" : "59df1a20",
        "type" : "ProcessMonitor",
        "display_name":"procG1|Notepad"
      },
      {
        "message_no" : "",
        "message_text" : "",
        "occurrence_time" : "2017-11-02T08:36:58+09:00",
        "severity" : "50",
        "state" : "running",
        "target" : "59df1a20",
        "type" : "ProcessMonitor",
        "display_name":"procG1|Notepad"
      }
      {
        "message_no" : "",
        "message_text" : "",
        "occurrence_time" : "2017-11-02T10:15:20+09:00",
        "severity" : "50",
        "state" : "close",
        "target" : "59df188b",
        "type" : "PortMonitor",
        "display_name":"http"
      }
    ],
    "tenant_id" : "DefaultTenant"
   }
 ]
}
0
```

3.6 Message store

3.6.1 Viewing a message

1. Process overview

   Retrieve the specified message information. A search is made for a message based on the specified search conditions and returned. Only the specified parameters initiate a response.

2. HTTP method

```
POST
```

3. URL

```
/v1/messagestore/messages/get
```

4. Parameter

Parameter	Type	Description	Required	Valid values
query	object	Message search condition object	Required	-
query.fields	string	Specify the JSON field to be included in the response. If omitted, all fields are returned. [message_no] is always output even when it is not specified.		Set the character string in the following format. (However, URL encoding is required before use because this is written without encoding.) fields=items(Field 1+Field 2+...) Example: Configure the following to retrieve the summary and category list. fields=items(summary+category)
query.order	string	Specify ascending or descending order.		"ASCEND": Ascending order "DESCEND": Descending order Default value: "DESCEND"
query.ordered	string	Specify the parameter name to which order is applied.		In this version, only "message_no" can be specified. Default value: "message_no"
query.limit	number	Specify the maximum number of items to output based on the specified search conditions.		Integer between 1 to 1000 Default value: 100
query.message_no	number	Specify the number as the start point of the messages to retrieve. A list of messages from the specified number to the set maximum number is retrieved. Messages are sorted in the order specified in the [order] parameter and are retrieved up to the number set in the [limit] parameter. If omitted, this parameter is not included in the search conditions.		Integer between 1 to 9223372036854775807
query.tenant_id	string	If the [agent_group_id] parameter is set in the message search conditions, this parameter also needs to be specified.		Up to 64 characters

Parameter	Type	Description	Required	Valid values
		This is available only to administrator users. For general users, the tenant ID of the tenant to which the user belongs is selected. If [tenant_id] is omitted, the tenant ID is retrieved from the session key of the specified HTTP header. If the tenant ID cannot be retrieved from the session key either, error 400 is returned. General users must not specify this parameter because a privilege error occurs if a tenant other than that to which the general user belongs is specified.		
query.agent_group_id	string	Retrieves messages for agents under an agent group that perfectly matches the specified agent group ID. If [agent_group_id] is set in the message search conditions, [tenant_id] also needs to be specified. If [tenant_id] is omitted, the tenant ID is retrieved from the session key of the specified HTTP header. If the tenant ID cannot be retrieved from the session key either, error 400 is returned. If the [agent_group_recursive] parameter is set to true, messages for agents under the specified agent group are returned. If this parameter is set to false or is omitted, messages for agents		Up to 512 characters

Parameter	Type	Description	Required	Valid values
		immediately under the specified group are returned. If omitted, this parameter is not included in the search conditions.		
query.agent_group_recursive	boolean	Specify whether agents under the specified agent group are to be retrieved recursively.		true: Retrieve recursively false: Retrieve only under the target group Default value: false
query.node_id	string	Extracts records that perfectly match the specified node ID. If omitted, this parameter is not included in the search conditions.		Up to 128 characters
query.component_type	string	Extracts records that perfectly match the specified component type. If omitted, this parameter is not included in the search conditions.		Up to 32 characters
query.node_type	string	Extracts records that perfectly match the specified node type. If omitted, this parameter is not included in the search conditions.		"MANAGER": Messages issued by the manager "AGENT": Messages reported from the agent For other agent types, enter a specific character string. If multiple values are specified, combine them with "+" (Example: "MANAGER +AGENT").
query.node_name	string	Extracts records with a node name that matches the specified search string. If omitted, this parameter is not included in the search conditions.		Up to 256 characters If the [reg_check] parameter is set to true, use a regular expression (compliant with POSIX) string for the search conditions. If the [reg_check] parameter is set to false, use a partial string for the search conditions.
query.system_name	string	Extracts records that perfectly match the specified system name. Specify the machine name. If omitted, this parameter is not		Up to 256 characters

Parameter	Type	Description	Required	Valid values
		included in the search conditions.		
query.application	string	Extracts records that perfectly match the specified application. If omitted, this parameter is not included in the search conditions.		Up to 1024 characters
query.object	string	Extracts records that perfectly match the specified object. If omitted, this parameter is not included in the search conditions.		Up to 1024 characters
query.category	string	Extracts records that perfectly match the specified type. If omitted, this parameter is not included in the search conditions.		"SYSTEM": System "APPLICATION": Application If multiple values are specified, combine them with "+" (Example: "SYSTEM +APPLICATION").
query.severity	string	Specify the severity of the message to be retrieved. If omitted, this parameter is not included in the search conditions.		If multiple values are specified, combine them with "+" (Example: "10+40+100"). Integer between 0 to 255 • 200: Abnormal • 150: Warning • 100: Unknown • 50: Normal • 15: No severity • 10: Monitoring stopped
query.summary	string	Extracts records with a message overview that matches the specified search string. If omitted, this parameter is not included in the search conditions.		Up to 256 characters If the [reg_check] parameter is set to true, use a regular expression (compliant with POSIX) string for the search conditions. If the [reg_check] parameter is set to false, use a partial string for the search conditions.
query.start_create_time	string	Extracts messages with an occurrence date and time after the specified time. If omitted, this parameter is not included in the search conditions.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00

Parameter	Type	Description	Required	Valid values
query.end_create_time	string	Extracts messages with an occurrence date and time before the specified time. If omitted, this parameter is not included in the search conditions.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
query.start_receive_time	string	Extracts messages with a receiving time after the specified time. If omitted, this parameter is not included in the search conditions.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
query.end_receive_time	string	Extracts messages with a receiving time before the specified time. If omitted, this parameter is not included in the search conditions.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
query.timezone	string	Specify the time zone for the time parameters, such as the output occurrence date and time and receiving time. Specify the offset value relative to UTC (Example: "+9"). [create_time] and [recieve_time] in the response are converted and returned according to the specified time zone. (Example: "+9" returns "2016-11-16T19:00:00 +09:00". "+0" returns "2016-11-16T10:00:00 +00:00". "-5" returns "2016-11-16T05:00:00 -05:00". "-3.5" returns "2016-11-16T06:30:00 -03:30".)		Up to 256 characters

Parameter	Type	Description	Required	Valid values
		If omitted, the time zone of the manager machine is used.		
query.confirm	string	Extracts records that perfectly match the specified check flag. If omitted, this parameter is not included in the search conditions.		"UNCHECKED": Not checked "CHECKED": Checked If multiple values are specified, combine them with "+" (Example: "UNCHECKED +CHECKED").
query.mark	string	Extracts records that perfectly match the specified mark.		User-specific string. "CHECKING", "SOLVED", etc. If multiple values are specified, combine them with "+" (Example: "CHECKING +SOLVED").
query.comment	string	Extracts records with a comment that matches the specified search string. If omitted, this parameter is not included in the search conditions.		Up to 1024 characters If the [reg_check] parameter is set to true, use a regular expression (compliant with POSIX) string for the search conditions. If the [reg_check] parameter is set to false, use a partial string for the search conditions.
query.message_id	string	Extracts records that perfectly match the specified message ID.		Up to 128 characters
query.message_text	string	Extracts records with a message text that matches the specified search string. If omitted, this parameter is not included in the search conditions.		Up to 1024 characters If the [reg_check] parameter is set to true, use a regular expression (compliant with POSIX) string for the search conditions. If the [reg_check] parameter is set to false, use a partial string for the search conditions.
query.report_status_id	string	Extracts records that perfectly match the specified service notification status ID. If this parameter is set in the search conditions, search parameters other than [fields], [order], [ordered], and [limit] cannot be specified simultaneously. If omitted, this parameter is not included in the search conditions.		If multiple values are specified, combine them with "+" (Example: "10+40+100").

Parameter	Type	Description	Required	Valid values
query.report_total_status	string	Extracts records that perfectly match the specified total service notification status. "SUCCESS", "PROCESSING", "ERROR", or "NONE" is set. This is the status combining multiple service notification statuses (report_statuses). "PROCESSING" is set when one of the service notification statuses is "PROCESSING". When there is no "PROCESSING", if one of the service notification statuses is "ERROR", this parameter is set to "ERROR". When there is no "PROCESSING" or "ERROR", it is set to "SUCCESS". If omitted, this parameter is not included in the search conditions.		"SUCCESS": Normal end "PROCESSING": Reporting "ERROR": Abnormal end "NONE": Not target If multiple values are specified, combine them with "+" (Example: "PROCESSING+ERROR").
query.definition_code	string	Extracts records that perfectly match the specified message definition ID. If omitted, this parameter is not included in the search conditions.		If multiple values are specified, combine them with "+" (Example: "10+40+100").
query.business_node_id	string	Extracts records that perfectly match the specified business node ID. If omitted, this parameter is not included in the search conditions.		Only business node ID with the type set to business category (node_type="CATEGORY") For details, see "3.8.2 Registering a business category (page 292)". Up to 36 characters
query.reg_check	bool	Specify the method to be used to search the node_name, summary, comment, and message_text parameters.		true: The [node_name], [summary], [comment], and [message_text] parameters are searched using regular expressions. false: The [node_name], [summary], [comment], and [message_text] parameters are searched using partial strings.

Parameter	Type	Description	Required	Valid values
				Default value: true

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	A list of messages was successfully retrieved.
400	Bad Request	The specified query condition is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The specified message is not found.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
messages[n]	object[]	Message object	-
messages[n].message_id	string	Message ID. ID indicating the message type	Up to 128 characters
messages[n].definition_code	string	ID indicating the message definition used to generate a message text. Unique ID on the system.	Up to 32 characters
messages[n].receipt_no	number	Delivery confirmation number	Integer between 1 to 9223372036854775807
messages[n].tenant_id	string	Stores the tenant ID to which the user registering the message belongs or the tenant ID reported from the agent.	Up to 64 characters
messages[n].component_type	string	Stores the component type of the service where the message was registered.	Up to 32 characters
messages[n].severity	number	Severity	Integer between 0 to 255 • 200: Abnormal • 150: Warning • 100: Unknown • 50: Normal • 15: No severity • 10: Monitoring stopped
messages[n].create_time	string	Occurrence time. Example: 2016-11-16T20:00:00+09:00 If omitted, the same time as the receiving time on the manager is set.	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00

Parameter	Type	Description	Valid values
messages[n].system_name	string	Stores the manager name, or the machine name for the external AP.	Up to 256 characters
messages[n].node_id	string	Unique ID indicating the node that created the message. If the message is reported from the agent, the agent ID is set.	Up to 128 characters
messages[n].node_type	string	"MANAGER" for messages issued by the manager. "AGENT" or other agent types for messages reported from the agent. For other messages, any string is set.	Up to 32 characters
messages[n].node_name	string	Stores the node name. If the [node_type] parameter is set to "MANAGER", the manager name is stored. If the parameter is set to "AGENT", the agent name is stored. For other external interface products, any string indicating the node that triggered the message is stored.	Up to 256 characters
messages[n].application	string	Stores the monitoring function name. The name of the monitoring function that reported the message, such as "SysLog monitoring", "Process monitoring", "LogFile monitoring", or "Performance monitoring", is stored.	Up to 1024 characters
messages[n].object	string	Stores the monitoring name, instance name, or object name. The setting name indicating the monitoring setting, such as facility in SysLog monitoring, process name in process monitoring, or log file name in Log file monitoring, is stored.	Up to 1024 characters
messages[n].category	string	For system messages indicating a system failure, "SYSTEM" is stored. This parameter is basically required but can be omitted when the message definition ID, which defines the category in the	"SYSTEM": System "APPLICATION": Application

Parameter	Type	Description	Valid values
		message definition file, is specified.	
messages[n].summary	string	Message overview	Up to 256 characters
messages[n].message_no	number	Message number	Integer between 1 to 9223372036854775807
messages[n].receive_time	string	Date and time at which the message was received on the manager.	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
messages[n].message_text	string	Message text (after setting embedded text)	Up to 8192 characters
messages[n].confirm	string	Check flag	"UNCHECKED": Not checked "CHECKED": Checked
messages[n].mark	string	Mark	User-specific string. "CHECKING", "SOLVED", etc. Up to 64 characters
messages[n].comment	string	Comment	Up to 64 characters
messages[n].report_total_status	string	Total service notification status. "SUCCESS", "PROCESSING", "ERROR", or "NONE" is set. This is the status combining multiple service notification statuses (report_statuses). "PROCESSING" is set when one of the service notification statuses is "PROCESSING". When there is no "PROCESSING", if one of the service notification statuses is "ERROR", this parameter is set to "ERROR". When there is no "PROCESSING" or "ERROR", it is set to "SUCCESS".	Up to 64 characters
messages[n].report_statuses[m]	object[n]	Service notification status	
messages[n].report_statuses[m].report_status_id	number	Service notification status ID. Specify the target service notification status ID.	Integer between 1 to 9223372036854775807
messages[n].report_statuses[m].status	string	Service notification status. Specify "SUCCESS", "PROCESSING", "ERROR", or "NONE".	Default value: NONE
messages[n].report_statuses[m].component_type	string	Component type of the notification destination service. Requests the	Up to 32 characters

Parameter	Type	Description	Valid values
		RestAPI of the micro service of specified component type and reports that the message has been registered.	
messages[n].report_statuses[m].trigger_id	string	Transfer ID to the notification destination service. This is an ID that is set arbitrarily by the micro service of specified component type. If the notification destination service is the reporting service, report_form_id (reporting ID) is set.	Up to 64 characters
messages[n].report_statuses[m].id	string	Filter ID of the filter setting that triggered the reporting. A unique UUID is assigned by the system when created. This parameter must be set when updating the filter setting. If omitted, it is treated as a new filter to be added.	Up to 64 characters
messages[n].business_node_id	string[]	Array of business node IDs	Only business node ID with the type set to business category (node_type="CATEGORY")

* Parameters with null data set are omitted from the response.

7. Change history
   - Version: 8.0.0
     - Newly added.
     - A correction has been made so that the time difference relative to Greenwich Mean Time must be specified in query.timezone.

8. Example

   [Request]

```
POST /v1/messagestore/messages/get HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Content-Type: application/json;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 356

{
   "query": {
```

```
      "agent_group_id": "0000000000",
      "agent_group_recursive": false,
      "category": "APPLICATION",
      "confirm": "UNCHECKED",
      "fields": "items(node_name+severity+mark+create_time+receive_tim
e+confirm+message_text+application+object+message_id+report_total_stat
us)",
      "limit": 11,
      "order": "DESCEND",
      "report_total_status": "SUCCESS+ERROR+PROCESSING+NONE",
      "timezone": "+9"
   }
}
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 19:34:58 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
   "messages": [
      {
         "application": "StatusMonitor",
         "business_node_id": [],
         "confirm": "UNCHECKED",
         "create_time": "2017-03-17T03:52:33+09:00",
         "mark": "PROCESSING",
         "message_id": "1100002",
         "message_no": 5730,
         "message_text": "(NODE=EdgeTest1)(PNAME=/bin/sleep)(OLD=)(NEW
=stop)(COUNT=0)(LOWER=1)(UPPER=3)",
         "node_name": "Edge1",
         "object": "ProcessMonitor",
         "receive_time": "2017-03-18T06:49:47+09:00",
         "report_statuses": [],
         "report_total_status": "NONE",
         "severity": 200
      },
      {
         "application": "StatusMonitor",
         "business_node_id": [
            "565326d2fe21bc89590baf82b43573ba"
         ],
         "confirm": "UNCHECKED",
         "create_time": "2017-03-17T03:55:23+09:00",
         "mark": "",
         "message_id": "1110000",
         "message_no": 3270,
         "message_text": "(PROCESS=/bin/sleep)(CONFNAME=ProcessDefinit
ion)",
         "node_name": "Edge1",
```

```
            "object": "ProcessMonitor",
            "receive_time": "2017-03-17T03:56:14+09:00",
            "report_statuses": [],
            "report_total_status": "NONE",
            "severity": 150
        }
    ]
}
```

3.6.2 Updating a message

1. Process overview

   Update a message. The parameters that can be updated are check flag, comment, and mark.

2. HTTP method

```
PUT
```

3. URL

```
/v1/messagestore/messages
```

4. Parameter

Parameter	Type	Description	Required	Valid values
messages[n]	object	Message object	Required	-
messages[n].message_no	number	Specify the message number of the message to be updated.	Required	Integer between 1 to 9223372036854775807
messages[n].confirm	string	Check flag		"UNCHECKED": Not checked "CHECKED": Checked
messages[n].mark	string	Specify the mark string.		Up to 64 characters
messages[n].comment	string	Specify the comment.		Up to 1024 characters

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The message was successfully updated.
400	Bad Request	The specified message number is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The specified message is not found.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
messages[n]	object	Message object	-

Parameter	Type	Description	Valid values
messages[n].message_id	string	Message ID. ID indicating the message type	Up to 128 characters
messages[n].definition_code	string	ID indicating the message definition used to generate a message text. Unique ID on the system.	Up to 32 characters
messages[n].receipt_no	number	Delivery confirmation number	Integer between 1 to 9223372036854775807
messages[n].tenant_id	string	Stores the tenant ID to which the user registering the message belongs or the tenant ID reported from the agent.	Up to 64 characters
messages[n].component_type	string	Stores the component type of the service where the message was registered.	Up to 32 characters
messages[n].severity	number	Severity	Integer between 0 to 255 • 200: Abnormal • 150: Warning • 100: Unknown • 50: Normal • 15: No severity • 10: Monitoring stopped
messages[n].create_time	string	Occurrence time. Example: 2016-11-16T20:00:00+09:00 If omitted, the same time as the receiving time on the manager is set.	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
messages[n].system_name	string	Stores the manager name, or the machine name for the external AP.	Up to 256 characters
messages[n].node_id	string	Unique ID indicating the node that created the message. If the message is reported from the agent, the agent ID is set.	Up to 128 characters
messages[n].node_type	string	"MANAGER" for messages issued by the manager. "AGENT" or other agent types for messages reported from the agent. For other messages, any string is set.	Up to 32 characters
messages[n].node_name	string	Stores the node name. If the [node_type] parameter is set to "MANAGER", the manager name is stored. If the parameter is set to "AGENT", the agent name is stored. For other external interface	Up to 256 characters

Parameter	Type	Description	Valid values
		products, any string indicating the node that triggered the message is stored.	
messages[n].application	string	Stores the monitoring function name. The name of the monitoring function that reported the message, such as "SysLog monitoring", "Process monitoring", "LogFile monitoring", or "Performance monitoring", is stored.	Up to 1024 characters
messages[n].object	string	Stores the monitoring name, instance name, or object name. The setting name indicating the monitoring setting, such as facility in SysLog monitoring, process name in process monitoring, or log file name in Log file monitoring, is stored.	Up to 1024 characters
messages[n].category	string	For system messages indicating a system failure, "SYSTEM" is stored. This parameter is basically required but can be omitted when the message definition ID, which defines the category in the message definition file, is specified.	"SYSTEM": System "APPLICATION": Application
messages[n].summary	string	Message overview	Up to 256 characters
messages[n].message_no	number	Message number	Integer between 1 to 9223372036854775807
messages[n].receive_time	string	Date and time at which the message was received on the manager.	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
messages[n].message_text	string	Message text (after setting embedded text)	Up to 8192 characters
messages[n].confirm	string	Check flag	"UNCHECKED": Not checked "CHECKED": Checked
messages[n].mark	string	Mark	User-specific string. "CHECKING", "SOLVED", etc. Up to 64 characters
messages[n].comment	string	Comment	Up to 64 characters
messages[n].report_total_status	string	Total service notification status. "SUCCESS", "PROCESSING",	Up to 64 characters "SUCCESS": Normal end "PROCESSING": Reporting "ERROR": Abnormal end "NONE": Not target

Parameter	Type	Description	Valid values
		"ERROR", or "NONE" is set. This is the status combining multiple service notification statuses (report_statuses). "PROCESSING" is set when one of the service notification statuses is "PROCESSING". When there is no "PROCESSING", if one of the service notification statuses is "ERROR", this parameter is set to "ERROR". When there is no "PROCESSING" or "ERROR", it is set to "SUCCESS".	
messages[n].report_statuses[m]	object[n]	Service notification status	
messages[n].report_statuses[m].report_status_id	number	Service notification status ID. Specify the target service notification status ID.	Integer between 1 to 9223372036854775807
messages[n].report_statuses[m].status	string	Service notification status. Specify "SUCCESS", "PROCESSING", "ERROR", or "NONE".	Default value: NONE
messages[n].report_statuses[m].component_type	string	Component type of the notification destination service. Requests the RestAPI of the micro service of specified component type and reports that the message has been registered.	Up to 32 characters
messages[n].report_statuses[m].trigger_id	string	Transfer ID to the notification destination service. This is an ID that is set arbitrarily by the micro service of specified component type. If the notification destination service is the reporting service, report_form_id (reporting ID) is set.	Up to 64 characters
messages[n].report_statuses[m].id	string	Filter ID of the filter setting that triggered the reporting. A unique UUID is assigned by the system when created. This parameter must be set when updating the filter setting. If omitted, it is treated as a new filter to be added.	Up to 64 characters

Parameter	Type	Description	Valid values
messages[n].business_node_id	string[]	Array of business node IDs	Only business node ID with the type set to business category (node_type="CATEGORY")

* Parameters with null data set are omitted from the response.

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
PUT /v1/messagestore/messages HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 1EFECD7965F72E48D98CF58078EBAE28
Content-Type: application/json;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 48

{
   "messages": [
      {
         "mark": "OPEN",
         "message_no": 5730
      }
   ]
}
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: PUT
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 20:46:34 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
   "messages": [
      {
         "application": "Unified Management Framework",
         "business_node_id": [
            "565326d2-fe21-bc89-590b-af82b43573ba"
         ],
         "category": "APPLICATION",
         "comment": "pending",
```

```
          "component_type": "msc_messagestore",
          "confirm": "UNCHECKED",
          "create_time": "2017-03-17T03:52:33+09:00",
          "definition_code": "1100002",
          "mark": "OPEN",
          "message_id": "1100002",
          "message_no": 5730,
          "message_text": "(NODE=Edge2)(PNAME=/bin/sleep)(OLD=)(NEW=sto
p)(COUNT=0)(LOWER=1)(UPPER=3)",
          "node_id": "SystemA0000000002",
          "node_name": "nodeA",
          "node_type": "AGENT",
          "object": "ProcessMonitor",
          "receive_time": "2017-03-18T06:49:47+09:00",
          "report_total_status":"SUCCESS",
          "report_statuses": [
             "report_status_id":100,
             "status":"SUCCESS",
             "component_type":"msc_report",
             "trigger_id":"418cd607-11a7-11e8-ac5d-0050569b1682",
             "id":"418cd608-11a7-11e8-a83a-0050569b1682"
          ],
          "report_total_status": "NONE",
          "severity": 200,
          "summary": "summary",
          "system_name": "SystemA",
          "tenant_id": "tenantA"
       }
    ]
}
```


3.6.3 Viewing a filter

1. Process overview

   Retrieve all the filter settings for the tenant to which the executing user belongs. All the filters for the tenant to which the specified user belongs are returned.

