NEC

MasterScope Network Management
Web Console
Getting Started Guide

for Linux

MasterScope

IMS0LSE0100-01

Copyrights

Trademarks

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.

: Administrators 

: 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 34)"	Describes how to configure the environment before using and operating the Web Console.	Admin
"Chapter 4. Basic Operations (page 44)"	Describes the basic operations of the Web Console.	User
"Chapter 5. Uninstallation of IMS component (page 62)"	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
Caution	Indicates important points that the user should observe to configure and use the product properly.

Notation	Description
Tip	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.	**Dashboard** menu, **OK**button
<userinput>	Indicates items that change depending on the user environment or items that the user must specify.	*<%INSTPATH%>*, *<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:

/opt/nec/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 can specify a different 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%>*. If you install this component and store the data in the same path, *<%DATAPATH%>* and *<%INSTPATH%>* indicate the same path.

Contents

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

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.

Tip

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.

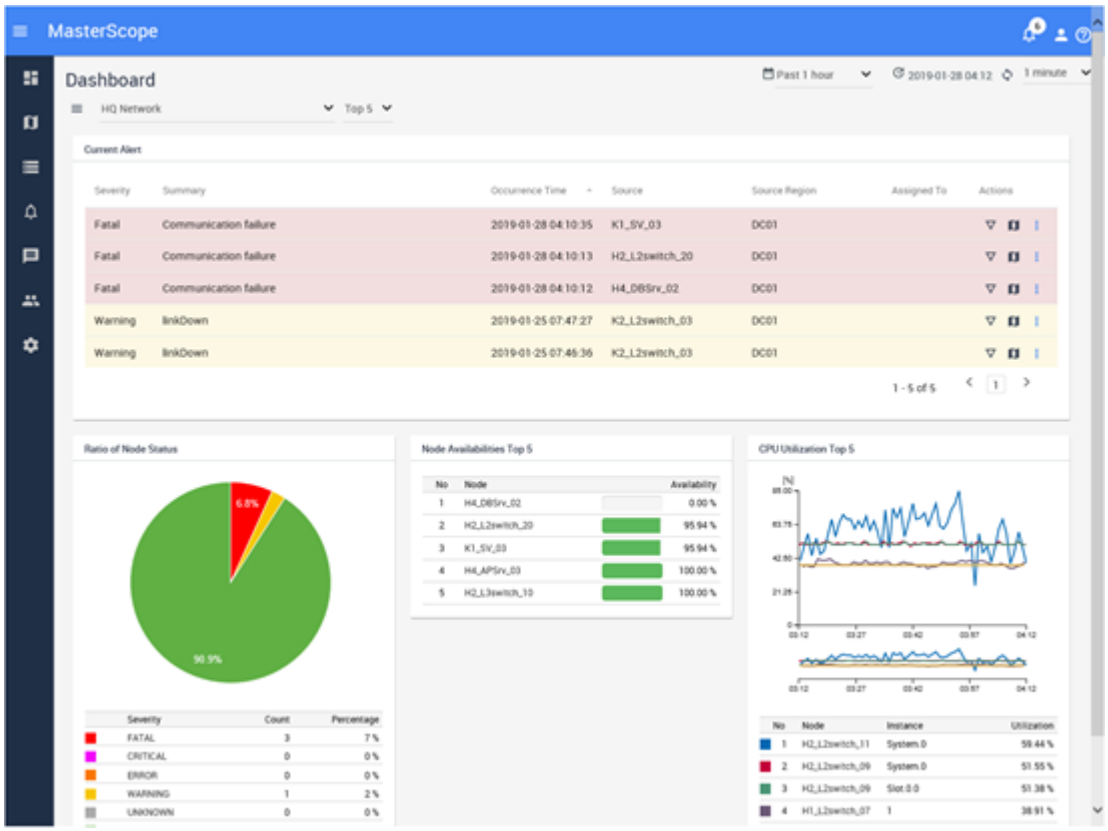

Figure 1-1 Dashboard

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.

