FUJITSU

FUJITSU Supercomputer PRIMEHPC FX700

BMC User's Guide

C120-0091-07EN

Preface

This document describes how to operate the BMC (Baseboard Management Controller) of FUJITSU Supercomputer PRIMEHPC FX700.
The BMC provides functions to manage and control the equipment.

Organization and Contents of This Manual

This document consists of the following chapters and appendix.

Chapter 1 Environment and Settings for Using the Web GUI

This chapter describes the environment for operating the BMC over the Web.

Chapter 2 Basic Web GUI Operations and Behavior

This chapter describes the screen configuration and logging in and out on Web screens for operating the BMC.

Chapter 3 Web GUI Functions

This chapter shows Web GUI categories and screens, and describes their functions.

Chapter 4 Command Support (IPMI)

This chapter describes the requests (commands) received by the BMC, command functions, and request/response data formats.

Appendix A REMCS

This appendix describes REMCS settings.

Warning and Important Notice Symbols

This manual uses the following symbols to provide warnings and indicate useful information to the user, to prevent personal injury and property damage.

WARNING

WARNING indicates a hazardous (potentially dangerous) situation that could result in death or serious personal injury if the product is not used properly.

CAUTION

CAUTION indicates a hazardous situation that could result in minor or moderate personal injury and/or property damage, such as to the product itself or the user's property, if the product is not used properly.

Alert Symbols in the Text

An alert statement follows an alert symbol. An alert statement is indented on both ends to distinguish it from regular text. Similarly, one line is inserted before and after the alert statement.

Revision History

Edition	Date	Changed Location (Change Classification)(*1)	Description
01	February 27, 2020	-	Created
02	March 17, 2020	Preface Chapter 3	Added "Safety, Radio, and Harmonics (Europe, UK)" Added "CE Compliance" to "Regulations" Updated "Table 3.28 Specifying SNMP Trap Setting Information" Changed order of display items on screens
03	June 25, 2020	Chapter 2 Chapter 3	Updated remarks in "Logging In" in "2.1.1 Login" Updated "Table 3.2 Display Items on the [FRU Information] Screen" and "3.5.2 Firmware Update"
04	September 25, 2020	Chapter 3 Chapter 4	Updated "3.3 Power Control" Updated "4.1 Command Tables"
05	November 24, 2020	Preface Chapter 2 Chapter 3 Chapter 4	Updated "Safety, Radio, and Harmonics (North America)," "Safety, Radio, and Harmonics (Europe, UK)," and "Caution Labels" Added description about screenshots and updated "2.1.1 Login" Updated "3.1 Server Status," "3.2 System Event Logs," and "3.4 Configuration" Added note on unsupported commands
06	January 28, 2021	Preface Chapter 4	Added "Taiwan" Deleted "Export Related" tables for each country and "Handling Lithium Batteries" Updated the title "4.1.6 Get Boot Script Number (NetFN: 34h, CMD: 4Fh)"
07	October 26, 2021	Preface Chapter 1 Chapter 2 Chapter 3	Updated "Compliance With Laws and Regulations in Each Country" Updated "1.1 Operating Environment" and "1.2 Various Settings" Updated "2.1 Login and Logout" Updated everything Added "3.5.3 CPU Feature Settings "

*1 The numbers/titles of the chapters/sections to which changes are made are those used in the latest version. However, the numbers/titles of the chapters/sections with an asterisk are those used in the old version.

This section describes the following:

For Your Safety

How to Use This Manual

This manual contains important information required for using this product safely. Read the *FUJITSU Supercomputer PRIMEHPC FX700 Operating Manual* (C120-0089EN), the *FUJITSU Supercomputer PRIMEHPC FX700 Getting Started Guide* (C120-0093XA), the *FUJITSU Supercomputer PRIMEHPC FX700 Safety and Regulatory Information* (C120-0092XA), the *FUJITSU Supercomputer PRIMEHPC FX700 BMC User's Guide* (C120-0091EN), and the *FUJITSU Supercomputer PRIMEHPC FX700 Upgrade and Maintenance Manual* (C120-0090EN) thoroughly before using this product. Before attempting to operate this device, carefully read and understand each manual, paying particular attention to the safety precautions.
Be sure to keep this manual in a safe and convenient location for quick reference.
Fujitsu makes every effort to prevent injury to users and bystanders as well as property damage. Be sure to use the product in accordance with the instructions in the manual.

Notes on This Product

This product is designed and manufactured for use in standard applications such as office work, personal devices, and general industrial use. The product is not intended for special uses (nuclear-reactor control in atomic energy facilities, aeronautic and space systems, air traffic control, operation control in mass transit systems, life support, or missile launch controls) where particularly high reliability requirements exist, where the pertinent levels of safety are not guaranteed, or where a failure, an operational error, or some other factor could be life-threatening or cause a physical injury (referred to below as "high-risk" use). Customers considering the use of this product for high-risk applications must have safety-assurance measures in place beforehand. Moreover, they are requested to consult our sales representative before embarking on such specialized use.

Compliance With Laws and Regulations in Each Country

The FX700 system complies with the laws and regulations listed below.

North America

Safety, Radio, and Harmonics (North America)

Certified Standard	Standard Number	Safety	Radio	Harmonics
UL	ANSI/UL 60950-1, 2nd Ed., 2014-10-14 ANSI/UL 62368-1, 2nd Ed., 2014-12-01	✓		
FCC	FCC Part-15 Subpart-B (2019)		✓	

Safety, Radio, and Harmonics (North America) *(continued)*

Certified Standard	Standard Number	Safety	Radio	Harmonics
CSA	CAN/CSA C22.2 No. 60950-1-07, 2nd Ed., 2014-10 CAN/CSA C22.2 No. 62368-1-14, 2nd Ed., 2014-12	✓		
ICES	ICES-003 Issue 7 (2020)		✓	

Environmental Substances (North America)

Standard Number	Energy-Saving	Environmental Substances	Recycling
Regulations on brominated flame retardants (Maine, Washington, Oregon, and Vermont in the U.S.)		✓	
Law on emission of perchloric acid compounds to the environment (California)		✓	
Proposition 65 (California)		✓	
Prohibition of Certain Toxic Substances Regulations (SOR/2012-285)		✓	

Europe, UK

Safety, Radio, and Harmonics (Europe, UK)