2. HTTP method

   ```
   GET
   ```

3. URL

   ```
   /v1/messagestore/filters
   ```

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The filter information was successfully retrieved.
401	Unauthorized	Authentication error. The request has no required authentication token.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
filter[n]	object[]	Filter setting	-
filter[n].id	string	Filter ID A unique UUID is assigned by the system when created. This parameter must be set when updating the filter setting. It is not necessary when making a new addition.	Up to 36 characters consisting of hexadecimal numbers and hyphens
filter[n].name	string	Filter name	-
filter[n].type	string	Type. Specify "EXCLUDE" to suppress reporting when it matches the filter.	"STORE": Store "EXCLUDE": Exclude
filter[n].status	string	Filter operating status. Only filters with the "STARTING" status are applied.	"STARTING": Starting "SUSPENDED": Stopping
filter[n].report_status	string	Operating status of the reporting setting in the message filter.	Enabled : Only for those message filters with the "STARTING" status, the reporting setting is enabled. Disabled : If the "SUSPENDED" status is set, all the reporting settings set in the filter are disabled.
filter[n].message_id	string	Message ID ID indicating the message type Use regular expressions. (Perfect match example: "^String$"). If omitted, this filter condition is ignored.	-
filter[n].not_message_id	boolean	Not (Message ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].definition_code	string	Message definition ID ID indicating the message definition used to generate a message text. Create this such that it is unique within the system.	-
filter[n].not_definition_code	boolean	Not (Message definition ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].severity	number	Specify the severity with a number. If omitted, this filter condition is ignored.	Integer between 0 to 255
filter[n].not_severity	boolean	Not (Severity)	false: Select matched messages. true: Select unmatched messages.
filter[n].severity_range	string	Severity range	">=": [severity] parameter or more "=": equal to [severity] parameter "<=": [severity] parameter or less
filter[n].confirm	string	Check flag	"UNCHECKED": Not checked

Parameter	Type	Description	Valid values
			"CHECKED": Checked
filter[n].not_confirm	boolean	Not (Check flag)	false: Select matched messages. true: Select unmatched messages.
filter[n].mark	string	Mark User-specific string. "CHECKING", "SOLVED", etc.	-
filter[n].not_mark	boolean	Noty (Mark)	false: Select matched messages. true: Select unmatched messages.
filter[n].comment	string	Comment	-
filter[n].not_comment	boolean	Not (Comment)	false: Select matched messages. true: Select unmatched messages.
filter[n].agent_group_tenant_id	string	Tenant ID of the tenant to which the agent group specified in [agent_group_id] belongs. To specify [agent_group_id] in the filter parameter, [agent_group_tenant_id] of the tenant to which the target agent group belongs must be specified.	-
filter[n].agent_group_id	string	Agent group ID. To specify [agent_group_id], [agent_group_tenant_id] must be specified. Use this parameter when filtering messages under the specified agent group. Filters messages for agents under the specified agent group. Regular expressions cannot be used. Use a perfectly matched character string. Even when [agent_group_id] is specified, if the [node_id] parameter is not set in the parameter of the reported message, the message is not filtered. Even when [agent_group_id] is specified, if the [node_type] parameter of the reported message is other than "AGENT", the message is not filtered.	-
filter[n].not_agent_group_id	boolean	Not (Agent group ID)	false: Select matched messages. true: Select unmatched messages.

Parameter	Type	Description	Valid values
filter[n].agent_group_recursive	boolean	When filtering messages for agents under the specified agent group, specify whether to filter all the agents recursively or agents immediately under the specified agent group.	true: Retrieve recursively false: Retrieve only agents immediately under the target group Default: false
filter[n].system_name	string	System name of the manager Stores the machine name.	-
filter[n].not_system_name	boolean	Not (System name)	false: Select matched messages. true: Select unmatched messages.
filter[n].node_id	string	Node ID. This matches the filter when the message for the specified node ID is registered.	-
filter[n].not_node_id	boolean	Not (Node ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].node_type	string	Extracts records that perfectly match the specified node type. Enter "MANAGER" for those messages that were issued by the manager, "AGENT" or a relevant agent type for those messages that were reported from the agent, or any string for other messages. If omitted, this filter condition is ignored.	-
filter[n].not_node_type	boolean	Not (Node type)	false: Select matched messages. true: Select unmatched messages.
filter[n].node_name	string	Node name. If omitted, this filter condition is ignored.	-
filter[n].not_node_name	boolean	Not (Node name)	false: Select matched messages. true: Select unmatched messages.
filter[n].application	string	Application. This matches the filter when a message for the specified application is registered. If omitted, this filter condition is ignored.	-
filter[n].not_application	boolean	Not (Application)	false: Select matched messages. true: Select unmatched messages.
filter[n].object	string	Object. This matches the filter when a message for the specified object is	-

Parameter	Type	Description	Valid values
		registered. If omitted, this filter condition is ignored.	
filter[n].not_object	boolean	Not (Object)	false: Select matched messages. true: Select unmatched messages.
filter[n].category	string	Type. If omitted, this filter condition is ignored.	"SYSTEM" "APPLICATION"
filter[n].not_category	boolean	Not (Type)	false: Select matched messages. true: Select unmatched messages.
filter[n].message_summary	string	Message overview. This matches the filter when a message for the specified message overview is registered. If omitted, this filter condition is ignored.	-
filter[n].not_message_summary	boolean	Not (Description)	false: Select matched messages. true: Select unmatched messages.
filter[n].message_text	string	Message text. This matches the filter when a message for the specified message text is registered. If omitted, this filter condition is ignored.	-
filter[n].not_message_text	boolean	Not (Message text)	false: Select matched messages. true: Select unmatched messages.
filter[n].tenant_id	string	Tenant ID of the tenant that created the filter.	-
filter[n].component_type	string	Component type of the micro service that created the filter.	-
filter[n].operation_type	string	Processing type "NONE" is always selected for the response.	"NONE": No change
filter[n].report[m]	object[]	Service notification setting	-
filter[n].report[m].component_type	string	Component type of the notification destination service Requests the RestAPI of the micro service of specified component type and reports that the message has been registered.	-
filter[n].report[m].trigger_id	string	Transfer ID to the notification destination service This is an ID that is set arbitrarily by the micro	-

Parameter	Type	Description	Valid values
		service of specified component type.	
filter[n].report[m].report_id	string	Service notification setting ID This parameter must be specified if "UPDATE" is set to the filter setting processing type (filter[n].operation_type). For values other than "UPDATE", this is ignored. A unique UUID is assigned by the system when created. This parameter must be set when updating the service notification setting.	-
filter[n].report[m].operation_type	string	Processing type Specify newly add, update, delete, or no change for each service notification setting. This parameter is required for a request. "NONE" is always selected for the response.	"NONE": No change

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/messagestore/filters HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
```

```
Date: Wed, 22 Mar 2017 19:33:03 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
    "filter": [
        {
            "agent_group_id": "msc_extlink_0000000002",
            "agent_group_recursive": false,
            "application": "Unified Management Framework",
            "category": "APPLICATION",
            "comment": "pending",
            "confirm": "UNCHECKED",
            "definition_code":"2000000000",
            "id": "9c96d4ec-0e78-11e7-8df0-005056b66332",
            "mark": "PROCESSING",
            "message_id": "00080003",
            "message_summary": "summary",
            "message_text": "abcdefghijklmnopqrstuvwxyz1234567890",
            "name": "filter name",
            "node_id": "msc_extlink_MANAGER~AGENT",
            "node_name": "nodeA",
            "node_type": "AGENT",
            "not_agent_group_id": false,
            "not_application": false,
            "not_category": false,
            "not_comment": false,
            "not_confirm": false,
            "not_mark": false,
            "not_message_id": false,
            "not_message_summary": false,
            "not_message_text": false,
            "not_node_id": false,
            "not_node_name": false,
            "not_node_type": false,
            "not_object": false,
            "not_severity": false,
            "not_system_name": false,
            "object": "ProcessMonitor",
            "operation_type": "NONE",
            "report" : [
                {
                    "component_type" : "msc_report",
                    "trigger_id" : "b4932012-de12-81e3-876a-83d0517323
01",
                    "operation_type" : "NONE",
                    "report_id" : "a82229f4-0e7a-11e7-a074-005056b6633
2"
                }
            ],
            "severity": 150,
            "severity_range":"=",
            "status": "STARTING",
            "report_status":"STARTING",
            "system_name": "System1",
            "tenant_id": "DefaultTenant",
            "type": "STORE"
        }
```

```
    ]
}
```

3.6.4 Uploading all filters simultaneously

1. Process overview

   Newly add, update, or delete a filter setting. Specify "ADD" (newly add), "UPDATE" (update), "DELETE" (delete), or "NONE" (no change) in the [operation_type] request parameter.

   If operation_type is set to "ADD", it is treated as a new filter to be added.

   If operation_type is set to "UPDATE", specify the filter ID you want to update and then update the parameter. String-type request parameters without this setting are updated without filter conditions.

   If operation_type is set to "DELETE", the filter setting is deleted.

   If operation_type is set to "NONE", the filter setting is ignored and not changed.

   In the filter list and response after upload, operation_type is always set to "NONE".

   To change the filter application priority, change the filter list order in the body message.

   The filters are applied in list order. In the filter list and response after upload, the priority order is applied.

   A filter setting not requested in the body message is ignored and not changed but is set to the lowest priority.

   If omitted, string-type request parameters are updated without filter conditions.

2. HTTP method

```
POST
```

3. URL

```
/v1/messagesore/filters/import
```

4. Parameter

Parameter	Type	Description	Required	Valid values
filter[n]	object[]	Filter definition setting	Required	Up to 36 characters consisting of hexadecimal numbers and hyphens
filter[n].id	string	Filter ID. A unique UUID is assigned by the system when created. This parameter must be set when updating the filter setting. It is not necessary when making a new addition.	-	Up to 64 characters
filter[n].name	string	Filter name	-	Up to 128 characters

Parameter	Type	Description	Required	Valid values
filter[n].type	string	Type. Specify "EXCLUDE" to suppress reporting when it matches the business message filter.	-	"STORE": Store "EXCLUDE": Exclude Default value: STORE Up to 16 characters
filter[n].status	string	Filter operation state	-	"STARTING": Starting "SUSPENDED": Stopping Default value: "STARTING" Up to 16 characters
filter[n].report_status	string	Operating status of the reporting setting in the message filter. Enabled : Only for those message filters with the [STARTING] status, the reporting setting is enabled. Disabled : If the [SUSPENDED] status is set, all the reporting settings set in the filter are disabled.	-	"STARTING": Enabled "SUSPENDED": Disabled Default value: "STARTING" Up to 16 characters
filter[n].message_id	string	Message ID. Specify the message type ID. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_message_id	boolean	Not (Message ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].definition_code	string	Message definition ID. ID indicating the message definition used to generate a message text. Create this such that it is unique within the system. Use regular expressions (perfect match example: "^String$").	-	Up to 1024 characters

Parameter	Type	Description	Required	Valid values
		If omitted, this filter condition is ignored.		
filter[n].not_definition_code	boolean	Not (Message definition ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].severity	number	Specify the severity with a number. If omitted, this filter condition is ignored.	-	Integer between 0 to 255 Default value: 15
filter[n].not_severity	boolean	Not (Severity) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].severity_range	string	Severity range If omitted, this filter condition is ignored. To specify [severity_range] in the filter parameter, [severity] must be specified.	-	">=": [severity] parameter or more "=": equal to [severity] parameter "<=": [severity] parameter or less Default value: [=]
filter[n].confirm	string	Check flag Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	"UNCHECKED": Not checked "CHECKED": Checked Up to 1024 characters
filter[n].not_confirm	boolean	Not (Check flag) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].mark	string	Mark Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_mark	boolean	Not (Mark)	-	false: Select matched messages. true: Select unmatched messages.

Parameter	Type	Description	Required	Valid values
		If this flag is set to true, the specified parameter becomes the filter exclusion condition.		Default value: false
filter[n].comment	string	Comment Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_comment	boolean	Not (Comment) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	Default value: false
filter[n].agent_group_tenant_id	string	Tenant ID of the tenant to which the agent group specified in [agent_group_id] belongs. To specify [agent_group_id] in the filter parameter, [agent_group_tenant_id] of the tenant to which the target agent group belongs must be specified.	-	Up to 1024 characters
filter[n].agent_group_id	string	Agent group ID Filters messages for agents under the specified agent group. To specify [agent_group_id], [agent_group_tenant_id] must be specified. Regular expressions cannot be used. Use a perfectly matched character string. Even when [agent_group_id] is specified, there are some restrictions on filtering due to the following notification message parameters.	-	Up to 1024 characters

Parameter	Type	Description	Required	Valid values
		When the [node_id] parameter is not specified, messages are not filtered. When the [node_type] parameter is other than "AGENT", messages are not filtered.		
filter[n].not_agent_group_id	boolean	Not (Agent group ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	Default value: false
filter[n].agent_group_recursive	boolean	When filtering messages for agents under the specified agent group, specify whether to filter all the agents recursively or only those agents immediately under the specified agent group.	-	true: Retrieve agents under the specified agent group recursively false: Retrieve only those agents immediately under the specified agent group Default value: false
filter[n].system_name	string	System name Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_system_name	boolean	Not (System name) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].node_id	string	Node ID. This matches the filter when a message for the specified node ID is registered. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_node_id	boolean	Not (Node ID) If this flag is set to true, the specified	-	false: Select matched messages. true: Select unmatched messages. Default value:

Parameter	Type	Description	Required	Valid values
		parameter becomes the filter exclusion condition.		false
filter[n].node_type	string	Node type Filters messages that perfectly match the specified node type. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	"MANAGER": Messages issued by the manager "AGENT": Messages reported from the agent A string of specific type can also be specified. Up to 1024 characters
filter[n].not_node_type	boolean	Not (Node type) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].node_name	string	Node name. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_node_name	boolean	Not (Node name) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].application	string	Application. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_application	boolean	Not (Application) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].object	string	Object. Use regular expressions (perfect	-	Up to 1024 characters

Parameter	Type	Description	Required	Valid values
		match example: "^String$"). If omitted, this filter condition is ignored.		
filter[n].not_object	boolean	Not (Object) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].category	string	Type. This matches the filter when a message for the specified type is registered. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	"SYSTEM" "APPLICATION" Up to 1024 characters
filter[n].not_category	boolean	Not (Type) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].message_summary	string	Message overview. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_message_summary	boolean	Not (Message overview) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].message_text	string	Message text. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 8192 characters
filter[n].not_message_text	boolean	Not (Message text)	-	Default value: false

Parameter	Type	Description	Required	Valid values
		If this flag is set to true, the specified parameter becomes the filter exclusion condition.		
filter[n].operation_type	string	Processing type Specify add, update, delete, or no change for each specified filter setting.	Required	"ADD": Add "UPDATE": Update "DELETE": Delete "NONE": No change Default value: NONE
filter[n].report[m]	object[]	Service notification setting	-	-
filter[n].report[m].component_type	string	Component type of the notification destination service. Requests the RESTful API of the micro service of specified component type and reports that the message has been registered.	-	Up to 32 characters
filter[n].report[m].trigger_id	string	Transfer ID to the notification destination service. This is an ID that is set arbitrarily by the micro service of specified component type.	-	Up to 256 characters
filter[n].report[m].report_id	string	Service notification setting ID A unique UUID is assigned by the system when adding a service notification setting. Whether this parameter can be omitted depends on the filter setting processing type (filter[n].operation_type). When filter[n].operation_type is "ADD": This parameter is ignored. When filter[n].operation_type is "UPDATE": Whether this parameter can be omitted depends on	-	Up to 256 characters

Parameter	Type	Description	Required	Valid values
		filter[n].report[m].operation_type. When filter[n].report[m].operation_type is "ADD": This parameter is ignored. When filter[n].report[m].operation_type is "UPDATE", "DELETE", or "NONE": This parameter must be specified. When filter[n].operation_type is "DELETE": This parameter is ignored. When filter[n].operation_type is "NONE": This parameter is ignored.		
filter[n].report[m].operation_type	string	Specify add, update, delete, or no change for the specified service notification setting. Whether this parameter can be omitted depends on the filter setting processing type (filter[n].operation_type). When filter[n].operation_type is "ADD": This parameter must be "ADD". When filter[n].operation_type is "UPDATE": This parameter must be "ADD", "UPDATE", "DELETE", or "NONE". When filter[n].operation_type is "DELETE": This parameter is ignored. When filter[n].operation_type	-	"ADD": Add "UPDATE": Update "DELETE": Delete "NONE": No change Up to 32 characters Default value: NONE

Parameter	Type	Description	Required	Valid values
		is "NONE": This parameter is ignored.		

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	All the filters were successfully uploaded simultaneously.
400	Bad Request	The specified filter setting is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The specified filter is not found.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
filter[n]	object[]	Filter definition setting	-
filter[n].id	string	Filter ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
filter[n].name	string	Filter name	Up to 128 characters
filter[n].type	string	Type	"STORE": Store "EXCLUDE": Exclude Default value:
filter[n].status	string	Filter operating status	"STARTING": Starting "SUSPENDED": Stopping Default value:
filter[n].report_status	string	Operating status of the reporting setting set in the message filter	"STARTING": Enabled "SUSPENDED": Disabled Up to 16 characters
filter[n].message_id	string	Message ID ID indicating the message type Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	Up to 1024 characters
filter[n].not_message_id	boolean	Not (Message ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].definition_code	string	Message definition ID ID indicating the message definition used to generate a message text. Create this	Up to 1024 characters

Parameter	Type	Description	Valid values
		such that it is unique within the system. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	
filter[n].not_definition_code	boolean	Not (Message definition ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].severity	number	Specify the severity with a number. If omitted, this filter condition is ignored.	Integer between 0 to 255
filter[n].not_severity	boolean	Not (Severity) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].severity_range	string	Severity range	">=": [severity] parameter or more "=": equal to [severity] parameter "<=": [severity] parameter or less
filter[n].confirm	string	Check flag Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	"UNCHECKED": Not checked "CHECKED": Checked Up to 1024 characters
filter[n].not_confirm	boolean	Not (Check flag) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].mark	string	Mark Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	Up to 1024 characters
filter[n].not_mark	boolean	Not (Mark) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].comment	string	[Comment] Use regular expressions (perfect match example: "^String$").	Up to 1024 characters

Parameter	Type	Description	Valid values
		If omitted, this filter condition is ignored.	
filter[n].not_comment	boolean	Not (Comment) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].agent_group_tenant_id	string	Tenant ID of the tenant to which the agent group specified in [agent_group_id] belongs. To specify [agent_group_id] in the filter parameter, [agent_group_tenant_id] of the tenant to which the target agent group belongs must be specified.	Up to 64 characters
filter[n].agent_group_id	string	Agent group ID. Filters messages for agents under the specified agent group. To specify [agent_group_id], [agent_group_tenant_id] must be specified. Regular expressions cannot be used. Use a perfectly matched character string. Even when [agent_group_id] is specified, there are some restrictions on filtering due to the following notification message parameters. When the [node_id] parameter is not specified, messages are not filtered. When the [node_type] parameter is other than "AGENT", messages are not filtered.	Up to 1024 characters
filter[n].not_agent_group_id	boolean	Not (Agent group ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].agent_group_recursive	boolean	When filtering messages for agents under the specified agent group, specify whether to filter all the agents recursively or only those agents	true: Retrieve agents under the specified agent group recursively false: Retrieve only those agents immediately under the specified agent group

Parameter	Type	Description	Valid values
		immediately under the specified agent group.	
filter[n].system_name	string	System name Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	Up to 1024 characters
filter[n].not_system_name	boolean	Not (System name) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].node_id	string	Node ID. This matches the filter when a message for the specified node ID is registered. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	Up to 1024 characters
filter[n].not_node_id	boolean	Not (Node ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].node_type	string	Node type Filters messages that perfectly match the specified node type. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	"MANAGER": Messages issued by the manager "AGENT": Messages reported from the agent A string of specific type can also be specified. Up to 1024 characters
filter[n].not_node_type	boolean	Not (Node type) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].node_name	string	Node name. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	Up to 1024 characters
filter[n].not_node_name	boolean	Not (Node name) If this flag is set to true, the specified parameter	false: Select matched messages. true: Select unmatched messages.

Parameter	Type	Description	Valid values
		becomes the filter exclusion condition.	
filter[n].application	string	Application. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	Up to 1024 characters
filter[n].not_application	boolean	Not (Application) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].object	string	Object. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	Up to 1024 characters
filter[n].not_object	boolean	Not (Object) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].category	string	Type. This matches the filter when a message for the specified type is registered. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	"SYSTEM" "APPLICATION" Up to 1024 characters
filter[n].not_category	boolean	Not (Type) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].message_summary	string	Message overview. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	Up to 1024 characters
filter[n].not_message_summary	boolean	Not (Description) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].message_text	string	Message text.	Up to 8192 characters

Parameter	Type	Description	Valid values
		If this flag is set to true, the specified parameter becomes the filter exclusion condition. If this flag is set to true, the specified parameter becomes the filter exclusion condition.	
filter[n].not_.message_text	boolean	Not (Message text) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].tenant_id	string	Tenant ID of the tenant that created the filter. This parameter is set when the Web GUI or external AP additionally creates the filter via the API Gateway.	Up to 64 characters
filter[n].operation_type	string	Processing type "NONE" is always selected for the response.	"NONE": No change Up to 32 characters
filter[n].report[m]	object[]	Service notification setting	-
filter[n].report[m].component_type	string	Component type of the notification destination service. Requests the RESTful API of the micro service of specified component type and reports that the message has been registered.	Up to 32 characters
filter[n].report[m].trigger_id	string	Transfer ID to the notification destination service. This is an ID that is set arbitrarily by the micro service of specified component type.	Up to 256 characters
filter[n].report[m].report_id	string	Service notification setting ID A unique UUID is assigned by the system when adding a service notification setting.	Up to 256 characters
filter[n].report[m].operation_type	string	Processing type "NONE" is always selected for the response.	"NONE": No change Up to 32 characters

* Parameters with null data set are omitted from the response.

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

Example: Configure the email reporting setting for a message with a severity of 200 for agent "nodeA".

a. Set the mail server used in email reporting according to the report mail server configuration file in the "Environmental Configuration Guide".

b. Use one of the following methods to retrieve the mail server ID.

   - Retrieve mail_servers[].server_id of the configured mail server.
     For details, see "3.7.1 Getting the mail server list (page 261)".
   - Retrieve mail_server$n.id of the mail server configuration file (the default is /opt/nec/pf/opm/manager/conf/msc_report_mail_server.properties).

c. Specify the retrieved mail_servers[].server_id and create an email form.
   For details, see "3.7.2 Getting an email reporting setting (page 262)".

d. Make a note of mail_report_forms[].report_form_id retrieved when creating the email form.

e. Specify mail_report_forms[].report_form_id for which you want to use the email form in filter[n].report[m].trigger_id of the filter creation API.

[Request]