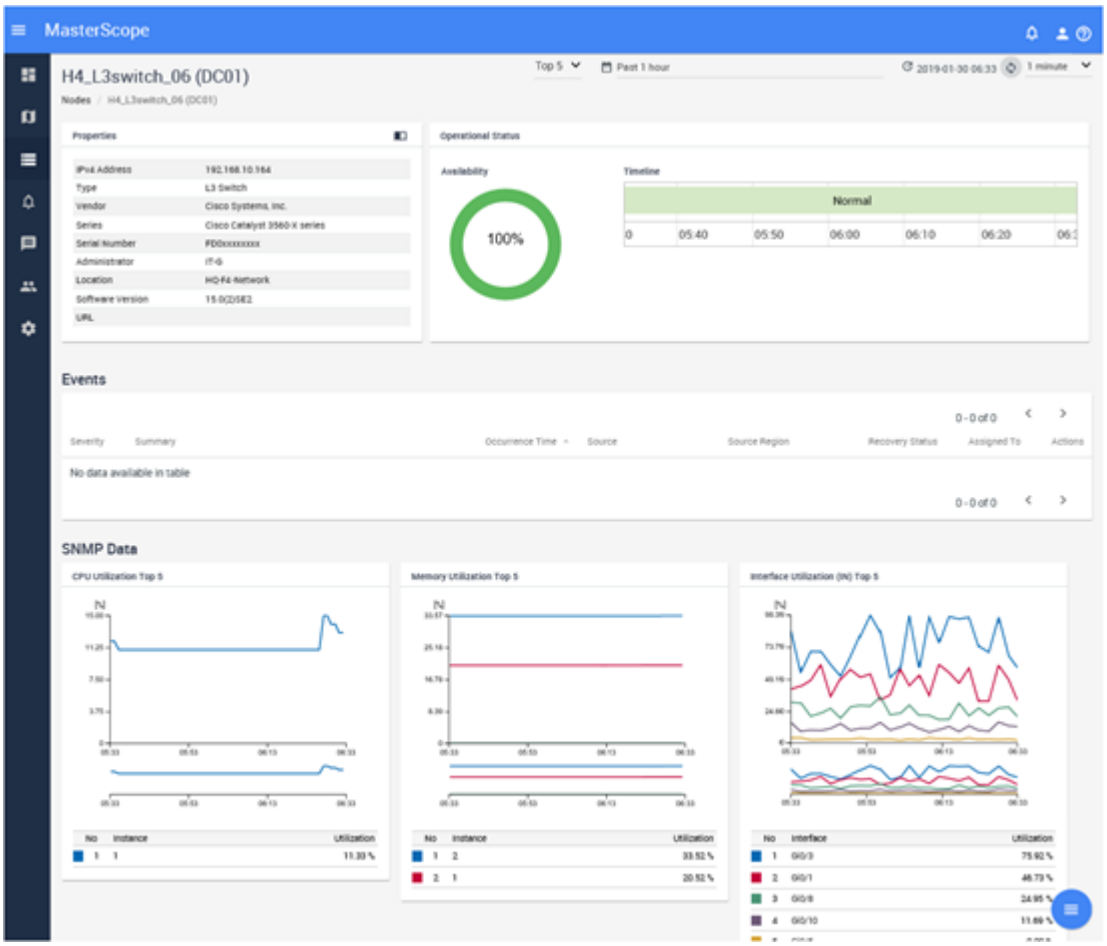

Figure 1-2 Node Detail

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.

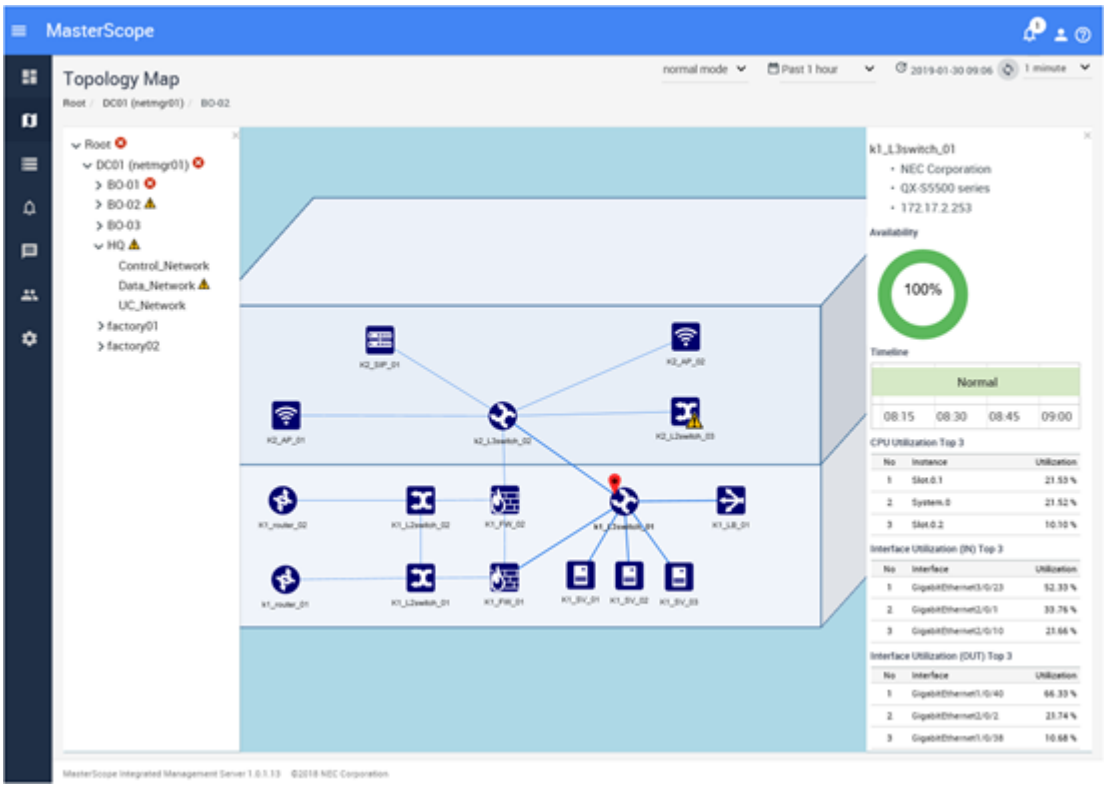

Figure 1-3 Topology Map

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.

