

# MasterScope Network Management Web Console Getting Started Guide

## for Windows / EXPRESSCLUSTER X



IMSWCSE0100-01

# Copyrights

The information in this document is the property of NEC Corporation. No part of this document may be reproduced or transmitted in any form by any means, electronic or mechanical, for any purpose, without the express written permission of NEC Corporation.

The information in this manual may not include all the information disclosed by NEC Corporation or may include expressions that differ from information disclosed by other means. Also, this information is subject to change or deletion without prior notice.

Although every effort has been made to ensure accuracy in producing this manual, NEC Corporation does not guarantee the accuracy or applicability of the information contained herein. In addition, NEC Corporation is not liable for any loss or damage incurred as a result of the use or non-use of this information by any party.

## Trademarks

- NEC and NEC logo are registered trademarks or trademarks of NEC Corporation in Japan and other countries.
- Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Google Chrome is a registered trademark or trademark of Google Inc.
- Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States and other countries.
- Red Hat is a trademark or registered trademark of Red Hat Software, Inc.
- Intel, Xeon, and Intel Core are trademarks or registered trademarks of Intel Corporation in the United States and other countries.
- Other company names and product names are trademarks or registered trademarks of their respective companies.
- Trademark symbols such as  $^{TM}$  and  $^{\mathbb{R}}$  are not indicated in the main text.

## **Preface**

Thank you for choosing MasterScope network management products. MasterScope network management products enable users to seamlessly integrate and operate the information and controls of multiple products on one Web Console by using the MasterScope Integrated Management Server component (hereafter referred to as IMS component).

This document describes how to set up the IMS component (version 1.0) that is necessary to use Web Console and the environment settings. Also, this document describes the basic operations of Web Console. Before configuring an environment to use Web Console, please read this document carefully.

## **Configuration of This Manual**

This manual consists of the following chapters. Read the chapters relevant to you according to your "Target Reader" classification in the table below.

Admin : Administrators User : All users of Web Console

#### **Configuration of This Manual**

Title	Content	Target reader		
"Chapter 1. Overview and Operating Environment of Web Console (page 1)"	Describes an overview and the operating environment of the Web Console.	User		
"Chapter 2. Installation of IMS Component (page 9)"	Describes how to set up the Web Console usage environment.	Admin		
"Chapter 3. Post-Installation Environment Settings (page 37)"	Describes how to configure the environment before using and operating the Web Console.	Admin		
"Chapter 4. Basic Operations (page 47)"	Describes the basic operations of the Web Console.	User		
"Chapter 5. Uninstallation of IMS component (page 65)"	Describes how to uninstall the Web Console usage environment.	Admin		
Appendix	Describes supplementary information related to construction task of Web Console usage environment.	Admin		

## Notations and Text Conventions

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

Notations of Items Requiring Attention and Supplementary Information

Notation	Description
A Caution	Indicates important points that the user should observe to configure and use the product properly.

Notation	Description
Тір	Indicates useful information.

In this manual, the following text conventions are used.

#### **Text Conventions**

Notation	Description	Example	
name	Indicates graphical user interfaces such as menus, items, and buttons.	<b>EDashboard</b> menu, <b>OK</b> button	
<userinput></userinput>	Indicates items that change depending on the user environment or items that the user must specify.	<%INSTPATH%>, <filepath></filepath>	
configuration file	Indicates the contents of the configuration file.	Set the following value:	
		port = 27120	
command line	Indicates command line operations.	Run the following command:	
		> Setup.exe	

In this manual, the following abbreviations are used.

#### Abbreviations

Formal Name	Abbreviation		
MasterScope Integrated Management Server	Integrated Management Server, IMS		
MasterScope Network Manager	Network Manager		
MasterScope Network Flow Analyzer	NFA		

To use Web Console, you need to install the component named IMS. The default installation path of the IMS component is as follows:

#### **Default installation path:**

 $C: \verb|Program Files \verb|NEC \verb|IMS||$ 

In this manual, the above installation path is referred to as *<%INSTPATH%>*. If you installed in another path, please replace this path name with the appropriate path name.

In addition, when you install IMS, you must specify the path on the shared disk as data storage path to store the data that will be managed by the IMS component. In this manual, the data storage path is referred to as <%DATAPATH%>.

# Contents

Chapte	er 1. Overview and Operating Environment of Web Console	1
1.1	Overview of Web Console	2
	1.1.1 The Usage of Web Console	2
	1.1.2 Functional overview of Web Console	2
1.2	Operating Environment	6
	1.2.1 System configuration	6
	1.2.2 System requirements	7
Chapte	er 2. Installation of IMS Component	9
2.1	Setup Flow for the IMS Component	10
2.2	Preparation for Setup	11
	2.2.1 Designing the installation parameters	11
	2.2.2 Checking the installation environment	16
2.3	Configuring a failover group	16
2.4	Installation	16
2.5	Configuring to connect the products	
2.6	Configuring the communication protocol settings of Web Console	
	2.6.1 Enabling HTTPS communication	
	2.6.2 Preparing the SSL server certificate	22
	2.6.2.1 Preparing a self-signed certificate	
	2.6.2.2 Preparing a certificate to be issued by a public certificate authority	
0.7	2.6.2.3 Using certificates created previously	
	Changing the communication port number from default value	
	Changing the firewall settings	
2.9	Configuring the additional settings on the installation environment	
	2.9.1 Setting a URL for notification	
	2.9.2 Configuring to delete the web server logs automatically	
	2.9.3 Changing the antivirus software settings	
	0 Configuring the services to support a cluster	
2.1	1 Checking the switching between the active server and standby server	
2.1	2 Setting up the products to be connected	
	2.12.1 Configure the connection setting for Network Manager	
	2.12.2 Configure the connection setting for NFA	
Chapte	er 3. Post-Installation Environment Settings	
3.1	Preparations for Using Web Console	
	3.1.1 Checking the web browser security settings	
	3.1.2 Importing the SSL server certificate into the web browser	
3.2	Accessing Web Console.	40
3.3	Registering users	41
	3.3.1 Groups and users	41

<ul><li>3.3.2 Adding a group</li><li>3.3.3 Adding a user</li></ul>	
3.4 Synchronizing the configuration information	
3.5 Confirming the managed node information	
3.6 Checking the network map configuration	
Chapter 4. Basic Operations	
4.1 Structure of Web Console	48
4.2 Updating own user information	
4.3 Checking the newly occurred events	51
4.4 Widget types	
4.5 Widget display contents	55
4.6 Basic operation of widgets	
4.6.1 Checking the details of the node	56
4.6.2 Checking the details of the network interface	
4.6.3 Checking the details of the flow information	
4.6.4 Filtering the items displayed on a chart	
4.6.5 Zooming in on a line chart	
4.6.6 Changing the IP address display to the hostname	
4.6.7 Changing the chart type	
4.7 Operations of specific widgets	
<ul><li>4.7.1 Performing operations related to the event</li><li>4.7.1.1 Checking the details of an event</li></ul>	
4.7.1.2 Performing operations on the event	
4.7.1.3 Checking the influence of the event on the topology map	
4.7.2 Checking the nodes with the specified status in a list	
Chapter 5. Uninstallation of IMS component	65
5.1 Notes on Uninstallation	
5.2 Uninstallation	66
Appendix A. Command Reference	67
A.1 ims-ssl-keytool	67
A.2 ims-app	70
Appendix B. Troubleshooting	72
B.1 Troubleshooting errors when running the installer	72
B.2 Troubleshooting errors when starting the service	72

## Chapter 1. Overview and Operating Environment of Web Console

This chapter describes an overview and the operating environment of the Web Console.

## Contents

1.1	Overview of Web Console	2
1.2	Operating Environment	6

## 1.1 Overview of Web Console

This chapter describes an overview and the purpose of the Web Console.

## 1.1.1 The Usage of Web Console

Web Console provides the mechanism to remotely operate from any terminal using a Web browser. In addition, it seamlessly integrates the operation of individual products for network monitoring, analysis and control, and provides a mechanism for streamlining network operation lifecycle management..

Web Console is useful when operating as follows.

• When checking the network status from an arbitrary terminal

Installation of client software is not necessary because Web Console is used on a web browser. Therefore, in the case of emergency, it is possible to check the network status using web browser on an arbitrary terminal.

For example, when using the Network Manager, in an environment where web communication is permitted, it is possible to check the status of each node and the scope of impact of the failure by accessing the Web Console remotely.

• When integrating operations of multiple MasterScope network management products

Web Console integrates the management information of multiple products into one place and displays it. When grasping the overall status of the network, you do not need to check the individual views provided by each product, and you can efficiently perform management tasks.

For example, It is possible to integrate management information of multiple Network Managers and integrate information of Network Manager and NFA.

Тір

Web Console can be used for routine operation such as checking the occurrence status of events, checking or analyzing the performance information of each node. However, not all functional operations provided by each product can be performed. If necessary, also use the management console provided by each product together.

## 1.1.2 Functional overview of Web Console

The following describes the functions on Web Console.

## Dashboard

- The current network performance and event occurrence status can be grasped promptly.
- Multiple display contents can be defined for each viewpoint. This enables the status to be viewed from various viewpoints by selecting the defined contents from a pull-down menu.
- A **Widget**, which is an element use to display a chart or list, can be freely located on the dashboard page by the intuitive drag-and-drop operation. Therefore, a dashboard definition according to the operations can be created easily.

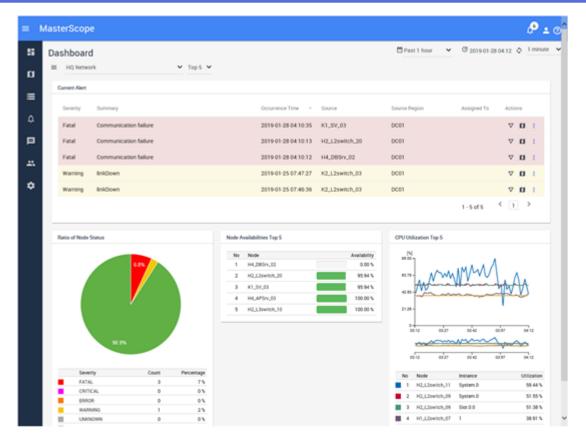


Figure 1-1 Dashboard

## Node management and analysis

- Nodes managed by Network Manager and exporters of NFA are managed as a "*Node*". Information of nodes that can be assumed to be the same in multiple products is integrated and managed in a single node.
- It is possible to search nodes that match a certain condition among all managed nodes, and also check and compare the property information.
- The dashboard (Node Detail page) of each node can be used to check and analyze the property information and load status of the specified node in detail. The dashboard (Network Interface Detail page) of each network interface can be used to check the property information and communication status of the specified network interface in detail.

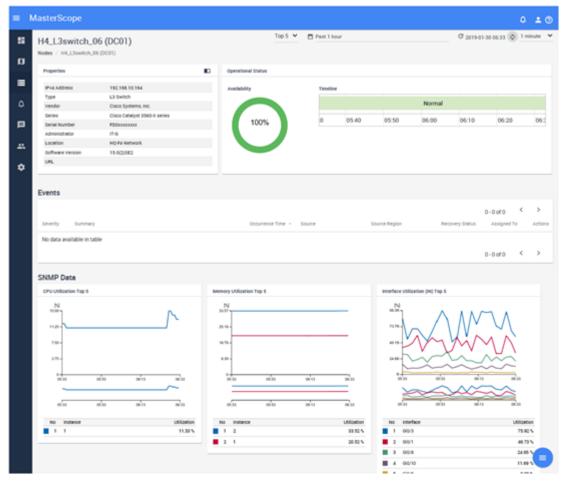


Figure 1-2 Node Detail

## **Topology Map (when using Network Manager)**

- As the topology map, it is possible to show the physical connections among the nodes, node placement in the building or on the floor, and so on. The topology map is helpful for operations such as checking the influence range when a fault occurs. The topology map provides various editing functions that make it easy to grasp network configuration such as insertion of background image.
- A mechanism (Side Panel) is provided to check the property and performance information of nodes while looking at the topology map. It can be used to investigate nodes, which are related to each other, one by one on the topology map.
- Displaying the topology map in **analysis mode** enables users to check the event severity of each node for a certain period in the past. This is called the Timeline function. For example, if an event that occurred last night has currently recovered, this function supports the situation grasping at the time of the event occurred by going back to the event occurrence time of the previous night and visualizing the event influence range on a topology map.

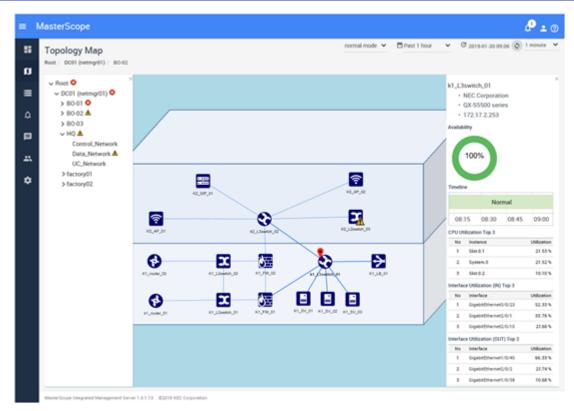


Figure 1-3 Topology Map

## **Event monitoring**

- Alerts detected by Network Manager and events exceeding the threshold of traffic volume detected by NFA are managed as an *"event"* integrally. Also, it is possible to investigate the cause smoothly from the event; for example, checking detailed information of the relevant node and jumping to the topology map.
- The occurred events can be checked the summary information in the event list. Also, it is possible to check only necessary information by narrowing down the display events by specifying a condition. Placing the **Current Alert** widget on the Dashboard page enables to grasp current fault events promptly.
- An action such as sending an Email or running a command can be executed when an event occurs by specifying a condition for events. This function can be used to send notifications to the person involved and to control automatic recovery.

=	Ma	aste	rScope						¢ <sup>®</sup> ± ⊙́
8	E	Ever	nts					C 2019-01-28 09:32	1 minute V
a		SE	LECT	SEARCH					
=	ľ	_				R	lows per page:	100 ¥ 1-100 of 104 <	1 2 >
۵			Severity	Summary	Occurrence Time -	Source	Source Region	Recovery Status Assigned To	Actions
			Normal	linkUp	2019-01-28 09:31:21	K2_L2switch_03	DC01		a v
			Warning	linkDown	2019-01-28 09:31:03	H2_L2switch_01	DC01	Unrecovered	a v
			Warning	linkDown	2019-01-28 09:16:09	K2_L2switch_04	DC01	Unrecovered	αv
\$			Warning	linkDown	2019-01-28 09:13:35	H3_L3switch_03	DC01	Unrecovered	αv
			Normal	linkUp	2019-01-28 09:09:56	K2_L2switch_03	DC01		αv
			Warning	linkDown	2019-01-28 09:09:46	K2_L2switch_03	DC01	Unrecovered	αv
			Fatal	Communication failure	2019-01-28 04:10:35	K1_SV_03	DC01	Unrecovered	αv
			Fatal	Communication failure	2019-01-28 04:10:13	H2_L2switch_20	DC01	Unrecovered	αv
			Fatal	Communication failure	2019-01-28 04:10:12	H4_DBSrv_02	DC01	Unrecovered	vα
			Normal	Cancel Event	2019-01-28 02:15:56	H2_L2switch_20	DC01		u v
			Normal	Cancel Event	2019-01-28 02:15:35	K1_SV_03	DC01		
			Normal	Cancel Event	2010-01-25 00-40-36	MA DRSvv 02	0001		7 0

Figure 1-4 Events

## **1.2 Operating Environment**

This chapter describes the operating environment of the Web Console.