```
POST /v1/messagestore/filters/import HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Content-Type: application/json;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 1447

{
  "filter" : [ {
    "name" : "filter name",
    "node_name" : "nodeA",
    "node_type" : "AGENT",
    "operation_type" : "ADD",
    "report" : [ {
      "component_type" : "msc_report",
      "trigger_id" : "b4932012-de12-81e3-876a-83d051732301",
      "operation_type" : "ADD"
    } ],
    "severity" : 200,
    "status" : "STARTING",
    "system_name" : "System1",
    "tenant_id" : "tenantA",
    "type" : "STORE"
  } ]
}
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
```

```
Access-Control-Allow-Methods: POST
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 19:33:12 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
   "filter": [
       {
           "agent_group_id":"msc_extlink_0000000002",
           "agent_group_recursive":false,
           "agent_group_tenant_id":"DefaultTenant",
           "application":"Unified Management Framework",
           "category":"APPLICATION",
           "component_type": "msc_messagestore",
           "definition_code":"2000000000",
           "id": "a56ecf62-0fd0-11e7-8285-4ccc6ac656d6",
           "name": "filter name",
           "node_id": "msc_extlink_MANAGER~AGENT",
           "node_name": "nodeA",
           "node_type": "AGENT",
           "not_agent_group_id":false,
           "not_application":false,
           "not_category":false,
           "not_definition_code":false,
           "not_message_id":false,
           "not_message_summary":false,
           "not_message_text":false,
           "not_node_id":false,
           "not_node_name":false,
           "not_node_type":false,
           "not_object":false,
           "not_severity":false,
           "not_system_name":false,
           "object":"ProcessMonitor",
           "operation_type": "NONE",
           "report": [
              {
                 "component_type": "msc_report",
                 "operation_type": "NONE",
                 "report_id": "a574b45e-0fd0-11e7-8185-4ccc6ac656d6",
                 "trigger_id": "b4932012-de12-81e3-876a-83d051732301"
              }
            ],
            "severity": 150,
            "severity_range":"=",
            "status": "STARTING",
            "report_status":"STARTING",
            "system_name": "System1",
            "tenant_id": "DefaultTenant",
            "type": "STORE"
        }
    ]
}
```

3.7 Report management

3.7.1 Getting the mail server list

1. Process overview

   Retrieve the mail server information.

2. HTTP method

```
GET
```

3. URL

```
/v1/report/reports/mail/servers
```

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Acquisition of the mail server information was successful.
400	Bad Request	An incorrect parameter was specified.
500	Internal Server Error	An internal error occurred.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
mail_servers[n]	object[]	Array of mail servers	-
mail_servers[n].server_id	string	Mail server ID. UUID value used to uniquely identify the mail server information.	Up to 36 characters consisting of hexadecimal numbers and hyphens
mail_servers[n].tenant_id	string	Tenant ID of the tenant to which the mail server information was registered or tenant ID reported from the agent or micro service.	Up to 64 characters
mail_servers[n].server_name	string	Mail server name. This can be specified with a specific character string.	Up to 64 characters
mail_servers[n].host_name	string	Host name or IP address of the mail server	Up to 64 characters
mail_servers[n].port	number	Mail server port number	Integer between 0 to 65535
mail_servers[n].from	string	Source mail address	Up to 256 characters
mail_servers[n].auth	string	Server authentication method	"NONE": Not perform SMTP authentication "CRAM-MD5": CRAM-MD5 authentication

Parameter	Type	Description	Valid values
			"PLAIN": PLAIN authentication
mail_servers[n].ssl	boolean	SSL communication settings	true: Use SSL. false: Not use SSL.

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/report/reports/mail/servers
Host: 192.168.100.10:22521
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
```

   [Response]

```
HTTP/1.1 200 OK
Date: Wed, 1 Mar 2017 00:00:00 GMT
Connection: Close
Transfer-Encoding: chunked

{
   "mail_servers" : [
     {
        "auth" : "NONE",
        "from" : "local@domain",
        "host_name" : "host or ip address",
        "port" : 25,
        "server_id" : "f5b02838-fec1-11e6-a97d-005056b62dc6",
        "server_name" : "server name 1",
        "ssl" : false,
        "tenant_id" : "DefaultTenant"
     },
     {
        "auth" : "PLAIN",
        "from" : "local@domain",
        "host_name" : "host or ip address",
        "port" : 25,
        "server_id" : "f5b02a86-fec1-11e6-a0e5-005056b62dc6",
        "server_name" : "server name 2",
        "ssl" : false,
        "tenant_id" : "DefaultTenant"
     }
   ]
 }
```

3.7.2 Getting an email reporting setting

1. Process overview

Search for an email reporting setting.

2. HTTP method

```
GET
```

3. URL

```
/v1/report/reports/mail/forms?report_form_id=report_form_id
```

Key name	Description	Omittable
report_form_id	Reporting ID. UUID value used to uniquely identify the reporting setting.	-

4. Parameter

None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The reporting setting was successfully retrieved.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
mail_report_forms[n]	object[n]	Array of email forms	-
mail_report_forms[n].operation_type	string	Reporting setting operation type	Fixed to NONE
mail_report_forms[n].report_form_id	string	Reporting ID. UUID value used to uniquely identify the reporting setting. This parameter must be set when updating or deleting the reporting setting. It is not required for a new addition.	Up to 36 characters consisting of hexadecimal numbers and hyphens
mail_report_forms[n].tenant_id	string	Tenant ID of the tenant for which the reporting setting was registered or tenant ID reported from the agent or micro service. If omitted, this parameter is not included in the search conditions. This is available only to administrator users. For general users, the tenant ID of the tenant to which the user belongs is selected. General users	Up to 64 characters

Parameter	Type	Description	Valid values
		must not specify this parameter because a privilege error occurs if a tenant other than that to which the general user belongs is specified.	
mail_report_forms[n].status	string	Reporting setting operating status.Enabled: Only business message filters with the [STARTING] status are enabled as filters.	"STARTING": Enabled "SUSPENDED": Disabled Default: "STARTING" Up to 16 characters
mail_report_forms[n].component_type	string	Stores the component type of the service for which the reporting setting was registered.	Up to 64 characters
mail_report_forms[n].report_form_name	string	Reporting setting name. This can be specified with a specific character string.	Up to 64 characters
mail_report_forms[n].report_form_type	string	Report type.	"MAIL": Email reporting
mail_report_forms[n].mail_servers{}	object{}	Mail server object	-
mail_report_forms[n].mail_servers{}.server_id	string	Mail server ID. UUID value used to uniquely identify the mail server information.	Up to 36 characters consisting of hexadecimal numbers and hyphens
mail_report_forms[n].mail_servers{}.tenant_id	string	Tenant ID of the tenant to which the mail server information was registered or tenant ID reported from the agent or micro service. If omitted, this parameter is not included in the search conditions. This is available only to administrator users. For general users, the tenant ID of the tenant to which the user belongs is selected. General users must not specify this parameter because a privilege error occurs if a tenant other than that to which the general user belongs is specified.	Up to 64 characters
mail_report_forms[n].mail_servers{}.server_name	string	Mail server name. This can be specified with a specific character string.	Up to 64 characters
mail_report_forms[n].mail_servers{}.host_name	string	Host name or IP address of the mail server	Up to 64 characters

Parameter	Type	Description	Valid values
mail_report_forms[n].mail_servers{}.port	number	Mail server port number	Integer between 0 to 65535
mail_report_forms[n].mail_servers{}.from	string	Source mail address	Up to 256 characters
mail_report_forms[n].mail_servers{}.auth	string	Server authentication method	"NONE": Not perform SMTP authentication "CRAM-MD5": CRAM-MD5 authentication "PLAIN": PLAIN authentication
mail_report_forms[n].mail_servers{}.ssl	boolean	SSL communication settings	true: Use SSL. false: Not use SSL.
mail_report_forms[n].send_to	string	Reporting destination (To). If multiple reporting destinations are specified, separate them with commas. Each reporting destination address must be 256 characters or less, giving a total 768 characters or less (including commas).	Up to 256 characters for each address. Up to 768 characters in total
mail_report_forms[n].send_cc	string	Reporting destination (Cc). If multiple reporting destinations are specified, separate them with commas. Each reporting destination address must be 256 characters or less, giving a total 768 characters or less (including commas).	Up to 256 characters for each address. Up to 768 characters in total
mail_report_forms[n].send_bcc	string	Reporting destination (Bcc). If multiple reporting destinations are specified, separate them with commas. Each reporting destination address must be 256 characters or less, giving a total 768 characters or less (including commas).	Up to 256 characters for each address. Up to 768 characters in total
mail_report_forms[n].subject	string	Subject of email reporting.	Up to 128 characters
mail_report_forms[n].mail_text	string	Text of email reporting.	Up to 8192 characters
mail_report_forms[n].encoding	string	Specify the encoding.	"UTF-8"

7. Change history
   - Version: 8.0.0
     - Newly added.

8. Example

[Request]

```
GET /v1/report/reports/mail/forms?report_form_id=200959a8-0e74-11e7-85
70-005056b62dc6
Host: 192.168.100.10:22521
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
```

[Response]

```
HTTP/1.1 200 OK
Date: Wed, 1 Mar 2017 00:00:00 GMT
Connection: Close
Transfer-Encoding: chunked

{
   "mail_report_forms" : [
      {
         "encoding" : "UTF-8",
         "mail_servers" :
            {
               "auth" : "PLAIN",
               "from" : "local@domain",
               "host_name" : "host",
               "port" : 25,
               "server_id" : "f5b02a86-fec1-11e6-a0e5-005056b62dc6",
               "server_name" : "server name",
               "ssl" : false,
               "tenant_id" : "DefaultTenant"
            },
            "mail_text" : "mail message",
            "operation_type" : "NONE",
            "report_form_id" : "200959a8-0e74-11e7-8570-005056b62dc6",
            "report_form_name" : "form name",
            "report_form_type" : "MAIL",
            "send_bcc" : "local@domain",
            "send_cc" : "local@domain",
            "send_to" : "local@domain",
            "subject" : "subject",
            "tenant_id":"DefaultTenant",
            "status":"STARTING"
        }
    ]
}
```

3.7.3 Uploading all email reporting settings simultaneously

1. Process overview

Newly add, update, or delete a reporting setting. Specify newly add, update, or delete in the reporting request parameter operation_type.

If operation_type is set to [ADD], it is treated as a new reporting setting to be added.

If operation_type is set to [UPDATE], the reporting setting linked to the specified reporting ID is updated.

If operation_type is set to [DELETE], the reporting setting linked to the specified reporting ID is deleted.

If operation_type is set to [NONE], the reporting setting is ignored and not changed.

In the reporting setting list and response after upload, operation_type is always set to "NONE".

2. HTTP method

```
POST
```

3. URL

```
/v1/report/reports/mail/forms/import
```

4. Parameter

Parameter	Type	Description	Required	Valid values
mail_report_forms[n]	object[n]	Array of email forms	Required	-
mail_report_forms[n].operation_type	string	Reporting setting operation type This is required when mail_report_forms[n].operation_type is "ADD".	-	"ADD": Newly add "UPDATE": Update "DELETE": Delete "NONE": Not target Default: NONE
mail_report_forms[n].report_form_id	string	Reporting ID. UUID value used to uniquely identify the reporting setting. This parameter must be set when updating or deleting the reporting setting. It is not required for a new addition.	-	Up to 36 characters consisting of hexadecimal numbers and hyphens
mail_report_forms[n].status	string	Reporting setting operating status.Enabled: Only business message filters with the [STARTING] status are enabled as filters.	-	"STARTING": Enabled "SUSPENDED": Disabled Default: "STARTING" Up to 16 characters
mail_report_forms[n].component_type	string	Stores the component type of the service for which the reporting setting was registered.	-	Up to 64 characters
mail_report_forms[n].report_form_name	string	Reporting setting name. This can be specified with a	Required	Up to 64 characters

Parameter	Type	Description	Required	Valid values
		specific character string. This is required when mail_report_forms[n].operation_type is "ADD".		
mail_report_forms[n].report_form_type	string	Report type. This is required when mail_report_forms[n].operation_type is "ADD".	Required	"MAIL": Email reporting
mail_report_forms[n].mail_server_id	string	Mail server ID used for reporting. UUID value used to uniquely identify the mail server information. If omitted, the default mail server is used. If the default mail server is not set, a reporting process ends with an error. This is required when mail_report_forms[n].operation_type is "ADD".	-	Up to 36 characters consisting of hexadecimal numbers and hyphens
mail_report_forms[n].send_to	string	Reporting destination (To). If multiple reporting destinations are specified, separate them with commas. Each reporting destination address must be 256 characters or less, giving a total 768 characters or less (including commas).	-	Up to 256 characters for each address. Up to 768 characters in total
mail_report_forms[n].send_cc	string	Reporting destination (Cc). If multiple reporting destinations are specified, separate them with commas. Each reporting destination address must be 256 characters or less, giving a total 768 characters or less (including commas).	-	Up to 256 characters for each address. Up to 768 characters in total
mail_report_forms[n].send_bcc	string	Reporting destination (Bcc). If multiple reporting destinations are specified, separate them with commas.	-	Up to 256 characters for each address. Up to 768 characters in total

<table>
<tr><th>Parameter</th><th>Type</th><th>Description</th><th>Required</th><th>Valid values</th></tr>
<tr><td></td><td></td><td>Each reporting destination address must be 256 characters or less, giving a total 768 characters or less (including commas).</td><td></td><td></td></tr>
<tr><td>mail_report_forms[n].subject</td><td>string</td><td>Subject of email reporting.</td><td>-</td><td>Up to 128 characters
The following replacement characters can be used in the email subject.<table><tr><th>Replacement character</th><th>Description</th></tr><tr><td>$message_id$</td><td>Message ID</td></tr><tr><td>$definition_code$</td><td>Message definition</td></tr><tr><td>$tenant_id$</td><td>Tenant ID</td></tr><tr><td>$severity$</td><td>Severity</td></tr><tr><td>$create_time$</td><td>Occurrence data and time</td></tr><tr><td>$system_name$</td><td>System name</td></tr><tr><td>$node_id$</td><td>Node ID</td></tr><tr><td>$node_type$</td><td>Node type</td></tr><tr><td>$node_name$</td><td>Node name</td></tr><tr><td>$object$</td><td>Object</td></tr><tr><td>$summary$</td><td>Message overview</td></tr><tr><td>$message_no$</td><td>Message number</td></tr><tr><td>$receive_time$</td><td>Reception date and time</td></tr><tr><td>$message_text$</td><td>Message text</td></tr><tr><td>$business_node_id$</td><td>Business category node ID set to the filter that triggered reporting. This parameter cannot be specified for node-reporting filters.</td></tr></table></td></tr>
<tr><td>mail_report_forms[n].mail_text</td><td>string</td><td>Text of email reporting.</td><td>-</td><td>Up to 8192 characters Specify CRLF for the line feed code.
The following replacement characters can be used in the email text.</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Type</th><th>Description</th><th>Required</th><th>Valid values</th></tr>
<tr><td></td><td></td><td></td><td></td><td>
<table>
<tr><th>Replacement character</th><th>Description</th></tr>
<tr><td>$message_id$</td><td>Message ID</td></tr>
<tr><td>$definition_code$</td><td>Message definition</td></tr>
<tr><td>$tenant_id$</td><td>Tenant ID</td></tr>
<tr><td>$severity$</td><td>Severity</td></tr>
<tr><td>$create_time$</td><td>Occurrence data and time</td></tr>
<tr><td>$system_name$</td><td>System name</td></tr>
<tr><td>$node_id$</td><td>Node ID</td></tr>
<tr><td>$node_type$</td><td>Node type</td></tr>
<tr><td>$node_name$</td><td>Node name</td></tr>
<tr><td>$object$</td><td>Object</td></tr>
<tr><td>$summary$</td><td>Message overview</td></tr>
<tr><td>$message_no$</td><td>Message number</td></tr>
<tr><td>$receive_time$</td><td>Reception date and time</td></tr>
<tr><td>$message_text$</td><td>Message text</td></tr>
<tr><td>$business_node_id$</td><td>Business category node ID set to the filter that triggered reporting. This parameter cannot be specified for node-reporting filters.</td></tr>
</table>
</td></tr>
<tr><td>mail_report_forms[n].encoding</td><td>string</td><td>Specify the encoding.</td><td>-</td><td>"UTF-8"
Default: "UTF-8"</td></tr>
</table>

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The email reporting was successfully set.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
mail_report_forms[n]	object[n]	Array of email forms	-
mail_report_forms[n].operation_type	string	Reporting setting operation type	Fixed to NONE
mail_report_forms[n].report_form_id	string	Reporting ID. UUID value used to uniquely identify the reporting setting. This parameter must be set when updating or deleting the reporting setting. It is not required for a new addition.	Up to 36 characters consisting of hexadecimal numbers and hyphens
mail_report_forms[n].component_type	string	Stores the component type of the service for which the reporting setting was registered.	Up to 64 characters
mail_report_forms[n].report_form_name	string	Reporting setting name. This can be specified with a specific character string.	Up to 64 characters
mail_report_forms[n].report_form_type	string	Report type.	"MAIL": Email reporting
mail_report_forms[n].mail_servers{}	object{}	Mail server object	-
mail_report_forms[n].mail_servers{}.server_id	string	Mail server ID. UUID value used to uniquely identify the mail server information.	Up to 36 characters consisting of hexadecimal numbers and hyphens
mail_report_forms[n].status	string	Reporting setting operating status.Enabled: Only business message filters with the [STARTING] status are enabled as filters.	"STARTING": Enabled "SUSPENDED": Disabled Default: "STARTING" Up to 16 characters
mail_report_forms[n].mail_servers{}.server_name	string	Mail server name. This can be specified with a specific character string.	Up to 64 characters
mail_report_forms[n].mail_servers{}.host_name	string	Host name or IP address of the mail server	Up to 64 characters
mail_report_forms[n].mail_servers{}.port	number	Mail server port number	Integer between 0 to 65535
mail_report_forms[n].mail_servers{}.from	string	Source mail address	Up to 256 characters
mail_report_forms[n].mail_servers{}.auth	string	Server authentication method	"NONE": Not perform SMTP authentication "CRAM-MD5": CRAM-MD5 authentication "PLAIN": PLAIN authentication
mail_report_forms[n].mail_servers{}.ssl	boolean	SSL communication settings	true: Use SSL.

Parameter	Type	Description	Valid values
			false: Not use SSL.
mail_report_forms[n].send_to	string	Reporting destination (To). If multiple reporting destinations are specified, separate them with commas. Each reporting destination address must be 256 characters or less, giving a total 768 characters or less (including commas).	Up to 256 characters for each address. Up to 768 characters in total
mail_report_forms[n].send_cc	string	Reporting destination (Cc). If multiple reporting destinations are specified, separate them with commas. Each reporting destination address must be 256 characters or less, giving a total 768 characters or less (including commas).	Up to 256 characters for each address. Up to 768 characters in total
mail_report_forms[n].send_bcc	string	Reporting destination (Bcc). If multiple reporting destinations are specified, separate them with commas. Each reporting destination address must be 256 characters or less, giving a total 768 characters or less (including commas).	Up to 256 characters for each address. Up to 768 characters in total
mail_report_forms[n].subject	string	Subject of email reporting.	Up to 128 characters
mail_report_forms[n].mail_text	string	Text of email reporting.	Up to 8192 characters Specify CRLF for the line feed code.
mail_report_forms[n].encoding	string	Specify the encoding.	"UTF-8"

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
POST /v1/report/reports/mail/forms/import
Host: 192.168.100.10:22521
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
{
   "mail_report_forms" : [
```

```
      {
         "operation_type" : "ADD",
         "report_form_name" : "form name 1",
         "report_form_type" : "MAIL",
         "mail_server_id" : "9643232c-ff2b-11e6-8cbe-005056b62dc6",
         "send_to" : "local@domain",
         "send_cc" : "local@domain",
         "subject" : "subject",
         "mail_text" : "mail message"
      }
   ]
}
```

[Response]

```
HTTP/1.1 200 OK
Date: Wed, 1 Mar 2017 00:00:00 GMT
Connection: Close
Transfer-Encoding: chunked

{
   "mail_report_forms" : [
   {
      "encoding" : "",
      "mail_servers" :
         {
            "auth" : "NONE",
            "from" : "local@domain",
            "host_name" : "host or ip address",
            "port" : 25,
            "server_id" : "9643232c-ff2b-11e6-8cbe-005056b62dc6",
            "server_name" : "server name",
            "ssl" : false,
            "tenant_id" : "DefaultTenant"
         },
         "mail_text" : "mail message",
         "operation_type" : "NONE",
         "report_form_id" : "36804d06-0f08-11e7-9ff4-005056b62dc6",
         "report_form_name" : "form name 1",
         "report_form_type" : "MAIL",
         "send_bcc" : "",
         "send_cc" : "local@domain",
         "send_to" : "local@domain",
         "subject" : "subject",
         "status":"STARTING"
      }
   ]
}
```

3.7.4 Getting an action reporting setting

1. Process overview

   Search for an action reporting setting.

2. HTTP method

```
GET
```

3. URL

```
/v1/report/reports/action/forms?report_form_id=report_form_id
```

Key name	Description	Omittable
report_form_id	Reporting ID. UUID value used to uniquely identify the reporting setting.	-

4. Parameter

None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The reporting setting was successfully retrieved.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
action_report_forms[n]	object[n]	Action reporting setting array	-
action_report_forms[n].operation_type	string	Reporting setting operation type	Fixed to NONE
action_report_forms[n].report_form_id	string	Reporting ID. UUID value used to uniquely identify the reporting setting. This parameter must be set when updating or deleting the reporting setting. It is not required for a new addition.	Up to 40 characters consisting of "CMD_" + hexadecimal numbers and hyphens
action_report_forms[n].tenant_id	string	Tenant ID of the tenant for which the reporting setting was registered or tenant ID reported from the agent or micro service. If omitted, this parameter is not included in the search conditions. This is available only to administrator users. For general users, the tenant ID of the tenant to which the user belongs is selected. General users must not specify this parameter because a privilege error occurs if a tenant other than that to which the general user belongs is specified.	Up to 64 characters Null characters not acceptable

Parameter	Type	Description	Valid values
action_report_forms[n].status	string	Reporting setting operating status.Enabled: Only business message filters with the [STARTING] status are enabled as filters.	"STARTING": Enabled "SUSPENDED": Disabled Default: "STARTING" Up to 16 characters
action_report_forms[n].component_type	string	Stores the component type of the service for which the reporting setting was registered.	Up to 64 characters
action_report_forms[n].report_form_name	string	Reporting setting name. This can be specified with a specific character string.	Up to 64 characters
action_report_forms[n].command	string	Specify the application to be used to execute the action. Specify the absolute or relative path. If the relative path is specified, the command is executed with a relative path from the working directory converted to an absolute path. Even when a path contains a blank space, do not enclose it in double quotation marks (""). If the manager is Windows, use \ as a delimiter, and if the manager is LINUX, use / as a delimiter. (If replacement characters are to be used, consider the number of actual characters that will replace them.)	Up to 256 characters
action_report_forms[n].work_dir	string	Specify the working directory for starting the command. Even when a path contains a blank space, do not enclose it in double quotation marks (""). If the manager is Windows, use a backslash (\ )as a delimiter, and if the manager is Linux, use a slash (/) as a delimiter. (If replacement characters are to be used, consider the number of actual characters that will replace them.)	Up to 256 characters
action_report_forms[n].option	string	Specify the argument for starting the command.	Up to 2048 characters

7. Change history

- Version: 8.0.0
  - Newly added.

8. Example

[Request]