Certified Standard	Standard Number	Safety	Radio	Harmonics
CE, UKCA	IEC 60950-1:2005 (2nd Ed.); Am1:2009+Am2:2013 EN 60950-1:2006 +A11:2009 +A1:2010+A12:2011+A2:2013 IEC 62368-1:2014 EN 62368-1:2014+A11:2017	✓		
	EN 62479 (2010) EN 55035 (2017), +A11 (2020) EN 55032 (2015), +A11 (2020); Class A EN 55024 (2010) EN 61000-4-2 (2009) EN 61000-4-3 (2006), +A1, +A2 EN 61000-4-4 (2012) EN 61000-4-5 (2014), +A1 EN 61000-4-6 (2014) EN 61000-4-8 (2010) EN 61000-4-11 (2004), +A1 EN 300 386 V2.1.1 (2016)		✓	
	EN 61000-3-2 (2014) EN 61000-3-3 (2013)			✓

Environmental Substances and Recycling/Disposal (Europe, UK)

Standard Number	Energy-Saving	Environmental Substances	Recycling
ErP Directive (2009/125/EC)	✓	✓	✓
RoHS II (2011/65/EU)		✓	
New chemical regulation (REACH: No. 1907/2006)		✓	
Directive 2006/66/EC of the European Parliament and of the Council of 6 September 2006 on batteries and accumulators and waste batteries and accumulators and repealing Directive 91/157/EEC		✓	
Waste Electrical and Electronic Equipment Directive (WEEE Directive)			✓
European Parliament and Council Directive 94/62/EC of 20 December, 1994 on packaging and packaging waste			✓
The Ecodesign for Energy-Related Products Regulations 2010	✓	✓	✓
The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012		✓	

Japan

Safety, Radio, and Harmonics (Japan)

Certified Standard	Standard Number	Safety	Radio	Harmonics
PSE	Act on Product Safety of Electrical Appliances and Materials	✓		
VCCI	VCCI (2016)/VCCI-CISPR 32 (2016)		✓	
-	JIS C 61000-3-2 (2019)			✓

Energy-Saving, Environmental Substances, and Recycling/Disposal (Japan)

Standard Number	Energy-Saving	Environmental Substances	Recycling
Act on the Rational Use of Energy	✓		
Law Concerning the Examination and Regulation of Manufacture, etc. of Chemical Substances		✓	
Act on Promotion of Procurement of Eco-Friendly Goods and Services by the State and Other Entities (Act on Promoting Green Procurement)		✓	
Act on the Promotion of Effective Utilization of Resources			✓

South Korea

Safety, Radio, and Harmonics (South Korea)

Certified Standard	Standard Number	Safety	Radio	Harmonics
KCC	K 60950-1 (2.0) (2011-12) (PSU only)	✓		
	KN32 Class A KN35 KN61000-4-2/3/4/5/6/8/11		✓	

Recycling and Disposal (South Korea)

Standard Number	Energy-Saving	Environmental Substances	Recycling
Display rules on package separation			✓

Australia/New Zealand

Safety, Radio, and Harmonics (Australia/New Zealand)

Certified Standard	Standard Number	Safety	Radio	Harmonics
RCM	IEC 60950-1:2005 (2nd Ed.); Amd1+ Amd2 with AU,NZ deviation	✓		
	AS/NZS CISPR 32 (2015)		✓	

Taiwan

Safety, Radio, and Harmonics (Taiwan)

Certified Standard	Standard Number	Safety	Radio	Harmonics
BSMI	CNS 14336-1	✓		
	CNS 13438		✓	

Environmental Substances (Taiwan)

Standard Number	Energy-Saving	Environmental Substances	Recycling
Taiwan RoHS		✓	

Regulatory Compliance Statements

The applicable regulatory compliance statements provided for this product are as follows:

- Voluntary Control Council for Interference (VCCI) - Japan

Be sure to read the notices on this product before installing the product.
The notices on the product are shown below.

- VCCI Class A Notice

> This equipment is Class A information technology equipment. Operation of this equipment in a residential area may cause radio interference, in which case the user may be required to correct the interference at the user's own expense.
>
> VCCI-A

Regulations

This section describes the applicable regulations.

CE Compliance

The system complies with the requirements of European regulations.

CAUTION

This product is a Class A product. Operation of this product in a residential area may cause radio frequency interference,
in which case the user will be required to correct the interference at the user's own expense.

FCC Class A Declaration of Conformity

The device may be marked with an FCC declaration, which would apply to the equipment covered in this document unless otherwise specified herein. The declaration for other products will appear in the accompanying documentation.

CAUTION

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules, and meets all requirements of the Canadian Interference-Causing Equipment Standard (ICES-003) for digital apparatus. These regulations are designed to provide reasonable protection against radio interference when the equipment is operated in a residential installation. This product generates, uses, and can radiate radio frequency energy and, if not installed and used in strict accordance with the instructions, may cause harmful interference to radio communications. However, there is no warranty that interference will not occur in the conditions at a particular installation. If the product causes harmful interference to radio or television reception (which can be confirmed by switching the equipment on and off), the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit separate from that connected to the receiver.
- Consult a reseller or experienced radio/TV technician for support.

Fujitsu is not responsible for any radio or television interference caused by unauthorized modification of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Fujitsu. The user shall be responsible for correcting the interference caused by such unauthorized modification, substitution, or attachment.
The use of shielded I/O cables is required when connecting the equipment to any optional peripheral or host device. Failure to use shielded I/O cables may violate FCC and ICES regulations.

Manuals in This Series

The documentation can be found online.
For the Japanese market
https://www.fujitsu.com/jp/products/computing/servers/supercomputer/downloads/
For the global market
https://www.fujitsu.com/global/products/computing/servers/supercomputer/documents/
See the following table for an overview of the documentation.

Document	Manual Code	Description
FUJITSU Supercomputer PRIMEHPC FX700 Operating Manual	C120-0089EN	Contains information about how to install, set up, and operate the device. (Provided online)
FUJITSU Supercomputer PRIMEHPC FX700 Upgrade and Maintenance Manual	C120-0090EN	Contains device upgrade procedures and replacement procedures for faulty hardware. (Provided online)
FUJITSU Supercomputer PRIMEHPC FX700 BMC User's Guide	C120-0091EN	Contains information about the BMC (Baseboard Management Controller), which manages the condition of the device. (Provided online)
FUJITSU Supercomputer PRIMEHPC FX700 Safety and Regulatory Information	C120-0092XA	Contains important safety information. (Provided online and as print version)
FUJITSU Supercomputer PRIMEHPC FX700 Getting Started Guide	C120-0093XA	Describes how to access the reference manuals and other important information after unpacking the equipment. (The manual is supplied with the product.)

Storage of Accessories

Keep the accessories in a safe place because they are required for FX700 main unit operation.

Notation

This document uses the following fonts and symbols to indicate special meanings.

Font or Symbol	Meaning	Example
AaBbCc123	Indicates what is input by users and displayed on screens. This font is used to indicate command input examples.	`# adduser jsmith`

AaBbCc123	Indicates the names of commands, files, and directories output by the computer and displayed on screens.
	This font is used to indicate command output examples in boxes.
		`Shell> showinfo`
		.
		.
		`M.2 Slot Device Status: PASS`

Italics	Indicates the name of a referenced manual.	See the *FUJITSU Supercomputer PRIMEHPC FX700 BMC User's Guide*.
" "	Indicates the title of a referenced chapter, section, or subsection.	See "Chapter 4 Operation."