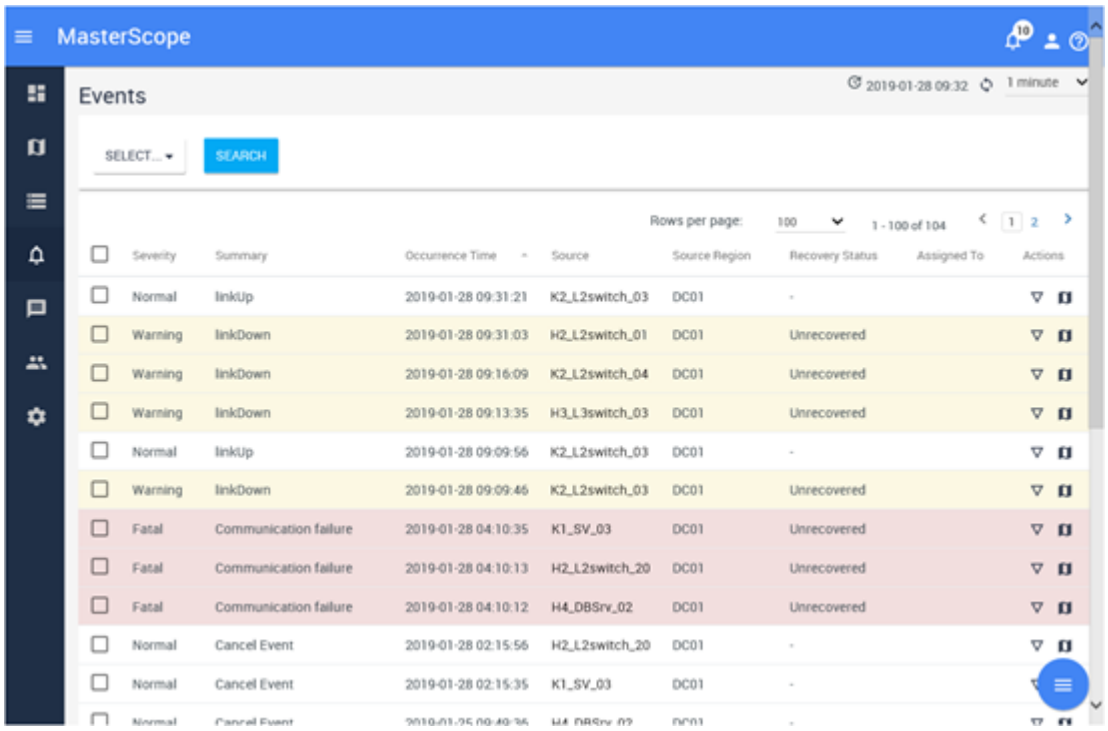

Figure 1-4 Events

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.

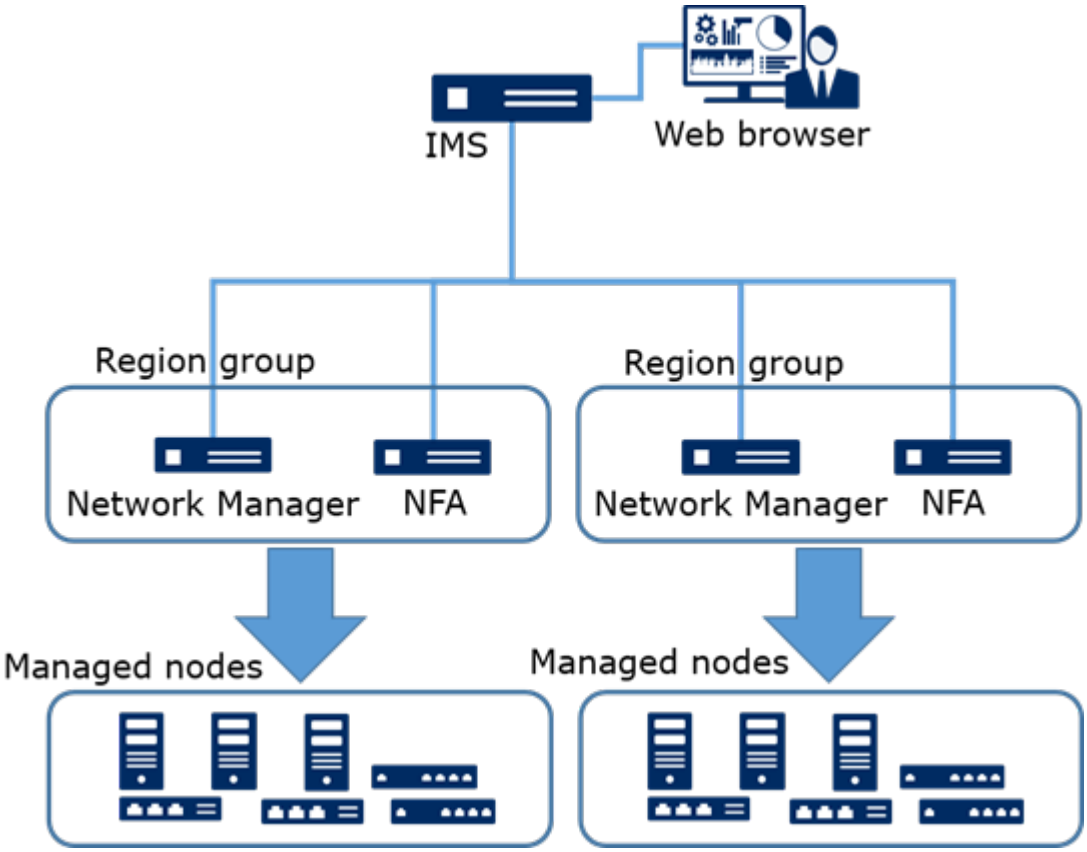

Figure 1-5 System Configuration Diagram

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.

Table 1-1 IMS requirements

Item	Description
CPU	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	• Red Hat Enterprise Linux 7 (x86_64) [1) 2)] • Red Hat Enterprise Linux 6 (x86_64) [1) 2)]

Note

1. SELinux must be disabled.
2. Operation with version 6.6 or higher OS is supported.

Table 1-2 Web browser requirements

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
CPU	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

The following describes the setup flow of the IMS component.