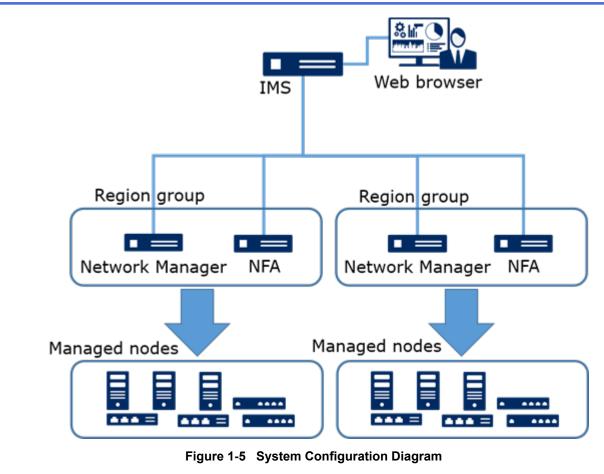
## 1.2.1 System configuration

The following describes the system configuration when using Web Console.

To use Web Console, set up the IMS component and connect the IMS component to the MasterScope network management products. When connecting the IMS component with multiple products, products managing the same node are grouped into the region group.

For example, if Network Manager managing Nodes 1 to 45 and NFA managing Nodes 40 to 45 as exporters exist in the same environment, these two products manage Nodes 40 to 45 redundantly. In this case, the two products are grouped into the region group. Information of Nodes 40 to 45 managed by the two products can be viewed in an integrated manner on Web Console.

"Figure 1-5 System Configuration Diagram (page 7)" shows a system configuration example consisting of multiple region groups.



Tip

- A system can be built by installing the IMS component and MasterScope network management products, such as Network Manager, on the same server.
- Note that installing the IMS component and multiple products on the same server may cause problems such as slow operational response of Web Console. Therefore, thoroughly assess the system configuration before starting operations. If possible, it is recommended that products be installed separately on multiple servers.

## 1.2.2 System requirements

The following describes the system requirements for properly operating the Web Console and the supported environment.

Item	Description		
СРИ	Intel Dual-Core Xeon or higher, or equivalent compatible processor recommended		
System memory	2 GB or more (8 GB or more recommended)		
Disk capacity	Installation path: 2 GB or more		
	Data path: 20 GB or more		
OS	• Windows Server 2019 (x64) <sup>1) 2)</sup>		
	• Windows Server 2016 (x64) <sup>1) 2)</sup>		
	• Windows Server 2012 R2 (x64) <sup>1)</sup>		

#### Table 1-1 IMS requirements

Item	Description
	• Windows Server 2012 (x64) <sup>1</sup> )
Supported cluster software	EXPRESSCLUSTER X 3.0 or later

#### Note

- 1. Windows Server Core is not supported.
- 2. Nano Server is not supported.

Table 1-2	Web	browser	rea	uirements
		010001		

Item	Description		
Supported web browser	The following web browsers running on Windows		
	Internet Explorer 11		
	Mozilla Firefox 60 or later		
	Google Chrome 71 or later		
СРИ	Intel Core i3 or higher, or equivalent compatible processor recommended		
System memory	1GB or more		

#### Tip

- It is recommended to apply the latest bug fix updates to the web browser before using it. If the bug fix updates have not been applied, some functions might not work properly.
- Depending on a web browser, a Unicode surrogate pair character is handled as two characters. In this case, an actual number of characters that can be input to each input field will be less.

# Chapter 2. Installation of IMS Component

This chapter describes how to set up the IMS component to use Web Console.

## Contents

2.1	Setup Flow for the IMS Component	10
2.1		10
2.2	Preparation for Setup	11
2.3	Configuring a failover group	16
2.4	Installation	16
2.5	Configuring to connect the products	18
2.6	Configuring the communication protocol settings of Web Console	21
2.7	Changing the communication port number from default value	26
2.8	Changing the firewall settings	27
2.9	Configuring the additional settings on the installation environment	28
2.10	Configuring the services to support a cluster	30
2.11	Checking the switching between the active server and standby server	31
2.12	Setting up the products to be connected	32

## 2.1 Setup Flow for the IMS Component

The following describes the flow to set up the IMS component on a cluster system.

The setup flow for the IMS component is described in "Table 2-1 Setup Flow for the IMS Component (page 10)".

No.	Summary	Description		
1	Determining the installation parameters	"2.2.1 Designing the installation parameters (page 11)" Determine the parameters necessary to install the IMS component and specify an appropriate value for each of parameters.		
2	Checking the installation environment [Active], [Standby]	<ul><li>"2.2.2 Checking the installation environment (page 16)"</li><li>Check that the active and standby servers satisfy the system requirements to use the IMS component.</li><li>For a shared disk configuration, be sure to check the available space of a shared disk.</li></ul>		
3	Configuring a failover group [Active], [Standby]	"2.3 Configuring a failover group (page 16)" Install EXPRESSCLUSTER X to both the active server and standby server, and then configure a failover group.		
4	Installing the IMS component [Active]	"2.4 Installation (page 16)" Run the installer stored in the installation media to install the IMS component to the active server.		
5	Installing the IMS component [Standby]	<ul><li>"2.4 Installation (page 16)"</li><li>Run the installer stored in the installation media to install the IMS component to the standby server.</li><li>Be careful so as not to install it under the data path.</li></ul>		
6	Configuring the settings to connect the products [Active]			
7	Configuring the communication protocol settings of Web Console [Active]	"2.6 Configuring the communication protocol settings of Web		
		When using HTTP communication to access Web Console, skip this step.		
8	Checking the port number to use [Active], [Standby]	<ul><li>"2.7 Changing the communication port number from default value (page 26)"</li><li>On both the active and standby servers, check that the port numbers used by the IMS component do not interfere with those used by other coexisting software.</li></ul>		
9	Configuring the firewall settings [Active], [Standby]	"2.8 Changing the firewall settings (page 27)" Check whether the firewall setting allows the IMS component of both the active and standby servers to communicate with external systems properly, and change the setting if necessary.		
10	Configuring the additional settings of the installation environment	"2.9 Configuring the additional settings on the installation environment (page 28)"		

Table 2-1 Setup Flow for the IMS Component

No.	Summary	Description		
	[Active], [Standby]	Configure the additional settings on both the active server and standby server.		
11	Configuring a cluster of services [Active], [Standby]	"2.10 Configuring the services to support a cluster (page 30)" Configure the settings to control starting and stopping the IMS component service so that the active and standby servers can switch between each other.		
12	Checking switching between the active server and standby server [Active], [Standby]	"2.11 Checking the switching between the active server and standby server (page 31)" Start the cluster of the IMS component and confirm that active and standby servers can switch between each other properly.		
13	Setting up the products to be connected	"2.12 Setting up the products to be connected (page 32)" Set up the MasterScope network management products to be connected to the IMS component.		

## 2.2 Preparation for Setup

The following describes preparations for setup of the IMS component.

## 2.2.1 Designing the installation parameters

The parameters necessary to install the IMS component must be prepared.

## Parameters necessary to run the installer

The following table shows the parameters necessary to run the IMS component installer. Before installing the IMS component, prepare the parameters that will be specified by using the installer.

Parameter name	Description	Default value
Install Path	Directory in which to install the IMS component execution file.	C:\Program Files\NEC\IMS
	Specify a local directory.	
	A maximum of 128 characters can be entered. Available characters are single-byte alphanumeric characters, underscore (_), hyphen (-), and dot (.).	
Data Path	Directory in which to save the environment settings and accumulated data.	C:\Program Files\NEC\IMS
	A maximum of 128 characters can be entered. Available characters are single-byte alphanumeric characters, underscore (_), hyphen (-), and dot (.).	
	Specify a path of a shared disk different from the installation path.	
	Data such as events and reports are accumulated in the data path. A lot of free space may be necessary for the data path depending on the operation environment.	

Table 2-2 Parameters Necessary to Run the Installer

# Parameters necessary to configure the settings to connect the products

The following table shows the parameters to connect the IMS component and the MasterScope network management products.

Parameter name	Description	Example
region id	This is necessary to configure the IMS component.	tokyo
	ID of a region group that is used to classify connecting products. Available characters are single-byte alphanumeric characters.	
	<u>▲</u> Caution	
	This ID cannot be changed after setting up.	
	When using multiple region groups, prepare multiple IDs.	
region name	This is necessary to configure the IMS component.	Tokyo
	Name of a region group corresponding a <b>region id</b> . A name can be specified with an arbitrary character string.	
	A Caution	
	You can use Windows code page for non-ASCII characters.	
	In the Web Console, the specified name is displayed as the name of the region group.	
manager id (InstanceID)	This is necessary to configure both IMS component and products connecting to it.	nvpro01 (belongs to <b>tokyo</b> region)
	ID that is used in the IMS component to identify the product instance. Specify an unique ID among the same product type. Available characters are single-byte alphanumeric characters.	
	A Caution	
	This ID cannot be changed after setting up.	
	When using multiple product instances with the same type, prepare multiple IDs.	
	For example, when using two Network Manager, prepare two unique IDs. IDs can be duplicated between dirrerent product types such as Network Manager and NFA.	
	When preparing <b>manager id</b> , you should also design a <b>region id</b> (region group) to which it belongs.	
manager host name	This is necessary to configure the IMS component.	NetMgr01
	Host name corresponding to <b>manager id</b> . A host name can be specified with an arbitrary character string.	
	▲ Caution	
	You can use Windows code page for non-ASCII characters.	

 Table 2-3
 Parameters Necessary to Configure the Settings to Connect the Products

Parameter name	Description	Example
	It is recommended to use the real host name of the server for convenient operation.	
	In the Web Console, the specified name is displayed as the name of the product instance.	
ims ip address	This is necessary to configure products connecting to the IMS component.	192.168.1.200
	Floating IPv4 address of the cluster system where the IMS component is installed.	

# Parameters necessary to configure the connection settings for Network Manager

The following table shows the parameters to connect the IMS and the Network Manager.

Parameter name	Description	Example
manager ip address	This is necessary to configure the IMS component. IPv4 address of the server where the connecting Network Manager manager function is installed.	192.168.1.100
	Тір	
	For servers with multiple IPv4 addresses, be sure to check the connectable IPv4 address from the IMS component.	

 Table 2-4
 Parameters Necessary to Configure the Settings to Connect the Network Manager

The IMS component uses the WebAPI of the Network Manager to control the Network Manager. If the parameters of the Network Manager WebAPI are changed from default, prepare the following parameters.

Table 2-5	Parameters	for the	Network	Manager WebAPI
-----------	------------	---------	---------	----------------

Parameter name	Description	Default value
webapi port number	This is necessary to configure both IMS component and Network Manager. Port number of the Network Manager WebAPI.	20100
webapi ssl flag ([Use HTTPS cryptogram] checkbox)	<ul> <li>This is necessary to configure both IMS component and Network Manager.</li> <li>Specify whether to use HTTPS for the Network Manager WebAPI as follows.</li> <li>true (on): <ul> <li>uses HTTPS.</li> <li>false (off):</li> <li>uses HTTP, not HTTPS.</li> </ul> </li> </ul>	false (checkbox: off)

# Parameters necessary to configure the connection settings for NFA

The following table shows the parameters to connect the IMS component and the NFA.

Parameter name	Description	Example
nfa web url	This is necessary to configure the IMS component. URL of the NFA Web console.	https://nfa01.nec.com/nfa
ims web url	This is necessary to configure the NFA. URL of the IMS Web console.	http://ims-cluster.nec.com

Table 2-6 Parameters Necessary to Configure the Settings to Connect the NFA

## Parameters for network communication

Both HTTP and HTTPS are supported for accessing the Web Console Web console. HTTP is the default. The IMS component also uses other ports for internal and external communication. The following table shows the default communication port numbers.

Confirm beforehand about the necessity of change from the default value for each communication port.

 Table 2-7
 Communication Port Number List (for External Communication)

Name	Port number	Protocol	Direc tion	Application
HTTP communication port	80	TCP	IN	Port for HTTP communication
HTTPS communication port	443	ТСР	IN	Port for HTTPS communication
Message Queue communication port	28110	ТСР	IN	Port for message send and receive communication

 Table 2-8
 Communication Port Number List (for Internal Communication)

Name	Port number	Protocol	Direc tion	Application
System Database communication port	28120	ТСР	IN	Port for communication with a system database
Key Store communication port	28130	TCP	IN	Port for communication with a key store

## Parameters necessary to create the SSL server certificate

When using HTTPS communication to access Web Console, the SSL server certificate must be created. Prepare the parameters necessary to create the SSL server certificate and those related to the identification name (Distinguished Name) of the certificate.

#### Tip

When using HTTP communication to access Web Console, skip this step.

Parameter name	Description	Default value
Keystore Password	Password for the keystore to save the SSL server certificate	None
Entry Alias	Display name of the entry to save the SSL server certificate Unless there is a special reason, it is recommended to use the default value.	tomcat
Key Encryption Algorithm	Encryption algorithm for the key of the SSL server certificate	RSA

 Table 2-9
 Parameters related to the SSL server certificate

Parameter name	Description	Default value
	When using a self-signed certificate, there is usually no problem using the default value. For details of the values that can be specified, refer to "A.1 ims-ssl-keytool (page 67)".	
Generated Key Size	Size of the key of the SSL server certificate When using a self-signed certificate, there is no problem in using the default value usually. For details of the values that can be specified, refer to "A.1 ims-ssl-keytool (page 67)".	2048
Signature Algorithm	Algorithm to be used to sign a self-signed certificate There is usually no problem using the default value. For details of the values that can be specified, refer to "A.1 ims- ssl-keytool (page 67)". When asking a public certificate authority to issue the SSL server certificate, you may specify the signature algorithm. For details, ask the relevant certificate authority.	SHA256withRSA
Self-signed Certificate Expiry Date	Expiry date to be specified when using a self-signed certificate. Specify the period of validity from the date of creation. When asking a public certificate authority to issue the SSL server certificate, the public certificate authority usually determines the expiry date. Therefore, preparation of this parameter is unnecessary.	3,650 days (approximately 10 years)

Table 2-10	Parameters Related to the SSL Server Certificate Identification Name (Distinguished
	Name)

Parameter name	Description	Example	
Server FQDN	The fully qualified domain name (FQDN) of the server to which to install the IMS component This is equivalent to Common Name of the SSL server certificate.	ims- cluster.nec.com	
	All web browsers accessing Web Console use this domain name in the URL. Therefore, this domain name must be able to be resolved by the web browsers.		
	<u>∧</u> Caution		
	Therefore, this name must be resolvable by the floating IP address of a cluster system.		
Department Name	Department name of the organization that owns and operates the products. This is equivalent to Organizational Unit of the SSL server certificate.	IT Operation Division	
Organization Name	Name of the organization that owns and operates the products. This is equivalent to Organizational Name of the SSL server certificate.	NEC Corporation	
	Specify a legally official English organization name.		
City Name	Name of the city to which the organization that owns and operates the products belongs. This is equivalent to Locality of the SSL server certificate.	Minato-ku	
	In the case of Minato-ku, Tokyo, specify "Minato-ku".		
Prefecture Name	Name of the prefecture to which the organization that owns and operates the products belongs. This is equivalent to State of the SSL server certificate.	Tokyo	
	In the case of Tokyo, specify "Tokyo".		