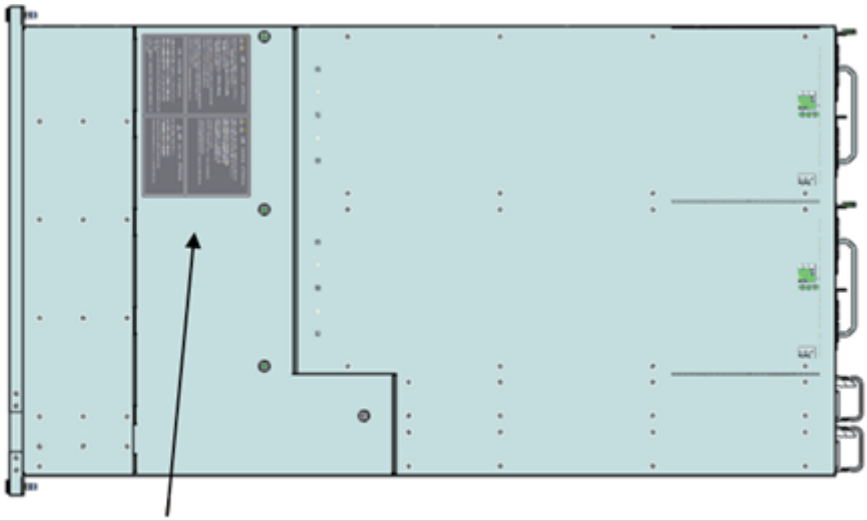
Caution Labels

Caution labels are affixed to this product.

CAUTION

Never peel off the labels.

Main Unit (Top)



感電 触电 注意 CAUTION ATTENTION

保守する前に、すべての電源コードを抜いてください。
（ただし、活性保守時はこの限りではない。）

在进行维护工作之前,请从插座上拔掉所有电源线。
（带电维护不在此范围内）

在進行維護工作之前,請從插座上拔掉所有電源線。
（帶電維護不在此範圍內）

DISCONNECT ALL POWER SUPPLY CORDS BEFORE SERVICE TO AVOID ELECTRIC SHOCK.
(EXCEPT FOR ACTIVE MAINTENACE.)

DEBRANCHER TOUS LES CORDONS D'ALIMENTATION AVANT LA MAINTENANCE POUR PREVENIR LES CHOCS ÉLECTRIQUES.
(EXCEPTÉ LORS DE LA MAINTENANCE ACTIVE.)

感電 触电 注意 CAUTION ATTENTION

内部には高電圧部分があり、感電する恐れがあります。
保守担当者以外の方は内部に触れないでください。

装置内有高电压部分,有引起触电的危险。
除保养担当者之外,请勿触摸装置内部。

裝置內有高壓部分,有引起觸電的危險。
除保養擔當者外,請勿觸摸裝置內部。

HAZARDOUS VOLTAGE.
SERVICE ENGINEER ONLY TOUCH THE INSIDE.

TENSIONS DANGEREUSES.
SEUL UN INGÉNIEUR PEUT VÉRIFIER L'INTÉRIEUR.

注意 CAUTION ATTENTION

本機器を搭載する前に、設置マニュアルをみてください。

请务必先阅读本装置安装手册之后,再进行机器的安装。

請務必先閱讀本裝置安裝手冊之後,再進行機器的安裝。

SEE INSTALLATION INSTRUCTIONS BEFORE INSTALLING THIS UNIT.

VOIR LE MANUEL D'INSTRUCTIONS AVANT D'INSTALLER CET UNITÉ.

注意 CAUTION ATTENTION

保守時は静電気を除去すること。

维护保养时必须佩带防静电腕带。

維護保養時必須佩帶防靜電腕帶。

ELECTROSTATIC SENSITIVE DEVICES.

CIRCUITS SENSIBLES A L'ELECTRICITÉ STATIQUE.

Trademarks

- Company names and product names are the trademarks or registered trademarks of their respective owners.
- Trademark indications (TM, (R)) are omitted for some system and product names in this document.

Notes on Product Handling

Maintenance

WARNING

Ask a certified service engineer or our sales representative to perform the inspection and repair work for this product and the optional products provided by Fujitsu. The work must not be done by the customer under any circumstances. Otherwise, electric shock, injury, or fire may result.

Modifying or Recycling the Product

CAUTION

Modifying this product or recycling and using a secondhand product may result in personal injury to users and/or bystanders or damage to the product and/or other property.

Disposal or Recycling of Products That Have Completed Their Life Cycle

Waste must be disposed of in a professional and responsible way in accordance with environmental regulations. For details, please contact your nearest environmental authority or our sales representative.

Contents

Figure Table Contents

Figure Contents

Table Contents

Chapter 1 Environment and Settings for Using the Web GUI

This chapter describes the environment for operating the BMC over the Web.

1.1 Operating Environment

This section outlines the Web GUI operating environment of the BMC.

1.1.1 OS and Browser

For the supported operating systems and browsers, see "Table 1.1 Correspondence Between Supported Operating Systems and Browsers."
The protocols supported in the browsers are http and https.
The operation of the Web GUI may vary depending on the browser used.

Table 1.1 Correspondence Between Supported Operating Systems and Browsers

		Browser	
		Microsoft Internet Explorer 11 or later	**Google Chrome 87 or later**
OS	Windows 8.1 or later	Supported	Supported (HCP 2000 or later)
	Red Hat Enterprise Linux 8.1 or later	Not supported	Supported (HCP 2000 or later)

1.1.2 Language

Web GUI screens: English
REMCS screens: English and Japanese
Since the following areas appear in the browser, their display language depends on the language settings in the OS:
- Dialog box titles
- Buttons for file selection fields

1.2 Various Settings

This section describes settings for using the Web GUI of the BMC.

1.2.1 Browser Settings

- Microsoft Internet Explorer Settings

- To use JavaScript, enable JavaScript in the browser.
- To use browser pop-ups, disable the pop-up blocker in the browser.
- To use cookie-based authentication, enable [Override automatic cookie handling].
- Uncheck to disable [Display intranet sites in Compatibility View].

- Google Chrome Settings

- To use JavaScript, allow [JavaScript].
- To use browser pop-ups, allow [Pop-ups and redirects].
- To use cookie-based authentication, set [Allow all cookies].

1.2.2 Network Settings

[Energy Efficient Ethernet] must be disabled in the settings.

Chapter 2 Basic Web GUI Operations and Behavior

This chapter describes the screen configuration and logging in and out on Web screens for operating the BMC.