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

Table 2-1 Setup Flow for the IMS Component

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	"2.2.2 Checking the installation environment (page 15)" Check that the installation destination server satisfies the system requirements to use the IMS component.
3	Installing the IMS component	"2.3 Installation (page 15)" Run the installer stored in the installation media to install the IMS component to the server.
4	Configuring the settings to connect the products	"2.4 Configuring to connect the products (page 17)" Configure the settings of the IMS component to connect the IMS component to the MasterScope network management products.
5	Configuring the communication protocol settings of Web Console	"2.5 Configuring the communication protocol settings of Web Console (page 20)" When using HTTPS communication to access Web Console, configure the settings to enable HTTPS communication and prepare the SSL server certificate. **Tip** When using HTTP communication to access Web Console, skip this step.
6	Checking the port numbers to use	"2.6 Changing the communication port number from default value (page 25)" Check that the port numbers used by the IMS component do not interfere with those used by other coexisting software.
7	Configuring the firewall settings	"2.7 Changing the firewall settings (page 26)" Check whether the firewall setting allows the IMS component to communicate with external systems properly, and change the setting if necessary.
8	Configuring the additional settings of the installation environment	"2.8 Configuring the additional settings on the installation environment (page 27)" Configure the additional settings on the environment where the IMS component is installed.
9	Start the IMS component service	"2.9 Starting the IMS component service (page 28)" Confirm that the IMS component service starts normally.
10	Setting up the products to be connected	"2.10 Setting up the products to be connected (page 29)" 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.

Table 2-2 Parameters Necessary to Run the Installer

Parameter name	Description	Default value
Install Path	Directory in which to install the IMS component execution file. A maximum of 128 characters can be entered. Available characters are single-byte alphanumeric characters, underscore (_), hyphen (-), and dot (.).	/opt/nec/ims
Data Path	Directory in which to save the environment settings and accumulated data. A maximum of 128 characters can be entered. Available characters are single-byte alphanumeric characters, underscore (_), hyphen (-), and dot (.). It is recommended to specify a path other than 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.	/opt/nec/ims

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.

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

Parameter name	Description	Example
region id	This is necessary to configure the IMS component. ID of a region group that is used to classify connecting products. Available characters are single-byte alphanumeric characters. **Caution** This ID cannot be changed after setting up. When using multiple region groups, prepare multiple IDs.	tokyo
region name	This is necessary to configure the IMS component. Name of a region group corresponding a **region id**. A name can be specified with an arbitrary character string.	Tokyo

Parameter name	Description	Example
	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. 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. **⚠ 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 **manager id**, you should also design a **region id** (region group) to which it belongs.	nvpro01 (belongs to **tokyo** region)
manager host name	This is necessary to configure the IMS component. Host name corresponding to **manager id**. A host name can be specified with an arbitrary character string. 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.	NetMgr01
ims ip address	This is necessary to configure products connecting to the IMS component. IPv4 address of the server where the IMS component is installed. **Tip** For servers with multiple IPv4 addresses, be sure to check the connectable IPv4 address from the product to be connected.	192.168.1.200

Parameters necessary to configure the connection settings for Network Manager

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

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

Parameter name	Description	Example
	Tip For servers with multiple IPv4 addresses, be sure to check the connectable IPv4 address from the IMS component.	

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**)	This is necessary to configure both IMS component and Network Manager. Specify whether to use HTTPS for the Network Manager WebAPI as follows. • true (on): uses HTTPS. • false (off): uses HTTP, not HTTPS.	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.

Table 2-6 Parameters Necessary to Configure the Settings to Connect 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.nec.com

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	Direction	Application
HTTP communication port	80	TCP	IN	Port for HTTP communication

Name	Port number	Protocol	Direction	Application
HTTPS communication port	443	TCP	IN	Port for HTTPS communication
Message Queue communication port	28110	TCP	IN	Port for message send and receive communication

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

Name	Port number	Protocol	Direction	Application
System Database communication port	28120	TCP	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.

When asking a public certificate authority to issue the SSL server certificate, conditions, such as a key encryption algorithm and identification name, may be specified for some parameters depending on the certificate authority. Therefore, check the conditions presented by the certificate authority.

Table 2-9 Parameters related to the SSL server certificate

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 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 64)".	RSA
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 64)".	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 64)". 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.	3,650 days (approximately 10 years)

Parameter name	Description	Default value
	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.	

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. 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.	ims.nec.com
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. Specify a legally official English organization name.	NEC Corporation
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. In the case of Minato-ku, Tokyo, specify "Minato-ku".	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. In the case of Tokyo, specify "Tokyo".	Tokyo
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. For Japan, the country code is usually specified as "JP".	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 13)" 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 Installation

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

1. Insert the installation media into the DVD-ROM drive and then mount the DVD-ROM.

In the following explanation, the DVD-ROM mount point is assumed to be `/media`. If you mounted the DVD-ROM to other locations, change the mount point accordingly.

2. Start the installer.

```
# /media/IMS/Linux/ims-install
```

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: `/Linux/Tools/NvPRO/IMS/ims-install`

3. Enter the install path.

```
Input installation path [default: /opt/nec/ims]
 >
```

The default value is displayed to the right of the first line. If you want to use the default value, press the Enter key without entering anything.

4. Enter the data path.

```
Input data installation path [default: /opt/nec/ims]
 >
```

The default value is displayed to the right of the first line. If you use the default value, press the Enter key without entering any.

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

```
Install application of MasterScope Network Manager? (y/n): y
Install application of MasterScope Network Flow Analyzer? (y/n): y
```

To select an application, enter `y` and press the Enter key.

Tip

- 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 67)".

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

  In the media: `/IMS/Linux/app/`

6. Installation starts.

The installation parameters are displayed. If the displayed parameters are correct, enter `y` and press the Enter key. Entering `n` displays the parameter input prompt again, prompting to modify the parameters.

```
----- Confirmation ----------------------------------------
Installation path      : /opt/nec/ims
Data installation path : /opt/nec/ims
Applications           : MasterScope Network Manager
                       : MasterScope Network Flow Analyzer
-----------------------------------------------------------

Is it OK to install? (y/n): y
```

If the following message is displayed, the installation is complete.

```
Installing package ..... done
```

If an error message is displayed during the installation, take appropriate action according to "B. 1 Troubleshooting errors when running the installer (page 69)".