Parameter name	Description	Example
Country Code	Name of the country to which the organization that owns and operates the products belongs. This is equivalent to Country of the SSL server certificate.	JP
	For Japan, the country code is usually specified as "JP".	

## 2.2.2 Checking the installation environment

Check whether the server to which to install the IMS component satisfies the installation environment requirements.

Check that the installation destination server satisfies the system requirements of the IMS component described in "1.2.2 System requirements (page 7)".

You should also check that the communication ports listed in "Parameters for network communication (page 14)" are not used by other software on the installation destination server. If a port is already used on the server, change the IMS component port number, or change other software configuration related to this port.

## 2.3 Configuring a failover group

Install EXPRESSCLUSTER X to both the active and standby servers, and then configure a failover group.

For details about how to install and set up EXPRESSCLUSTER X, refer to the EXPRESSCLUSTER X documentation.

After installing EXPRESSCLUSTER X, configure the following settings.

1. Synchronizing the system time

Configure the setting so that the system times of the active and standby servers always synchronize by using NTP (Network Time Protocol) and the like.

2. Creating a failover package

Create a failover group for IMS consisting of two servers (active and standby) on the operation window of EXPRESSCLUSTER X.

3. Configuring shared disk resources

Register the following resources to the failover group for the IMS component.

- Floating IP resource
- Mirror disk resource or shared disk resource
- Script resource

## 2.4 Installation

Run the installer stored in the installation media to install the IMS component.

When installing on the cluster system, install on both active and standby server.

#### 🕂 Caution

When installing on the active server, installation needs to be performed with the shared disk space accessible.

- 1. Insert the installation media into the DVD-ROM drive.
- 2. Start the installer.

Run IMS\Windows\ImsSetup.exe in the DVD-ROM drive.

#### Tip

Depending on the type of installation media you use, the path of the installer differs. In the case of MasterScope Media, the installer is located in the following path:

In the media: \Windows\Tools\NvPRO\IMS\ImsSetup.exe

After the installer is started, the installation environment is checked. If already installed, installation process is canceled at this point.

When the check is completed, the installation wizard will be displayed.

3. Confirm the installation version.

The installation version of the IMS is displayed on the wizard screen. If it is correct, click the **Next** button.

4. Enter the install path.

Enter the install path prepared in "2.2.1 Designing the installation parameters (page 11)".

5. Enter the data path.

Enter the data path prepared in "2.2.1 Designing the installation parameters (page 11)". Be sure to enter the path of a shared disk.

6. Confirm the status of the **Install initial data** checkbox.

On the active server, check the check box in order to perform the shared data installation on the data path.

On the standby server, clear the check box in order to skip the shared data installation.

Confirm the status of the check box and then click **Next** button.

7. Select product applications to be incorporated in the IMS component.

Check the check boxes of the applications to be incorporated. You need to check the applications that correspond to the products you want to connect to the IMS component.

After selecting the applications, click the **Next** button.

#### Тір

- If a product application is not incorporated in the IMS component, a related product cannot connect to the IMS component.
- To incorporate an application after IMS installation completed, use ims-app command. For details of ims-app command, refer to "A.2 ims-app (page 70)".

Application files are stored in the following path on the installation media.

In the media:  $\IMS\Windows\app\$ 

8. Confirm the installation contents.

The installation parameters are displayed in **Current Settings**. If the displayed contents are incorrect, click the **Back** button, and then correct the parameters.

9. Installation starts.

Click the **Start** button to start the installation process. Once the installation process is started, you cannot cancel it.

When the installation is completed, the result is displayed.

Check that the IMS component has been successfully installed.

If an error message is displayed, take appropriate action according to "B.1 Troubleshooting errors when running the installer (page 72)".

## 2.5 Configuring to connect the products

To perform operations of Web Console, the MasterScope network management products must be connected with the IMS component.

To connect each product to the IMS component, the settings to allow connection must be configured on both sides. The following describes the settings to be configured on the IMS component.

On the IMS component side, based on the parameters prepared in "2.2.1 Designing the installation parameters (page 11)", change and save the contents of the configuration file (ims-conf.ini).

#### **Configuration file path**

```
<%DATAPATH%>\conf\ims-conf.ini
```

#### Тір

Changes made to the configuration file (ims-conf.ini) are reflected when the services start up.

Configurations in ims-conf.ini are as follows.

"Region group settings (page 18)"

Configure region group settings that classify the connecting products.

"Common settings for connecting products (page 19)"

Configure common settings for connecting products.

"Connection settings for Network Manager (page 19)"

Configure Network Manager specific settings.

"Connection settings for NFA (page 20)"

Configure NFA specific settings.

• "Single sign-on settings (page 21)"

Configure settings for single sign-on access to the web console of the connected products from Web Console provided by the IMS component.

The details of settings are explained below.

### **Region group settings**

The format of region group settings is as follows.

noms.core.regions.<region id>.name = <region name>

<region id>

Specify a region group ID prepared as **region id** parameter in "Parameters necessary to configure the settings to connect the products (page 12)".

<region name>

Specify a region group name corresponding to the **region id** parameter. This group name is prepared as **region name** parameter in "Parameters necessary to configure the settings to connect the products (page 12)".

Example:

noms.core.regions.tokyo.name = Tokyo

This example specifies the region name "Tokyo" for the ID "tokyo".

### Common settings for connecting products

The format of common settings for connecting products is as follows.

```
noms.<type>.managers.<manager id>.name = <manager host name>
noms.<type>.managers.<manager id>.region-id = <region id>
```

#### <type>

Specify a type of product as follows.

- For Network Manager: nvp
- For NFA: nfa

#### <manager id>

Specify an ID for the connecting product. This ID is prepared as **manager id** in "Parameters necessary to configure the settings to connect the products (page 12)".

#### <manager host name>

Specify a host name prepared as **manager host name** in "Parameters necessary to configure the settings to connect the products (page 12)". The specified host name is associated with the **manager id** parameter.

#### <region id>

Specify a region group ID (**region id** parameter) to which the product belongs. The specified host name is associated with the **manager id** parameter.

#### Example:

noms.nvp.managers.nvpro01.name = NetMgr01
noms.nvp.managers.nvpro01.region-id = tokyo

noms.nfa.managers.nfa01.name = FlowMgr01
noms.nfa.managers.nfa01.region-id = tokyo

In this example, the ID "*nvpro01*" is assigned for the host "*NetMgr01*" of Network Manager and the ID "*nfa01*" is assigned for the host "*FlowMgr01*" of NFA. Each product belongs to the region that has the ID "*tokyo*".

### **Connection settings for Network Manager**

The format of connection settings for Network Manager is as follows.

```
noms.nvp.managers.<manager id>.ip-address = <manager ip address>
```

#### <manager id>

Specify the ID (manager id parameter) for the target Network Manager.

#### <manager ip address>

Specify the IPv4 address of the server where the manager function of Network Manager is installed. This IPv4 address is prepared as **manager ip address** in "Parameters necessary to configure the connection settings for Network Manager (page 13)".

If the manager function of Network Manager is installed on the cluster system, specify the floating IPv4 address of the cluster system.

The IMS component uses the WebAPI of the Network Manager to control the Network Manager. If the parameters for the Network Manager WebAPI are changed from default, add the following settings.

```
noms.nvp.managers.<manager id>.webapi-port = <webapi port number>
noms.nvp.managers.<manager id>.webapi-use-ssl = <true | false>
```

#### <webapi port number>

Specify the WebAPI port number prepared in "Parameters necessary to configure the connection settings for Network Manager (page 13)".

#### <true|false>

Specify whether to use HTTPS for the WebAPI.

- true : use HTTPS.
- false : use HTTP, not HTTPS.

Specify it as prepared in "Parameters necessary to configure the connection settings for Network Manager (page 13)".

Example:

```
noms.nvp.managers.nvpro01.ip-address = 192.168.1.100
noms.nvp.managers.nvpro01.webapi-port = 20110
noms.nvp.managers.nvpro01.webapi-use-ssl = true
```

In this example, "192.168.1.100" is specified as an IPv4 address of the Network Manager host that has the ID "*nvpro01*", and "*HTTPS*" with the port number "20110" is used for the WebAPI.

### **Connection settings for NFA**

The format of connection settings for NFA is as follows.

noms.nfa.managers.<manager id>.url = <nfa web url>

<manager id>

Specify the ID (manager id parameter) for the target NFA.

<nfa web url>

Specify the URL of the NFA Web console. This URL is prepared as **nfa web url** parameter "Parameters necessary to configure the connection settings for NFA (page 13)".

Example:

noms.nfa.managers.nfa01.url = https://nfa01.nec.com/nfa

This example specifies "*https://nfa01.nec.com/nfa*" for the Web console URL of the NFA host that has the ID "*nfa01*".

## Single sign-on settings

The format of settings for single sign-on access is as follows.

```
ssolite.server.permitted-domains[n] = <web url>/sso-login
```

n

Specify an index starting with "0". Single sign-on access can be configured for multiple products.

<web url>

Specify the Web console URL for the connecting product.

Example:

```
ssolite.server.permitted-domains[0] = https://nfa01.nec.com/nfa/sso-login
ssolite.server.permitted-domains[1] = https://nfa02.nec.com/nfa/sso-login
```

This example enables single sign-on access for two NFA.

# 2.6 Configuring the communication protocol settings of Web Console

HTTP or HTTPS communication can be selected for accessing Web Console.

Immediately after installation of the IMS component, HTTP communication is configured to be used by default.

Therefore, to use HTTPS communication, the following settings must be configured.

- Changing the setting values in the configuration file (ims-conf.ini)
- Preparing the SSL server certificate

#### Tip

There is no additional setting when using HTTP communication for accessing Web Console.

### 2.6.1 Enabling HTTPS communication

The following describes how to specify the configuration file to use HTTPS communication to access Web Console.

When using HTTPS communication to access Web Console, it is necessary to change the following setting in the configuration file.

## **Configuration file path**

<%DATAPATH%>\conf\ims-conf.ini

## Format

The format of the parameters is as follows.

```
noms.tomcat.http.enabled = <true | false>
```

```
noms.tomcat.https.enabled = <true | false>
```

To enable HTTPS and disable HTTP, specify as follows.

noms.tomcat.http.enabled = false

noms.tomcat.https.enabled = true

#### Tip

- By running the ims-ssl-keytool genkeypair command in order to create an SSL certificate, noms.tomcat.https.enabled value in the ims-conf.ini file is modified to "*true*" automatically.
- Changes made to the ims-conf.ini file are reflected when the services start up.

### 2.6.2 Preparing the SSL server certificate

The SSL server certificate needs to be prepared to access Web Console via HTTPS.

Perform this certificate preparation only on the active server.

When the IMS component is set up on a cluster system, use a self-signed certificate as the SSL server certificate.

#### 🕂 Caution

The supported certificate format is X.509, which is equivalent to the format that can be handled by Java keytool. This format is supported by many certificate authorities. However, check in advance whether the certificate authority that you intend to use supports this format.

## 2.6.2.1 Preparing a self-signed certificate

The following describes how to create a self-signed certificate as the SSL server certificate.

Use the ims-ssl-keytool command provided by the product for operations related to the SSL server certificate. For details, refer to "A.1 ims-ssl-keytool (page 67)".

Distribute and import the created certificate into all web browsers that you will use to access Web Console.

1. Run the following command to generate a key pair (public key and private key) and create a certificate for the generated keys.

> <%INSTPATH%>\bin\ims-ssl-keytool genkeypair

Enter the password of the keystore storing the keys and certificate, identification name of the certificate, and information about the key password.

- The default value is displayed in []. The default value is used by pressing the Enter key without entering anything.
- If you press the Enter key without entering anything for the key password, the same password as that of the keystore is set.

```
What is your server domain name? (FQDN)
[ims.nec.com]: ims-cluster.nec.com
What is the name of your organizational unit?
[Unknown]: IT Operation Division
What is the name of your organization?
[Unknown]: NEC Corporation
What is the name of your City or Locality?
[Unknown]: Minato-ku
What is the name of your State or Province?
[Unknown]: Tokyo
What is the two-letter country code for this unit?
[Unknown]: JP
Is CN=ims-cluster.nec.com, OU=IT Operation Division,
O=NEC Corporation, L=Minato-ku, ST=Tokyo, C=JP correct?
[No]: yes
```

#### Тір

• For the ims-ssl-keytool command, multiple arguments can be specified. If you want to change the algorithm, size, and expiry date of the key, specify the proper option according to "A.1 ims-ssl-keytool (page 67)".

An example on how to set the key algorithm and size to ECDSA and 256 bits, respectively:

```
> cd C:\Program Files\NEC\IMS\bin
> ims-ssl-keytool genkeypair -keyalg EC -keysize 256
```

• If you want to recreate the key by changing its contents, run the ims-ssl-keytool delete command and then the ims-ssl-keytool genkeypair command again.

```
For details about the commands, refer to "A.1 ims-ssl-keytool (page 67)".
```

The created certificate is self-signed.

2. Run the following command to output a certificate to import into web browsers to a file.

> <%INSTPATH%>\bin\ims-ssl-keytool exportcert <filename>

For *<filename>*, any file name can be specified. However, it is strongly recommended that you specify .cer as the extension of a file to easily import the file into web browsers.

When the command terminates successfully, a certificate in binary encoding format is output to the specified file.

Distribute and import the certificate file output by using the ims-ssl-keytool exportcert command into all web browsers that you will use to access Web Console. Importing a certificate into a web browser prevents problems such as a phishing attack pretending to be the web browser that can be used to access the IMS component.

For how to import the certificate into a web browser, refer to "3.1.2 Importing the SSL server certificate into the web browser (page 39)".

# 2.6.2.2 Preparing a certificate to be issued by a public certificate authority

The following describes how to have a public certificate authority issue a signed certificate as the SSL server certificate.