Remarks

The Web GUI screens are examples and may differ from the actual screens, depending on the HCP firmware version, etc.

2.1 Login and Logout

This section describes the login and logout procedures for the Web GUI.

2.1.1 Login

1. Open the browser.
2. Enter either the standard address or the SSL address.

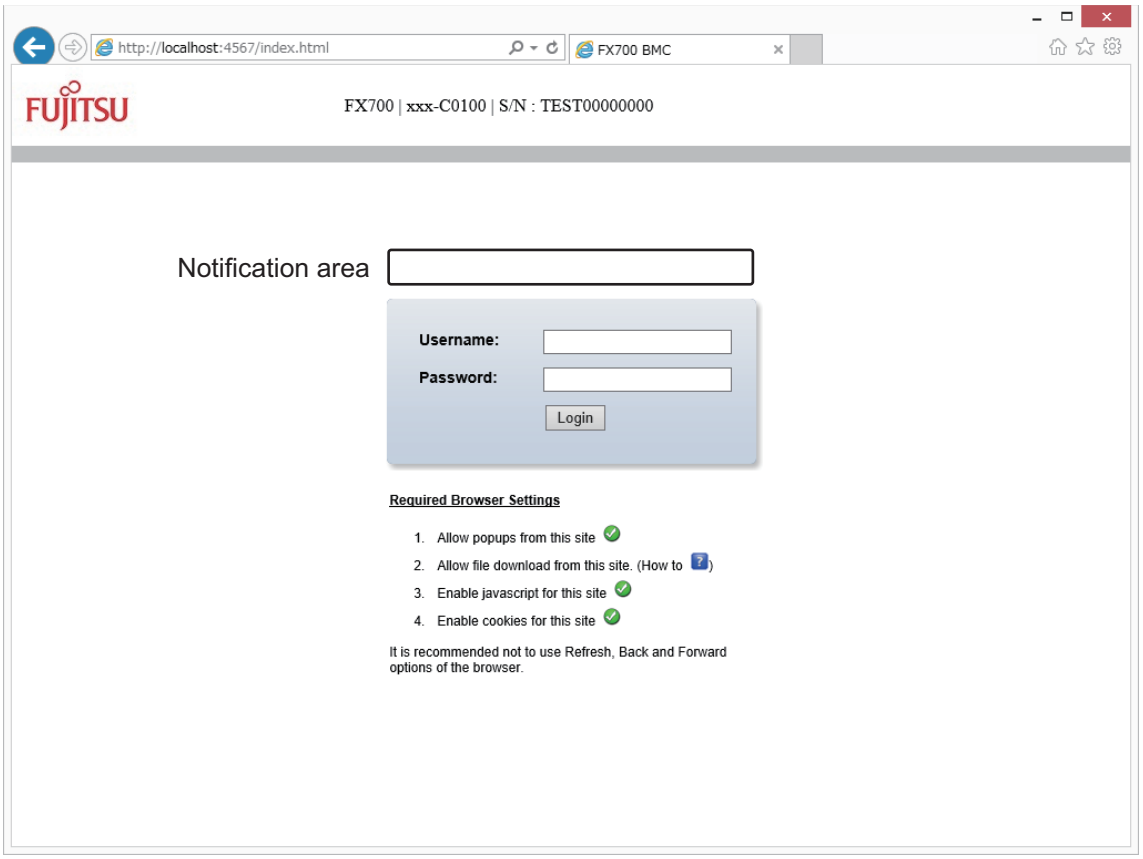
   Standard: http://nodename:adminport

   SSL: https://nodename:adminport

   - nodename
     Specify the IP address of the BMC (control port [default: DHCP] or maintenance port [default: 172.16.0.1/24]).
   - adminport
     Specify the port number assigned to the LAN port of the BMC.
     Default
     Standard: 8081
     SSL: 432

Log in to the Web GUI from the login screen.

Figure 2.1 Login Screen



You can perform the following operations on this screen.

Table 2.1 Operation Items on the Login Screen

Operation Item	Description
Username	Enter the login user name (up to 16 characters).
Password	Enter the password (up to 16 characters).
Login	Click to execute login processing. For the procedure, see "Logging In."

The accounts that can be used with the Web GUI, IPMI, and the OS console are shown below.

Table 2.2 User Accounts

Initial Username	Initial Password	IPMI Privilege	Usage
hpcmainte	HPCMAINTE	Operator	For administrators
hpcipmi	HPCIPMI	User	For users

See "Table 3.1 Web GUI Screens" for the account authority differences for the Web GUI.

Logging In

1. Fill in [Username] and [Password].
2. Click the [Login] button.

   The [FRU Information] screen appears.

Remarks

- If authentication fails, the browser returns to the login screen.
- If the user name or password contains an error, an error message appears.
- The guaranteed number of simultaneous logins is 9.
- You will be automatically logged out after 30 minutes of inactivity.
- Multiple accesses from the same PC are not supported.

This screen displays the following items.

Table 2.3 Display Items on the Login Screen

Display Item	Details of Display
(Notification area)	Displays an error message when login authentication has failed. The area is blank when no error has occurred.
Required Browser Settings	Displays the results of an operating environment check. - Allow popups from this site Result from a check of whether pop-ups are allowed - Allow file download from this site. (How to) How to allow download Click to display help (See "Help Screen") - Enable JavaScript for this site Result from a check of whether JavaScript is enabled - Enable cookies for this site Result from a check of whether cookies are enabled
It is recommended not to use Refresh, Back and Forward options of the browser.	Displays a precaution on using the Web GUI.

The meaning represented by an [icon] is as follows.

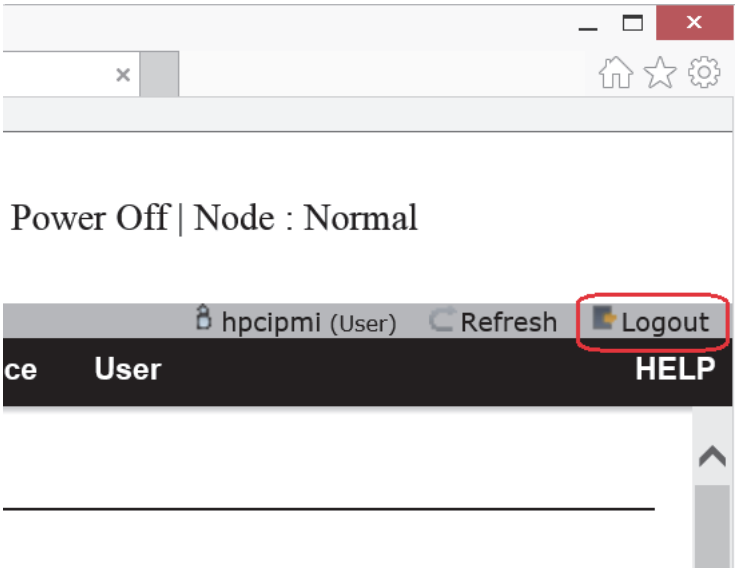
Table 2.4 Icons on the Screen

Icon	Meaning
	OK
	Not acceptable
	Used to display the help screen

2.1.2 Logout

Disconnect a session and log out.