2.4 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

Tip

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 17)"

  Configure region group settings that classify the connecting products.
- "Common settings for connecting products (page 18)"

  Configure common settings for connecting products.
- "Connection settings for Network Manager (page 18)"

  Configure Network Manager specific settings.
- "Connection settings for NFA (page 19)"

  Configure NFA specific settings.
- "Single sign-on settings (page 20)"

  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 11)".

<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 11)".

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 11)".

<manager host name>

Specify a host name prepared as **manager host name** in "Parameters necessary to configure the settings to connect the products (page 11)". 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 12)".

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 12)".

<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 12)".

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.

2.5 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.

2.5.1 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.

2.5.2 Preparing the SSL server certificate

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

There are two types of SSL server certificates as shown below.

- Self-signed certificate
- Certificate to be issued by a public certificate authority

Certificates created previously can also be used by using Java keytool.

Refer to the following sections for the preparation procedure of each certificate.

- "2.5.2.1 Preparing a self-signed certificate (page 21)"
- "2.5.2.2 Preparing a certificate to be issued by a public certificate authority (page 22)"
- "2.5.2.3 Using certificates created previously (page 24)"

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.

2.5.2.1 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 64)".

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]:
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.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 64)".

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

  ```
  # cd /opt/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 64)".

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 36)".

2.5.2.2 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 64)".

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]:
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.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 64)".

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

```
# cd /opt/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 64)".

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.

2.5.2.3 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.

2.6 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.

Table 2-11 Communication Port Numbers

Communication type	Specification format

HTTP communication	• Configuration file
	`<%DATAPATH%>\conf\ims-conf.ini`
	`<%DATAPATH%>` /conf/ims-conf.ini
	• Specification format
	`noms.tomcat.http.port = <Port number>`
	By setting the following property in the configuration file to *"true"* , the above setting becomes to enable.
	If *"false"*, the port is nor opened.
	`noms.tomcat.http.enabled = true`

HTTPS communication	• Configuration file
	`<%DATAPATH%>` `/conf/ims-conf.ini`
	• Specification format
	`noms.tomcat.https.port = <Port number>`
	By setting the following property in the configuration file to *"true"* , the above setting becomes to enable.
	If *"false"*, the port is nor opened.
	`noms.tomcat.https.enabled = true`

Message Queue communication	• Configuration file
	`<%DATAPATH%>/conf/ims-conf.ini`
	• Specification format
	By adding the following property in the configuration file, a port number can be set.
	`amqphub.amqp10jms.remote-url = amqps://localhost:<Port number>?transport.trustAll=true`

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 "2.10 Setting up the products to be connected (page 29)" for details.

System Database communication	• Configuration file
	`<%DATAPATH%>/conf/ims-conf.ini`
	• 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
	`<%DATAPATH%>/conf/systemdb-extra.conf`
	• Specification format
	`port = <Port number>`

Key Store communication	• Configuration file
	`<%DATAPATH%>/conf/ims-conf.ini`
	• Specification format
	By adding the following property in the configuration file, a port number can be set.
	`spring.redis.port = <Port number>`
	Also update the following setting file according to the above setting.
	• Configuration file
	`<%DATAPATH%>/conf/redis-extra.conf`
	• Specification format
	`port = <Port number>`

⚠ 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.

2.7 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 27)" and "Table 2-13 Communication Port Number List (for Internal Communication) (page 27)".

If the communication ports are changed in the procedure of "2.6 Changing the communication port number from default value (page 25)", read the communication port numbers accordingly.

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

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

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

Name	Port number	Protocol	Direction	Application
System Database communication port	28120	TCP	IN	Port for communication with a system database
Key Store communication port	28130	TCP	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.

Tip

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

2.8 Configuring the additional settings on the installation environment

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

2.8.1 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.nec.com
```

Tip

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

2.8.2 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 are accumulated in the following directory. These logs are not deleted automatically. Configure the setting to delete old logs automatically if necessary by using *"cron"*.

- `<%INSTPATH%>/tomcat/logs/localhost_access_log.yyyy-mm-dd.txt`

yyyy-mm-dd represents the date on the web server. For example, `localhost_access_log.2018-10-31.txt` is an access log for Web Console on October 31, 2018.

Setting example

The following is an example of the cron setting to check and delete log files that are 30 days or older at 1 am every day.

```
0 1 * * *    /usr/bin/find /opt/nec/ims/tomcat/logs/
   -type f -regex '^.*\.[0-9]+-[0-9]+-[0-9]+\.txt$'
   -mtime +30 -exec /bin/rm -f {} \;
```

For details about the cron settings, refer to the manual provided by the OS.

2.8.3 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.

2.9 Starting the IMS component service

If the setup in the previous sections have all been done properly, the IMS component service can be started.

Run the startup script (System V init script) directly, or restart the OS to start the IMS component services.

The following describes how to start the service by running the startup script.

1. Log in to the server as the root user.
2. Run the command to start the service.

```
# /etc/init.d/nec-ims start
```

If all daemon processes of IMS started successfully, the command returns 0 as the return value.

- For Red Hat Enterprise Linux 6

```
# /etc/init.d/nec-ims start

Starting systemdb:                [  OK  ]
Starting key store:               [  OK  ]
Starting message queue:           [  OK  ]
Starting event manager:           [  OK  ]
Starting web server:              [  OK  ]
```

- For Red Hat Enterprise Linux 7

```
# systemctl start nec-ims

Starting nec-ims (via systemctl):  [  OK  ]
```

For the processes that could not start normally, instead of [OK], [NG] is displayed.

3. Confirm the activation states of daemon processes.

Wait for a while, and then run the following command to check whether daemon processes are still running.

```
# /etc/init.d/nec-ims status
```

When all daemon processes are running, the following messages are displayed. The command also returns 0 as the return value.