Use the ims-ssl-keytool command provided by the product for operations related to the SSL server certificate. For details, refer to "A.1 ims-ssl-keytool (page 67)".

The supported certificate format is X.509, which is equivalent to the format that can be handled by Java keytool. This format is supported by many certificate authorities. However, check in advance whether the certificate authority that you intend to use supports this format.

1. Run the following command to generate a key pair (public key and private key) and create a certificate for the generated keys.

> <%INSTPATH%>\bin\ims-ssl-keytool genkeypair

Enter the password of the keystore storing the keys and certificate, identification name of the certificate, and information about the key password.

- The default value is displayed in []. The default value is used by pressing the Enter key without entering anything.
- If you press the Enter key without entering anything for the key password, the same password as that of the keystore is set.

```
What is your server domain name? (FQDN)
[ims.nec.com]: ims-cluster.nec.com
What is the name of your organizational unit?
[Unknown]: IT Operation Division
What is the name of your organization?
[Unknown]: NEC Corporation
What is the name of your City or Locality?
[Unknown]: Minato-ku
What is the name of your State or Province?
[Unknown]: Tokyo
What is the two-letter country code for this unit?
[Unknown]: JP
Is CN=ims-cluster.nec.com, OU=IT Operation Division,
O=NEC Corporation, L=Minato-ku, ST=Tokyo, C=JP correct?
[No]: yes
```

#### Tip

• For the ims-ssl-keytool command, multiple arguments can be specified. If you want to change the algorithm, size, and expiry date of the key, specify the proper option according to "A.1 ims-ssl-keytool (page 67)".

An example on how to set the key algorithm and size to ECDSA and 256 bits, respectively:

```
> cd C:\Program Files\NEC\IMS\bin
> ims-ssl-keytool genkeypair -keyalg EC -keysize 256
```

• If you want to recreate the key by changing its contents, run the ims-ssl-keytool delete command and then the ims-ssl-keytool genkeypair command again.

For details about the commands, refer to "A.1 ims-ssl-keytool (page 67)".

2. Run the following command to output a certificate signing request (CSR) to send to a certificate authority to a file.

```
> <%INSTPATH%>\bin\ims-ssl-keytool
certreq -dns <FQDN> <filename>
```

The contents of CSR are output in the specified file in text format.

3. Submit a certificate signing request (CSR) to a certificate authority.

Submit the CSR file output by using the ims-ssl-keytool certreq command to a certificate authority.

The certificate authority signs a certificate according to the contents of the CSR file and returns the signed certificate to the requester. Some certificate authorities may take several days to return the signed certificate.

4. When the signed certificate arrives, import the root certificate of the certificate authority first.

Next, save the root certificate as a file on the server where the IMS component is installed and then import the file by using the following command.

```
> <%INSTPATH%>\bin\ims-ssl-keytool
importcert -alias <alias> <filename>
```

For *<alias>*, any name can be specified. Specify a meaningful name such as a certificate authority name.

Depending on a certificate authority, it is necessary to import an intermediate certificate in addition to the root certificate. For details about the certificates to be imported, ask the relevant certificate authority.

5. After importing the root and intermediate certificates, install your own signed certificate.

Use the ims-ssl-keytool importcert command to import your own signed certificate. Run this command without the -alias option.

> <%INSTPATH%>\bin\ims-ssl-keytool importcert <filename>

If the message Failed to establish chain from reply is displayed during execution of the above command, the certificate chain could not be resolved. The root certificate of the certificate authority or the intermediate certificate may not be imported. For the certificates to be imported, ask the relevant certificate authority.

This completes the preparation of the certificates for the IMS component.

Depending on the certificate authority to be used, it may be necessary to import its certificates in a web browser. For details, follow the instructions of the certificate authority.

## 2.6.2.3 Using certificates created previously

The following describes how to use certificates created previously as the SSL server certificate.

Prepare a keystore in PKCS12 format and create a valid key and certificate in the keystore. Allocate the file prepared in the keystore to the server where the IMS component is installed.

1. Open the following text file.

<%DATAPATH%>\conf\ims-conf.properties

If this file does not exist, create a new one. The encoding format of the file must be UTF-8.

2. Describe the following in the ims-conf.properties file.

```
ims.tomcat.https.keyAlias = Alias of the entry containing a key
ims.tomcat.https.keystoreFile = Absolute path of a keystore file
ims.tomcat.https.keystorePass = Password for the keystore
```

#### 🛕 Caution

If the setting to use the external keystore is described in the ims-conf.properties file, the ims-ssl-keytool command cannot be used. Use the commands of Java keytool directly for management.

The commands of Java keytool are installed together with the IMS component.

```
<%INSTPATH%>\jre\bin\keytool
```

For a self-signed certificate, output a certificate (.cer) in binary encoding format and import the file into a web browser.

# 2.7 Changing the communication port number from default value

The following describes how to modify the configuration file to change the port number used by the IMS component from default value.

When you need to change the port number used by the IMS component from default value in "2.2.1 Designing the installation parameters (page 11)", change the configuration file corresponding to the communication type and save it according to the following contents.

#### Tip

You do not need to perform this task when operating the communication port number with default value.

Communication type	Specification format				
HTTP communication	Configuration file				
	<%DATAPATH%>\conf\ims-conf.ini				
	<%datapath%> /conf/ims-conf.ini				
	Specification format				
	<pre>noms.tomcat.http.port = <port number=""></port></pre>				
	By setting the following property in the configuration file to <i>"true"</i> , the above setting becomes to enable.				
	If "false", the port is nor opened.				
	<pre>noms.tomcat.http.enabled = true</pre>				
HTTPS communication	Configuration file				
	<%DATAPATH%>\conf\ims-conf.ini				
	Specification format				
	<pre>noms.tomcat.https.port = <port number=""></port></pre>				
	By setting the following property in the configuration file to <i>"true"</i> , the above setting becomes to enable.				
	If "false", the port is nor opened.				
	<pre>noms.tomcat.https.enabled = true</pre>				
Message Queue	Configuration file				
communication	<%DATAPATH%>\conf\ims-conf.ini				
	Specification format				
	By adding the following property in the configuration file, a port number can be set.				
	<pre>amqphub.amqp10jms.remote-url = amqps://localhost:<port number=""> ?transport.trustAll=true</port></pre>				

#### Table 2-11 Communication Port Numbers

Communication type	Specification format					
	On the Products connected to the IMScompornent, it is needed to change the setting according to the above changed port number. Refer to "2.12 Setting up the products to be connected (page 32)" for details.					
System Database communication	<ul> <li>Configuration file         <pre> &lt;%DATAPATH%&gt;\conf\ims-conf.ini</pre> </li> <li>Specification format         By adding the following property in the configuration file, a port number can be         set.         noms.tomcat.jndi.port = <port number="">         Also update the following setting file according to the above setting.         Configuration file         &lt;%DATAPATH%&gt;\conf\systemdb-extra.conf         Specification format </port></li></ul>					
	<pre>port = <port number=""></port></pre>					
Key Store communication	<ul> <li>Configuration file &lt;\\$DATAPATH\$&gt;\conf\ims-conf.ini</li> <li>Specification format By adding the following property in the configuration file, a port number can be set.</li> </ul>					
	<pre>spring.redis.port = <port number=""></port></pre>					
	<ul> <li>Also update the following setting file according to the above setting.</li> <li>Configuration file <pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre></li></ul>					
	<pre>port = <port number=""></port></pre>					

#### 🕂 Caution

If a port is described and set up in multiple configuration files, edit all the configuration files at the same time and specify the same port number. If the port numbers are different between the related configuration files, communication cannot be performed properly.

#### Tip

Changes made to each configuration file are reflected when the services start up.

## 2.8 Changing the firewall settings

The firewall settings need to be changed so that the communication ports used by the IMS component are not blocked by the firewall.

For the default communication ports used by the IMS component, refer to "Table

2-12 Communication Port Number List (for External Communication) (page 28)" and "Table

2-13 Communication Port Number List (for Internal Communication) (page 28)".

If the communication ports are changed in the procedure of "2.7 Changing the communication port number from default value (page 26)", read the communication port numbers accordingly.

Name	Port number	Protocol	Direc tion	Application
HTTP communication port	80	ТСР	IN	Port for HTTP communication
HTTPS communication port	443	ТСР	IN	Port for HTTPS communication
Message Queue communication port	28110	ТСР	IN	Port for message send and receive communication

 Table 2-12
 Communication Port Number List (for External Communication)

Table 2-13 Communication Port Number List (for Internal Communication)

Name	Port number	Protocol	Direc tion	Application
System Database communication port	28120	ТСР	IN	Port for communication with a system database
Key Store communication port	28130	ТСР	IN	Port for communication with a key store

Check the firewall settings, and if necessary, change the settings so that these port numbers are not blocked by the firewall.

#### Тір

The firewall in the description indicates the following two types of firewalls:

- Personal firewall on the server where the IMS component is installed.
- Firewall on a communication path

# 2.9 Configuring the additional settings on the installation environment

The following describes the additional settings on the environment where the IMS component is installed.

## 2.9.1 Setting a URL for notificaiton

This section describes the setting of the URL of the Web Console used for notification process.

Web Console provides a function called "event action" to send e-mails or run commands when receiving events (alerts). In this function, a URL of an event detail information (Event Detailswindow) can be notified. For details, refer to *"MasterScopeNetwork ManagementWeb Console Reference Manual"*.

This section explains how to configure the URL of Web Console used in this notification function.

#### 🔥 Caution

The URL should be accessible where notifications are received.

To configure the URL of Web Console, edit the following configration file (ims-conf.ini).

## Path of the configuration file

<%DATAPATH%>\conf\ims-conf.ini

## **Specification format**

The followings describes the format for the parameter.

```
noms.core.url.external-base-url = <base url>
```

Example:

noms.core.url.external-base-url = http://ims-cluster.nec.com

Tip

Changes made to the configuration file (ims-conf.ini) is reflected when the service starts up.

## 2.9.2 Configuring to delete the web server logs automatically

The following describes the setting to automatically delete the web server logs in the IMS component on a regular basis.

Access logs of Web Console and operation logs of the web server are accumulated in the following directories. These logs are not deleted automatically. Configure the setting to delete old logs automatically if necessary by using *"the task scheduler"*.

- <%INSTPATH%>\tomcat\logs\localhost\_access\_log.yyyy-mm-dd.txt
- <%INSTPATH%>\logs\artemis.yyyy-mm-dd.log
- <%INSTPATH%>\logs\eventmgr.yyyy-mm-dd.log
- <%INSTPATH%>\logs\webserver.yyyy-mm-dd.log

*yyyy-mm-dd* represents the date on the web server. For example, localhost\_access\_log.2018-1 0-31.txt is an access log for Web Console on October 31, 2018.

## Setting example

The following is an example of a batch file to delete log files that are 30 days or older.

```
@echo off
set IMS_LOG="C:\Program Files\NEC\IMS\log"
set TOMCAT_LOG="C:\Program Files\NEC\IMS\tomcat\logs"
set OLDER_DAY=30
set FILE_NOT_FOUND=0
forfiles /p %TOMCAT_LOG% /m localhost_access_log.*.txt /s /d -%OLDER_DAY%
/c "cmd /c del @file"
forfiles /p %IMS_LOG% /m artemis.*.log /s /d -%OLDER_DAY% /c "cmd /c
del @file"
forfiles /p %IMS_LOG% /m eventmgr.*.log /s /d -%OLDER_DAY% /c "cmd /c
del @file"
forfiles /p %IMS_LOG% /m webserver.*.log /s /d -%OLDER_DAY% /c "cmd /c
del @file"
```

By running the above batch file periodically once a day by using the task scheduler, it is possible to keep the number of log files constant. For details about the task scheduler settings, see the Windows help.

## 2.9.3 Changing the antivirus software settings

If the IMS component and antivirus software are installed in the same server, it is necessary to review the antivirus software settings so that the antivirus software does not affect operations of the IMS component.

When the IMS component operates, it reads or writes files to or from the directories specified as the install path and data path. In addition, this component connects and communicates with the MasterScope network management products deployed outside the server.

If the coexisting antivirus software inhibits either of the above operations, Web Console cannot operate properly. Be sure to check the specifications of the coexisting antivirus software and review the settings so that the antivirus software does not inhibit operations of the IMS component.

# 2.10 Configuring the services to support a cluster

Register the IMS component services as the service resource of EXPRESSCLUSTER X. This enables the services to be controlled properly when switching between the active server and standby server.

The specific steps to configure the settings to control the starting and stopping of the services are shown below.

1. Register the service resources.

Register the following IMS component services as the service resources of EXPRESSCLUSTER X.

- MasterScope IMS System Database
- MasterScope IMS Key Store
- MasterScope IMS Message Queue
- MasterScope IMS Event Manager
- MasterScope IMS Web Server

#### A Caution

- Stop any services that have already started.
- On both the active and standby servers, set **Startup Type** of each service to **Manual** so that the IMS component services do not start automatically at OS startup, at a timing unintended by EXPRESSCLUSTER X.
- 2. Add the registered component services to the script resource.

To make sure that the internally used database starts, if the following file exists before the IMS component services start, add the process to delete the file.

• <%DATAPATH%>\db\systemdb\dbms1\data\postmaster.pid

The following is a setting example of the script resource startup script (start.bat) to delete the above file. For details about the script resource, refer to the EXPRESSCLUSTER X documentation.

File deletion setting example

```
set IMS_DATA_PATH=X:\share\MasterScope\IMS
rem normal startup processing
* * * * * * * * * * * * *
:NORMAL
rem diskcheck
IF "%CLP DISK%" == "FAILURE" GOTO ERROR DISK
del %IMS DATA PATH%\db\systemdb\dbms1\data\postmaster.pid 2>NUL
(Omitted)
rem failover processing
:FAILOVER
rem diskcheck
IF "%CLP DISK%" == "FAILURE" GOTO ERROR DISK
del %IMS DATA PATH%\db\systemdb\dbms1\data\postmaster.pid 2>NUL
(Omitted)
```

3. Set the dependencies among the resources.

Set the dependencies among the registered resources so that the IMS component services start and stop in the correct order.

Configure the settings so that all the dependency conditions among the resources are satisfied. Clear the **Follow the default dependence** check box of the dependency setting of each service and add the resource on which the service depends.

Resource name	Dependent resource
Script resource	Floating IP resource
	Shared disk resource
MasterScope IMS System Database	Script resource
MasterScope IMS Key Store	Script resource
MasterScope IMS Message Queue	Script resource
MasterScope IMS Event Manager	MasterScope IMS System Database
	MasterScope IMS Message Queue
MasterScope IMS Web Server	MasterScope IMS System Database
	MasterScope IMS Key Store
	MasterScope IMS Message Queue

Table 2-14 Resource dependencies

# 2.11 Checking the switching between the active server and standby server

Start the cluster of the IMS component and confirm that active and standby servers can switch between each other properly.

The specific setting steps are shown below.