Figure 2.2 [Logout] Button



You can perform the following operation.

Table 2.5 [Logout] Button

Operation Item	Description
Logout	Click to execute logout processing. For the procedure, see "Logging Out."

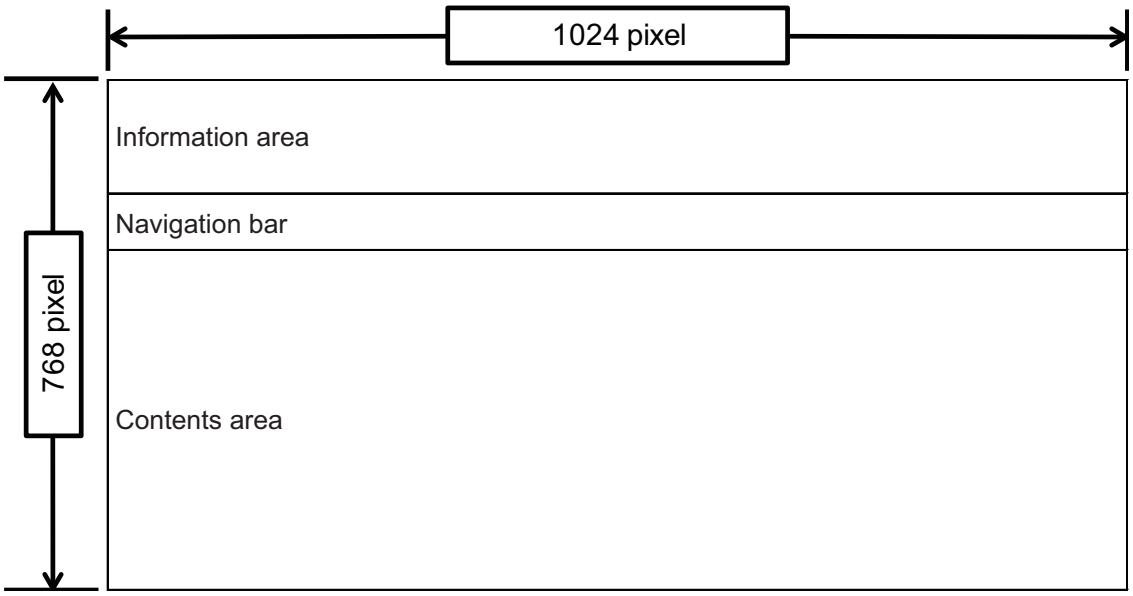
Logging Out

1. Click the [Logout] button to log out.

2.2 Description of Web GUI Screens

This section shows the screen configuration and size.

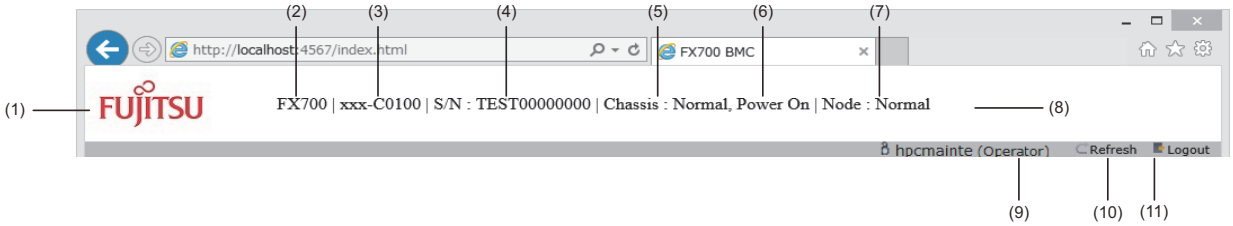
Figure 2.3 Screen Configuration and Size



Information Area

This area displays the following content.

Figure 2.4 Information Area



	Item Name	Description	Display Condition
(1)	Logo	Displays the Fujitsu logo.	
(2)	Series Name	Displays the series name that is set for the chassis.	
(3)	Chassis Name	Displays the FX700 main unit name that is set for the chassis.	Always displayed
(4)	Serial Number	Displays after "S/N:" the serial number that is set for the chassis.	Always displayed

	Item Name	Description	Display Condition
(5)	Chassis Status	Displays after "Chassis:" any of the following: - Normal - Warning - Alarm - ReservedAlarm - EPO (Emergency Power Off)	Not displayed on the login screen
(6)	Chassis Power Status	Displays the power supply status of the chassis. - Power On - Power Off	Not displayed on the login screen
(7)	Node Status	Displays after "Node:" the most significant error among all nodes. The priority of display is in the order shown below according to the severity for node replacement: - RouterEAlarm (Router Emergency Alarm) - Alarm - ReservedAlarm - ResetRequest-U - ResetRequest-C - Warning - Normal	Not displayed on the login screen
(8)	Maintenance Status	Displays the maintenance status. - Cold Maintenance - Warm Maintenance **Remarks** "Warm Maintenance" or "Cold Maintenance" is displayed when maintenance mode is set. Also, the entire Information area is displayed in orange.	Displayed during maintenance
(9)	Login User	Displays the user name and authority.	Not displayed on the login screen
(10)	Refresh	Click to update the screen display.	Not displayed on the login screen
(11)	Logout	Click to log out.	Not displayed on the login screen

Navigation Bar

Selecting a menu will display a description in the content area.

Content Area

This area displays help or the page selected on the menu of the navigation bar under the Information area. The Error Status background color and text color indicate the status as follows.

Table 2.6 Error Status Background and Text Colors

Status	Background Color	Text Color
Normal	Page background color	Black
Warning	Yellow	Black
Failure	Red	White
Not mounted	Gray	White

Screen Information Updates

The status of the Information area is automatically updated every 10 seconds. The content area is not automatically updated.
To manually obtain the latest information, perform either of the following operations.
- Click the [Refresh] button.
- Select the same menu again from the navigation bar.

Help Screen

Click HELP on the navigation bar to display the help screen.
To exit the help menu, click the [x] button of the help screen.

Chapter 3 Web GUI Functions

This chapter shows Web GUI categories and screens, and describes their functions.
The term HCP**** refers to the version number of the HCP firmware (****: 4-digit number).

The following table lists BMC screens.