```
GET /v1/report/reports/action/forms?report_form_id=3b2f23f8-027a-11e7-
b132-005056b62dc6
Host: 192.168.100.10:22521
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
```

[Response]

```
HTTP/1.1 200 OK
Date: Wed, 1 Mar 2017 00:00:00 GMT
Connection: Close
Transfer-Encoding: chunked

{
   "action_report_forms" : [
      {
         "component_type":"msc_messagestore",
         "command" : "$REPORT_HOME$\\action.exe",
         "work_dir" : "C:\\Users\\Administrator\\report",
         "option" : "-w $node_name$",
         "operation_type" : "NONE",
         "report_form_id" : "3b2f23f8-027a-11e7-b132-005056b62dc6",
         "report_form_name" : "action policy",
         "status":"STARTING",
         "tenant_id":"DefaultTenant"
       }
    ]
}
```

3.7.5 Uploading all action reporting settings simultaneously

1. Process overview
Newly add, update, or delete an action reporting setting. Specify newly add, update, or delete in the action report request parameter operation_type.

   If operation_type is set to [ADD], it is treated as a new reporting setting to be added.

   If operation_type is set to [UPDATE], the reporting setting linked to the specified reporting ID is updated.

   If operation_type is set to [DELETE], the reporting setting linked to the specified reporting ID is deleted.

   If operation_type is set to [NONE], the reporting setting is ignored and not changed.

   In the reporting setting list and response after upload, operation_type is always set to "NONE".

2. HTTP method

```
POST
```

3. URL

```
/v1/report/reports/action/forms/import
```

4. Parameter

Parameter	Type	Description	Required	Valid values
action_report_forms[n]	object[n]	Action reporting setting array	Required	-
action_report_forms[n].operation_type	string	Reporting setting operation type This is required when mail_report_forms[n].operation_type is "ADD".	-	"ADD": Newly add "UPDATE": Update "DELETE": Delete "NONE": Not target
action_report_forms[n].report_form_id	string	Reporting ID. UUID value used to uniquely identify the reporting setting. This parameter must be set when updating or deleting the reporting setting. It is not required for a new addition.	-	Up to 40 characters consisting of "CMD_" + hexadecimal numbers and hyphens
action_report_forms[n].status	string	Reporting setting operating status.Enabled: Only business message filters with the [STARTING] status are enabled as filters.	-	"STARTING": Enabled "SUSPENDED": Disabled Default: "STARTING" Up to 16 characters
action_report_forms[n].component_type	string	Stores the component type of the service for which the reporting setting was registered.	-	Up to 64 characters
action_report_forms[n].report_form_name	string	Reporting setting name. This can be specified with a specific character string. This is required when mail_report_forms[n].operation_type is "ADD".	Required	Up to 64 characters
action_report_forms[n].command	string	Specify the application to be used to execute the action. Specify the absolute or relative path. If the relative path is specified, the	-	Specify this parameter using a character string within 256 characters. (If replacement characters are to be used, consider the number of actual characters that will replace them.)

<table>
<tr><th>Parameter</th><th>Type</th><th>Description</th><th>Required</th><th>Valid values</th></tr>
<tr><td></td><td></td><td>command is executed with a relative path from the working directory converted to an absolute path. Even when a path contains a blank space, do not enclose it in double quotation marks (""). If the manager is Windows, use \ as a delimiter, and if the manager is LINUX, use / as a delimiter. (If replacement characters are to be used, consider the number of actual characters that will replace them.)
This is required when mail_report_forms[n].operation_type is "ADD".</td><td></td><td></td></tr>
<tr><td>action_report_forms[n].work_dir</td><td>string</td><td>Specify the working directory for starting the command. Even when a path contains a blank space, do not enclose it in double quotation marks (""). If the manager is Windows, use a backslash (\ )as a delimiter, and if the manager is Linux, use a slash (/) as a delimiter. (If replacement characters are to be used, consider the number of actual characters that will replace them.)</td><td>-</td><td>Specify this parameter using a character string within 256 characters. If omitted, the working directory would be <installation path>/bin.</td></tr>
<tr><td>action_report_forms[n].option</td><td>string</td><td>Specify the argument for starting the command.</td><td>-</td><td>Specify this parameter using a character string within 2048 characters. Replacement characters are available. (If replacement characters are to be used, consider the number of actual characters that will replace them. If the number of characters after replacement exceeds 2048, command execution ends with an error.)
<table><tr><th>Replacement character</th><th>Description</th></tr><tr><td>$message_id$</td><td>Message ID</td></tr></table></td></tr>
</table>

Parameter	Type	Description	Required	Valid values

Replacement character	Description
$definition_code$	Message definition
$tenant_id$	Tenant ID
$severity$	Severity
$create_time$	Occurrence data and time
$system_name$	System name
$node_id$	Node ID
$node_type$	Node type
$node_name$	Node name
$object$	Object
$summary$	Message overview
$message_no$	Message number
$receive_time$	Reception date and time
$message_text$	Message text
$business_node_id$	Business category node ID set to the filter that triggered reporting. This parameter cannot be specified for node-reporting filters.

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The action reporting was successfully set.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
action_report_forms[n]	object[n]	Action reporting setting array	-
action_report_forms[n].operation_type	string	Reporting setting operation type	Fixed to NONE
action_report_forms[n].report_form_id	string	Reporting ID. UUID value used to uniquely identify the reporting setting. This parameter must be set when updating or deleting the reporting setting. It is not required for a new addition.	Up to 40 characters consisting of "CMD_" + hexadecimal numbers and hyphens
action_report_forms[n].status	string	Reporting setting operating status.Enabled: Only business message filters with the [STARTING] status are enabled as filters.	"STARTING": Enabled "SUSPENDED": Disabled Default: "STARTING" Up to 16 characters
action_report_forms[n].component_type	string	Stores the component type of the service for which the reporting setting was registered.	Up to 64 characters
action_report_forms[n].report_form_name	string	Reporting setting name. This can be specified with a specific character string.	Up to 64 characters
action_report_forms[n].command	string	Specify the application to be used to execute the action. Specify the absolute or relative path. If the relative path is specified, the command is executed with a relative path from the working directory converted to an absolute path. Even when a path contains a blank space, do not enclose it in double quotation marks (""). If the manager is Windows, use \ as a delimiter, and if the manager is LINUX, use / as a delimiter. (If replacement characters are to be used, consider the number of actual characters that will replace them.)	Specify this parameter using a character string within 256 characters. (If replacement characters are to be used, consider the number of actual characters that will replace them.)
action_report_forms[n].work_dir	string	Specify the working directory for starting the command. Even when a path contains a blank space, do not enclose it in double quotation marks (""). If the manager is	Specify this parameter using a character string within 256 characters. If omitted, the working directory would be <installation path>/bin.

Parameter	Type	Description	Valid values
		Windows, use a backslash (\ )as a delimiter, and if the manager is Linux, use a slash (/) as a delimiter. (If replacement characters are to be used, consider the number of actual characters that will replace them.)	
action_report_forms[n].option	string	Specify the argument for starting the command.	Specify this parameter using a character string within 2048 characters. Replacement characters are available. (If replacement characters are to be used, consider the number of actual characters that will replace them. If the number of characters after replacement exceeds 2048, command execution ends with an error.)

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
POST /v1/report/reports/action/forms/import
Host: 192.168.100.10:22521
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
{
   "action_report_forms" : [
      {
         "command" : "action.exe",
         "work_dir" : "C:\\Users\\Administrator",
         "option" : "-t 100",
         "operation_type" : "UPDATE",
         "report_form_id" : "200959a8-0e74-11e7-8570-005056b62dc6",
         "report_form_name" : "action policy 1"
      },
      {
          "operation_type" : "ADD",
          "report_form_name" : "action policy 2",
          "command" : "$REPORT_HOME$\\action.exe",
          "work_dir" : "C:\\Users\\Administrator",
          "option" : "-w $node_name$"
      }
   ]
}
```

   [Response]

```
HTTP/1.1 200 OK
Date: Wed, 1 Mar 2017 00:00:00 GMT
Connection: Close
Transfer-Encoding: chunked

{
   "action_report_forms" : [
      {
         "command" : "action.exe",
         "work_dir" : "C:\\Users\\Administrator",
         "option" : "-t 100",
         "operation_type" : "NONE",
         "report_form_id" : "200959a8-0e74-11e7-8570-005056b62dc6",
         "report_form_name" : "action policy 1",
         "tenant_id":"DefaultTenant",
         "status":"STARTING"
      },
      {
         "command" : "$REPORT_HOME$\\action.exe",
         "work_dir" : "C:\\Users\\Administrator",
         "option" : "-w $node_name$",
         "operation_type" : "NONE",
         "report_form_id" : "3b2f23f8-027a-11e7-b132-005056b62dc6",
         "report_form_name" : "action policy 2",
         "tenant_id" : "DefaultTenant",
         "status":"STARTING"
      }
   ]
}
```

3.7.6 Getting the reporting history list

1. Process overview
   Retrieve the reporting history. Parameters without search conditions specified are not used for filtering.
2. HTTP method

```
POST
```

3. URL

```
/v1/report/reports/histories/get
```

4. Parameter

Parameter	Type	Description	Required	Valid values
query	object	History search condition object	Required	-
query.limit	number	Specify the maximum number of items to output by the specified search conditions.	-	Minimum value: 1 Maximum value: 1000

Parameter	Type	Description	Required	Valid values
				Default value: 100
query.message_no	string	Number indicating the start point of the messages to retrieve.	-	If omitted, this parameter is not included in the search conditions. A list of messages from the specified number to the set maximum number is retrieved. Messages are sorted in the order specified in the order parameter and are retrieved up to the maximum number set in the limit parameter. Minimum value: 1 Maximum value: 9223372036854775807
query.report_form_id	string	Reporting ID. If omitted, this parameter is not included in the search conditions. UUID value used to uniquely identify the reporting setting. For action reporting, "CMD_" is added at the beginning.	-	Email reporting: Up to 36 characters consisting of hexadecimal numbers and hyphens Action reporting: Up to 36 characters consisting of hexadecimal numbers and hyphens
query.report_form_name	string	Reporting name. If omitted, this parameter is not included in the search conditions. Extracts records that perfectly match the specified form name.	-	Up to 64 characters
query.report_status	string	Reporting status. If omitted, this parameter is not included in the search conditions. Extracts records that perfectly match the specified reporting status.	-	"SUCCESS": Normal end "PROCESSING": Reporting "ERROR": Abnormal end "NONE": Not target
query.report_status_id	string	Message service reporting status ID. If omitted, this parameter is not included in the search conditions. Extracts records that perfectly match the specified reporting status.	-	Integer between 1 to 9223372036854775807 If multiple values are specified, combine them with "+" (Example: "1+2+3").
query.order	string	Specify ascending or descending order.	-	"ASCEND": Ascending "DESCEND": Descending Default value: "DESCEND"

Parameter	Type	Description	Required	Valid values
query.ordered	string	Specify the parameter name to which order is applied.	-	Only "message_no" can be specified. Default value: "message_no"
query.confirm_flag	string	Check flag	-	"TRUE": Confirmed. (To be hidden) "FALSE": Not confirmed.
query.timezone	string	Specify the time zone for the reporting date and time parameter. [report_time] in the response is returned according to the specified time zone. (Example: "+9" returns "2016-11-16T19:00:00 +09:00". "+0" returns "2016-11-16T10:00:00 +00:00". "-5" returns "2016-11-16T05:00:00 -05:00". "-3.5" returns "2016-11-16T06:30:00 -03:30".) If omitted, the time zone of the manager machine is used.	-	Specify the time difference relative to UTC, such as "+09". Default value: +00: UTC standard time

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The reporting history was successfully retrieved.
400	Bad Request	An incorrect parameter was specified.
500	Internal Server Error	An internal error occurred.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
histories[n]	object[n]	History array	-
histories[n].message_number	number	Target message number	Integer between 1 to 9223372036854775807
histories[n].confirm_flag	string	Check flag for the reported message	"TRUE": Confirmed. (To be hidden) "FALSE": Not confirmed.
histories[n].report[m]	object[]	Reporting status array	-

Parameter	Type	Description	Valid values
histories[n].report[m].report_status_id	number	Message service notification status ID	Integer between 1 to 9223372036854775807
histories[n].report[m].report_form_id	string	Reporting ID. UUID value used to uniquely identify the reporting setting. For action reporting, "CMD_" is added at the beginning.	Email reporting: Up to 36 characters consisting of hexadecimal numbers and hyphens Action reporting: Up to 40 characters consisting of "CMD_" + hexadecimal numbers and hyphens
histories[n].report[m].report_form_name	string	Reporting name	Specify this item within 64 characters. Null characters not acceptable
histories[n].report[m].report_status	string	Reporting status.	"SUCCESS": Normal end "PROCESSING": Reporting "ERROR": Abnormal end "NONE": Not target
histories[n].report[m].report_type	string	Report type.	"MAIL": Email reporting "ACTION": Action reporting
histories[n].report[m].report_time	string	Reporting date and time	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
histories[n].report[m].output	string	Application standard output and standard error output	Within 8191 bytes.
histories[n].report[m].exit_code	string	Application exit code. If the command times out, no value is set. A value is set if receiving of the standard output is set in the action reporting setting.	Up to 128 characters
histories[n].report[m].error_info	string	Error information on a reporting failure is set.	Up to 1024 characters

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
POST /v1/report/reports/histories/get
Host: 192.168.100.10:22521
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
{
  "query" : {
    "order" : "DESCEND",
    "ordered" : "message_no",
    "limit" : 3,
    "message_no" : "8525"
```

```
  }
}
```

[Response]

```
HTTP/1.1 200 OK
Date: Wed, 1 Mar 2017 00:00:00 GMT
Connection: Close
Transfer-Encoding: chunked

{
  "histories" : [
    {
      "confirm_flag" : "FALSE",
      "message_number" : 8525,
      "report" : [
        {
          "report_form_id" : "3b2f23f8-027a-11e7-b132-005056b62dc6",
          "report_form_name" : "mail form 1",
          "report_status" : "ERROR",
          "report_status_id" : 7199,
          "report_time" : "2017-03-15T05:52:20+09:00",
          "report_type" : "MAIL"
        }
      ]
    },
    {
      "confirm_flag" : "FALSE",
      "message_number" : 8522,
      "report" : [
        {
          "report_form_id" : "3b2f23f8-027a-11e7-b132-005056b62dc6",
          "report_form_name" : "mail form 1",
          "report_status" : "ERROR",
          "report_status_id" : 7196,
          "report_time" : "2017-03-15T04:16:19+09:00",
          "report_type" : "MAIL"
        }
      ]
    },
    {
      "confirm_flag" : "FALSE",
      "message_number" : 8519,
      "report" : [
        {
          "report_form_id" : "3b2f23f8-027a-11e7-b132-005056b62dc6",
          "report_form_name" : "mail form 2",
          "report_status" : "ERROR",
          "report_status_id" : 7193,
          "report_time" : "2017-03-15T03:57:42+09:00",
          "report_type" : "MAIL"
        }
      ]
    }
  ]
}
```

3.7.7 Updating the reporting history

1. Process overview
   Update the reporting history.
2. HTTP method

```
PUT
```

3. URL

```
/v1/report/reports/histories
```

4. Parameter

Parameter	Type	Description	Required	Valid values
histories[n]	object[n]	History search condition object	Required	-
histories[n].message_number	number	Target message number.	-	Minimum value: 1 Maximum value: 9223372036854775807
histories[n].confirm_flag	string	Check flag for the reported message.	-	"TRUE": Confirmed. (To be hidden) "FALSE": Not confirmed.

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The reporting history was successfully updated.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The specified target is not found.
500	Internal Server Error	An internal error occurred.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
histories[n]	object[n]	History array	-
histories[n].message_number	string	Target message number	Integer between 1 to 9223372036854775807
histories[n].confirm_flag	string	Check flag for the reported message	"TRUE": Confirmed. (To be hidden) "FALSE": Not confirmed.
histories[n].report[m]	object[]	Reporting status array	-

Parameter	Type	Description	Valid values
histories[n].report[m].report_status_id	number	Message service notification status ID	Integer between 1 to 9223372036854775807
histories[n].report[m].report_form_id	string	Reporting ID. UUID value used to uniquely identify the reporting setting. For action reporting, "CMD_" is added at the beginning.	Email reporting: Up to 36 characters consisting of hexadecimal numbers and hyphens Action reporting: Up to 40 characters consisting of "CMD_" + hexadecimal numbers and hyphens
histories[n].report[m].report_form_name	string	Reporting name	Specify this item within 64 characters. Null characters not acceptable
histories[n].report[m].report_status	string	Reporting status.	"SUCCESS": Normal end "PROCESSING": Reporting "ERROR": Abnormal end "NONE": Not target
histories[n].report[m].report_type	string	Report type.	"MAIL": Email reporting "ACTION": Action reporting
histories[n].report[m].report_time	string	Reporting date and time	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
histories[n].report[m].output	string	Application standard output and standard error output	Within 8191 bytes.
histories[n].report[m].exit_code	string	Application exit code. If the command times out, no value is set. A value is set if receiving of the standard output is set in the action reporting setting.	Up to 128 characters
histories[n].report[m].error_info	string	Error information on a reporting failure is set.	Up to 1024 characters

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
PUT /v1/report/reports/histories
Host: 192.168.100.10:22521
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
{
   "histories" : [
      {
          "message_number" : "8310",
          "confirm_flag" : "TRUE"
      }
```

```
    ]
}
```

[Response]

```
HTTP/1.1 200 OK
Date: Wed, 1 Mar 2017 00:00:00 GMT
Connection: Close
Transfer-Encoding: chunked

{
  "histories" : [
    {
      "confirm_flag" : "TRUE",
      "message_number" : 8310,
      "report" : [
        {
          "report_form_id" : "3b2f23f8-027a-11e7-b132-005056b62dc6",
          "report_form_name" : "mail form 1",
          "report_status" : "ERROR",
          "report_status_id" : 7084,
          "report_time" : "2017-03-14T04:28:22+09:00",
          "report_type" : "MAIL"
        }
      ]
    }
  ]
}
```

3.8 Business

3.8.1 Viewing a business node

1. Process overview
   Retrieve the business node information for the specified business node ID.
2. HTTP method

```
GET
```

3. URL

```
/v1/businessview/nodes/node_id
```

   In ***node_id***, specify the business node ID of the target business category group or business category.

   For the root, specify 0 in ***node_id***.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The business node information was successfully retrieved.

HTTP status code	Meaning	Description
206	Partial Content	status[n].severity was not successfully retrieved.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The resource specified in the URI does not exist. Deleted
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
node_id	string	Business node ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
display_name	string	Display name	If the root is specified for the target business node ID, "BusinessView" is returned. Up to 128 characters
node_type	string	Type	A character string is returned according to the type. "GROUP": Business category group. "CATEGORY": Business category
parent_node_id	string	New business node ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
status	object[]	Array of severity information	-
status[n].name	string	Severity status name	Returns a string of up to 128 characters. In this version, this parameter is always "MESSAGES".
status[n].severity	number	Severity	Integer between 0 to 255 (*1)
child_nodes	object[]	Array of child business node information	The information about the business category group/business category node under the specified business category group node is returned.
child_nodes[m].node_id	string	Business node ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
child_nodes[m].display_name	string	Display name	Up to 128 characters
child_nodes[m].node_type	string	Type	"GROUP": Business category group. "CATEGORY": Business category
child_nodes[m].parent_node_id	string	New business node ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens

Parameter	Type	Description	Valid values
child_nodes[m].status	object[]	Array of severity information	-
child_nodes[m].status[n].name	string	Severity status name	Returns a string of up to 128 characters. In this version, this parameter is always "MESSAGES".
child_nodes[m].status[n].severity	number	Severity	Integer between 0 to 255 (*1) • 200: Abnormal • 150: Warning • 100: Unknown • 50: Normal • 15: No severity • 10: Monitoring stopped

(*1)

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/business/nodes/0 HTTP/1.1
referer: http://192.168.18.64:12080/umftool/vDCToolFreeRequest.jsp
accept-language: ja,en-US;q=0.7,en;q=0.3
x-authorization: token 1EFECD7965F72E48D98CF58078EBAE28
cookie: JSESSIONID=1C5F043EF655FC10A1D34B1B8DCC0EF3
accept: */*
authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
if-modified-since: Thu, 01 Jun 1970 00:00:00 GMT
x-cmtool-host: localhost
x-requested-with: XMLHttpRequest
x-cmtool-port: 8280
accept-encoding: gzip, deflate
user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20
100101 Firefox/49.0
X-UMF-API-Version: 2.0
Date: Wed, 22 Mar 2017 21:14:54 GMT
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Host: localhost:8280
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 21:14:54 GMT
```

```
Transfer-Encoding: chunked
Connection: keep-alive

{
   "display_name": "BusinessView",
   "node_id": "0",
   "node_type": "GROUP",
   "status": [
      {
         "name": "MESSAGES",
         "severity": 200
      }
    ],
    "child_nodes": [
       {
          "display_name": "Application",
          "node_id": "373786f3de23ad60267cfd62a43451ab",
          "node_type": "GROUP",
          "status": [
             {
                "name": "MESSAGES",
                "severity": 100
             }
          ]
       },
       {
          "display_name": "System",
          "node_id": "565326d2fe21bc89590baf82b43573ba",
          "node_type": "CATEGORY",
          "status": [
             {
                "name": "MESSAGES",
                "severity": 200
             }
          ]
       }
    ]
}
```

3.8.2 Registering a business category

1. Process overview
   Create and register a new business category under the business node ID of the specified business category group.
2. HTTP method

```
POST
```

3. URL

```
/v1/businessview/nodes/categories/node_id
```

   In ***node_id***, specify the business node ID of the business category group that would be the parent of the business category to be created.

   For the root, specify 0 in ***node_id***.

4. Parameter

Parameter	Type	Description	Required	Valid values
display_name	string	Display name of the business category to be registered newly	Required	Up to 128 characters

5. Response (HTTP status code)

HTTP status code	Meaning	Description
201	Created	The business category information was successfully registered.
400	Bad Request	The request is incorrect. The parameter is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The business category group of the node ID specified in the URI does not exist.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
node_id	string	Registered business node ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
display_name	string	Display name of the newly registered business category	Up to 128 characters

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
POST /v1/business/nodes/categories/0 HTTP/1.1
referer: http://192.168.18.64:12080/umftool/vDCToolFreeRequest.jsp
accept-language: ja,en-US;q=0.7,en;q=0.3
x-authorization: token 1EFECD7965F72E48D98CF58078EBAE28
cookie: JSESSIONID=1C5F043EF655FC10A1D34B1B8DCC0EF3
accept: */*
authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
if-modified-since: Thu, 01 Jun 1970 00:00:00 GMT
x-cmtool-host: localhost
x-requested-with: XMLHttpRequest
x-cmtool-port: 8280
accept-encoding: gzip, deflate
user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20
100101 Firefox/49.0
X-UMF-API-Version: 2.0
```

```
Date: Wed, 22 Mar 2017 21:14:54 GMT
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Host: localhost:8280
Connection: keep-alive

{
    "display_name": "Application"
}
```

[Response]

```
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 21:14:54 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
    "display_name": "Application",
    "node_id": "565326d2fe21bc89590baf82b43573ba"
}
```

3.8.3 Updating a business category

1. Process overview
   Update the business category display name of the specified business node ID.
2. HTTP method

```
PUT
```

3. URL

```
/v1/businessview/nodes/categories/node_id
```

   In ***node_id***, specify the business node ID of the target business category.
4. Parameter

Parameter	Type	Description	Required	Valid values
display_name	string	Display name to be updated	Required	Up to 128 characters

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The business category information was successfully updated.