```
systemdb (pid 12341) is running...
key store (pid 12342) is running...
message queue (pid 12343) is running...
event manager (pid 12344) is running...
web server (pid 12345) is running...
```

When all daemon processes stop, the following messages are displayed. The command also returns 3 as the return value.

```
systemdb is stopped
key store is stopped
message queue is stopped
event manager is stopped
web server is stopped
```

2.10 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 compornent varies depending on each product. Refer the description of each product.

2.10.1 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 11)".

The default value is *"1"*.

This parameter must match the value in the IMS component configuration file (ims-conf.ini). See also "2.4 Configuring to connect the products (page 17)".

<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 11)".

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 "2.6 Changing the communication port number from default value (page 25)".

<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.

1. 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 (ims-conf.ini) of the IMS component. See also "2.4 Configuring to connect the products (page 17)".

   - **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.

2.10.2 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 11)".

There is no default value.

This parameter must match the value in the IMS component configuration file (ims-conf.ini). See also "2.4 Configuring to connect the products (page 17)".

<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 11)".

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 "2.6 Changing the communication port number from default value (page 25)".

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"*.

⚠ 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.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

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 36)" 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"*.

    Tip

    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.

  Tip

  - 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.

Tip

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 `exportcert` command of "A.1 ims-ssl-keytool (page 64)" 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.

   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 35)" 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.

   Tip

   - 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.

Tip

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 38)".

     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

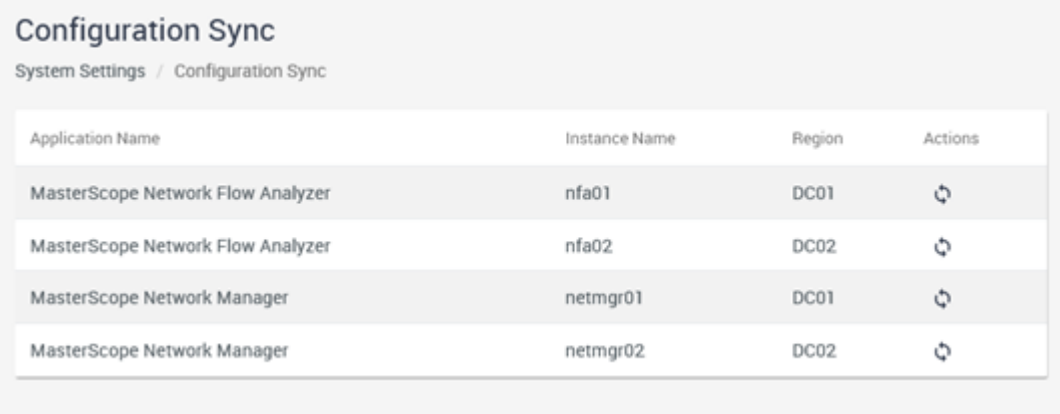

Figure 3-1 Configuration Sync page

In the Configuration Sync page, click the **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 **Nodes** menu.

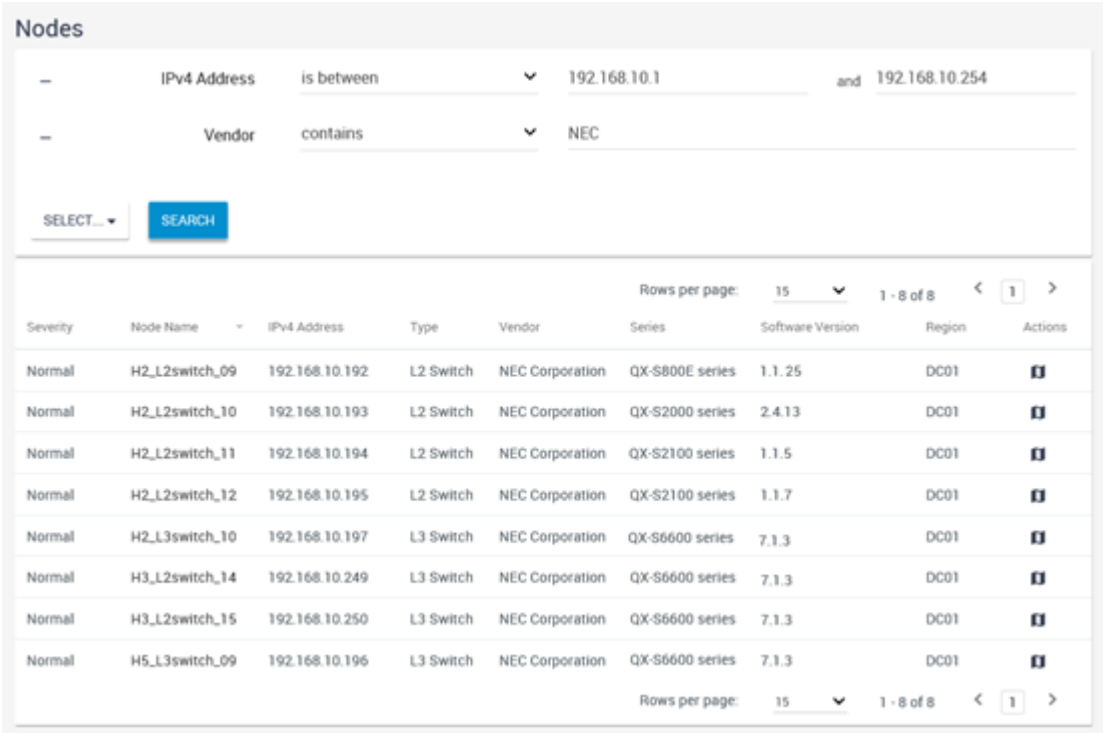

Figure 3-2 Nodes page

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"*.

Tip

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**.

Tip

- 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

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 45)".