#### Тір

Before starting the cluster, stop all of the IMS component services.

1. Start the cluster.

Start the cluster of the IMS component on the operation window of EXPRESSCLUSTER X.

After the cluster starts, the IMS component services start on the active server.

2. Switch between the active server and standby server.

Switch between the active server and standby server by operating EXPRESSCLUSTER X.

The IMS component services start on the standby server. Then, that server operates as the active server.

Switch between the active server and standby server by using EXPRESSCLUSTER X and confirm that the IMS component services run on both servers properly.

### 2.12 Setting up the products to be connected

To connect the IMS component to the MasterScope products, the connection settings need to be configured not only for the IMS component but also for the products.

The connection settings on the product side connected to the IMS comportent varies depending on each product. Refer the description of each product.

### 2.12.1 Configure the connection setting for Network Manager

This section describes the settings to be configured on the Network Manager side in order to connect the IMS component and Network Manager.

The configuration is performed after the setup of Network Manager. For details of the Network Manager setup procedure, refer to *"Setup Guide"* of Network Manager.

On the Network Manager side, configure the following settings.

- Edit the configuration file (NvPROIms.ini).
- Enable WebAPI.

### Edit the configuration file

There is the configuration file (NvPROIms.ini) in Network Manager. Edit this configuration file and save it.

Configuration file path

On Network Manager, <%DATAPATH%>\Manager\sg\NvPRO\NvPROIms.ini

Format

```
[NOMS]
InstanceID=<manager id>
MessageQueueIP=<ims ip address>
MessageQueuePort=<port number>
[EVENT]
sendEvent=<1|0>
[SnmpDataDb]
ShiftTimeZone=<timezone offset>
```

#### <manager id>

Specify the ID of connecting Network Manager for identification on the IMS component. Use **manager id** parameter prepared in "Parameters necessary to configure the settings to connect the products (page 12)".

```
The default value is "1".
```

This parameter must match the value in the IMS component configuration file (imsconf.ini). See also "2.5 Configuring to connect the products (page 18)".

#### <ims ip address>

Specify the IPv4 address of the server where the IMS component is installed. Use **ims ip address** parameter prepared in "Parameters necessary to configure the settings to connect the products (page 12)".

```
The default value is "127.0.0.1".
```

#### <port number>

Specify the port number used for the communication with the Message Queue of the IMS component.

The default value is "28110".

This parameter must be changed when the port number is changed from default in "2.7 Changing the communication port number from default value (page 26)".

<1|0>

Specify whether to send alert information detected in Network Manager to the IMS component.

- 1 : enables sending alert information. Basically, specify "1".
- 0 : enables sending alert information.

The default value is "1".

#### timezone offset

Specify the time difference from UTC (Coordinated Universal Time) in the form "(+|-) *HHMM*". For example, specify "+0900" in Japan.

Example:

```
InstanceID=nvpro01
MessageQueueIP=192.168.1.200
MessageQueuePort=28110
[EVENT]
sendEvent=1
[SnmpDataDb]
ShiftTimeZone=+0900
```

#### Tip

You do not need to change the following parameters in NvPROIms.ini.

[SnmpDataDb] Port=28100

Port

Port number used in Performance Database. Normally, you do not need to change it.

### 🕂 Caution

To reflect changes made to the configuration file (NvPROIms.ini), restart all the Network Manager services.

### Enable WebAPI

Enable the Network Manager WebAPI in order that the IMS component can use the Network Manager WebAPI.

To enable it, perform the following procedure on the monitoring terminal of Network Manager.

- Change to the configuration mode.
   In the main menu, select Setting>Configuration Mode.
- 2. Open the Option Setting dialog box.

In the main menu, select **Setting>Option**.

The Option Setting dialog box is displayed.

- 3. Click the **Web Monitoring View** tab.
- 4. Enable the WebAPI function.

Check the **Use Web API Function** check box.

5. Change the parameters for the WebAPI.

To change from the default, specify the same value as specified in the configuration file (imsconf.ini) of the IMS component. See also "2.5 Configuring to connect the products (page 18)".

• Port

Specify the port number for the WebAPI function.

- Use HTTPS cryptogram check box
  - On : uses HTTPS.
  - Off : uses HTTP, not HTTPS.
- 6. Click the **OK** button to save changes.

### 2.12.2 Configure the connection setting for NFA

This section describes the settings to be configured on the NFA side in order to connect the IMS component and NFA.

The configuration is performed after the setup of NFA. For details of the NFA setup procedure, refer to *"Startup Guide"* of NFA.

On the NFA side, configure the following settings.

- Connection settings between the IMS component and NFA.
- Settings for single sign-on access to the web console of the NFA from Web Console provided by the IMS component.

Edit the following configuration file (controller.properties) on the NFA.

#### **Configuration file path**

```
On NFA, <%DATAPATH%>/controller/conf/controller.properties
```

#### 🛕 Caution

- If the configuration file (controller.properties) does not exist, create a new one.
- To reflect changes made to the configuration file (controller.properties), restart the NFA services.

### Format of connection setting

Edit the following parameters in the configuration file (controller.properties) and save it.

```
ims.application-instance-id = <manager id>
ims.msgqueue.host = <ims ip address>
ims.msgqueue.port = <port number>
```

#### <manager id>

Specify the ID of connecting NFA for identification on the IMS component. Use **manager id** parameter prepared in "Parameters necessary to configure the settings to connect the products (page 12)".

There is no default value.

This parameter must match the value in the IMS component configuration file (ims-conf.ini). See also "2.5 Configuring to connect the products (page 18)".

#### <ims ip address>

Specify the IPv4 address of the server where the IMS component is installed. Use **ims ip address** parameter prepared in "Parameters necessary to configure the settings to connect the products (page 12)".

The default value is "127.0.0.1".

#### <port number>

Specify the port number used for the communication with the Message Queue of the IMS component.

```
The default value is "28110".
```

This parameter must be changed when the port number is changed from default in "2.7 Changing the communication port number from default value (page 26)".

Example:

```
ims.application-instance-id = nfa01
ims.msgqueue.host = 192.168.1.200
ims.msgqueue.port = 28110
```

### Format of single sign-on access setting

Edit the following parameters in the configuration file (controller.properties) and save it.

```
ims.webserver.base-url = <base url>
ims.sso.enabled = <true|false>
```

#### <base url>

Specify the URL to access the Web Console of the IMS. Use **ims web url** parameter prepared in "Parameters necessary to configure the connection settings for NFA (page 13)"

The default value is "http://localhost".

### A Caution

This URL must be accessible from the browser and the NFA server.

#### <true|false>

Specify whether single sign-on access is enabled or not.

- true : enables single sign-on access.
- false : disables single sign-on access.

The default value is "false". Specify "true" when connecting to the IMS component.

#### Example:

```
ims.webserver.base-url = http://ims-cluster.nec.com
ims.sso.enabled = true
```

## Chapter 3. Post-Installation Environment Settings

This chapter describes how to configure the environment before using and operating the Web Console.

### Contents

3.1	Preparations for Using Web Console	38
3.2	Accessing Web Console	40
3.3	Registering users	41
3.4	Synchronizing the configuration information	44
3.5	Confirming the managed node information	44
3.6	Checking the network map configuration	45

### 3.1 Preparations for Using Web Console

This section describes preparations for using the Web Console.

Before using the Web Console, configure your web browser. This only needs to be configured once.

### 3.1.1 Checking the web browser security settings

This section describes the web browser security settings required to use the Web Console.

JavaScript and Cookies must be enabled for the web browser to access the Web Console.

JavaScript and Cookies are enabled by default for supported browsers. Therefore, it is not necessary to specify a particular setting. If you have changed the security settings, check whether the changed settings are appropriate to use the Web Console.

For Windows Server, if **Enhanced Security Configuration** is set to *"Enabled"*, the setting described in "Configuring settings on a Windows Server OS (page 39)" is required.

### **Checking the Internet Explorer settings**

Check the Internet Explorer settings on the Internet Options dialog box. Press the Alt+T key on the Internet Explorer window, and then select **Internet Options** from the displayed menu. For details about the setting on each tab, refer to the help of Internet Explorer.

- Security tab
  - Registering the URL to "Trusted sites"

Register the URL of the server where the IMS component is installed to "Trusted sites".

#### Тір

If you do not want to register the URL to "*Trusted sites*", configure the setting so that the server where the IMS component is installed is classified into other than the "*Restricted sites*".

- Enabling JavaScript

Confirm that Active scripting is set to "Enable" on Custom Level of "Trusted sites".

Privacy tab

If the server where the IMS component is installed is the "Internet" zone, confirm that Cookies are allowed.

#### Тір

- If the server where the IMS component is installed is the *"Trusted sites"* or *"Local Intranet"* zone, Cookies are not blocked.
- If the server where the IMS component is installed is in the *"Restricted sites"* zone, Cookies are always blocked and the Web Console cannot be used.

### **Checking the Mozilla Firefox settings**

Check the settings on the Options page of Mozilla Firefox. For details about the settings, refer to the help of Mozilla Firefox.

#### • Privacy & Security panel

Confirm that the **History** setting is configured to keep Cookies from the visited websites.

### Checking the Google Chrome settings

Check the settings on the Settings page of Google Chrome. Click **Advanced** at the bottom of the page, and then click the **Content settings** button under **Privacy and security**. You can check the settings on the displayed Content settings dialog box. For details about the settings, refer to the help of Google Chrome.

Cookie

Confirm that the setting is configured to keep Cookies.

JavaScript

Confirm that JavaScript is permitted.

### **Configuring settings on a Windows Server OS**

If **Enhanced Security Configuration** is set to *"Enabled"*, add *"about:blank"* to *"Trusted sites"* on the Internet Options dialog box.

## 3.1.2 Importing the SSL server certificate into the web browser

The SSL server certificate required to be imported to the web browser to access the Web Console via HTTPS.

If you select a self-signed type SSL server certificate, you can access the Web Console safely by importing the certificate into the web browser.

#### Тір

Even for a certificate issued by a certificate authority, some certificate authorities may instruct you to import a root certificate to the web browser. In this case, follow the instructions of the certificate authority.

### 🕂 Caution

If you use Internet Explorer without importing the certificate and if the warning continues to be displayed, aberrant behavior might occur such as a page being unable to be displayed or operations being unable to be performed on the web browser. It is therefore strongly recommended to import a certificate when using a web browser.

- For Internet Explorer and Google Chrome, perform the following procedure.
  - 1. Place the certificate (.cer file) output by the export cert command of "A.1 ims-ssl-keytool (page 67)" on the terminal where the Web browser operates.
  - 2. Double-click the certificate file.
  - 3. On the displayed Certificate dialog box, click the **Install Certificate** button.

Certificate Import Wizard is displayed. Click the Next button.

- 4. Select **Place all certificates in the following store** and then click the **Browse** button.
- 5. On the Select Certificate Store dialog box, select *"Trusted Root Certification Authorities"*, and then click the **OK** button.
- 6. Click the **Next** button.
- 7. Click the **Finish** button.

8. Although Security Warning is displayed because of a self-signed certificate, click the **Yes** button.

When the dialog message "The import was successful." is displayed, the certificate is successfully imported.

- For Mozilla Firefox, perform the following procedure.
  - 1. Access the following URL by using the web browser.

https://<domain name (FQDN) of IMS sever>/ims/

Tip

It is necessary to be able to resolve the domain name (FQDN) of the IMS server specified for the URL.

The warning is displayed indicating that it is not a secure connection.

- 2. Click the **Advanced** button, and then click the displayed **Add Exception** button.
- 3. On the Add Security Exception dialog box, confirm that **Permanently store this exception** is selected, and then click the **Confirm Security Exception** button.

#### A Caution

When adding a security exception, be sure to check that the contents of the certificate to be added are correct in advance.

The certificate is successfully imported if the login page is displayed.

### 3.2 Accessing Web Console.

This section describes how to access the Web Console from a web browser.

Configure the web browser according to "3.1 Preparations for Using Web Console (page 38)" in advance.

Perform the following procedure to access the Web Console.

- 1. Specify the URL of Web Console on a web browser.
  - URL for HTTP communication

http://<domain name (FQDN) of IMS sever>/

URL for HTTPS communication

https://<domain name (FQDN) of IMS sever>/

<domain name (FQDN) of IMS sever> must be the same as the name specified when creating an SSL server certificate. Otherwise, the certificate is regarded as invalid and a warning is displayed.

#### Тір

- To access Web Console, it is necessary to be able to resolve the <domain name (FQDN) of the IMS server> specified for the URL.
- If you changed the communication port number for accessing the Web Console, add the changed port number to the above URL and specify it.

For example: http://webconsole.co.jp:8080/

When access to the Web Console is successful, the login page is displayed.

2. Enter the user name and password to log in to the Web Console.

The initial user name and password are "admin" and "password", respectively.

When login to the Web Console is successful, the Dashboard page that is individually set to each user is displayed.

### 🕂 Caution

- The following are cautions on logging in to the Web Console and operations.
  - After the initial login, be sure to change the password of the admin user.

To change the password, click on in the upper right of the page and display the Profile Edit page from **Profile Edit** menu.

- If it detects more than five login failures in 30 minutes, the user is locked and can not log in for 30 minutes.

If you want to immediately release the locked state, you can unlock it by the user belonging the group who has the role of Account Manager.

- It is possible to operate (add, change, delete, etc.) the setting information from multiple Web Console instances at the same time. However, in the case of operate on the same page, in order to maintain consistency of data, the operation performed later may be made to fail.
- The following are cautions when enabling single sign-on behavior to the Web Console of the connected products.
  - Users with the same name must be registered with the IMS component and the connected products. Single sign-on works only for users with the same name.
  - With the IMS component stopped, you may not be able to access the Web Console of the connected product. In this case, specify the URL to access the login page of the connected product directly, and access the Web Console.

### 3.3 Registering users

Users who will access and use Web Console must be registered.

The following provides a summary of user management and how to register users.

### 3.3.1 Groups and users

This section describes the relationship between and operation authorities of groups and users in user management.

Users who operate the Web Console must belong to a group. The users can operate the Web Console within the scope of the role assigned to that group. The operation range of users can be managed by creating multiple groups that have different roles and assigning users to an appropriate group.

There are the following three roles to be assigned to groups.

- Administrator
- Operator
- Observer

Details about each role and authority are as follows:

### Administrator

It has the role for all operations and management using the Web Console. And it has the authority of reference, operation, and definition on all pages.

In addition, it is possible to be assigned **Account Manager** role. When **Account Manager** is assigned, it is possible to perform operations for group and user management.

### Operator

It has the role of performing network monitoring operation using the Web Console. And it has the authority of reference and operation on each page.

Тір

The "operation" in the above description means execution of processes on each page. For example, event checking and recovery processing can be executed.

### Observer

It has the role of observing the status of the network using the Web Console. And it only has the authority of reference on each page.

### 3.3.2 Adding a group

The following describes how to add a new group.