Table 3.1 Web GUI Screens

Category Name	Screen Name	Authority		Description
		Operator	User	
Server Status	FRU Information	Display	Display	Display the serial number, part number, and other information on each unit.
	CMU Information	Display	Display	Display the CMU/node status.
System Event Logs	System Event Logs	Display/ Operate	Display/ Operate	- Instruct that a snapshot be collected. / Download a snapshot. - Download an environment log. - Display System Event Log information. - Download System Event Log information. - Display another supplementary log.
Power Control	Power Control	Display/ Operate	Display/ Operate	- Instruct that node power be turned on/off. - Display the status of each node.
Configuration	Chassis Settings	Display/ Operate	Display	- Display/Set the FX700 main unit name. - Display/Set the altitude.
	Services	Display/ Operate	Display	- Display/Set whether the http/https/ssh/ snmp service is enabled/disabled. - Display/Set the port number of each service.
	Network Settings	Display/ Operate	Display	- Display/Set an IP address and net mask. - Display/Set routing information.
	Time Settings	Display/ Operate	Display	- Display/Set the date and time. - Display/Set time zone information. - Instruct synchronization with the NTP server. - Display/Set the NTP server.
	SNMP Trap Settings	Display/ Operate	Display	Display/Set SNMP traps.

Table 3.1 Web GUI Screens *(continued)*

Category Name	Screen Name	Authority		Description
		Operator	User	
	SSL Certificate Configuration	Display/ Operate	Display	- Upload a signed Web server certificate. - Upload a private key of a Web server. - Display CSR content.
Maintenance	Maintenance	Display/ Operate	Display	- Instruct that maintenance mode be started/ended. - Issue a CMU/PSU power operation instruction.
	Firmware Update	Display/ Operate	Display	- Display the current firmware version. - Upload a firmware image. - Apply a firmware image.
	CPU Feature Settings	Display/ Operate	Display	Display/Set the Speculative store bypass disable (SSBD).
	REMCS	Display/ Operate	-	- Display the [REMCS] screen - Set REMCS
	REMCS Detail Setup	Display/ Operate	-	Display the [REMCS Detail Setup] screen
User	User Admin	Display/ Operate	Display/ Operate	- Display/Change a user name. - Change a password. (Can change only own users)
	One Time Password	Display/ Operate	Display	Issue a One Time Password.

3.1 Server Status

This category mainly provides functions to display the hardware information for the device.

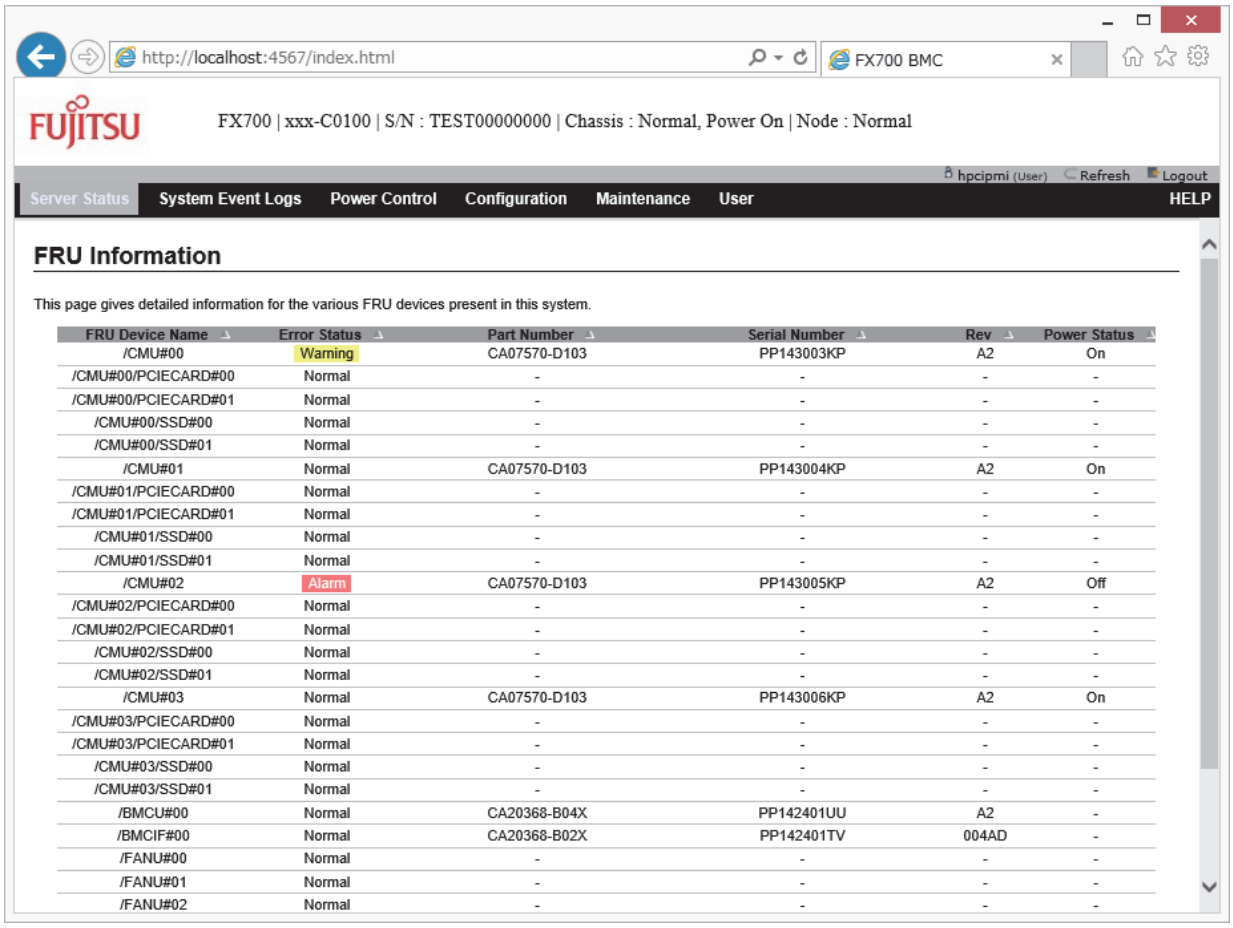
3.1.1 FRU Information

On the [FRU Information] screen, you can check the serial number, version number, failure status, and power supply status of each unit.

Remarks

- The screen displays "Not-Present" for parts not yet mounted.
- For details on the status indicated by the Web screen background color, see "Table 2.6 Error Status Background and Text Colors."