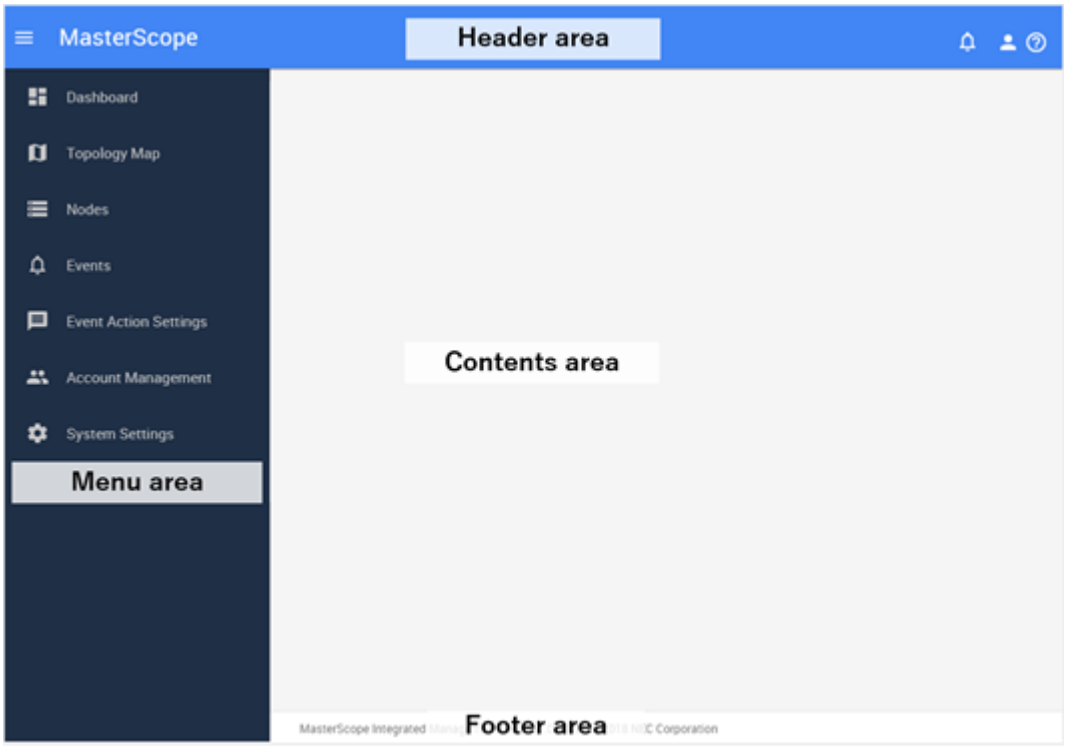

Figure 4-1 Structure of Web Console

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.

- **Help** 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.

- **Dashboard** menu

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

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

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

- **Nodes** 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.

Tip

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.

Tip

User Name and **Group** cannot be changed.

1. Display the Edit Profile page.

   Click icon at the upper right of the page and select the **Edit Profile** menu.

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.

  Tip

  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 **Notifications** icon at the upper right of the page.

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

   Tip

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

2. Click the **Notifications** icon.

   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 ✕ icon for the notification in the Notification list, you can delete the notification from the list. By clicking the **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 50)" shows a sample line chart widget.

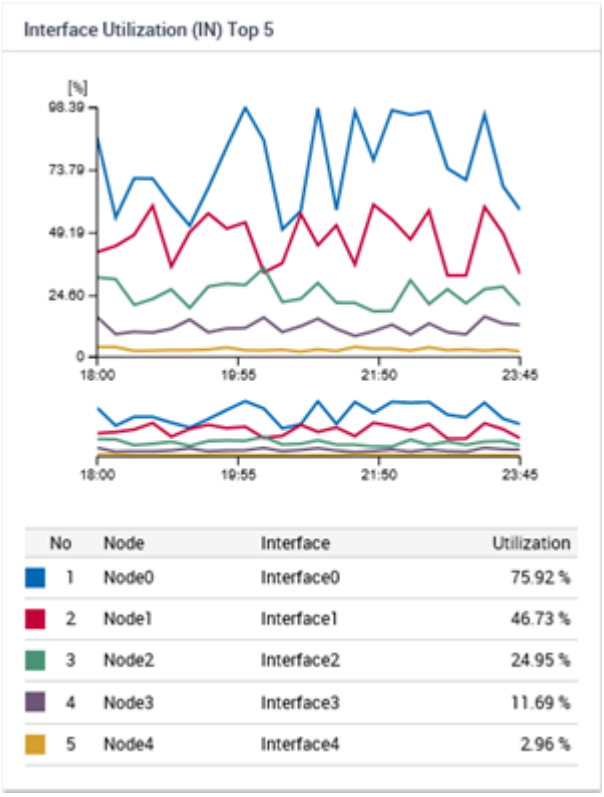

Figure 4-2 Line chart widget

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 51)" shows a sample pie chart widget.

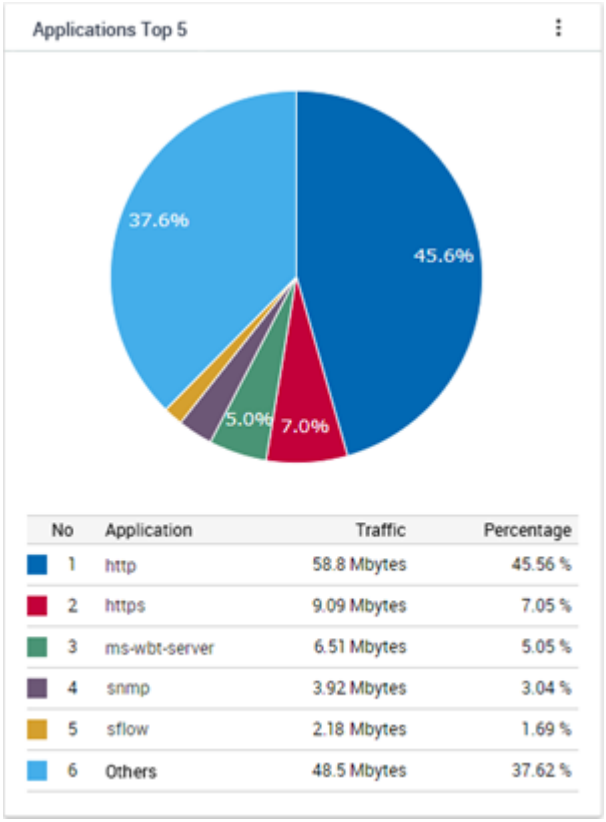

Figure 4-3 Pie chart widget

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 52)" shows a sample list widget.

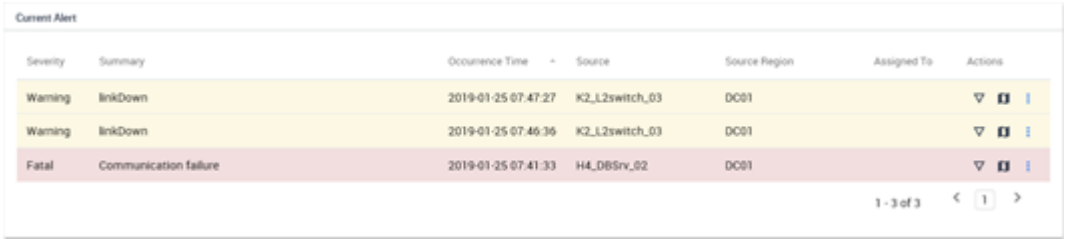

Figure 4-4 List widget

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.

"Figure 4-5 Other widget (page 52)" shows a sample other widget.

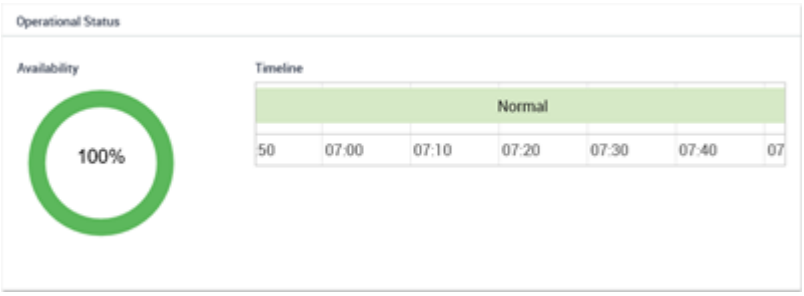

Figure 4-5 Other widget

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.

Tip

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.

Tip

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 **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**.

5. 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.

Tip

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 ⋮ 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 ⋮ 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 **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.

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

     Tip

     - The **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 **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 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 **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

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.

1. Log in as the root user.
2. Stop the IMS component services.
   - For Red Hat Enterprise Linux 6

     ```
     # /etc/init.d/nec-ims stop
     ```

   - For Red Hat Enterprise Linux 7

     ```
     # systemctl stop nec-ims
     ```

3. Uninstall the IMS component.

   ```
   # rpm -e nec-ims
   ```

4. 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/unix/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]
```