The specific procedure is described below using an example of how to add a group named *"Operations team"* as a group for members in charge of operational practices.

1. Display the Groups page.

### Click Account Management>Groups.

2. Click the **NEW GROUP** button.

The New Group page is displayed.

- 3. On the New Group page, specify the following appropriately.
  - Group Name

Specify a unique group name. Up to 128 characters are available. It is impossible to specify a duplicate name as an existing group name.

In this example, "Operations team" is specified.

Description

Specify the description of the group. Up to 512 characters are available.

In this example, "Group including members in charge of operational practices" is specified.

Role

Select one of the following role to be assigned to the group.

- Administrator
- Operator
- Observer

For details about the roles, refer to "3.3.1 Groups and users (page 41)". In this example, " **Operator** " is selected.

#### Tip

When **Administrator** is selected, it is possible to select whether to assign **Account Manager**.

4. Save the group information.

Confirm the settings and then click the **SAVE** button.

The group is newly added with the specified contents.

On the Groups page, check that "Operations team" has been added as a group.

### 3.3.3 Adding a user

The following describes how to add a new user.

The specific procedure is described below using an example of how to add "*tyamada*" to "*Operations team*".

1. Display the Users page.

### Click Account Management>Users.

2. Click the **NEW USER** button.

The New User page is displayed.

- 3. On the New User page, specify the following appropriately.
  - User Name

Specify a unique user name by using single-byte alphanumeric characters. Up to 64 characters are available. It is impossible to specify a duplicate name as an existing user name.

In this example, "tyamada" is specified.

#### Display Name

Specify a user name to be displayed on the page. Up to 128 characters are available.

If this is omitted, the name specified for **User Name** is used as the display name.

In this example, "Taro Yamada" is specified.

#### Password

Specify the initial password of the user to be registered. The password must be specified at least 8 characters and consisted of a combination of single-byte alphanumeric characters and the symbol "!"#\$%&'()\*+,./:;<=>?@/\]/^ `{|}~-".

#### Password (Confirm)

Specify the same password as specified by **Password**.

Group

From the created groups, select the group to which the user will belong.

In this example, "Operations team" is selected.

#### Default Dashboard

Select the definition of the first dashboard displayed after the user logs in.

#### Tip

If you have not added the definition of dashboard in advance, select from the built-in dashboards provided by the connected products.

4. Save the user information.

Confirm the settings and then click the **SAVE** button.

The user is newly added with the specified contents.

On the Users page, Check that the user "*tyamada*" belonging to the group "*Operations team*" has been added.

### 3.4 Synchronizing the configuration information

Before starting operation of Web Console, managed nodes should be registered correctly to the IMS component.

After connecting the IMS component and each product, you need to synchronize the configuration information on the Configuration Sync page of Web Console. To display the Configuration Sync

page, click System Settings>Configuration Sync menu.

#### Tip

Only users with the Administrator role can display the Configuration Sync page

Configuration Sync System Settings / Configuration Sync			
Application Name	Instance Name	Region	Actions
MasterScope Network Flow Analyzer	nfa01	DC01	φ
MasterScope Network Flow Analyzer	nfa02	DC02	\$
MasterScope Network Manager	netmgr01	DC01	0
MasterScope Network Manager	netmgr02	DC02	0

#### Figure 3-1 Configuration Sync page

In the Configuration Sync page, click the  $\bigcirc$  **Synchronize this instance** button in the list of the product instances to synchronize the configuration information.

For details, refer to "Synchronizing the configuration information" in "Reference Manual".

After synchronization, as long as the IMS and each product are connected, configuration changes on each product is automatically reflected in the IMS component.

### 3.5 Confirming the managed node information

Before starting Web Console operation, confirm that managed node information is correctly registered to the IMS component.

You can confirm node information registered to the IMS component on the Nodes page of Web Console. To display the Node page, click **ENOdes** menu.

-	IPv4 Address	is between		~	192.16	8.10.1	an	d 192.168.10.254	
-	Vendor	contains		~	NEC				
SELECT	SEARCH								
						Rows per page:	15 🗸	1-8 of 8 <	1
Severity	Node Name	IPv4 Address	Туре	Vendor		Series	Software Version	n Region	Action
Normal	H2_L2switch_09	192.168.10.192	L2 Switch	NEC Corpo	oration	QX-SB00E series	1.1.25	DC01	a
Normal	H2_L2switch_10	192.168.10.193	L2 Switch	NEC Corpo	oration	QX-S2000 series	2.4.13	DC01	a
Normal	H2_L2switch_11	192.168.10.194	L2 Switch	NEC Corpo	oration	QX-S2100 series	1.1.5	DC01	a
iormal	H2_L2switch_12	192.168.10.195	L2 Switch	NEC Corpo	oration	QX-S2100 series	1.1.7	DC01	a
iormal	H2_L3switch_10	192.168.10.197	L3 Switch	NEC Corpo	oration	QX-S6600 series	7.1.3	DC01	a
iormal	H3_L2switch_14	192.168.10.249	L3 Switch	NEC Corpo	oration	QX-S6600 series	7.1.3	DC01	a
iormal	H3_L2switch_15	192.168.10.250	L3 Switch	NEC Corpo	oration	QX-S6600 series	7.1.3	DC01	a
vormal	H5_L3switch_09	192.168.10.196	L3 Switch	NEC Corpo	oration	QX-S6600 series	7.1.3	DC01	a

Figure 3-2 Nodes page

If you have changed the configuration information on each product while stopping the IMS component, those changes are not reflected to the IMS component. In this case, you need to perform synchronizing the configuration information again.

For details about the configuration information synchronization, refer to "Synchronizing the configuration information" in "Reference Manual".

#### Тір

When multiple products are registered in one region, it is automatically determined whether the nodes managed by each product are physically the same node.

For details on how to determine the same node, refer to "Mapping node information" in "Reference Manual".

### 3.6 Checking the network map configuration

Before using Web Console, it is necessary to check that the network map is properly configured. Edit the configuration as necessary.

Web Console incorporates the following configuration information registered to Network Manager Map View and creates network map data for Web Console.

- Network configuration (Layered structure of the map)
- Node information
- Connections among nodes

Web Console displays a network map on the Topology Map page using this information.

Tip

When the IMS component connects to Network Manager, the IMS component incorporates the above information automatically and creates network map data for Web Console.

Since information from Network Manager other than the above is not incorporated in Web Console, graphics and background images placed on each Network Manager Map View are not reflected in the Topology Map page of Web Console. Edit the network map displayed on the Topology Map page on Web Console to insert graphics and background images to the network map or to change the position of the icon indicating a node.

When editing a network map, change the mode of the Topology Map page from **View mode** to **Edit mode**.

#### Тір

- The Topology Map page is displayed only when Network Manager is used. Therefore, if you do not use Network Manager, skip this step.
- If the node icon positions located on a network map are not determined by editing the network map configuration as described above, Web Console calculates the proper icon positions automatically when displaying them. Therefore, if a new node icon is registered for Network Manager, each icon may be displayed in a place different from the previous one.

## Chapter 4. Basic Operations

This chapter describes the basic operations of the Web Console.

### Contents

4.1	Structure of Web Console	48
4.2	Updating own user information	50
4.3	Checking the newly occurred events	51
4.4	Widget types	52
4.5	Widget display contents	55
4.6	Basic operation of widgets	56
4.7	Operations of specific widgets	60

### 4.1 Structure of Web Console

This section describes the structure of the Web Console.

The Web Console consists of four areas described in "Figure 4-1 Structure of Web Console (page 48)".

=	MasterScope		Header area		۵	<b>±</b> Ø
	Dashboard					
a	Topology Map					
≡	Nodes					
¢	Events					
₽	Event Action Settings					
*	Account Management		Contents area			
٥	System Settings					
	Menu area					
		MasterScope Integrat	Footer area	Corporation		

Figure 4-1 Structure of Web Console

### Header area

Displays the logged-in user name, the state of new notifications and the like.

• 🔳 icon

Maximize or minimize the width of the menu area.

### Notifications icon

Displays the status of new events and messages that occurred after logging in to the Web Console.

The displayed number indicates the number of new events or messages.

Tip

A message is a notice such as an error on the operation or processing of the Web Console.

### icon

Clicking this icon displays the following.

- User name

Displays the logged-in user name (Display Name).

- Edit Profile menu

Displays the Edit Profile page. The Edit Profile page allows users to change their own user information such as **Password** for login.

#### Tip

After the initial login, be sure to change the password.

- Logout menu

Logs out from the Web Console.

• **OHelp** icon

Displays the help of the Web Console.

### Menu area

Displays the menus of the functions that can be operated on the Web Console.

### 🛕 Caution

The menu contents to be displayed vary depending on the role of the logged-in user or the products constructing the system.

### Bashboard menu

Displays the Dashboard page. You can check the current network status.

• **I**Topology Map menu (displayed when using the Network Manager)

Displays the Topology Map page. You can check the network topology configuration.

### • ENodes menu

Displays the Nodes page. You can check the information on all the managed nodes.

#### Events menu

Displays the Events page. You can check the information on the event that occurred.

### Event Action Settings menu

Clicking this menu displays the sub menu related to the event action (notification).

#### Tip

Only users belonging to a group with Administrator role can display and select menus.

#### - Event Actions menu

Displays the Event Actions page. You can configure the notification processing triggered by event occurrence.

#### - Email Servers menu

Displays the Email Servers page. You can configure the server settings for the Email notification.

#### - Action Logs menu

Displays the Action Logs page. You can check the execution log of the Event Action.

### • Account Management menu

Clicking this menu displays the sub menu related to the account management of Web Console.

Tip

Only users belonging to a group with Account Manager role can display and select menus.

- Users menu

Displays the Users page. You can manage the user information.

- Groups menu

Displays the Groups page. You can manage groups that define user roles.

### System Settings menu

Clicking this menu displays the sub menu related to the system settings.

#### Тір

Only users belonging to a group with Administrator role can display and select menus.

#### - Node Mappings menu

Displays the Node Mappings page. It determines and manages whether the nodes managed by multiple products are physically identical or not.

#### - Configuration Sync menu

Displays the Configuration Sync page. Synchronize configuration information between IMS component and the connected products.

### Contents area

Displays the operation page corresponding to the selected menu.

### Footer area

Displays the version and copyright information of the IMS component.

### 4.2 Updating own user information

This section describes the procedure to be used by the user logged in to Web Console to update own user information including the login password.

### Тір

User Name and Group cannot be changed.

1. Display the Edit Profile page.

Click click

2. Change own user information on the Edit Profile page.

On the Edit Profile page, you can change the two settings of display information and password in the Web Console.

- Display information
  - Display Name

Specify the display user name on the page with arbitrary characters. The maximum number of characters is 128 characters.

If omitted, also use the name specified by the **User Name** as the display name.

- Default Dashboard

By checking the check box in the list, select the definition of the first dashboard displayed after the user logs in.

#### Тір

If you have not added the definition of dashboard in advance, select from the built-in dashboards provided by the connected products.

• Password

#### - Password (Old)

Specify the current password.

#### - Password

Specify a new password. The password must be specified at least 8 characters and consisted of a combination of single-byte alphanumeric characters and the symbol  $"!"#\$\%\&'()*+,./:;<=>?@/\]^^ `{|}~-".$ 

#### - Password (Confirm)

For confirmation of input, specify the same password as specified by **Password**.

3. Save the changes.

Confirm the changes and then click the **SAVE** button corresponding to the changes.

A message indicating that the user information has been updated with the specified content is displayed.

### 4.3 Checking the newly occurred events

In the Web Console, even if you are viewing a page other than the Dashboard and Events pages, you can grasp whether there is a newly occurred event.

The following describes how to grasp a newly occurred event and confirm its contents.

1. Check whether there is a new notification.

Check the state of the **ANOTIFICATIONS** icon at the upper right of the page.

The displayed number indicates the number of events or messages that have newly occurred.

Тір

A message is a notice such as an error on the operation or processing of the Web Console.

2. Click the **Provide Click** the **Provide Click** the **Click** the

The Notification list is displayed.

3. Check whether there is an event.

If an event has occurred, a notification indicating the occurrence of the event is displayed in the Notification list. Also, in addition, the occurrence time and severity information for the

events are displayed. From the notified severity information, you can grasp the urgency of the event.

4. Confirm the details of the event.

To confirm the details of the event, click on the **Events** menu to display the Events page.Confirm the details of the event by comparing the event occurrence time with the display information on the Events page.

5. Delete the event whose contents have been confirmed from the list of notifications.

By clicking the  $\times$  icon for the notification in the Notification list, you can delete the notification from the list. By clicking the **\equiv Clear all notifications** icon in the Notification list, you can delete all notifications in the Notification list.

Tip

- Up to 10 notifications will be made on the Notification list. If it exceeds 10, the oldest notification is deleted.
- If two or more events with the same severity occur at the same time, they are notified in one form.

### 4.4 Widget types

On the pages such as the Dashboard and Node Detail pages, various information, including the data traffic status, load of each node, and event occurrence status, is displayed in a chart or list by using the component called a widget. This section explains the widget types that are displayed on the Web Console.

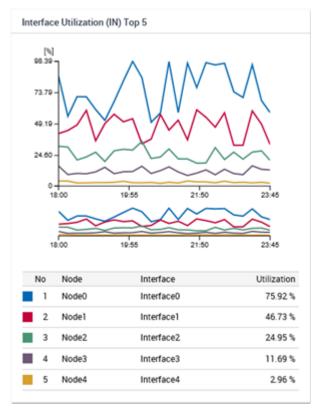
The supported widgets are roughly classified into the following four types depending on the contents to display.

### Line chart widgets

The temporal transition of the values of the target items within the specified period is displayed in a line chart. The ranks of the items within the specified period are displayed in a list.

For example, on the **Interface Utilization (IN) Top5** widget, the change in the utilization (%) of the top five network interfaces with high input utilization (%) is displayed in a line chart. In the list, the top five of the average utilization for network interfaces within the specified period is displayed in descending order.

"Figure 4-2 Line chart widget (page 53)" shows a sample line chart widget.





The following display operations can be performed on the line chart widget.

• Zooming in on a line chart by using the Range Selector

You can zoom in a line chart by narrowing down the time width with the **Range Selector** between the line chart and the list.

• Narrowing the display items by using the filtering settings

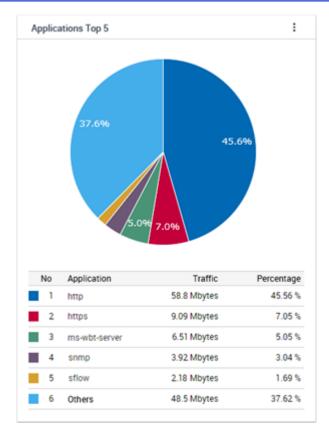
You can narrow down the display items of the chart by clicking the mark showing the chart color to be placed on the left side of each item in the list.