HTTP status code	Meaning	Description
400	Bad Request	The request is incorrect. The parameter is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	When the root is set to the target business node ID The business category of the node ID specified in the URI does not exist.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
node_id	string	Updated business node ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
display_name	string	Updated display name	Up to 128 characters

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
PUT /v1/business/nodes/categories/565326d2fe21bc89590baf82b43573ba HTT
P/1.1
referer: http://192.168.18.64:12080/umftool/vDCToolFreeRequest.jsp
accept-language: ja,en-US;q=0.7,en;q=0.3
x-authorization: token 1EFECD7965F72E48D98CF58078EBAE28
cookie: JSESSIONID=1C5F043EF655FC10A1D34B1B8DCC0EF3
accept: */*
authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
if-modified-since: Thu, 01 Jun 1970 00:00:00 GMT
x-cmtool-host: localhost
x-requested-with: XMLHttpRequest
x-cmtool-port: 8280
accept-encoding: gzip, deflate
user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20
100101 Firefox/49.0
X-UMF-API-Version: 2.0
Date: Wed, 22 Mar 2017 21:14:54 GMT
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Host: localhost:8280
Connection: keep-alive

{
    "display_name": "Urgent obstacle"
}
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: PUT
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 21:14:54 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
    "display_name": "Urgent obstacle",
    "node_id": "565326d2fe21bc89590baf82b43573ba"
}
```

3.8.4 Deleting a business category

1. Process overview

   Delete the business category of the specified business node ID.

   If the business message filter definition is specified in the specified business category, the definition is also deleted.

2. HTTP method

   ```
   DELETE
   ```

3. URL

   ```
   /v1/businessview/nodes/categories/node_id
   ```

   In ***node_id***, specify the business node ID of the target business category.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
204	No Content	The business category information was successfully deleted.
400	Bad Request	The request is incorrect. The parameter is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	When the root is set to the target business node ID The business category of the node ID specified in the URI does not exist.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

   None

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
DELETE /v1/business/nodes/categories/565326d2fe21bc89590baf82b43573ba
HTTP/1.1
referer: http://192.168.18.64:12080/umftool/vDCToolFreeRequest.jsp
accept-language: ja,en-US;q=0.7,en;q=0.3
x-authorization: token 1EFECD7965F72E48D98CF58078EBAE28
cookie: JSESSIONID=1C5F043EF655FC10A1D34B1B8DCC0EF3
accept: */*
authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
if-modified-since: Thu, 01 Jun 1970 00:00:00 GMT
x-cmtool-host: localhost
x-requested-with: XMLHttpRequest
x-cmtool-port: 8280
accept-encoding: gzip, deflate
user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20
100101 Firefox/49.0
X-UMF-API-Version: 2.0
Date: Wed, 22 Mar 2017 21:14:54 GMT
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Host: localhost:8280
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: DELETE
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 21:14:54 GMT
Transfer-Encoding: chunked
Connection: keep-alive
```

3.8.5 Registering a business category group

1. Process overview
   Create and register a new business category group under the business node ID of the specified business category group.
2. HTTP method

```
POST
```

3. URL

```
/v1/businessview/nodes/groups/node_id
```

In ***node_id***, specify the business node ID of the business category group that would be the parent of the business category group to be created.

For the root, specify 0 in ***node_id***.

4. Parameter

Parameter	Type	Description	Required	Valid values
display_name	string	Display name of the business category group to be registered newly	Required	Up to 128 characters

5. Response (HTTP status code)

HTTP status code	Meaning	Description
201	Created	The business category group information was successfully registered.
400	Bad Request	The request is incorrect. The parameter is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The parent business category group to be added specified in the URI does not exist.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
node_id	string	Registered business node ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
display_name	string	Display name of the newly registered business category group	Up to 128 characters

7. Change history

- Version: 8.0.0
  - Newly added.

8. Example

[Request]

```
POST /v1/business/nodes/groups/0 HTTP/1.1
referer: http://192.168.18.64:12080/umftool/vDCToolFreeRequest.jsp
accept-language: ja,en-US;q=0.7,en;q=0.3
x-authorization: token 1EFECD7965F72E48D98CF58078EBAE28
cookie: JSESSIONID=1C5F043EF655FC10A1D34B1B8DCC0EF3
accept: */*
authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
```

```
if-modified-since: Thu, 01 Jun 1970 00:00:00 GMT
x-cmtool-host: localhost
x-requested-with: XMLHttpRequest
x-cmtool-port: 8280
accept-encoding: gzip, deflate
user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20
100101 Firefox/49.0
X-UMF-API-Version: 2.0
Date: Wed, 22 Mar 2017 21:14:54 GMT
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Host: localhost:8280
Connection: keep-alive

{
    "display_name": "Application"
}
```

[Response]

```
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 21:14:54 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
    "display_name": "Application",
    "node_id": "373786f3de23ad60267cfd62a43451ab"
}
```

3.8.6 Updating a business category group

1. Process overview
   Update the business category group display name of the specified business node ID.
2. HTTP method

```
PUT
```

3. URL

```
/v1/businessview/nodes/groups/node_id
```

   In ***node_id***, specify the business node ID of the target business category group.
4. Parameter

Parameter	Type	Description	Required	Valid values
display_name	string	Display name to be updated	Required	Up to 128 characters

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The business category group information was successfully updated.
400	Bad Request	When the root is set to the target business node ID
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The business category group of the node ID specified in the URI does not exist.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
node_id	string	Updated business node ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
display_name	string	Updated display name	Up to 128 characters

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
PUT /v1/business/nodes/groups/373786f3de23ad60267cfd62a43451ab HTTP/1.
1
referer: http://192.168.18.64:12080/umftool/vDCToolFreeRequest.jsp
accept-language: ja,en-US;q=0.7,en;q=0.3
x-authorization: token 1EFECD7965F72E48D98CF58078EBAE28
cookie: JSESSIONID=1C5F043EF655FC10A1D34B1B8DCC0EF3
accept: */*
authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
if-modified-since: Thu, 01 Jun 1970 00:00:00 GMT
x-cmtool-host: localhost
x-requested-with: XMLHttpRequest
x-cmtool-port: 8280
accept-encoding: gzip, deflate
user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20
100101 Firefox/49.0
X-UMF-API-Version: 2.0
```

```
Date: Wed, 22 Mar 2017 21:14:54 GMT
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Host: localhost:8280
Connection: keep-alive

{
    "display_name": "System"
}
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: PUT
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 21:14:54 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
    "display_name": "System",
    "node_id": "373786f3de23ad60267cfd62a43451ab"
}
```

3.8.7 Deleting a business category group

1. Process overview

   Delete the business category group of the specified business node ID.

   If a business category group/business category belongs to the specified business category group, deletion fails.

   In such a case, remove the business category group/business category from the specified business category group before requesting.

2. HTTP method

```
DELETE
```

3. URL

```
/v1/businessview/nodes/groups/node_id
```

   In ***node_id***, specify the business node ID of the target business category group.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
204	No Content	The business category group information was successfully deleted.

HTTP status code	Meaning	Description
400	Bad Request	When the root is set to the target business node ID
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The business category group of the node ID specified in the URI does not exist.
412	Precondition Failed	A business node belongs to the specified business category group.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

   None

7. Change history

   - Version: 8.0.0
     - Newly added.

8. Example

   [Request]

```
DELETE /v1/business/nodes/groups/373786f3de23ad60267cfd62a43451ab HTTP
/1.1
referer: http://192.168.18.64:12080/umftool/vDCToolFreeRequest.jsp
accept-language: ja,en-US;q=0.7,en;q=0.3
x-authorization: token 1EFECD7965F72E48D98CF58078EBAE28
cookie: JSESSIONID=1C5F043EF655FC10A1D34B1B8DCC0EF3
accept: */*
authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
if-modified-since: Thu, 01 Jun 1970 00:00:00 GMT
x-cmtool-host: localhost
x-requested-with: XMLHttpRequest
x-cmtool-port: 8280
accept-encoding: gzip, deflate
user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20
100101 Firefox/49.0
X-UMF-API-Version: 2.0
Date: Wed, 22 Mar 2017 21:14:54 GMT
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Host: localhost:8280
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: DELETE
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 21:14:54 GMT
```

```
Transfer-Encoding: chunked
Connection: keep-alive
```

3.8.8 Viewing a business message filter

1. Process overview
   Retrieve the business message filter setting for the business category of the specified business node ID.
2. HTTP method

```
GET
```

3. URL

```
/v1/businessview/node_id/filters/messages
```

   In ***node_id***, specify the business node ID of the business category.
4. Parameter

   None
5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The business message filter information was successfully retrieved.
400	Bad Request	The request is incorrect. The parameter is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The business category of the node ID specified in the URI does not exist.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
filter[n]	object[]	Business message filter setting	-
filter[n].id	string	Business message filter ID A unique UUID is assigned by the system when created. This parameter must be set when updating the filter setting. It is not necessary when making a new addition.	Up to 36 characters consisting of hexadecimal numbers and hyphens
filter[n].name	string	Business message filter name	-
filter[n].type	string	Type. Specify "EXCLUDE" to suppress reporting when it matches the filter.	"STORE": Store "EXCLUDE": Exclude
filter[n].status	string	Business message filter operating status. Only filters with the "STARTING" status are applied.	"STARTING": Enabled "SUSPENDED": Disabled
filter[n].report_status	string	Operating status of the reporting setting set in the business message filter.	Enabled : Only for those business message filters

Parameter	Type	Description	Valid values
			with the "STARTING" status, the reporting setting is enabled. Disabled : If the "SUSPENDED"status is set, all the reporting settings set in the filter are disabled.
filter[n].message_id	string	Message ID. ID indicating the message type	-
filter[n].not_message_id	boolean	Not (Message ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].definition_code	string	Message definition ID. ID indicating the message definition used to generate a message text. Create this such that it is unique within the system.	-
filter[n].not_definition_code	boolean	Not (Message definition ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].severity	number	Specify the severity with a number. If omitted, this filter condition is ignored.	Integer between 0 to 255
filter[n].not_severity	boolean	Not (Severity)	false: Select matched messages. true: Select unmatched messages.
filter[n].severity_range	string	Severity range	">=": [severity] parameter or more "=": equal to [severity] parameter "<=": [severity] parameter or less
filter[n].confirm	string	Check flag	"UNCHECKED": Not checked "CHECKED": Checked
filter[n].not_confirm	boolean	Not (Check flag)	false: Select matched messages. true: Select unmatched messages.
filter[n].mark	string	Mark User-specific string. "CHECKING", "SOLVED", etc.	-
filter[n].not_mark	boolean	Not (Mark)	false: Select matched messages. true: Select unmatched messages.
filter[n].comment	string	Comment	-
filter[n].not_comment	boolean	Not (Comment)	false: Select matched messages. true: Select unmatched messages.
filter[n].agent_group_tenant_id	string	Tenant ID of the tenant to which the agent group specified in [agent_group_id] belongs. To specify [agent_group_id] in the filter parameter, [agent_group_tenant_id] of the tenant to which the target agent group belongs must be specified.	-

Parameter	Type	Description	Valid values
filter[n].agent_group_id	string	Agent group ID. To specify [agent_group_id], [agent_group_tenant_id] must be specified. Use this parameter when filtering messages under the specified agent group. Messages for agents under the specified agent group are filtered. Regular expressions cannot be used. Use a perfectly matched character string. Even when [agent_group_id] is specified, if the [node_id] parameter is not specified in the parameter of the reported message, the message is not filtered. Even when [agent_group_id] is specified, if the [node_type] parameter of the reported message is other than "AGENT", the message is not filtered.	-
filter[n].not_agent_group_id	boolean	Not (Agent group ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].agent_group_recursive	boolean	When filtering messages for agents under the specified agent group, specify whether to filter all the agents recursively or only those agents immediately under the specified agent group.	true: Retrieve agents under the specified agent group recursively, false: Retrieve only those agents immediately under the specified agent group, Default: false
filter[n].system_name	string	System name of the manager Stores the machine name.	-
filter[n].not_system_name	boolean	Not (System name)	false: Select matched messages. true: Select unmatched messages.
filter[n].node_id	string	Node ID. This matches the filter when a message for the specified node ID is registered.	-
filter[n].not_node_id	boolean	Not (Node ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].node_type	string	Records that perfectly match the specified node type are extracted. Enter "MANAGER" for those messages that were issued by the manager, "AGENT" or a relevant agent type for those messages that were reported from the agent, or any string for other messages. If omitted, this filter condition is ignored.	-
filter[n].not_node_type	boolean	Not (Node type)	false: Select matched messages. true: Select unmatched messages.
filter[n].node_name	string	Node name. If omitted, this filter condition is ignored.	-

Parameter	Type	Description	Valid values
filter[n].not_node_name	boolean	Not (Node name)	false: Select matched messages. true: Select unmatched messages.
filter[n].application	string	Application. This matches the filter when a message for the specified application is registered. If omitted, this filter condition is ignored.	-
filter[n].not_application	boolean	Not (Application)	false: Select matched messages. true: Select unmatched messages.
filter[n].object	string	Object. This matches the filter when a message for the specified object is registered. If omitted, this filter condition is ignored.	-
filter[n].not_object	boolean	Not (Object)	false: Select matched messages. true: Select unmatched messages.
filter[n].category	string	Type. If omitted, this filter condition is ignored.	"SYSTEM" "APPLICATION"
filter[n].not_category	boolean	Not (Type)	false: Select matched messages. true: Select unmatched messages.
filter[n].message_summary	string	Description. This matches the filter when a message for the specified message overview is registered. If omitted, this filter condition is ignored.	-
filter[n].not_message_summary	boolean	Not (Description)	false: Select matched messages. true: Select unmatched messages.
filter[n].message_text	string	Message text. This matches the filter when a message for the specified message text is registered. If omitted, this filter condition is ignored.	-
filter[n].not_message_text	boolean	Not (Message text)	false: Select matched messages. true: Select unmatched messages.
filter[n].tenant_id	string	Tenant ID of the tenant that created the business message filter.	-
filter[n].operation_type	string	Processing type. "NONE" is always selected for the response.	"NONE": No change
filter[n].overwrite_summary	string	Replaces the summary of the filtered message with the specified character string.	-
filter[n].knowledge[m]	object[]	Knowledge information about the filtered message.	-
filter[n].knowledge[m].id	string	Knowledge definition ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
filter[n].knowledge[m].operation_type	string	Processing type. Specify newly add, update, delete, or no change.	-

Parameter	Type	Description	Valid values
		This parameter is required for a request. "NONE" is always selected for the response.	
filter[n].knowledge[m].title	string	Title of the knowledge information about the filtered message.	Up to 1024 characters
filter[n].knowledge[m].type	string	Type of the knowledge information about the filtered message.	TEXT: Text, HTML: HTML, Default: Text
filter[n].knowledge[m].text	string	Text of the knowledge information about the filtered message.	Up to 16384 characters
filter[n].report[m]	object[]	Service notification setting	-
filter[n].report[m].component_type	string	Component type of the notification destination service. Requests the RestAPI of the micro service of specified component type and reports that the message has been registered.	-
filter[n].report[m].trigger_id	string	Transfer ID to the notification destination service. This is an ID that is set arbitrarily by the micro service of specified component type.	-
filter[n].report[m].report_id	string	Service notification setting ID. This parameter must be specified if "UPDATE" is set to the filter setting processing type (filter[n].operation_type). For values other than "UPDATE", this is ignored. A unique UUID is assigned by the system when created. This parameter must be set when updating the service notification setting.	-
filter[n].report[m].operation_type	string	Processing type. Specify newly add, update, delete, or no change for the service notification setting. This parameter is required for a request. "NONE" is always selected for the response.	"NONE": No change

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/business/filters/messages/565326d2fe21bc89590baf82b43573ba HTT
P/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
```

```
Connection: keep-alive
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 19:33:03 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
   "filter": [
      {
         "agent_group_id": "msc_extlink_0000000002",
         "agent_group_recursive": false,
         "application": "Unified Management Framework",
         "category": "APPLICATION",
         "comment": "pending",
         "confirm": "UNCHECKED",
         "definition_code":"2000000000",
         "id": "9c96d4ec-0e78-11e7-8df0-005056b66332",
         "mark": "PROCESSING",
         "message_id": "00080003",
         "message_summary": "summary",
         "message_text": "abcdefghijklmnopqrstuvwxyz1234567890",
         "name": "filter name",
         "node_id": "msc_extlink_MANAGER~AGENT",
         "node_name": "nodeA",
         "node_type": "AGENT",
         "not_agent_group_id": false,
         "not_application": false,
         "not_category": false,
         "not_comment": false,
         "not_confirm": false,
         "not_mark": false,
         "not_message_id": false,
         "not_message_summary": false,
         "not_message_text": false,
         "not_node_id": false,
         "not_node_name": false,
         "not_node_type": false,
         "not_object": false,
         "not_severity": false,
         "not_system_name": false,
         "operation_type": "NONE",
         "object": "ProcessMonitor",
         "overwrite_summary": "business message",
         "report" : [
            {
                "component_type" : "msc_report",
                "operation_type" : "NONE",
                "report_id" : "a82229f4-0e7a-11e7-a074-005056b66332",
```

```
                "trigger_id" : "b4932012-de12-81e3-876a-83d051732301"
            }
          ],
          "severity": 150,
          "severity_range":"=",
          "status": "STARTING",
          "report_status":"STARTING",
          "system_name": "System1",
          "tenant_id": "DefaultTenant",
          "type": "STORE",
          "knowledge":[
             {
                "id": "5c96d4ec-0e78-11e7-8df0-005056b66332",
                "operation_type" : "NONE",
                "title":"recovery info",
                "type":"html",
                "text":"<html><title>recovery info<\/title><body><p><a
 href=\"http:\/\/host.nec.co.jp\/knowledge\/recovery\">recovery info<\
/a><\/p><\/body><\/html>"
             }
          ]
       }
    ]
}
```


3.8.9 Uploading all business message filters simultaneously

1. Process overview

   Newly add, update, or delete business message filter setting for the specified business node ID. Specify ADD (newly add), UPDATE (update), DELETE (delete), or NONE (not change) in the [operation_type] request parameter.

   If operation_type is set to "ADD", it is treated as a new business message filter to be added.

   If operation_type is set to "UPDATE", specify the business message filter ID you want to update and then update the parameter. String-type request parameters without this setting are updated without filter conditions.

   If operation_type is set to "DELETE", the business message filter setting is deleted.

   If operation_type is set to "NONE", the business message filter setting is ignored and not changed.

   In the business message filter list and responses after upload, operation_type is always set to "NONE".

   To change the business message filter application priority, change the business message filter list order in the body message.

   The business message filters are applied in the list order. In the business message filter list and responses after upload, the priority order is applied.

   A business message filter setting not requested in the body message is ignored and not changed but is set to the lowest priority.

   If omitted, string-type request parameters are updated without filter conditions.

2. HTTP method

```
POST
```

3. URL

```
/v1/businessview/node_id/filters/messages/import
```

In ***node_id***, specify the business node ID of the business category.

4. Parameter

Parameter	Type	Description	Required	Valid values
filter[n]	object[]	Business message filter definition setting	Required	-
filter[n].id	string	Business message filter ID A unique UUID is assigned by the system when created. This parameter must be set when updating the business message filter setting. It is not necessary when making a new addition.	-	Up to 36 characters consisting of hexadecimal numbers and hyphens
filter[n].name	string	Business message filter name	-	Up to 128 characters
filter[n].type	string	Type. Specify "EXCLUDE" to suppress reporting when it matches the business message filter.	-	"STORE": Store "EXCLUDE": Exclude Default value: STORE Up to 16 characters
filter[n].status	string	Business message filter operating status. Enabled: Only business message filters with the [STARTING] status are enabled as filters.	-	"STARTING": Enabled "SUSPENDED": Disabled Default value: "STARTING" Up to 16 characters
filter[n].report_status	string	Operating status of the reporting setting set in the business message filter. Enabled: For those business message filters with the [STARTING] status, the reporting setting is enabled. Disabled: If the [SUSPENDED] status is set, all the reporting	-	"STARTING": Enabled "SUSPENDED": Disabled Default value: "STARTING" Up to 16 characters

Parameter	Type	Description	Required	Valid values
		settings set in the filter are disabled.		
filter[n].message_id	string	Message ID. ID indicating the message type Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_message_id	boolean	Not (Message ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].definition_code	string	Message definition ID. ID indicating the message definition used to generate a message text. Create this such that it is unique within the system. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_definition_code	boolean	Not (Message definition ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].severity	number	Specify the severity with a number. If omitted, this filter condition is ignored.	-	Integer between 0 to 255 Default value: 15
filter[n].not_severity	boolean	Not (Severity) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false

Parameter	Type	Description	Required	Valid values
filter[n].severity_range	string	If omitted, this filter condition is ignored. To specify [severity_range] in the filter parameter, [severity] must be specified.	-	">=": [severity] parameter or more "=": equal to [severity] parameter "<=": [severity] parameter or less Default value: [=]
filter[n].confirm	string	Check flag. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	"UNCHECKED": Not checked "CHECKED": Checked Up to 1024 characters
filter[n].not_confirm	boolean	Not (Check flag) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].mark	string	Mark Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_mark	boolean	Not (Mark) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].comment	string	Comment Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 4096 characters
filter[n].not_comment	boolean	Not (Comment) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].agent_group_tenant_id	string	Tenant ID of the tenant to which the agent group specified in	-	Up to 1024 characters

Parameter	Type	Description	Required	Valid values
		[agent_group_id] belongs. To specify [agent_group_id] in the business message filter parameter, [agent_group_tenant_id] of the tenant to which the target agent group belongs must be specified.		
filter[n].agent_group_id	string	Agent group ID. Filters messages for agents under the specified agent group. To specify [agent_group_id], [agent_group_tenant_id] must be specified. Regular expressions cannot be used. Use a perfectly matched character string. Even when [agent_group_id] is specified, there are some restrictions on filtering due to the following notification message parameters. When the [node_id] parameter is not specified, messages are not filtered. When the [node_type] parameter is not "AGENT", messages are not filtered.	-	Up to 1024 characters
filter[n].not_agent_group_id	boolean	Not (Agent group ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].agent_group_recursive	boolean	When filtering messages for agents under the specified agent group, specify whether to filter all the agents recursively or only those agents	-	true: Retrieve agents under the specified agent group recursively false: Retrieve only those agents immediately under the specified agent group Default value: false