Figure 3.1 [FRU Information] Screen



FRU Device Name	Error Status	Part Number	Serial Number	Rev	Power Status
/CMU#00	Warning	CA07570-D103	PP143003KP	A2	On
/CMU#00/PCIECARD#00	Normal	-	-	-	-
/CMU#00/PCIECARD#01	Normal	-	-	-	-
/CMU#00/SSD#00	Normal	-	-	-	-
/CMU#00/SSD#01	Normal	-	-	-	-
/CMU#01	Normal	CA07570-D103	PP143004KP	A2	On
/CMU#01/PCIECARD#00	Normal	-	-	-	-
/CMU#01/PCIECARD#01	Normal	-	-	-	-
/CMU#01/SSD#00	Normal	-	-	-	-
/CMU#01/SSD#01	Normal	-	-	-	-
/CMU#02	Alarm	CA07570-D103	PP143005KP	A2	Off
/CMU#02/PCIECARD#00	Normal	-	-	-	-
/CMU#02/PCIECARD#01	Normal	-	-	-	-
/CMU#02/SSD#00	Normal	-	-	-	-
/CMU#02/SSD#01	Normal	-	-	-	-
/CMU#03	Normal	CA07570-D103	PP143006KP	A2	On
/CMU#03/PCIECARD#00	Normal	-	-	-	-
/CMU#03/PCIECARD#01	Normal	-	-	-	-
/CMU#03/SSD#00	Normal	-	-	-	-
/CMU#03/SSD#01	Normal	-	-	-	-
/BMCU#00	Normal	CA20368-B04X	PP142401UU	A2	-
/BMCIF#00	Normal	CA20368-B02X	PP142401TV	004AD	-
/FANU#00	Normal	-	-	-	-
/FANU#01	Normal	-	-	-	-
/FANU#02	Normal	-	-	-	-

The [FRU Information] screen displays the following items.

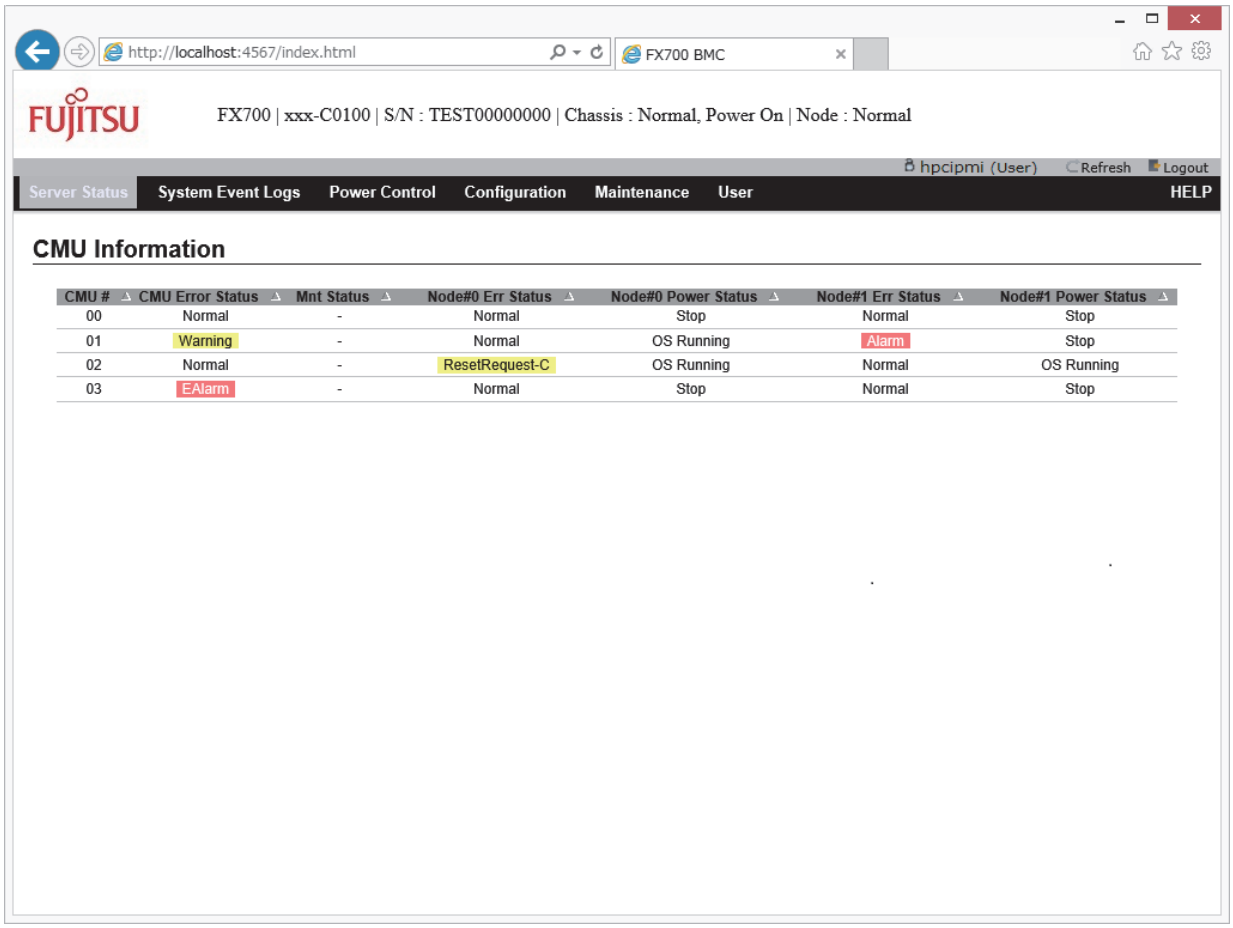
Table 3.2 Display Items on the [FRU Information] Screen

Display Item	Details of Display
FRU Device Name	Displays the names of the FRUs.
Error Status	Displays the operating status of each FRU: - Normal (Normal) - Warning (Warning) - Alarm (Failure) - EAlarm (Failure) - AC-Lost (Failure) - Not-Present (Not mounted) - Unknown (Normal) (Displayed when Error Status retrieval failed) For details on background colors displayed to indicate the status, see "Table 2.6 Error Status Background and Text Colors." **Remarks** If the FRU is not mounted (Not-Present) or unknown, "-" is displayed and grayed out in the columns after [Part Number].
Part Number	Displays the part numbers of the FRUs (CMU, BMCU, BMCIF).
Serial Number	Displays the serial numbers of the FRUs (CMU, BMCU, BMCIF).
Rev	Displays the version numbers of the FRUs (CMU, BMCU, BMCIF).
Power Status	Displays the power supply status.

3.1.2 CMU Information

On the [CMU Information] screen, you can check CMU failure information, the maintenance status, and the operating status of nodes in the CMU.

Figure 3.2 [CMU Information] Screen



The [CMU Information] screen displays the following.