### **Pie chart widgets**

The proportion of the values of the target items within the specified period is displayed in a pie chart. Also, the ranks of the items within the specified period are displayed in the list.

For example, on the **Applications Top5** widget, among the flow information collected on the specified network interface, the traffic volume proportion of the top five applications with high traffic volume and other applications is displayed in a pie chart. In the list, the top five traffic volumes for network interfaces within the specified period are displayed in descending order.

"Figure 4-3 Pie chart widget (page 54)" shows a sample pie chart widget.





The following display operations can be performed on the pie chart widget.

• Switching to the line chart

By clicking the icon on the widget and operating, you can switch the display from a pie chart to a line chart, or from a line chart to a pie chart.

• Narrowing the display items by using the filtering settings

You can display the pie chart excluding specific items by clicking the mark showing the chart color to be placed on the left side of each item in the list.

#### Tip

The above operations may not be performed for some target items. For example, on the **Ratio of Node Status** widget, the above two operations cannot be performed.

### List widgets

Event information, node availabilities, etc. are displayed in a list.

For example, on the **Current Alert** widget, a list of fault events that have not yet been recovered is displayed.

"Figure 4-4 List widget (page 55)" shows a sample list widget.

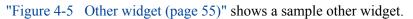
Current Alert						
Severity	Summary	Occurrence Time -	Source	Source Region	Assigned To	Actions
Warning	linkDown	2019-01-25 07:47:27	K2_L2switch_03	DC01		V D I
Warning	linkDown	2019-01-25 07:46:36	K2_L2switch_03	DC01		⊽ <b>Ø</b> I
Fatal	Communication failure	2019-01-25 07:41:33	H4_DBSrv_02	DC01		v a i
					1-3 of 3	< 1 →

Figure 4-4 List widget

### Other widgets

Depending on the features of individual pages, special types of widgets may be displayed.

On the Node Detail page, the **Operational Status** widget for the node that Network Manager is monitoring is displayed. This **Operational Status** widget displays a donut chart showing the availability of the node and a chart showing the change of the node status (severity) for time transition.



Timeline						
			Normal			
50	07:00	07:10	07:20	07:30	07:40	0
	50	50 07:00	50 07:00 07:10			

Figure 4-5 Other widget

### 4.5 Widget display contents

This section describes the information range that can be displayed on each widget and the behavior of the widget for various parameters of the page.

### Range of the data to be aggregated for one widget

For the widgets displayed on the Dashboard page, the data is aggregated each region group and displayed in ranking (Top N). It does not display the ranking by aggregating the data of multiple region groups.

#### Тір

The following three widgets related to the occurrence status of fault events are exceptionally able to display data of all nodes that span multiple region groups in one widget.

- Current Alert widget
- Ratio of Node Status widget
- Node Availabilities widget

The Node Detail page displays data for the range of one selected node and the Network Interface Detail page displays data for the range of one selected network interface.

### Specification of Period

For each page displaying the widget, specify the data range in **Period**. The granularity of data to be displayed varies depending on the time width of the specified period or the specified past time.

### Тір

The following widgets always display the current status regardless of the specified value of **Period**.

• Ratio of Node Status widget

### Specification of Top N (rank)

For each page displaying the widget, specify the data range with **Top N**. The specified number of the data is displayed in ascending or descending rank order (Top N) of the values within the specified period. In Web Console, data up to Top 20 can be displayed.

### Tip

The following widgets display regardless of the specified value of  $\ensuremath{\text{Top N}}$  .

- Events widget
- Current Alert widget
- Ratio of Node Status widget

### 4.6 Basic operation of widgets

Clicking the link of listed items on each widget displays the page to check the details of the clicked item. Furthermore, each widget provides a mechanism to check the details of the displayed contents.

The following sections describes the basic operations of widgets.

### 4.6.1 Checking the details of the node

From the link of the node name displayed by the widget, you can easily display the Node Detail page for the node.

If the Node Detail page is displayed from a widget, **Period** specified on the previous page is kept.

#### Tip

On all pages including widgets, when clicking the node name link indicating the managed node, the Node Detail page for the node is displayed.

The specific procedure is described below using an example to display the Node Detail page from the **Node Availabilities** widget displayed on the Dashboard page.

1. Display the Dashboard page.

Click **Dashboard** menu.

2. Specify **Period** on the Dashboard page.

In this description, select **Past 24 hours** from the pull-down menu.

3. Check the contents of the Node Availabilities widget.

Search for the nodes with low availability in the past 24 hours.

4. Select the node whose details you want to check.

Click the node name link displayed on the Node Availabilities widget.

The Node Detail page for the node is displayed by specifying **Past 24 hours** for **Period**.

 Identify the cause of low availability by referring to Events widget on the Node Detail page. The availability decreases if an event whose severity is Fatal occurs.

### 4.6.2 Checking the details of the network interface

From the link of the network interface name displayed by the widget, you can easily display the Network Interface Detail page for the network interface.

If the Network Interface Detail page is displayed from a widget, **Period** specified on the previous page is kept.

#### Tip

On all pages including widgets, when clicking the link of the network interface name, the Network Interface Detail page for the network interface is displayed.

The specific procedure is described below using an example to display the Network Interface Detail page from the **Interface Utilization (IN)** widget displayed on the Dashboard page.

1. Display the Dashboard page.

Click **Dashboard** menu.

2. Specify **Period** on the Dashboard page.

In this description, select **Past 24 hours** from the pull-down menu.

3. Check the contents of the Interface Utilization (IN) widget.

Search for network interfaces with high input utilization in the past 24 hours.

4. Select the network interface whose details you want to check.

Click the link of the network interface name displayed on the **Interface Utilization (IN)** widget.

The Network Interface Detail page for the network interface is displayed by specifying **Past 24 hours** for **Period**.

5. Identify the cause of high utilization by referring to **Flow Data** on the Network Interface Detail page.

It is possible to identify the cause of an increase in the utilization from the information of the **Applications** and **Conversations** widgets.

If you want to investigate the communication traffic in more detail, click the **FLOW ANALYZE** button to access to Web Console of the NFA.

### 4.6.3 Checking the details of the flow information

The Exporter Analysis page of the NFA can be displayed easily by clicking the link of the flow information displayed in the widget, such as the IP address of the endpoint or the application name.

If the Exporter Analysis page of the NFA is displayed from a widget, **Period** specified on the previous page is kept. In addition, the contents of the clicked item and the like are automatically set to **Filter Conditions** when Exporter Analysis page is displayed.

The specific procedure is described below using an example to display the Exporter Analysis page of the NFA from the **Applications** widget displayed on the Node Detail page.

1. Display the Node Detail page.

Click **Nodes** menu. On the displayed Nodes page, click the node name link of the node for which you want to check the details.

2. Specify **Period** on the Node Detail page.

In this description, select **Past 24 hours** from the pull-down menu.

3. Check the contents of the **Application** widget.

Check the applications with high communication traffic in the past 24 hours.

4. Select the application for which you want to check the details.

Click the link of the application name displayed on the **Applications** widget.

In this case, Exporter Analysis page of the NFA is displayed by specifying the node in **Target Exporter** and the application in **Filter Conditions**. and **Period** is specified as **Past 24** hours.

5. Identify the cause of high communication traffic by referring to each widget of the Exporter Analysis page.

It is possible to identify the cause of an increase in the communication traffic from the information such as the **Conversations** widget.

### 4.6.4 Filtering the items displayed on a chart

For line chart and pie chart widgets, the filtering function allows you to exclude some of the items currently being displayed from the display targets.

Filtering is useful if you want to make a chart more visible by temporarily hiding some items so that you can focus on the desired items.

For example, if you want to compare the 10th to 20th items of the Top 20, you can make a chart more visible by excluding the 1st to 9th items. The specific steps are shown below.

#### Тір

When operating the following, it is recommended to specify **Nothing** for **Update interval** of the displayed page. Updating the displayed page resets the filter settings described later.

1. On the target widget, set the filtering of display items.

It is possible to be excluded the display items of the chart by clicking the mark showing the chart color to be placed on the left side of each item in the list on the widget.

2. Check that the selected item has been excluded on the chart.

If you want to exclude multiple items, repeat the above steps.

Click the mark of the exclusion item again to return the chart of that item to the display target.

### 4.6.5 Zooming in on a line chart

For line chart widgets, a chart can be zoomed in on by reducing the the time width of the line chart that shows the entire specified period.

To narrow down the time width from the range specified in **Period** on the display page and check the details of communication traffic, perform the following operations.

#### Tip

When operating the following, it is recommended to specify **Nothing** for **Update interval** of the displayed page. Updating the displayed page resets the setting of **Range Selector** that is described later.

1. Select the time width to display using the lower line chart (called the **Range Selector**) that shows the overall period.

Specify the display range with drag-and-drop.

The display of the upper line chart is switched to the range selected by the **Range Selector**.

2. Specify the display range in detail.

When specifying the display range in detail, perform the following operations.

- Adjust the time width by drag-and-drop the left and right border lines in the range specified by the **Range Selector**.
- Drag-and-drop the area specified by the **Range Selector**, and change the displayed area itself.
- Cancel the display range by clicking outside of the area specified by the **Range Selector** and specify a new display range by drag-and-drop.

#### Tip

It is possible to specify the display range simply by dragging the area outside the display range without canceling the display range.

The operation of the **Range Selector** is reflected only in the display of the line chart. The display content of the list does not change.

### 4.6.6 Changing the IP address display to the hostname

When the IP address of the endpoint in the flow information is displayed, it is possible to change to the display of the corresponding hostname.

To change the IP address that indicates an endpoint to the corresponding hostname, the NFA that receives flow information must be able to inquire about the hostname to the Domain Name System (DNS) that manages hostnames and IP addresses of endpoints via the network.

#### Tip

- For an endpoint that is not registered to the DNS, the IP address will be displayed as is because inquiries about hostnames will fail.
- The hostname to be displayed instead of an IP address by executing the following procedure is the hostname that is obtained from the DNS when the NFA receives the analysis target flow information, not the hostname obtained by executing this procedure. Therefore, when analyzing the past communication status, if the previous hostname at reception of the analysis target flow information differs from the current hostname, the previous hostname is displayed.

The following steps show how to change an IP address of an endpoint for flow information to a hostname.

1. Click the *i* icon of the target widget.

When clicking on the *icon*, a check box of the display items is displayed.

2. Select the check box of the **Show Hostname** 

The IP address of the endpoint changes to the hostname.

To display the IP address again, clear the **Show Hostname** check box according to the above steps.

### 4.6.7 Changing the chart type

For a pie chart widget, it is possible to change the display from a pie chart to a line chart and vice versa.

With this operation, it is possible to check both the proportion and the temporal transition for the communication traffic of each item within the specified period from the information of one widget. The specific steps are shown below.

### 🔥 Caution

The **Ratio of Node Status** widget is a pie chart widget, but it is impossible to change the chart type.

1. Click the *i* icon of the target widget.

When clicking on the *icon*, a check box of the display items is displayed.

2. Clear the check box of the **Show Pie Chart**.

The pie chart of the widget changes to a line chart. In changing the chart type in this procedure, if you move to another page or update the entire page by pressing F5 key, you will return to the default chart type.

When defining a line chart widget as the default graph type, you can change the chart type to a pie chart by checking the **Show Pie Chart** check box with the same procedure.

### 4.7 Operations of specific widgets

Some widgets provide a mechanism to display unique links and icons according to the type of widget so that widget specific operations can be performed.

This section describes specific operations that can be performed only for specific widgets.

### 4.7.1 Performing operations related to the event

For **Current Alert** and **Events** widgets, it is possible to perform specific operations on occurred events.

The following describes the details of the operation for the events.

### 4.7.1.1 Checking the details of an event

For **Current Alert** and **Events** widgets, it is possible to check the details of an event by displaying the Event Detail dialog box.

In the list of events displayed by the **Current Alert** and **Events** widgets, since it is the primary purpose to grasp the state of failure occurrence, only the summary information of the event that occurred is displayed. To check the details of a specific event, display the Event Detail dialog box.

The specific procedure is described below using an example operation of the Current Alert widget.

1. Display the Dashboard page.

Click **Dashboard** menu.

2. Check the contents of the **Current Alert** widget.

The **Current Alert** widget displays the currently occurring fault events.

3. Display the Event Detail dialog box of the event to be checked.

Click the  $\nabla$  Event Detail icon in the Actions column of the target event.

4. Check the contents of the Event Detail dialog box.

The Event Detail dialog box displays the following information.

Summary

Displays summary information of the event.

Severity

Displays the severity of the event.

Recovery Status

Displays the recovery status of the event. **Unrecovered** is displayed for currently occurring events.

Occurrence Time

Displays the occurrence time of the event.

Source

Displays the name of the node and network interface as the source of the event. Also, the IP address of the relevant node and the region group to which the node belongs are displayed.

#### **A** Caution

The value of the IP address to be notified as the source of the event is the value of the IP address managed by the product that detected the event. Therefore, depending on the environment, it may be different from the IP address value managed by the IMS component displayed on the Node Detail page of the Web Console.

Clicking the **DTopology Map** icon displays the topology map in which the node where the event occurred is placed.

#### Тір

- The **D**Topology Map icon is displayed when using the Network Manager.
- In case of the Event Detail dialog box activated from the Current Alert widget, the Topology Map page is displayed in the normal mode displaying the current situation. Otherwise, the Topology Map page is displayed in the analysis mode which can display the situation at the time of the event occurrence, and the Period is set a period centered on the occurrence time of the event.
- If the node is located on multiple maps, a dialog box to select the map to be displayed is displayed.

#### Assigned To

The user name (display name) responsible for handling the event is displayed. If no one is assigned, it will be blank.

#### Detail

Displays the detail of the event.

#### Action

Displays the action for the event.

### Application Name

Displays the application name that detected the event. This application name indicates the name of the product connected to the IMS component.

### 4.7.1.2 **Performing operations on the event**

For **Current Alert** and **Events** widgets, the operations can be performed for the event displayed in the list.

In the Web Console, the following operations are possible for the notified events.

- Assign yourself as responsible for event handling
- Cancel assignments responsible for event handling
- Recover the state of the event
- Delete the event

The specific procedure is described below using an example operation of the **Current Alert** widget.

1. Display the Dashboard page.

Click **Dashboard** menu.

2. Check the contents of the **Current Alert** widget.

The **Current Alert** widget displays the currently occurring fault events.

3. Check the details of the event as necessary.

Click on the  $\nabla$ **Event Detail** icon to display the Event Detail dialog box and check the details of the event.

4. Perform the operation on the event.

Click the <sup>1</sup> icon for the event to display the following menu.

• Assign me menu

Assign yourself as responsible for event handling. When selected, your user name is registered in the **Assign To** field for the event. also, it is possible to perform the operation for the assigned event.

• Unassign menu

Cancel assignments responsible for event handling. When selected, The **Assign To** field for the event is blank. It is also possible to cancel assignment other than yourself.