Parameter	Type	Description	Required	Valid values
		immediately under the specified agent group.		
filter[n].system_name	string	System name Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_system_name	boolean	Not (System name) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].node_id	string	Node ID. This matches the business message filter when the message for the specified node ID is registered. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_node_id	boolean	Not (Node ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].node_type	string	Node type. Filters messages that perfectly match the specified node type. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	"MANAGER": Messages issued by the manager "AGENT": Messages reported from the agent A string of specific type can also be specified. Up to 1024 characters
filter[n].not_node_type	boolean	Not (Node type) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false

Parameter	Type	Description	Required	Valid values
filter[n].node_name	string	Node name Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_node_name	boolean	Not (Node name) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].application	string	Application Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_application	boolean	Not (Application) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].object	string	Object. Use regular expressions (perfect match example: "^String$"). If omitted, this filter condition is ignored.	-	Up to 1024 characters
filter[n].not_object	boolean	Not (Object) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].category	string	Type. This matches the business message filter when a message for the specified type is registered. Use regular expressions (perfect match example: "^String$").	-	"SYSTEM" "APPLICATION" Up to 1024 characters

Parameter	Type	Description	Required	Valid values
		If omitted, this filter condition is ignored.		
filter[n].not_category	boolean	Not (Type) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].message_summary	string	Definition. If this flag is set to true, the specified parameter becomes the filter exclusion condition. If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	Up to 1024 characters
filter[n].not_message_summary	boolean	Not (Definition) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].message_text	string	Message text. If this flag is set to true, the specified parameter becomes the filter exclusion condition. If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	Up to 8192 characters
filter[n].not_.message_text	boolean	Not (Message text) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	-	false: Select matched messages. true: Select unmatched messages. Default value: false
filter[n].operation_type	string	Processing type. Specify add, update, delete, or no change for each specified business filter setting.	-	"ADD": Add "UPDATE": Update "DELETE": Delete "NONE": No change Up to 32 characters Default value: "NONE"

<table>
<tr><th>Parameter</th><th>Type</th><th>Description</th><th>Required</th><th>Valid values</th></tr>
<tr><td>filter[n].overwrite_summary</td><td>string</td><td>Replaces the summary of the filtered message with the specified character string.</td><td>-</td><td>Up to 256 characters
The following replacement character strings can be used in overwrite_summary.<table><tr><th>Replacement character</th><th>Description</th></tr><tr><td>$message_id$</td><td>Message ID</td></tr><tr><td>$definition_code$</td><td>Message definition</td></tr><tr><td>$tenant_id$</td><td>Tenant ID</td></tr><tr><td>$severity$</td><td>Severity</td></tr><tr><td>$create_time$</td><td>Occurrence date and time</td></tr><tr><td>$system_name$</td><td>System name</td></tr><tr><td>$node_id$</td><td>Node ID</td></tr><tr><td>$node_type$</td><td>Node type</td></tr><tr><td>$node_name$</td><td>Node name</td></tr><tr><td>$application$</td><td>Application</td></tr><tr><td>$object$</td><td>Object</td></tr><tr><td>$summary$</td><td>Message overview</td></tr><tr><td>$message_no$</td><td>Message number</td></tr><tr><td>$receive_time$</td><td>Reception date and time</td></tr><tr><td>$message_text$</td><td>Message text</td></tr></table></td></tr>
<tr><td>filter[n].knowledge[m]</td><td>object[]</td><td>Knowledge information about the filtered message.</td><td>-</td><td>-</td></tr>
<tr><td>filter[n].knowledge[m].id</td><td>string</td><td>Knowledge definition ID. A unique UUID is assigned by the system when created.
Whether this parameter can be omitted depends on the filter setting processing type (filter[n].operation_type).
When filter[n].operation_type is "ADD": This parameter is ignored.
When filter[n].operation_type is "UPDATE":</td><td>-</td><td>Up to 36 characters consisting of hexadecimal numbers and hyphens</td></tr>
</table>

Parameter	Type	Description	Required	Valid values
		Whether this parameter can be omitted depends on filter[n].report[m].operation_type. When filter[n].knowledge[m].operation_type is "ADD": This parameter is ignored. When filter[n].knowledge[m].operation_type is "UPDATE" or "DELETE": This parameter must be specified. When filter[n].operation_type is "DELETE": This parameter is ignored. When filter[n].operation_type is "NONE": This parameter is ignored.		
filter[n].knowledge[m].operation_type	string	Processing type. Specify newly add, update, delete, or no change. This parameter is required for a request. "NONE" is always selected for the response.	-	"ADD": Add "UPDATE": Update "DELETE": Delete "NONE": No change Up to 32 characters Default value: NONE
filter[n].knowledge[m].title	string	Title of the knowledge information about the filtered message.	-	Up to 1024 characters
filter[n].knowledge[m].type	string	Type of the knowledge information about the filtered message.	-	TEXT: Text, HTML: HTML, Default: Text
filter[n].knowledge[m].text	string	Text of the knowledge information about the filtered message. This would be HTML text in the <BODY> tag if "HTML" is specified for the knowledge information type.	-	Up to 16384 characters The following replacement character strings can be used in the knowledge text. **Replacement character** / **Description** $message_id$ / Message ID $definition_code$ / Message definition $tenant_id$ / Tenant ID

<table>
<tr><th>Parameter</th><th>Type</th><th>Description</th><th>Required</th><th>Valid values</th></tr>
<tr><td></td><td></td><td></td><td></td><td>
<table>
<tr><th>Replacement character</th><th>Description</th></tr>
<tr><td>$severity$</td><td>Severity</td></tr>
<tr><td>$create_time$</td><td>Occurrence data and time</td></tr>
<tr><td>$system_name$</td><td>System name</td></tr>
<tr><td>$node_id$</td><td>Node ID</td></tr>
<tr><td>$node_type$</td><td>Node type</td></tr>
<tr><td>$node_name$</td><td>Node name</td></tr>
<tr><td>$application$</td><td>Application</td></tr>
<tr><td>$object$</td><td>Object</td></tr>
<tr><td>$summary$</td><td>Message overview</td></tr>
<tr><td>$message_no$</td><td>Message number</td></tr>
<tr><td>$receive_time$</td><td>Reception date and time</td></tr>
<tr><td>$message_text$</td><td>Message text</td></tr>
<tr><td>$confirm$</td><td>Check flag</td></tr>
<tr><td>$mark$</td><td>Mark</td></tr>
<tr><td>$comment$</td><td>Comment</td></tr>
</table>
If the character limit is exceeded after replacement, the text up to the limit is displayed when the business knowledge viewing API is executed.
</td></tr>
<tr><td>filter[n].report[m]</td><td>object[]</td><td>Service notification setting</td><td>-</td><td>-</td></tr>
<tr><td>filter[n].report[m].component_type</td><td>string</td><td>Component type of the notification destination service. Requests the RESTful API of the micro service of specified component type and reports that the message has been registered.</td><td>-</td><td>Up to 32 characters
Default value:
msc_report</td></tr>
<tr><td>filter[n].report[m].trigger_id</td><td>string</td><td>Transfer ID to the notification destination service. This is an ID that is set arbitrarily by the micro service of specified component type.</td><td>-</td><td>Up to 256 characters</td></tr>
<tr><td>filter[n].report[m].report_id</td><td>string</td><td>Service notification setting ID A unique UUID is assigned by</td><td>-</td><td>Up to 256 characters</td></tr>
</table>

Parameter	Type	Description	Required	Valid values
		the system when adding a service notification setting. Whether this parameter can be omitted depends on the filter setting processing type (filter[n].operation_type). When filter[n].operation_type is "ADD": This parameter is ignored. When filter[n].operation_type is "UPDATE": Whether this parameter can be omitted depends on filter[n].report[m].operation_type. When filter[n].report[m].operation_type is "ADD": This parameter is ignored. When filter[n].report[m].operation_type is "UPDATE" or "DELETE": This parameter must be specified. When filter[n].operation_type is "DELETE": This parameter is ignored. When filter[n].operation_type is "NONE": This parameter is ignored.		
filter[n].report[m].operation_type	string	Specify add, update, delete, or no change for the specified service notification setting. Whether this parameter can be omitted depends on the filter setting processing type (filter[n].operation_type).	-	"ADD": Add "UPDATE": Update "DELETE": Delete "NONE": No change Default value: NONE

Parameter	Type	Description	Required	Valid values
		When filter[n].operation_type is "ADD": This parameter must be "ADD". When filter[n].operation_type is "UPDATE": This parameter must be "ADD", "UPDATE", "DELETE", or "NONE". When filter[n].operation_type is "DELETE": This parameter is ignored. When filter[n].operation_type is "NONE": This parameter is ignored.		

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	Business message filter information registered after update. For those parameters with a null data set, the response JSON key is omitted.
400	Bad Request	The request is incorrect. The parameter is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The business category of the node ID specified in the URI does not exist.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
filter[n]	object[]	Business message filter definition setting	-
filter[n].id	string	Business message filter ID A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
filter[n].name	string	Business message filter name	Up to 128 characters
filter[n].type	string	Type	"STORE": Store "EXCLUDE": Exclude

Parameter	Type	Description	Valid values
			Up to 16 characters
filter[n].status	string	Business message filter operating status	"STARTING": Enabled "SUSPENDED": Disabled Up to 16 characters
filter[n].report_status	string	Operating status of the reporting setting set in the business message filter	"STARTING": Enabled "SUSPENDED": Disabled Up to 16 characters
filter[n].message_id	string	Message ID. ID indicating the message type	Up to 1024 characters
filter[n].not_message_id	boolean	Not (Message ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].definition_code	string	Message definition ID. ID indicating the message definition used to generate a message text. Create this such that it is unique within the system.	Up to 1024 characters
filter[n].not_definition_code	boolean	Not (Message definition ID)	false: Select matched messages. true: Select unmatched messages.
filter[n].severity	number	Specify the severity with a number.	Integer between 0 to 255
filter[n].not_severity	boolean	Not (Severity) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].severity_range	string	Severity range	">=": [severity] parameter or more "=": equal to [severity] parameter "<=": [severity] parameter or less
filter[n].confirm	string	Check flag	"UNCHECKED": Not checked "CHECKED": Checked Up to 1024 characters
filter[n].not_confirm	boolean	Not (Check flag) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].mark	string	Mark	Up to 1024 characters
filter[n].not_mark	boolean	Not (Mark) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].comment	string	Comment	Up to 1024 characters
filter[n].not_comment	boolean	Not (Comment) If this flag is set to true, the specified parameter	false: Select matched messages. true: Select unmatched messages.

Parameter	Type	Description	Valid values
		becomes the filter exclusion condition.	
filter[n].agent_group_tenant_id	string	Tenant ID of the tenant to which the agent group specified in [agent_group_id] belongs. To specify [agent_group_id] in the filter parameter, [agent_group_tenant_id] of the tenant to which the target agent group belongs must be specified.	Up to 64 characters
filter[n].agent_group_id	string	Agent group ID. Filters messages for agents under the specified agent group. To specify [agent_group_id], [agent_group_tenant_id] must be specified. Regular expressions cannot be used. Use a perfectly matched character string. Even when [agent_group_id] is specified, there are some restrictions on filtering due to the following notification message parameters. When the [node_id] parameter is not specified, messages are not filtered. When the [node_type] parameter is other than "AGENT", messages are not filtered.	Up to 1024 characters
filter[n].not_agent_group_id	boolean	Not (Agent group ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].agent_group_recursive	boolean	When filtering messages for agents under the specified agent group, specify whether to filter all the agents recursively or only those agents immediately under the specified agent group.	true: Retrieve agents under the specified agent group recursively false: Retrieve only those agents immediately under the specified agent group Default value: false
filter[n].system_name	string	System name	Up to 1024 characters

Parameter	Type	Description	Valid values
filter[n].not_system_name	boolean	Not (System name) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].node_id	string	Node ID. This matches the filter when a message for the specified node ID is registered.	Up to 1024 characters
filter[n].not_node_id	boolean	Not (Node ID) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].node_type	string	Node type. Filters messages that perfectly match the specified node type.	"MANAGER": Messages issued by the manager "AGENT": Messages reported from the agent String of specific type Up to 1024 characters
filter[n].not_node_type	boolean	Not (Node type) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].node_name	string	Node name.	Up to 1024 characters
filter[n].not_node_name	boolean	Not (Node name) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].application	string	Application	Up to 1024 characters
filter[n].not_application	boolean	Not (Application) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].object	string	Object	Up to 1024 characters
filter[n].not_object	boolean	Not (Object) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].category	string	Type. This matches the filter when a message for the specified type is registered.	"SYSTEM" "APPLICATION" Up to 1024 characters
filter[n].not_category	boolean	Not (Type)	false: Select matched messages. true: Select unmatched messages.

Parameter	Type	Description	Valid values
		If this flag is set to true, the specified parameter becomes the filter exclusion condition.	
filter[n].message_summary	string	Description	Up to 1024 characters
filter[n].not_message_summary	boolean	Not (Description) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].message_text	string	Message text	Up to 8192 characters
filter[n].not_.message_text	boolean	Not (Message text) If this flag is set to true, the specified parameter becomes the filter exclusion condition.	false: Select matched messages. true: Select unmatched messages.
filter[n].tenant_id	string	Tenant ID of the tenant that created the business message filter	Up to 64 characters
filter[n].operation_type	string	Processing type. "NONE" is always selected for the response.	If this flag is set to true, the specified parameter becomes the filter exclusion condition. "NONE": No change
filter[n].overwrite_summary	string	Replaces the summary of the filtered message with the specified character string.	-
filter[n].knowledge[m]	object	Knowledge information about the filtered message.	-
filter[n].knowledge[m].id	string	Knowledge definition ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
filter[n].knowledge[m].operation_type	string	Processing type. "NONE" is always selected for the response.	"NONE": No change
filter[n].knowledge[m].title	string	Title of the knowledge information about the filtered message.	Up to 1024 characters
filter[n].knowledge[m].type	string	Type of the knowledge information about the filtered message.	TEXT: Text HTML: HTML Default: TEXT
filter[n].knowledge[m].text	string	Text of the knowledge information about the filtered message.	Up to 16384 characters
filter[n].report[m]	object[]	Service notification setting	-
filter[n].report[m].component_type	string	Component type of the notification destination service. Requests the	Up to 32 characters

Parameter	Type	Description	Valid values
		RESTful API of the micro service of specified component type and reports that the message has been registered.	
filter[n].report[m].trigger_id	string	Transfer ID to the notification destination service. This is an ID that is set arbitrarily by the micro service of specified component type.	Up to 256 characters
filter[n].report[m].report_id	string	Service notification setting ID. A unique UUID is assigned by the system when adding a service notification setting.	Up to 256 characters
filter[n].report[m].operation_type	string	Processing type. "NONE" is always selected for the response.	"NONE": No change Up to 32 characters

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
POST /v1/business/filters/messages/import/565326d2fe21bc89590baf82b435
73ba HTTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Content-Type: application/json;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 1447

{
   "filter" : [
      {
         "agent_group_id": "msc_extlink_0000000002",
         "agent_group_recursive": false,
         "application": "Unified Management Framework",
         "category": "APPLICATION",
         "comment": "pending",
         "confirm": "UNCHECKED",
         "definition_code":"2000000000",
         "name" : "filter name",
         "node_name" : "nodeA",
         "node_id": "msc_extlink_MANAGER~AGENT",
         "node_type" : "AGENT",
```

```
         "operation_type" : "ADD",
         "object": "ProcessMonitor",
         "overwrite_summary": "business message",
         "mark": "PROCESSING",
         "message_id": "00080003",
         "message_summary": "summary",
         "message_text": "abcdefghijklmnopqrstuvwxyz1234567890",
         "report" : [
            {
                "component_type" : "msc_report",
                "trigger_id" : "b4932012-de12-81e3-876a-83d051732301",
                "operation_type" : "ADD"
            }
        ],
        "severity" : 150,
        "severity_range":"=",
        "status" : "STARTING",
        "report_status" : "STARTING",
        "system_name" : "System1",
        "tenant_id" : "DefaultTenant",
        "type" : "STORE",
        "knowledge":[
           {
              "operation_type" : "ADD",
              "title":"recovery info",
              "type":"html",
              "text":"<html><title>recovery info<\/title><body><p><a h
ref=\"http:\/\/host.nec.co.jp\/knowledge\/recovery\">recovery info<\/a
><\/p><\/body><\/html>"

           }
        ]
      }
   ]
}
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 19:33:12 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
   "filter": [
      {
         "agent_group_id": "msc_extlink_0000000002",
         "agent_group_recursive": false,
         "application": "Unified Management Framework",
         "category": "APPLICATION",
         "comment": "pending",
         "confirm": "UNCHECKED",
         "definition_code":"2000000000",
```

```
          "id": "9c96d4ec-0e78-11e7-8df0-005056b66332",
          "mark": "PROCESSING",
          "message_id": "00080003",
          "message_summary": "summary",
          "message_text": "abcdefghijklmnopqrstuvwxyz1234567890",
          "name": "filter name",
          "node_id": "msc_extlink_MANAGER~AGENT",
          "node_name": "nodeA",
          "node_type": "AGENT",
          "not_agent_group_id": false,
          "not_application": false,
          "not_category": false,
          "not_comment": false,
          "not_confirm": false,
          "not_mark": false,
          "not_message_id": false,
          "not_message_summary": false,
          "not_message_text": false,
          "not_node_id": false,
          "not_node_name": false,
          "not_node_type": false,
          "not_object": false,
          "not_severity": false,
          "not_system_name": false,
          "operation_type": "NONE",
          "object": "ProcessMonitor",
          "overwrite_summary": "business message",
          "report" : [
             {
                 "component_type" : "msc_report",
                 "operation_type" : "NONE",
                 "report_id" : "a82229f4-0e7a-11e7-a074-005056b66332",
                 "trigger_id" : "b4932012-de12-81e3-876a-83d051732301"
             }
           ],
           "severity": 150,
           "severity_range":"=",
           "status": "STARTING",
           "report_status":"STARTING",
           "system_name": "System1",
           "tenant_id": "DefaultTenant",
           "type": "STORE",
           "knowledge":[
              {
                 "id": "5c96d4ec-0e78-11e7-8df0-005056b66332",
                 "operation_type" : "NONE",
                 "title":"recovery info",
                 "type":"html",
                 "text":"<html><title>recovery info<\/title><body><p><a
 href=\"http:\/\/host.nec.co.jp\/knowledge\/recovery\">recovery info<\
/a><\/p><\/body><\/html>"
              }
           ]
       }
    ]
}
```

3.8.10 Getting the number of business category messages

1. Process overview
   Retrieve the number of business category messages of the specified business node ID by severity.
2. HTTP method

```
POST
```

3. URL

```
/v1/businessview/summaries/categories/messages
```

4. Parameter

Parameter	Type	Description	Required	Valid values
node_ids	string[]	Array of business node IDs	Required	Business node ID of the business category retrieved by viewing the business node Up to 36 characters consisting of hexadecimal numbers and hyphens

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The number of business category messages was successfully retrieved.
206	Partial Content	Some business category messages were not successfully retrieved.
400	Bad Request	The request is incorrect. The parameter is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	None of the business categories of business node IDs specified in node_ids exists, or all the business node IDs specified in node_ids are business category groups.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
business_nodes	object[]	Array of business node information	-
business_nodes[n].node_id	string	Business node ID. A unique UUID is assigned by the system when created.	Up to 36 characters consisting of hexadecimal numbers and hyphens
business_nodes[n].summaries	object[]	Message overview object	-

Parameter	Type	Description	Valid values
business_nodes[n].summaries[m].severity	number	Severity	Integer between 0 to 255 • 200: Abnormal • 150: Warning • 100: Unknown • 50: Normal • 15: No severity • 10: Monitoring stopped
business_nodes[n].summaries[m].number	number	Number of specified business category messages by severity.	Integer of 9223372036854775807 or less

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
POST /v1/business/summaries/categories/messages HTTP/1.1
referer: http://192.168.18.64:12080/umftool/vDCToolFreeRequest.jsp
accept-language: ja,en-US;q=0.7,en;q=0.3
x-authorization: token 1EFECD7965F72E48D98CF58078EBAE28
cookie: JSESSIONID=1C5F043EF655FC10A1D34B1B8DCC0EF3
accept: */*
authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
if-modified-since: Thu, 01 Jun 1970 00:00:00 GMT
x-cmtool-host: localhost
x-requested-with: XMLHttpRequest
x-cmtool-port: 8280
accept-encoding: gzip, deflate
user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20
100101 Firefox/49.0
X-UMF-API-Version: 2.0
Date: Wed, 22 Mar 2017 21:14:54 GMT
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Host: localhost:8280
Connection: keep-alive

{
    "node_ids": [
        "565326d2-fe21-bc89-590b-af82b43573ba",
        "0d753ba0-0e21-11d2-da1b-00003987b123"
    ]
}
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
```

```
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 22 Mar 2017 21:14:54 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
    "business_nodes": [
        {
            "node_id": "565326d2-fe21-bc89-590b-af82b43573ba",
            "summaries": [
                {
                    "number": 0,
                    "severity": 0
                },
                {
                    "number": 0,
                    "severity": 1
                },
                {
                    "number": 0,
                    "severity": 2
                },

                ---- Omitted ----

                {
                    "number": 0,
                    "severity": 254
                },
                {
                    "number": 0,
                    "severity": 255
                }
            ]
        },
        {
            "node_id": "0d753ba0-0e21-11d2-da1b-00003987b123",
            "summaries": [
                {
                    "number": 0,
                    "severity": 0
                },
                {
                    "number": 0,
                    "severity": 1
                },
                {
                    "number": 0,
                    "severity": 2
                },

                ---- Omitted ----

                {
                    "number": 0,
                    "severity": 254
                },
```

```
                {
                    "number": 0,
                    "severity": 255
                }
            ]
        }
    ]
}
```

3.8.11 Viewing business knowledge

1. Process overview
   Retrieve the knowledge information about the message for the specified business node ID.
2. HTTP method

   ```
   GET
   ```

3. URL

   ```
   /v1/businessview/node_id/message_no/knowledge
   ```

   In ***node_id***, specify the business node ID of the business category. In ***message_no***, specify the message number for which you want to view the knowledge information.
4. Parameter

   None
5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The knowledge information was successfully retrieved.
400	Bad Request	The request is incorrect. The parameter is incorrect.
401	Unauthorized	Authentication error. The request has no required authentication token.
404	Not Found	The business category of the node ID specified in the URI does not exist. The business category is not filtered by the message number specified in the URI.
500	Internal Server Error	This is an internal error on the server.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
message	object	Message object	-
messages.tenant_id	string	Stores the tenant ID to which the user registering the message belongs or the tenant ID reported from the agent.	Up to 64 characters
messages.business_node_id	string	Business node ID	Only business node ID with the type set to business category

Parameter	Type	Description	Valid values
			(node_type="CATEGORY")
messages.message_no	number	Message number	Integer between 1 to 9223372036854775807
message.knowledge[m]	object[]	Knowledge information about the filtered message.	-
message.knowledge[m].title	string	Title of the knowledge information about the filtered message.	Up to 1024 characters
message.knowledge[m].type	string	Type of the knowledge information about the filtered message.	TEXT: Text HTML: HTML Default: TEXT
message.knowledge[m].text	string	Text of the knowledge information about the filtered message.	Up to 16384 characters If the character limit is exceeded, text up to the limit is displayed.