*1 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 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

*2 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.

Non-root user cannot access the install path

The following message is displayed when a user cannot access the install path because the user does not have OS administrator privileges.

```
ERROR: Non-root user cannot access the install path: <%INSTPATH%>
       Check the permission of the install destination.
```

Change the permission setting so that users without OS administrator privileges can access the directory specified as the install path and its upper-level directories. Then, run the installer again.

installing package nec-ims-1.0.1.15-1.x86_64 needs *XXX*MB on the / file system

The following message is displayed when free space of the file system specified for the install path is insufficient or when the specified file system is write-disabled.

```
Installing controller . failed
ERROR: Failed to install package: code=1
        installing package nec-ims-1.0.1.15-1.x86_64 needs XXXMB
        on the / filesystem.
```

Specify the write-enabled location that has enough free space for the install path. After allocating enough free space, run the installer again.

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 install
    -silent /media/IMS/Linux/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.
   - For Red Hat Enterprise Linux 6

     ```
     # /etc/init.d/nec-ims stop
     ```
   - For Red Hat Enterprise Linux 7

     ```
     # systemctl stop nec-ims
     ```
2. Confirm the data path state.

   Run the following restore 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 "2.5.2 Preparing the SSL server certificate (page 21)".
4. Start the IMS component service again.
   - For Red Hat Enterprise Linux 6

     ```
     # /etc/init.d/nec-ims start
     ```
   - For Red Hat Enterprise Linux 7

     ```
     # systemctl start nec-ims
     ```

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 "2.5.2 Preparing the SSL server certificate (page 21)".

2. Restart the IMS component services.

   - For Red Hat Enterprise Linux 6

     ```
     # /etc/init.d/nec-ims stop
     # /etc/init.d/nec-ims start
     ```

   - For Red Hat Enterprise Linux 7

     ```
     # systemctl restart nec-ims
     ```

The service does not start automatically at OS startup.

If the IMS component service does not start automatically at OS startup even if it is possible to start the IMS component service manually, the automatic start setting may have been changed by the `chkconfig` command and the like.

To make the service start automatically at OS startup, run the following command.

- For Red Hat Enterprise Linux 6

  ```
  # chkconfig nec-ims on
  ```

- For Red Hat Enterprise Linux 7

  ```
  # systemctl enable nec-ims
  ```

MasterScope Network Management
Web Console
Getting Started Guide
for Linux

IMS0LSE0100-01

January, 2019 01 Edition

NEC Corporation