• Recover event menu

Recover the state of the event. When selected, the **Recovery Status** of the event changes from **Unrecovered** to **Recovered** and The display of the event on the **Current Alert** widget disappears.

Tip

Depending on the specification of the product that detected the event, there are events where the recovery operation cannot be performed. For such the event, the recovery state is automatically detected and recovery processing is performed

• Delete event menu

Delete the event. When selected, the event is deleted and the display of the event in the list disappears.

When the above menu is selected, the Confirmation dialog box will be displayed. After confirming the contents, processing is executed by clicking the **OK** button.

5. Check the contents of the **Current Alert** widget after the operation.

Confirm that the operation of the selected menu is being processed properly in the list of events.

## 4.7.1.3 Checking the influence of the event on the topology map

For **Current Alert** and **Events** widgets, you can easily display the Topology Map page where the source node is registered from the displayed event.

On the Topology Map page, the influence range of the occurred event can be checked directly by referring to the connections among nodes.

The specific procedure is described below using an example of a Topology Map page that is displayed on the **Current Alert** widget on the Dashboard page.

1. Display the Dashboard page.

Click **Dashboard** menu.

2. Check the contents of the **Current Alert** widget.

The Current Alert widget displays the currently occurring fault events.

3. Display the Topology Map page for the event whose influence range is to be checked.

Click the **D**Topology Map icon in the Actions column of the target event.

If the node where the event occurred is registered in a single map, the Topology Map page to which the node is registered is displayed.

If the node where the event occurred is registered in multiple maps, a list of display candidate maps is displayed. Click the link of the map to display the Topology Map page.

#### Tip

- From the **Current Alert** widget, the Topology Map page is displayed in **normal mode**.
- From the **Events** widget, the Topology Map page is displayed in **analysis mode** and the **Period** is set a period centered on the occurrence time of the event. This enables users to check the state of the map where the event occurred.
- 4. Check the nodes around the relevant node on the Topology Map page.

Investigate the influence on the entire network by checking the nodes adjacent to the node in which the event occurred and nodes next to the adjacent nodes.

### 4.7.2 Checking the nodes with the specified status in a list

The **Ratio of Node Status** widget allows users to easily search for the nodes with the specified state.

On the **Ratio of Node Status** widget, the current state of the managed nodes is shown by the number and percentage of nodes to severity. The following describes how to check the nodes in each severity level.

1. Check the contents of the **Ratio of Node Status** widget on the Dashboard page.

The Ratio of Node Status widget displays the current severity states of the managed nodes.

2. Click the link with the severity you want to check for the specific node name.

When clicking on the severity link of **Ratio of Node Status** widget, the Nodes page is displayed with severity specified for the **Search Conditions**.

The displayed node list shows the specific node name currently in the state of the specified severity.

## Chapter 5. Uninstallation of IMS component

This chapter describes how to uninstall the IMS component.

### Contents

5.1	Notes on Uninstallation	.66
5.2	Uninstallation	.66

### 5.1 Notes on Uninstallation

The notes on uninstalling the IMS component are described below.

- If the install path and data path are separately set at installation, the data path will not be deleted automatically at uninstallation. Therefore, you must delete the data path manually.
- If the install path and data path are the same, the uninstaller will delete all of the data at uninstallation.

### 5.2 Uninstallation

The following describes how to uninstall the IMS component.

Tip

The following procedure must be performed by a user with OS administrator privileges.

- 1. Stop the IMS component services.
  - a. Open the Control Panel page, and select **Administrative Tools**.
  - b. Select **Services** on the Administrative Tools page.
  - c. From the list in the Services page, select the following services in this order and execute **Stop**.
    - i. MasterScope IMS Web Server
    - ii. MasterScope IMS Event Manager
    - iii. MasterScope IMS Message Queue
    - iv. MasterScope IMS Key Store
    - v. MasterScope IMS System Database
- 2. Open the Programs and Features window of Windows OS.

Open the Control Panel and then select **Programs and Features**.

3. Start uninstallation.

In the program list, select the MasterScope Integrated Management Server and run uninstallation.

The confirmation dialog is displayed. Click the **Yes** button to proceed uninstallation.

4. Confirm that the uninstallation is completed.

Confirm that the uninstallation is successfully terminated by checking the displayed completion result.

5. If the install path and data path are different, delete the data path manually.

## Appendix A. Command Reference

The following describes the commands that are provided by IMS.

### A.1 ims-ssl-keytool

This command creates and manages an SSL server certificate to be used in HTTPS communication.

This command is a wrapper command that provides the functions of the Java keytool command in an easy-to-use format for this product. Note that this command can use only some functions of the Java keytool command. The names and meanings of the argument of this command are the same as those of the Java keytool command.

For details on the Java keytool command, refer to the following URL.

http://docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html \*1

The differences from the Java keytool command are as follows:

- A subcommand name such as genkeypair is specified for the first argument. is not attached at the beginning of the argument name of the subcommand.
- For this command, the keystore path is fixed to <%DATAPATH%>\conf\server.keystore.
- By running the genkeypair subcommand, the password of the keystore and aliases of entries in the keystore are saved in the following file.

<%DATAPATH%>\conf\ims-conf.ini

Information saved in the above file are used automatically when the -storepass and -alias options are omitted when running each subcommand. This enables to run this command by specifying minimal options.

- The default values of the -keyalg and -validity options are different from those of the Java keytool command.
- This command implements its own subcommand, initstore.

### 🔥 Caution

This command requires OS administrator privileges.

### Path

<%INSTPATH%>\bin\ims-ssl-keytool

### Syntax

```
ims-ssl-keytool genkeypair [-help] [-storepass PASS] [-alias ALIAS]
    [-keyalg KEYALG] [-keysize KEYSIZE] [-sigalg SIGALG]
    [-validity DAYS] [-dname DNAME] [-dns DNS]

ims-ssl-keytool selfcert [-help] [-storepass PASS] [-alias ALIAS]
    [-sigalg SIGALG] [-validity DAYS] [-dname DNAME]
```

<sup>\*1</sup> This URL is current as of January 2019.

```
ims-ssl-keytool certreq [-help] [-storepass PASS] [-alias ALIAS]
      [-dns DNS] FILE
ims-ssl-keytool importcert [-help] [-storepass PASS] [-alias ALIAS]
      FILE
ims-ssl-keytool exportcert [-help] [-storepass PASS] [-alias ALIAS] FILE
ims-ssl-keytool list [-help] [-storepass PASS] [-alias ALIAS] [-rfc | -v]
ims-ssl-keytool delete [-help] [-storepass PASS] [-alias ALIAS]
ims-ssl-keytool delete [-help]
ims-ssl-keytool initstore [-help]
ims-ssl-keytool -help
```

### Description

The subcommands are described below.

genkeypair

Creates and stores a pair of keys (public key and associated private key) in the keystore. In addition, this subcommand writes Information to use keys generated by a web server to the following files.

<%DATAPATH%>\conf\ims-conf.properties

#### 🕂 Caution

The value of noms.tomcat.https.enabled in the ims-conf.ini is updated to "true" by this command.

selfcert

Creates a self-signed certificate for the key of the keystore entry.

certreq

Generates a certificate signing request (CSR) in the PKCS#10 format.

• importcert

Reads a certificate or certificate chain from a file and stores it to the keystore.

exportcert

Reads a certificate from the keystore and stores it in a file in binary encoding format.

• list

Displays the contents of a certain keystore entry or of the entire keystore.

• delete

Deletes a certain entry from the keystore.

initstore

Deletes the keystore file.

### Arguments

#### -storepass PASS

Specify the password of the keystore.

If this argument is omitted when running the genkeypair subcommand, you will be prompted to enter your password while the subcommand is running. If this argument is omitted when running other subcommands, the value read from the ims-conf.properties file is used.

#### -alias ALIAS

Specify an alias for the entry in the keystore.

If this argument is omitted when running the genkeypair subcommand, the default value "*tomcat*" is used. If this argument is omitted when running the list subcommand, an alias is specified for all entries. If this argument is omitted when running other subcommands, the value read from the ims-conf.properties file is used.

#### -keyalg KEYALG

Specify the encryption algorithm for the key. For example, "*RSA*", "*DSA*", and "*EC*" can be specified. The default is "*RSA*".

For the algorithms that can be specified for -keyalg and -sigalg, refer to Java Cryptography Architecture Specification and Reference. \*2

#### -keysize KEYSIZE

Specify the size of the key to be generated.

The setting range and default value comply with the Java keytool specifications.

#### -sigalg SIGALG

Specify the algorithm to be used to sign a self-signed certificate.

Be sure to specify the algorithm that is compatible with -keyalg. The setting range and default value comply with the Java keytool specifications.

#### -validity DAYS

Specify the valid period of a self-signed certificate in days. Values from 0 to 365000 can be specified. The default is 3650 (Approx. 10 years).

#### -dname DNAME

Specify the X.500 identification name to be used as the issuer and subject fields of a self-signed certificate.

If the identification name is not specified, you will be prompted to enter the identification name while the command is running.

#### -dns DNS

Specifies the FQDN for Subject Alternative Name (SAN) extension.

In genkeypair subcommand, if this argument is omitted, Common Name of a certificate is used as SAN.

-rfc

This option is used to specify the output format of the list subcommand. The contents of a certificate will be output in the specified encoding format.

This option cannot be specified together with the -v option.

-v

<sup>\*2</sup> This URL is current as of October 2018.

This option is used to specify the output format of the list subcommand. The detailed contents of a certificate will be output in the human readable format.

This option cannot be specified together with the -rfc option.

-help

Displays the usage of all or each of the commands.

### **Return values**

Upon success, 0 is returned. In case of failure, a value other than 0 is returned.

### A.2 ims-app

This command manages the applications incorporated in the IMS component

This command is used to perform the following three tasks.

- Conforms versions of the IMS component and incorporated applications.
- · Installs applications into the IMS component.
- · Uninstalls applications incorporated in the IMS component.

#### 🕂 Caution

- · This command requires OS administrator privileges.
- Before installing or uninstalling applications, you need to stop the services of the IMS component.

### Path

```
<%INSTPATH%>\bin\ims-app
```

### Syntax

ims-app list

```
ims-app install [-help] [-silent] [-overwrite] [-ignore-dependencies]
WAR FILE
```

ims-app uninstall [-help] [-silent] ID

ims-app -help

### Description

The subcommands are described below.

• list

Displays the IMS version, and applications that are incorporated in the IMS component.

• install

Installs the application file (WAR file) specified as *WAR\_FILE* and enables it on the IMS component.

• uninstall

Uninstalls the application the IMS component by specifying the application ID.

### Arguments

-silent

Specify it to run the command in non-interactive mode (silent mode).

### -overwrite

It is enabled in the install subcommands with non-interactive mode.

Overwrites the application without confirmation even if the application is already installed.

### -ignore-dependencies

It is enabled in the install subcommands

Ignores dependencies between applications and performs installation.

-help

Displays the usage of all or each of the commands.

### **Return values**

Upon success, 0 is returned. In case of failure, a value other than 0 is returned.

## Appendix B. Troubleshooting

The following describes the problems that might occur while setting up IMS and the suggested actions to take to resolve those problems.

# **B.1** Troubleshooting errors when running the installer

The following describes errors that occur while the installer runs and how to troubleshoot them.

### Failed to initialize data. Directory exists

The following message is displayed when a directory to be created at installation already exists in the directory specified as the data path.

```
Installing XXXX . failed
ERROR: Failed to initialize data.
Directory exists: <%DATAPATH%>\conf
```

The following recovery command is displayed under Failed to initialize data.

```
Try to run the following command later.
"<%INSTPATH%>\bin\ims-init" -data "<%DATAPATH%>"
```

Delete the directory displayed in the error message, and then run the displayed command as a user with Windows OS administrator privileges.

### Other errors

Some other error message may be displayed. If a recovery command is displayed with an error message, try to run the displayed command to recover the installation.

Example of recovery command:

```
Try to run the following command later.
    "<%INSTPATH%>\bin\ims-app.cmd" install
    -silent "D:\IMS\Windows\app\nvp.war"
```

If an unrecoverable error occurs, please contact the NEC Customer Support Center.

# **B.2** Troubleshooting errors when starting the service

The following describes errors that may occur when starting the IMS component service and how to troubleshoot them.

### Starting the service immediately after installation failed

The data path may not have been initialized properly.

Troubleshoot this error as follows:

- 1. Stop the IMS component services.
  - a. Open the Control Panel page, and select Administrative Tools.

- b. Select **Services** on the Administrative Tools page.
- c. From the list in the Services page, select the following services in this order and execute **Stop**.
  - i. MasterScope IMS Web Server
  - ii. MasterScope IMS Event Manager
  - iii. MasterScope IMS Message Queue
  - iv. MasterScope IMS Key Store
  - v. MasterScope IMS System Database
- d. From the list in the Services page, select the above services in reverse order of stopping the services and execute **Start**.
- 2. Confirm the data path state.

Start the command prompt and run the following command.

> <%INSTPATH%>\bin\ims-init -data <%DATAPATH%>

The following errors are displayed when the data path directory is not empty.

ERROR: Directory exists: <%DATAPATH%>\conf

If these errors are displayed, delete the displayed directories, and then run the command again.

3. If necessary, create an SSL server certificate.

For the environment on which Web Console is accessed via HTTPS, execute the procedure in "2.6.2 Preparing the SSL server certificate (page 22)".

- 4. Start the IMS component service again.
  - a. Open the Control Panel page, and select **Administrative Tools**.
  - b. Select **Services** on the Administrative Tools page.
  - c. From the list in the Services page, select the following services in this order and execute **Start**.
    - i. MasterScope IMS System Database
    - ii. MasterScope IMS Key Store
    - iii. MasterScope IMS Message Queue
    - iv. MasterScope IMS Event Manager
    - v. MasterScope IMS Web Server

## The web server listen port "443/tcp" does not exist or its state is not LISTEN.

When the IMS component checks the state of the web server listen port "443/tcp" on the environment on which Web Console is accessed via HTTPS, an SSL certificate may not have been created properly if there is no open port.

Troubleshoot this error as follows:

1. Create an SSL server certificate.

Execute the procedure in "2.6.2 Preparing the SSL server certificate (page 22)".

- 2. Restart the IMS component services.
  - a. Open the Control Panel page, and select Administrative Tools.
  - b. Select **Services** on the Administrative Tools page.
  - c. From the list in the Services page, select the following services in this order and execute **Stop**.
    - i. MasterScope IMS Web Server
    - ii. MasterScope IMS Event Manager
    - iii. MasterScope IMS Message Queue
    - iv. MasterScope IMS Key Store
    - v. MasterScope IMS System Database
  - d. From the list in the Services page, select the above services in reverse order of stopping the services and execute **Start**.

MasterScope Network Management Web Console Getting Started Guide for Windows / EXPRESSCLUSTER X

IMSWCSE0100-01

January, 2019 01 Edition

**NEC Corporation** 

© NEC Corporation 2019 -