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/businessview/565326d2fe21bc89590baf82b43573ba/3270/knowledge H
TTP/1.1
Authorization: Bearer 6350ad89-faac-3429-b391-a4a99bd7fe94
X-Authorization: token 7AEFEB99CA184A3361344918B2325162
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_121
Host: localhost:8280
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Content-Type: application/json
Date: Wed, 25 Oct 2017 19:33:03 GMT
Transfer-Encoding: chunked
Connection: keep-alive

{
   "messages":
      {
         "tenant_id": "DefaultTenant",
```

```
        "business_node_id": "565326d2fe21bc89590baf82b43573ba",
        "message_no": 3270,
        "knowledge":[
            {
                "title":"recovery info",
                "type":"HTML",
                "text":"<html><title>recovery info<\/title><body><p><a
href=\"http:\/\/host.nec.co.jp\/knowledge\/recovery\">recovery info<\/
a><\/p><\/body><\/html>"
            },
            {
                "title":"recovery info",
                "type":"TEXT",
                "text":"Please read recovery.pdf."
            }
        ]
    }
  ]
}
```


3.9 External interface

3.9.1 Getting the node list

1. Process overview

   Retrieve a list of node information.

   For details about the information that can be retrieved, see "6. Response (HTTP body)."

2. HTTP method

```
GET
```

3. URL

```
/v1/extlink/nodes?limit=limit&offset=offset&group_id=group_id&recursive=recursive&os_type=os_type
```

Key name	Description	Omittable
limit	Specify the maximum number of items to be retrieved between 0 and 32767. If omitted (or if a value outside the range is set), the number is unlimited.	-
offset	Specify the acquisition start position between 0 and 32767. If 200 nodes match the search conditions and the limit is 100, specify the offset as follows to retrieve the nodes. To retrieve the 1st to 100th nodes: offset=0 To retrieve the 101st to 200th nodes: offset=100	-
group_id	Specify the group ID. If omitted, all the nodes in the tenant are retrieved.	-
recursive	Specify whether to search under the group recursively with true or false. Specifically, select "true" (search recursively) or "false" (not search recursively). If omitted, "false" (not search recursively) is assumed.	-

os_type	Specify the OS type. The following types are available. Windows, Linux, HP-UX, Solaris, AIX, ESX, AWS * This item is case-insensitive.	-

If multiple queries are specified as node search conditions, information of the nodes that match all the conditions (AND condition) is retrieved.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	A list of node information was successfully retrieved.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target is not found.
405	Method Not Allowed	The specified method is not authorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Return value
total_item	number	Total number of items	-
items_per_page	number	Number of items retrieved in the request	-
next_offset	number	Start position for requesting of next acquisition If all the items are retrieved as a result of this request, 0 is returned.	-
node_list	object[]	Array of node information	-
node_list[n]. management_type	string	Linkage destination component type	SystemManagerG-FW
node_list[n]. node_id	string	Node ID	Format: msc_extlink_{manager-name} to {agent-name}
node_list[n]. node_name	string	Node name	-
node_list[n]. node_type	string	Node type	Host
node_list[n]. os_type	string	OS type of the node	Windows, Linux, HP-UX, Solaris, AIX, ESX, AWS
node_list[n].	string	OS version of the node	-

Parameter	Type	Description	Return value
os_ver			
node_list[n]. tenant_id	string	Organization tenant ID	-
node_list[n]. parent_group_id	string	Organization group ID	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 7.1.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/extlink/nodes HTTP/1.1
Host: localhost:8280
Accept: */*
X-Authorization: token E798DF701E3528E737353EAFEE4E68A8
Authorization: df95d309-c5fe-196f-2622-416d19be6894
Date: Mon, 19 Feb 2018 15:56:56 GMT
```

   [Response]

```
HTTP/1.1 200 OK
Date: Mon, 19 Feb 2018 15:56:57 GMT
Connection: Close
Content-Type: application/json; charset=utf-8
Content-Length: 1259

{
  "items_per_page" : 3,
  "next_offset" : 0,
  "node_list" : [
    {
      "management_type" : "SystemManagerG-FW",
      "node_id" : "msc_extlink_managerA~agent3",
      "node_name" : "agent3",
      "node_type" : "Host",
      "order" : "",
      "os_type" : "Linux",
      "os_ver" : "Red Hat Enterprise Linux Server release 7.3 (Maipo)"
,
      "parent_group_id" : "msc_extlink_0000000000",
      "tenant_id" : "DefaultTenant"
    },
    {
      "management_type" : "SystemManagerG-FW",
      "node_id" : "msc_extlink_managerB~agent6",
      "node_name" : "agent6",
      "node_type" : "Host",
      "order" : "",
      "os_type" : "Windows",
```

```
      "os_ver" : "Windows 2018 Server",
      "parent_group_id" : "msc_extlink_0000000000",
      "tenant_id" : "TenantB"
    },
    {
      "management_type" : "SystemManagerG-FW",
      "node_id" : "msc_extlink_localhost.localdomain~localhost.localdo
main",
      "node_name" : "localhost.localdomain",
      "node_type" : "Host",
      "order" : "",
      "os_type" : "Linux",
      "os_ver" : "Red Hat Enterprise Linux Server release 7.2 (Maipo)"
,
      "parent_group_id" : "msc_extlink_0000000000",
      "tenant_id" : "DefaultTenant"
    }
  ],
  "total_item" : 3
}
```

3.9.2 Getting a node

1. Process overview

   Retrieve node information.

   For details about the information that can be retrieved, see "6. Response (HTTP body)."

2. HTTP method

   ```
   GET
   ```

3. URL

   ```
   /v1/extlink/nodes/node_id
   ```

   In ***node_id***, specify the node ID.

   Format: msc_extlink_{manager-name} to {agent-name}

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The node information was successfully retrieved.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target is not found.
405	Method Not Allowed	The specified method is not authorized.
500	Internal Server Error	An internal error occurred.

HTTP status code	Meaning	Description
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Return value
management_type	string	Linkage destination component type	SystemManagerG-FW
node_id	string	Node ID	Format: msc_extlink_{manager-name} to {agent-name}
node_name	string	Node name	-
node_type	string	Node type	Host
os_type	string	OS type of the node	Windows, Linux, HP-UX, Solaris, AIX, ESX, AWS
os_ver	string	OS version of the node	-
tenant_id	string	Organization tenant ID	-
parent_group_id	string	Organization group ID	22 characters
order	string	Specific character string used for sorting at the call source	-
comment	string	Comment	Up to 256 characters
option	string	Specific additional information	-
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 7.1.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/extlink/nodes/msc_extlink_managerA~agent3 HTTP/1.1
Host: localhost:8280
Accept: */*
X-Authorization: token E798DF701E3528E737353EAFEE4E68A8
Authorization: df95d309-c5fe-196f-2622-416d19be6894
Date: Mon, 19 Feb 2018 15:58:50 GMT
```

   [Response]

```
HTTP/1.1 200 OK
Date: Mon, 19 Feb 2018 15:58:51 GMT
Connection: Close
Content-Type: application/json; charset=utf-8
Content-Length: 365

{
```

```
  "comment" : "",
  "management_type" : "SystemManagerG-FW",
  "node_id" : "msc_extlink_managerA~agent3",
  "node_name" : "agent3",
  "node_type" : "Host",
  "option" : "{}",
  "order" : "",
  "os_type" : "Linux",
  "os_ver" : "Red Hat Enterprise Linux Server release 7.3 (Maipo)",
  "parent_group_id" : "msc_extlink_0000000000",
  "tenant_id" : "DefaultTenant"
}
```

3.9.3 Updating a node

1. Process overview

   Update node information.

   For details about the information that can be updated, see "4. Parameter."

2. HTTP method

   ```
   PUT
   ```

3. URL

   ```
   /v1/extlink/nodes/node_id
   ```

   In ***node_id***, specify the node ID.

4. Parameter

Parameter	Type	Description	Required	Valid values
parent_group_id	string	Organization group ID	-	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)
comment	string	Comment	-	Up to 256 characters If the specified value exceeds 256 characters, only the first 256 characters are updated.

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The node information was successfully updated.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target is not found.
405	Method Not Allowed	The specified method is not authorized.
500	Internal Server Error	An internal error occurred.

HTTP status code	Meaning	Description
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 7.1.0
     - Newly added.
8. Example

   [Request]

```
PUT /v1/extlink/nodes/msc_extlink_managerA~agent5 HTTP/1.1
Host: localhost:8280
Accept: */*
X-Authorization: token E798DF701E3528E737353EAFEE4E68A8
Authorization: df95d309-c5fe-196f-2622-416d19be6894
Date: Mon, 19 Feb 2018 17:12:38 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 102

{
  "parent_group_id":"msc_extlink_0000000001",
  "comment":"this is comment.",
  "order":"01"
}
```

   [Response]

```
HTTP/1.1 200 OK
Date: Mon, 19 Feb 2018 17:12:39 GMT
Connection: Close
```

3.9.4 Deleting a node

1. Process overview

   Delete a node.

2. HTTP method

```
DELETE
```

3. URL

```
/v1/extlink/nodes/node_id
```

   Format: msc_extlink_{manager-name} to {agent-name}

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
204	No Content	The node information was successfully deleted.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target is not found.
405	Method Not Allowed	The specified method is not authorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 7.1.0
     - Newly added.
8. Example

   [Request]

```
DELETE /v1/extlink/nodes/msc_extlink_managerA~agent5 HTTP/1.1
Host: localhost:8280
Accept: */*
X-Authorization: token E798DF701E3528E737353EAFEE4E68A8
Authorization: df95d309-c5fe-196f-2622-416d19be6894
Date: Mon, 19 Feb 2018 17:04:21 GMT
```

   [Response]

```
HTTP/1.1 204 No Content
Date: Mon, 19 Feb 2018 17:04:22 GMT
Connection: Close
```

3.9.5 Getting the group list

1. Process overview

   Retrieve a list of group information.

   For details about the information that can be retrieved, see "6. Response (HTTP body)."
2. HTTP method

```
GET
```

3. URL

```
/v1/extlink/groups?limit=limit&offset=offset&parent_group_id=parent_group_id
```

Key name	Description	Omittable
limit	Specify the maximum number of items to be retrieved between 0 and 32767. If omitted (or if a value outside the range is set), the number is unlimited.	-
offset	Specify the acquisition start position between 0 and 32767. If 200 nodes match the search conditions and the limit is 100, specify the offset as follows to retrieve the nodes. To retrieve the 1st to 100th nodes: offset=0 To retrieve the 101st to 200th nodes: offset=100	-
parent_group_id	Specify the organization group ID. If the organization group ID key is omitted, a list of all groups in the tenant is retrieved. If the organization group ID value is omitted (by specifying ""), a list of groups immediately under the root in the tenant is retrieved.	-

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	A list of group information was successfully retrieved.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target is not found.
405	Method Not Allowed	The specified method is not authorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Return value
total_item	number	Total number of items	-
items_per_page	number	Number of items retrieved in the request	-
next_offset	number	Start position for requesting of next acquisition	-
parent_group_id	string	Organization group ID	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)
group_list[n]. group_id	string	Group ID	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)
group_list[n]. group_name	string	Group name	Up to 128 characters

Parameter	Type	Description	Return value
group_list[n]. order	string	Specific character string used for sorting at the call source	-
group_list[n]. comment	string	Comment	Up to 256 characters
group_list[n]. parent_group_id	string	Organization group ID	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)
group_list[n]. tenant_id	string	Tenant ID	-

7. Change history
   - Version: 7.1.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/extlink/groups?parent_group_id= HTTP/1.1
Host: localhost:8280
Accept: */*
X-Authorization: token E798DF701E3528E737353EAFEE4E68A8
Authorization: df95d309-c5fe-196f-2622-416d19be6894
Date: Wed, 21 Feb 2018 10:39:27 GMT
```

   [Response]

```
HTTP/1.1 200 OK
Date: Wed, 21 Feb 2018 10:39:27 GMT
Connection: Close
Conten-Type: application/json; charset=utf-8
Content-Length: 782

{
  "group_list" : [
    {
      "comment" : "A-def",
      "group_id" : "msc_extlink_0000000000",
      "group_name" : "DEFAULT_GROUP",
      "order" : "01",
      "parent_group_id" : "",
      "tenant_id" : "DefaultTenant"
    },
    {
      "comment" : "A-A00",
      "group_id" : "msc_extlink_0000000025",
      "group_name" : "LST_A00_group",
      "order" : "02",
      "parent_group_id" : "",
      "tenant_id" : "DefaultTenant"
    },
    {
      "comment" : "A-J00",
```

```
      "group_id" : "msc_extlink_0000000034",
      "group_name" : "LST_J00_group",
      "order" : "11",
      "parent_group_id" : "",
      "tenant_id" : "DefaultTenant"
    }
  ],
  "items_per_page" : 3,
  "next_offset" : 0,
  "parent_group_id" : "",
  "total_item" : 3
}
```

3.9.6 Getting a group

1. Process overview

   Retrieve the details of a group.

   For details about the information that can be retrieved, see "6. Response (HTTP body)."

2. HTTP method

```
GET
```

3. URL

```
/v1/extlink/groups/group_id
```

   In ***group_id***, specify the group ID with 22 characters.
   Format: "msc_extlink_" + 10-digit decimal (leading zero)

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The group information was successfully retrieved.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target is not found.
405	Method Not Allowed	The specified method is not authorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Return value
group_id	string	Group ID	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)
group_name	string	Group name	Up to 128 characters

Parameter	Type	Description	Return value
tenant_id	string	Organization tenant ID	-
parent_group_id	string	Organization group ID	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)
order	string	Specific character string used for sorting at the call source	-
comment	string	Comment	Up to 256 characters
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 7.1.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/extlink/groups/msc_extlink_0000000034 HTTP/1.1
Host: localhost:8280
Accept: */*
X-Authorization: token 2692CC573FCFD94F462A19E0957BCBAE
Authorization: Bearer db937918-656d-1906-89c0-8071d9f5e21a
Date: Wed, 21 Feb 2018 14:27:44 GMT
```

   [Response]

```
HTTP/1.1 200 OK
Date: Wed, 21 Feb 2018 14:27:44 GMT
Connection: Close
Content-Type: application/json; charset=utf-8
Content-Length: 186

{
  "comment" : "A-J00",
  "group_id" : "msc_extlink_0000000034",
  "group_name" : "LST_J00_group",
  "order" : "11",
  "parent_group_id" : "",
  "tenant_id" : "DefaultTenant"
}
```

3.9.7 Registring a group

1. Process overview

   Register group information.

   For details about the information that can be registered, see "4. Parameter."

2. HTTP method

```
POST
```

3. URL

```
/v1/extlink/groups
```

4. Parameter

Parameter	Type	Description	Required	Valid values
group_name	string	Group name	Required	Up to 128 characters
parent_group_id	string	Organization group ID If the key is omitted or null, the group is registered immediately under the root.	-	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)
order	string	Specific character string used for sorting at the call source	-	-
comment	string	Comment	-	Up to 256 characters If the specified value exceeds 256 characters, the first 256 characters are registered.

5. Response (HTTP status code)

HTTP status code	Meaning	Description
201	Created	The group information was successfully registered.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target is not found.
405	Method Not Allowed	The specified method is not authorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Return value
group_id	string	Group ID	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)
message	string	Character string showing the cause of the error	-

7. Change history

- Version: 7.1.0
  - Newly added.

8. Example

[Request]

```
POST /v1/extlink/groups HTTP/1.1
Host: localhost:8280
Accept: */*
X-Authorization: token E798DF701E3528E737353EAFEE4E68A8
Authorization: df95d309-c5fe-196f-2622-416d19be6894
Date: Mon, 19 Feb 2018 17:04:21 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 88

{
  "group_name":"ADD_A00_group",
  "order":"order_01",
  "comment":"comment_01"
}
```

[Response]

```
HTTP/1.1 201 Created
Date: Mon, 19 Feb 2018 17:04:22 GMT
Connection: Close
Content-Length: 47

{
  "group_id" : "msc_extlink_0000000002"
}
```

3.9.8 Updating a group

1. Process overview

Update group information.

For details about the information that can be updated, see "4. Parameter."

2. HTTP method

```
PUT
```

3. URL

```
/v1/exlink/groups/group_id
```

In ***group_id***, specify the group ID with 22 characters.

4. Parameter

Parameter	Type	Description	Required	Valid values
group_name	string	Group name	-	Up to 128 characters The name can be duplicated in a system.
parent_group_id	string	Organization group ID	-	22 characters Format: "msc_extlink_" + 10-digit decimal (leading zero)

Parameter	Type	Description	Required	Valid values
comment	string	Comment	-	Up to 256 characters If the specified value exceeds 256 characters, only the first 256 characters are updated.

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The group information was successfully updated.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target is not found.
405	Method Not Allowed	The specified target is not found.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history
   - Version: 7.1.0
     - Newly added.
8. Example

   [Request]

```
PUT /v1/extlink/groups/msc_extlink_0000000019 HTTP/1.1
Host: localhost:8280
Accept: */*
X-Authorization: token 06E164CE06FA35D2EA56469C1CD4C59D
Authorization: df95d309-c5fe-196f-2622-416d19be6894
Date: Wed, 21 Feb 2018 09:32:15 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 50

{
  "parent_group_id":"msc_extlink_0000000020"
}
```

   [Response]

```
HTTP/1.1 200 OK
Date: Wed, 21 Feb 2018 09:32:15 GMT
Connection: Close
```

3.9.9 Deleting a group

1. Process overview

   Delete a group.

   If a node exists under the group to be deleted, the target group is deleted after the node is removed from the group.

   If a group exists under the group to be deleted, the target group is not deleted and it is handled as a deletion failure.

2. HTTP method

   ```
   DELETE
   ```

3. URL

   ```
   /v1/extlink/groups/group_id
   ```

   In ***group_id***, specify the group ID with 22 characters.

   Format: "msc_extlink_" + 10-digit decimal (leading zero)

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
204	No content	The group information was successfully deleted.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target is not found.
405	Method Not Allowed	The specified method is not authorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Return value
message	string	Character string showing the cause of the error	-

7. Change history

   - Version: 7.1.0
     - Newly added.

8. Example

[Request]

```
DELETE /v1/extlink/groups/msc_extlink_0000000001 HTTP/1.1
Host: localhost:8280
Accept: */*
X-Authorization: token 2692CC573FCFD94F462A19E0957BCBAE
Authorization: Bearer db937918-656d-1906-89c0-8071d9f5e21a
Date: Wed, 21 Feb 2018 14:27:44 GMT
```

[Response]

```
HTTP/1.1 204 No Content
Date: Wed, 21 Feb 2018 09:16:21 GMT
Connection: Close
```

3.10 Performance data store

3.10.1 Viewing the counter details

1. Process overview

Retrieve the details of the counter information.

2. HTTP method

```
GET
```

3. URL

```
/v1/perfdatastore/counters/counter_id
```

Parameter	Type	Description	Required	Valid values
counter_id	string	Specify a counter ID.	Required	0000000001 to 9999999999

4. Parameter

None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The counter information was successfully viewed.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target was not found.
405	Method Not Allowed	The specified HTTP method is unauthorized.

HTTP status code	Meaning	Description
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
system_name	string	System name	1 to 128 characters
node_name	string	Node name.	1 to 128 characters
node_id	string	Node ID.	-
counter_name	string	Counter name	1 or more characters (No upper limit)
counter_id	string	Counter ID	0000000001 to 9999999999
tenant_id	string	Tenant ID	0 or more characters.
product_name	string	Linkage destination product name	1 to 128 characters
target_type	string	Counter monitoring target type	1 to 64 characters
description	string	Description	Up to 1024 characters
monitor_type	string	Threshold determination method	"onepoint": Sequential, "continuous": Continuous, "average": Average
monitor_count	number	Number of times monitoring is performed to determine the threshold (*1)	2 to 16 This is enabled only when the threshold determination method is "continuous" or "average".
thresholds	object[]	Threshold information	-
thresholds[n].detect_type	string	Threshold monitoring method	"over": Monitor to determine whether the upper limit is exceeded, "under": Monitor to determine whether the lower limit is exceeded.
thresholds[n].value	number	Threshold	Real value that is available in double (64-bit) format
thresholds[n].severity	number	Severity.	0 to 255
thresholds[n].threshold_enable	boolean	Whether to enable or disable threshold monitoring	true: Monitor the threshold, false: Do not monitor the threshold
thresholds[n].alert_message	boolean	Whether to output messages when the threshold is exceeded	true: Output, false: Not output
message	string	Character string showing the cause of the error	-
status	string	Status name showing the cause of the error	-

(*1) If "monitor_type" is "onepoint", this key is not included in the response.

7. Change history

- Version: 8.0.0
  - Newly added.

8. Example

[Request]

```
GET /v1/perfdatastore/counters/1234567890 HTTP/1.1
Host: 192.168.100.10:8243
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
Authorization: Bearer 09c6fa49-c39b-3d50-9320-716b2e420daa
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: DELETE,POST,PUT,GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Connection: Close
Content-Length: 0
Date: Wed, 1 Mar 2017 00:00:00 GMT
Transfer-Encoding: chunked
{
  "system_name" : "manager",
  "node_name": "agent",
  "node_id": "msc_extlink_manager~agent",
  "counter_name" : "Processor::%Idle Time::_Total",
  "counter_id" : "1234567890",
  "tenant_id" : "tenantA",
  "product_name" : "SystemManagerG-FW",
  "target_type" : "System",
  "description" : "This counter is about CPU monitoring at agent",
  "monitor_type" : "continuous",
  "monitor_count" : 5,
  "thresholds":[
    {
      "detect_type": "under",
      "value" : 80,
      "severity" : 150,
      "threshold_enable" : true,
      "alert_message" : true
    }
  ]
}
```

3.10.2 Viewing the counter list

1. Process overview

Retrieve a list of counter information.

2. HTTP method

```
GET
```

3. URL

```
/v1/perfdatastore/counters?node_id=node_id&search=search&limit=limit&offset=offset
```

Parameter	Type	Description	Required	Valid values
node_id	string	Specify the node ID. If omitted, all nodes are selected.		-
search	string	Specify the counter search string. Regular expressions are available for this parameter. If omitted, all nodes are selected.		Character string indicating the counter name
limit	number	Specify the maximum number of items to be retrieved. If this parameter is omitted or set to 0, all the data in the specified range is returned.		1 to 9999
offset	number	Specify the acquisition start position. If this parameter is omitted or set to 0, data starting from the first search result are returned as a response.		-

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The counter information was successfully viewed.
400	Bad Request	An incorrect parameter was specified. A value greater than the number of items retrieved was specified in the offset query.
401	Unauthorized	Authentication failed.
405	Method Not Allowed	The specified HTTP method is unauthorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
total_item	number	Total number of items	-
items_per_page	number	Number of items retrieved in the request	-
next_offset	number	Start position when requesting the next acquisition	-
counters	object[]	Counter information	-
counters[n].system_name	string	System name	1 to 128 characters
counters[n].node_name	string	Node name.	1 to 128 characters
counters[n].node_id	string	Node ID.	-
counters[n].counter_name	string	Counter name	1 or more characters (No upper limit)
counters[n].counter_id	string	Counter ID	0000000001 to 9999999999
counters[n].tenant_id	string	Tenant ID	0 or more characters.
counters[n].product_name	string	Linkage destination product name	1 to 128 characters
counters[n].target_type	string	Counter monitoring target type	1 to 64 characters
counters[n].description	string	Description	Up to 1024 characters
counters[n].monitor_type	string	Threshold determination method	"onepoint": Sequential, "continuous": Continuous, "average": Average
counters[n].monitor_count	number	Number of times monitoring is performed to determine the threshold (*1)	2 to 16 This is enabled only when the threshold determination method is "continuous" or "average".
counters[n].thresholds	object[]	Threshold information	-
counters[n].thresholds[m].detect_type	string	Threshold monitoring method	"over": Monitor to determine whether the upper limit is exceeded, "under": Monitor to determine whether the lower limit is exceeded.
counters[n].thresholds[m].value	number	Threshold	Real value that is available in double (64-bit) format
counters[n].thresholds[m].severity	number	Severity.	0 to 255
counters[n].thresholds[m].threshold_enable	boolean	Whether to enable or disable threshold monitoring	true: Monitor the threshold, false: Do not monitor the threshold
counters[n].thresholds[m].alert_message	boolean	Whether to output messages when the threshold is exceeded	true: Output, false: Not output
message	string	Character string showing the cause of the error	-
status	string	Status name showing the cause of the error	-

(*1) If "monitor_type" is "onepoint", this key is not included in the response.

7. Change history

- Version: 8.0.0
  - Newly added.

8. Example

[Request]

```
GET /v1/perfdatastore/counters HTTP/1.1
Host: 192.168.100.10:8243
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
Authorization: Bearer 09c6fa49-c39b-3d50-9320-716b2e420daa
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: DELETE,POST,PUT,GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Connection: Close
Content-Length: 0
Date: Wed, 1 Mar 2017 00:00:00 GMT
Transfer-Encoding: chunked
{
  "total_item" : 1,
  "item_per_page" : 1,
  "counters" : [
    {
      "system_name" : "manager",
      "node_name": "agent",
      "node_id": "msc_extlink_manager~agent",
      "counter_name" : "Processor::%Idle Time::_Total",
      "counter_id" : "1234567890",
      "tenant_id" : "tenantA",
      "product_name" : "SystemManagerG-FW",
      "target_type" : "System",
      "description" : "This counter is about CPU monitoring at agent",
      "monitor_type" : "continuous",
      "monitor_count" : 5,
      "thresholds":[
        {
          "detect_type": "under",
          "value" : 80,
          "severity" : 150,
          "threshold_enable" : true,
          "alert_message" : true
        }
      ]
    }
  ]
}
```

3.10.3 Deleting performance data

1. Process overview

Delete the performance data of the specified counter.

2. HTTP method

```
DELETE
```

3. URL

```
/v1/perfdatastore/counters/counter_id/metrics?start_time=start_time&end_time=end_time
```

Parameter	Type	Description	Required	Valid values
counter_id	string	Specify a counter ID.	Required	0000000001 to 9999999999
start_time	string	Specify the start date and time of the specified range. If omitted, the oldest performance data is set.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
end_time	string	Specify the end date and time of the specified range. If omitted, the time at which the request was accepted is set.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00

4. Parameter

None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
204	No Content	The performance data was successfully deleted.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target was not found.
405	Method Not Allowed	The specified HTTP method is unauthorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
message	string	Character string showing the cause of the error	-

Parameter	Type	Description	Valid values
status	string	Status name showing the cause of the error	-

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
DELETE /v1/perfdatastore/counters/1234567890/metrics HTTP/1.1
Host: 192.168.100.10:8243
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
Authorization: Bearer 09c6fa49-c39b-3d50-9320-716b2e420daa
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
```

   [Response]

```
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: DELETE,POST,PUT,GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Connection: Close
Content-Length: 0
Date: Wed, 1 Mar 2017 00:00:00 GMT
Transfer-Encoding: chunked
```

3.10.4 Viewing performance data

1. Process overview

   View the performance data for the specified counter.
2. HTTP method

```
GET
```

3. URL

```
/v1/perfdatastore/counters/counter_id/metrics?start_time=start_time&end_time=end_time&limit=limit&completion=completion&continue=continue
```

Parameter	Type	Description	Required	Valid values
counter_id	string	Specify a counter ID.	Required	0000000001 to 9999999999

Parameter	Type	Description	Required	Valid values
start_time	string	Specify the start date and time of the specified range. If omitted, the oldest performance data is set.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
end_time	string	Specify the end date and time of the specified range. If omitted, the time at which the request was accepted is set.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
limit	number	Specify the maximum number of items to be retrieved. If this parameter is omitted or set to 0, all the data in the specified range is returned. If the number of data items to be returned exceeds the limit, data is returned in order starting from the oldest. The data is returned with the measurement date and time of the next performance data set in the next_start_time parameter. To view the subsequent performance data, set the next_start_time value to start_time in the query.		1 to 9999
completion	number	Specify the number of data items to be completed before and after the acquisition results. If this value is omitted or set to 0, completion data is not returned. When completion is selected, the number of completion data items specified in completion is not included in the number of returned data items specified in limit.		1 to 10

Parameter	Type	Description	Required	Valid values
		Forward completion data (future-oriented) is not included in the response if returnable data exists following the performance data included in the response. If all the performance data in the specified range are included in the response, forward completion data is granted.		
continue	string	Specify this value (true) when continuing to retrieve performance data. If this value is omitted or set to "false", it is not treated as continuous acquisition. When continue is selected, backward completion data (past-oriented) is not included in the response, even if completion is specified.		True (Continuous), false (Not continuous)

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The performance data was successfully viewed.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target was not found.
405	Method Not Allowed	The specified HTTP method is unauthorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
total_item	number	Total number of items	-
items_per_page	number	Number of items retrieved in the request	-
complements_forward	number	Number of backward completion data items (past-oriented)	-
complements_backward	number	Number of forward completion data items (future-oriented)	-
next_start_time	string	Time of performance data when requesting the next acquisition	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
metrics	object[]	Performance data array	-
metrics[n].time	string	Performance data acquisition time	YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
metrics[n].value	number	Performance data This key is omitted if an invalid value is specified.	Real value that is available in double (64-bit) format
message	string	Character string showing the cause of the error	-
status	string	Status name showing the cause of the error	-

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/perfdatastore/counters/1234567890/metrics?start_time=2016-10-3
1T21:15:38+09:00&limit=2 HTTP/1.1
Host: 192.168.100.10:8243
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
Authorization: Bearer 09c6fa49-c39b-3d50-9320-716b2e420daa
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: DELETE,POST,PUT,GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Connection: Close
Content-Length: 0
```

```
Date: Wed, 1 Mar 2017 00:00:00 GMT
Transfer-Encoding: chunked

{
  "total_item": 300,
  "items_per_page": 2,
  "next_start_time": "2016-10-31T21:18:25+09:00",
  "metrics" : [
    {
      "time" : "2016-10-31T21:16:24+9:00",
      "value" : 90.1
    },
    {
      "time" : "2016-10-31T21:17:24+9:00"
    }
  ]
}
```

3.10.5 Viewing statistical data

1. Process overview

   View the statistical data of the specified counter.

2. HTTP method

```
GET
```

3. URL

```
/v1/perfdatastore/counters/counter_id/statistics?start_time=start_time&end_time=end_time&limit=limit&completion=completion&continue=continue&statistics_type=statistics_type
```

Parameter	Type	Description	Required	Valid values
counter_id	string	Specify a counter ID.	Required	0000000001 to 9999999999
start_time	string	Specify the start date and time of the specified range. If omitted, the oldest statistical data is set.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
end_time	string	Specify the end date and time of the specified range. If omitted, the time at which the request was accepted is set. end_time is adjusted according to start_time.		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00

Parameter	Type	Description	Required	Valid values
limit	number	Specify the maximum number of items to be retrieved. If this parameter is omitted or set to 0, all the data in the specified range is returned. If the number of data items to be returned exceeds the limit, data is returned in order starting from the oldest. The data is returned with the measurement date and time of the next statistical data set in the next_start_time parameter. To view the subsequent statistical data, set the next_start_time value to start_time in the query.		1 to 9999
completion	number	Specify the number of data items to be completed before and after the acquisition results. If this value is omitted or set to 0, completion data is not returned. Statistical data during the completion period converted based on the number of completions and acquisition interval is returned as the completion data. When completion is selected, the number of completion data items specified in completion is not included in the number of returned data items specified in limit. Forward completion data (future-oriented) is not included in the response if returnable data exists following the statistical data included in the		1 to 10

Parameter	Type	Description	Required	Valid values
		response. If all the statistical data in the specified range are included in the response, backward completion data is granted.		
continue	string	Specify this value (true) when continuing to retrieve statistical data. If this value is omitted or set to "false", it is not treated as continuous acquisition. When continue is selected, backward completion data (past-oriented) is not included in the response, even if completion is specified.		True (Continuous), false (Not continuous)
statistics_type	string[]	Specify the statistical data type. The options are latest, min, average, and max. To specify multiple types, separate them with commas. If omitted, all types are selected. (*1)		latest, min, average, max

(*1) The same type cannot be selected multiple times.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The statistical data was successfully viewed.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
404	Not Found	The specified target was not found.
405	Method Not Allowed	The specified HTTP method is unauthorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
total_item	number	Total number of items	-
items_per_page	number	Number of items retrieved in the request	-
complements_forward	number	Number of backward completion data items (past-oriented)	-
complements_backward	number	Number of forward completion data items (future-oriented)	-
next_start_time	string	Time of statistical data when requesting the next acquisition	YYYY-MM-DDTHH:MM:SS±HH:MM Example:2016-11-16T20:00:00+09:00
interval	number	Acquisition time (minutes)	60, 1440
statistics_type	string[]	Statistical data type	latest, min, average, max
statistics	object[]	Statistical data array	-
statistics[n].time	string	Statistical data acquisition date and time	YYYY-MM-DDTHH:MM:SS±HH:MM Example:2016-11-16T20:00:00+09:00
statistics[n].latest_value	number	Statistical data (latest) This key is omitted if an invalid value is specified. This key is omitted if the data is not the target.	Real value that is available in double (64-bit) format
statistics[n].min_value	number	Statistical data (minimum) This key is omitted if an invalid value is specified. This key is omitted if the data is not the target.	Real value that is available in double (64-bit) format
statistics[n].average_value	number	Statistical data (average) This key is omitted if an invalid value is specified. This key is omitted if the data is not the target.	Real value that is available in double (64-bit) format
statistics[n].max_value	number	Statistical data (maximum) This key is omitted if an invalid value is specified. This key is omitted if the data is not the target.	Real value that is available in double (64-bit) format
message	string	Character string showing the cause of the error	-
status	string	Status name showing the cause of the error	-

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/perfdatastore/counters/1234567890/statistics?start_time=2017-1
0-31T21:00:00+09:00&limit=2 HTTP/1.1
Host: 192.168.100.10:8243
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
Authorization: Bearer 09c6fa49-c39b-3d50-9320-716b2e420daa
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
```

[Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: DELETE,POST,PUT,GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Connection: Close
Content-Length: 0
Date: Wed, 1 Mar 2017 00:00:00 GMT
Transfer-Encoding: chunked

{
  "total_item": 300,
  "items_per_page": 2,
  "next_start_time": "2017-10-31T23:00:00+09:00",
  "interval": 60,
  "statistics_type": [
    "latest", "min", "average", "max"
  ],
  "statistics" : [
    {
      "time" : "2017-10-31T21:00:00+09:00",
      "latest_value" : 9.01,
      "min_value" : 1.2,
      "average_value" : 2.33,
      "max_value" : 9.01
    },
    {
      "time" : "2017-10-31T22:00:00+09:00"
      "latest_value" : 9.01,
      "min_value" : 1.5,
      "average_value" : 2.56,
      "max_value" : 9.01
    }
  ]
}
```

3.10.6 Viewing the ranking

1. Process overview

   View the rankings using the performance data or statistical data of the specified counter.

2. HTTP method

```
GET
```

3. URL

```
/v1/perfdatastore/counters/statistics/ranking?search=search&group_id=group_id&
recursive=recursive&statistics_type=statistics_type&count=count&sort=sort&time
=time&start_time=start_time&end_time=end_time
```

Parameter	Type	Description	Required	Valid values
search	string	Specify the counter search string. Regular expressions are available for this parameter. (*1)		Character string indicating the counter name
group_id	string	Specify the group ID of the external interface. (*1)		Character string indicating the group ID of the external interface
recursive	string	Specify recursive search (true) under the group ID of the external interface. If this value is omitted or set to "false", data are not searched recursively. This is enabled only when group_id is specified.		true (Search recursively), false (Do not search recursively)
statistics_type	string	Specify the statistical data type. The options are latest, min, average, max, and latest_metric (latest performance data).	Required	latest, min, average, max, latest_metric
count	number	Specify the maximum number of items to be retrieved. If omitted, the top 10 data items are returned.		1 to 100
sort	string	Specify the statistical data sort order. If omitted, desc (descending) is selected.		asc (ascending order), desc (descending order)
time	string	Specify the date and time. (*2)		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
start_time	string	Specify the start date and time of the specified range. (*2)		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00
end_time	string	Specify the end date and time of the specified range. (*2)		YYYY-MM-DDTHH:MM:SS±HH:MM YYYY-MM-DDTHH:MM:SSZ Example:2016-11-16T20:00:00+09:00

(*1) "search" or "group_id" must be specified.

(*2) If all of "time", "start_time", and "end_time" are omitted, the ranking is viewed based on the statistical data right immediately before the time at which the request was accepted.

If all of "time", "start_time", and "end_time" are omitted and "latest_metric" is set to "statistics_type", the ranking is viewed based on the latest performance data.

If both "start_time" and "end_time" are specified, the ranking is viewed using statistical data included in the specified period.

"end_time" is adjusted according to "start_time" and statistical data generation interval.

Both "start_time" and "end_time" must be specified.

"time", "start_time", and "end_time" cannot be specified simultaneously.

4. Parameter

   None

5. Response (HTTP status code)

HTTP status code	Meaning	Description
200	OK	The ranking was successfully viewed.
400	Bad Request	An incorrect parameter was specified.
401	Unauthorized	Authentication failed.
405	Method Not Allowed	The specified HTTP method is unauthorized.
500	Internal Server Error	An internal error occurred.
503	Service Unavailable	The service is unavailable.

6. Response (HTTP body)

Parameter	Type	Description	Valid values
rankings	object[]	Ranking array	-
rankings[n].counter_id	string	Counter ID	0000000001 to 9999999999
rankings[n].value	number	Statistical data	Real value that is available in double (64-bit) format
rankings[n].node_id	string	Node ID.	-
rankings[n].system_name	string	System name	1 to 128 characters
rankings[n].node_name	string	Node name.	1 to 128 characters
rankings[n].counter_name	string	Counter name	1 or more characters (No upper limit)
rankings[n].tenant_id	string	Tenant ID	0 or more characters.
rankings[n].product_name	string	Linkage destination product name	1 to 128 characters
rankings[n].target_type	string	Counter monitoring target type	1 to 64 characters
message	string	Character string showing the cause of the error	-
status	string	Status name showing the cause of the error	-

7. Change history
   - Version: 8.0.0
     - Newly added.
8. Example

   [Request]

```
GET /v1/perfdatastore/counters/statistics/ranking?group_id=0000000001&
count=3&sort=desc&statistics_type=max HTTP/1.1
Host: 192.168.100.10:8243
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 0
Authorization: Bearer 09c6fa49-c39b-3d50-9320-716b2e420daa
X-Authorization: token 94A5E744423AB35717AD87C0B3BF1206
```

   [Response]

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: DELETE,POST,PUT,GET
Access-Control-Allow-Headers: authorization,Access-Control-Allow-Origi
n,Content-Type,SOAPAction
Connection: Close
Content-Length: 0
Date: Wed, 1 Mar 2017 00:00:00 GMT
Transfer-Encoding: chunked

{
  "rankings" : [
    {
      "counter_id" : "0000000001",
      "value" : 9.873e+002,
      "node_id" : "msc_extlink~Agent-A",
      "system_name" : "ManagerA",
      "node_name" : "Agent-A",
      "counter_name" : "CPU %",
      "tenant_id" : "TenantA",
      "produt_name" : "",
      "target_type" : "System"
    },
    {
      "counter_id" : "0000000002",
      "value" : 500,
      "node_id" : "msc_extlink~Agent-B",
      "system_name" : "ManagerA",
      "node_name" : "Agent-B",
      "counter_name" : "CPU %",
      "tenant_id" : "TenantA",
      "produt_name" : "",
      "target_type" : "System"
    },
    {
      "counter_id" : "0000000003",
      "value" : 200,
      "node_id" : "msc_extlink~Agent-C",
```

```
      "system_name" : "ManagerA",
      "node_name" : "Agent-C",
      "counter_name" : "CPU %",
      "tenant_id" : "TenantA",
      "produt_name" : "",
      "target_type" : "System"
    }
  ]
}
```

Appendix A. How to Start and Stop the Product

This product automatically starts and stops in response to the start and stop of the OS. When it is necessary to start or stop this product manually, execute the following services.

A.1 How to start and stop SystemManager G WebConsole Option (Windows)

Start or stop each service through the dialog box that is displayed by selecting [START], [Control Panel], [Administrative Tools], and then [Service] of Windows.

Target services

- Database
  - postgresql-x64-9.6 - PostgreSQL Server 9.6
- msc components
  - SystemManager G API Gateway Service
  - SystemManager G MessageStore Service
  - SystemManager G Authorization Service
  - SystemManager G ExternalLink Service
  - SystemManager G Status Service
  - SystemManager G Report Service
  - SystemManager G BusinessView Service
  - SystemManager G PerformanceDataStore Service
- Portal/user authentication platform
  - Apache Tomcat 8.5 Service Governor

A.2 How to start and stop SystemManager G WebConsole Option (Linux)

Start method

- Database

```
# systemctl start postgresql-9.6
```

- msc components

```
# systemctl start msc_apigateway         (API gateway)
# systemctl start msc_messagestore       (Message store)
# systemctl start msc_auth               (Authority management)
# systemctl start msc_extlink            (External interface)
# systemctl start msc_status             (Status management)
# systemctl start msc_report             (Reporting)
# systemctl start msc_business           (Business view)
# systemctl start msc_perfdatastore      (Performance data store)
```

- Portal/user authentication platform

```
# systemctl start ServiceGovernor
```

Stop method

- Portal/user authentication platform

```
# systemctl stop ServiceGovernor
```

- msc components

```
# systemctl stop msc_perfdatastore      (Performance data store)
# systemctl stop msc_business           (Business view)
# systemctl stop msc_report             (Reporting)
# systemctl stop msc_status             (Status management)
# systemctl stop msc_extlink            (External interface)
# systemctl stop msc_auth               (Authority management)
# systemctl stop msc_messagestore       (Message store)
# systemctl stop msc_apigateway         (API gateway)
```

- Database

```
# systemctl stop postgresql-9.6
```

Appendix B. Information on Field Mapping Between Monitoring Terminal (View) and WebConsole

- Message mapping

  This section describes the correspondences between the items displayed on a monitoring terminal (View) and those displayed on WebConsole.

Monitoring terminal (View)	Linkage	WebConsole	Supplementary
Node	Y	Node	
Severity	Y*	Severity	For details about the correspondence between the severities displayed on a monitoring terminal (View) and those displayed on WebConsole, see "Setting up Correspondences Between the Manager and WebConsole Option Severities" in the "Installation Guide".
Mark	N	Mark	"Mark" is set for the operation performed after the event and is not applied to WebConsole.
Occurrence time	Y	Generated	
Reception time	N	Received	The date and time of reception on the WebConsole side is displayed.
Verifying	N	Confirmation condition	"Verifying" is set for the operation performed after the event and is not applied to WebConsole.
Message text	Y	Message text	
Description	N	Description	Both the monitoring terminal (View) and WebConsole are independently equipped with a message filter and display an overview separately.
Application	Y	Application	
Object	Y	Object	
Category	N	-	WebConsole does not have a corresponding item.
-	-	Message definition ID	The monitoring terminal (View) does not have a corresponding item.
Message ID	Y	Message ID	
Comment	N	Comment	"Comment" is set for the operation performed after the event and is not applied to WebConsole.

Appendix C. Synchronizing SystemManager G Manager with WebConsole Option by Running a Command

In some situations, inconsistency in the data may occur between SystemManager G Manager and WebConsole Option.

This appendix describes the command that synchronizes data if an inconsistency in the data occurs between SystemManager G Manager and WebConsole Option.

Inconsistency in the data may occur in the following cases.

Table C-1 Inconsistency cases

No.	Case	Relevant component of WebConsole Option
1	When restore is performed on WebConsole Option	All
2	When restore is performed on SystemManager G Manager	All
3	When the command (PerformanceCmd.exe RE-SETUP -P) for changing the Processor object of the performance monitoring from a single-core configuration to a multi-core configuration is run on SystemManager G Manager	Performance data store
4	When the node name of a node under the network view is changed with SystemManager G Manager installed on the same core as of NetvisorPro V * Only when performance data, sent to the performance management service, has been included in the registration targets by running the data acquisition narrowing-down operation command (nvpdatacolfilter) on the system in which settings for data acquisition have been made	Performance data store
5	When a change to severity is made in accordance with "Setting up Correspondences Between the Manager and WebConsole Option Severities" in the "Installation Guide" after a setup for the linkage to the performance data store, a component of WebConsole Option, is made on SystemManager G Manager	Performance data store

The target components of the data synchronization performed by the synchronizing command are the monitoring status management (Status), the external interface linkage (ExtLink), and the performance data store (PerformanceDataStore). This is performed while SystemManager G Manager and WebConsole Option are operating.

For details about how to use the synchronizing command, see the following command specifications.

- Path

  Windows manager: <manager-install-path>\Manager\bin\HttpClientCmd.exe

  Linux manager: <manager-install-path>/Manager/bin/HttpClientCmd.exe
- Format

  HttpClientCmd.exe SYNC [-C [S][E][P]]
- Options

SYNC Synchronizes SystemManager G Manager with the components of WebConsole Option.

-C [S][E][P] Specify this option by listing synchronization-target components in line. If the entire option including -C is omitted, all the components will be synchronized. (When -C is specified, the option cannot be omitted. Lowercase characters are not acceptable; multiple components can be designated; no particular order is required.) S: Monitoring status management E: External interface P: Performance data store

- Return values

Return value	Description	Action
0	Normal end	Command execution was completed normally. No action is required.
1	Internal software error	Contact the support center if this error occurs.

- Cautions
  - The return value is used for making a judgment on whether the command was accepted by SystemManager G Manager. The result of the processing for synchronization with WebConsole Option is not returned.
  - The commands must be run with Administrator authority. Start the command prompt with Administrator authority for Windows Server 2008 or later versions.
  - To run these commands on the Linux manager, the following preparations are required.
    * Add the following path to the library path setting environment variable LD_LIBRARY_PATH:. <manager-install-path>/Manager/bin
    * Specify UTF-8 for the locale of the locale setting execution environment.
- Examples

・HttpClientCmd.exe SYNC

The status of SystemManager G Manager is synchronized with those of all the components of WebConsole Option.

・HttpClientCmd.exe SYNC -C SE

The status of SystemManager G Manager is synchronized with those of the monitoring status management and external interface linkage of WebConsole Option.

Appendix D. Revision History

- First edition (July 2018): Newly created

MasterScope SystemManager G 8.0 WebConsole Option
Function Reference Guide

SMG0800E-FUNC-1820

July, 2018 First Edition

NEC Corporation

©NEC Corporation 2018-2018