Table 3.3 Display Items on the [CMU Information] Screen

Display Item	Details of Display
CMU #	Displays the CMU numbers.
CMU Error Status	Displays the operating status of each CMU: - Normal (Normal) - Warning (Warning) - Alarm (Failure) - EAlarm (Failure) - Not-Present (Not mounted) - Unknown (Normal) (Displayed when Error Status retrieval failed) For details on background colors displayed to indicate the status, see "Table 2.6 Error Status Background and Text Colors."
Mnt Status	Displays the maintenance status: - On: Warm maintenance in progress - − : Other than the above - Unknown: Displayed when Mnt Status retrieval failed

Table 3.3 Display Items on the [CMU Information] Screen *(continued)*

Display Item	Details of Display
Node#0 Err Status	Displays the operating status of Node#0 (node on the CPU#0 side) in the CMU: - Normal (Normal) - Warning (Warning) - ReservedAlarm (Failure) - ResetRequest-C (Warning) - Alarm (Failure) - RouterEAlarm (Failure) - ResetRequest-U (Failure) - Unknown (Normal) (Displayed when Error Status retrieval failed) For details on background colors displayed to indicate the status, see "Table 2.6 Error Status Background and Text Colors."
Node#0 Power Status	Displays the operating status of Node#0 (node on the CPU#0 side) in the CMU: - Stop - Reset - POST - OS Booting - OS Running - OS Shutdown - OS Panic - UEFI Shell - Unknown (Displayed when Error Status retrieval failed)
Node#1 Err Status	Displays the operating status of Node#1 (node on the CPU#1 side) in the CMU: - Normal (Normal) - Warning (Warning) - ReservedAlarm (Failure) - ResetRequest-C (Warning) - Alarm (Failure) - RouterEAlarm (Failure) - ResetRequest-U (Failure) - Unknown (Normal) (Displayed when Error Status retrieval failed) For details on background colors displayed to indicate the status, see "Table 2.6 Error Status Background and Text Colors."

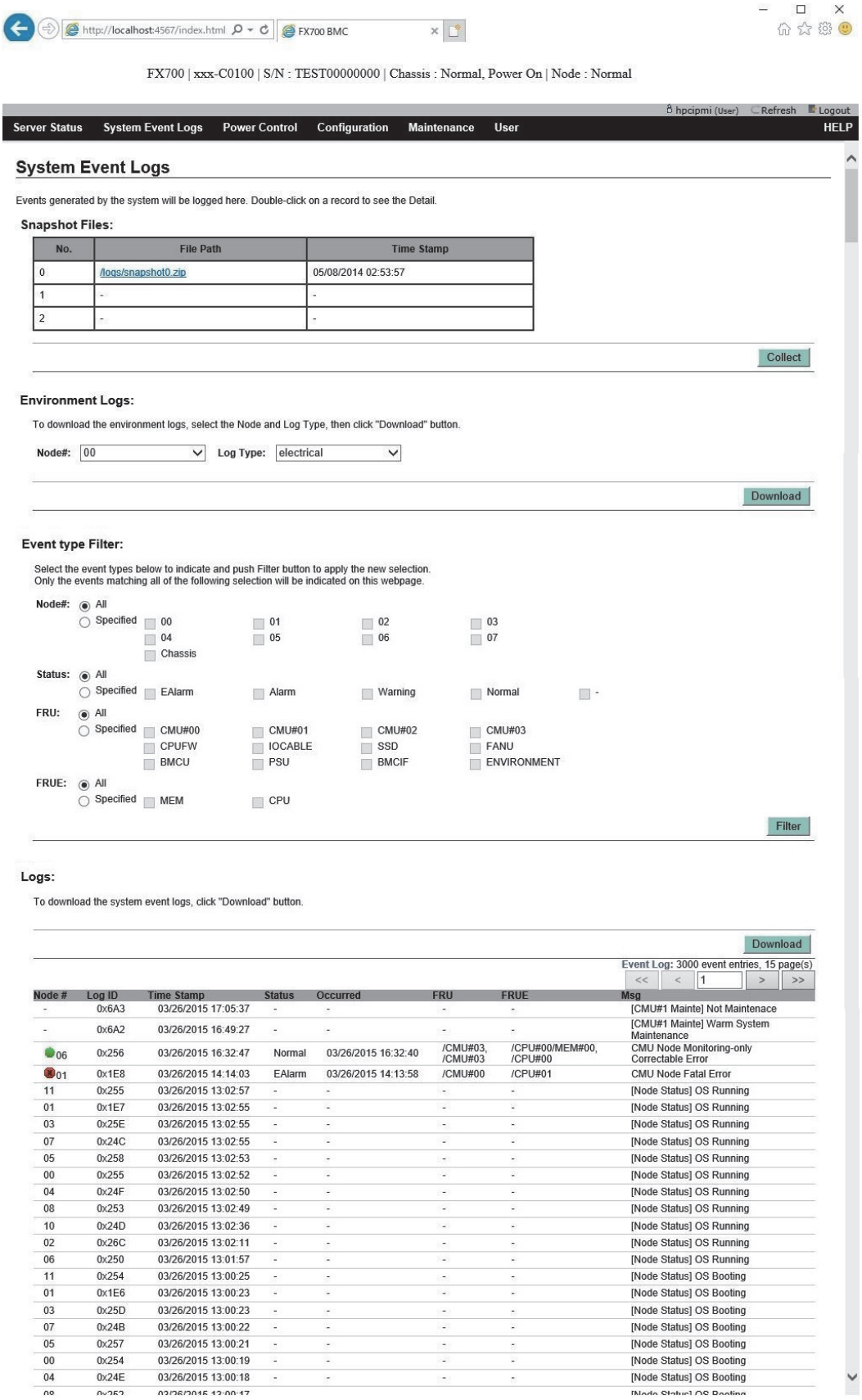
Table 3.3 Display Items on the [CMU Information] Screen *(continued)*

Display Item	Details of Display
Node#1 Power Status	Displays the operating status of Node#1 (node on the CPU#1 side) in the CMU: - Stop - Reset - POST - OS Booting - OS Running - OS Shutdown - OS Panic - UEFI Shell - Unknown (Normal) (Displayed when Error Status retrieval failed)

3.2 System Event Logs

On the [System Event Logs] screen, you can check events that occurred in the device. You can also check details by double-clicking a displayed event log.

Figure 3.3 [System Event Logs] Screen



You can perform the following operations on the [System Event Logs] screen.

Table 3.4 Operation Items on the [System Event Logs] Screen

Operation Item	Description
Collect	Collect a snapshot. For the procedure, see "Collecting a Snapshot."
Download (Environment Logs)	Download an environment log. For the procedure, see "Downloading an Environment Log."
Filter	Redisplay a list of events according to the specified filter conditions. For the procedure, see "Redisplaying a List of Events According to the Specified Filter Conditions."
Download (Logs)	Download an event log. For the procedure, see "Downloading an Event Log."

Collecting a Snapshot

A snapshot is used to investigate in detail a hardware failure.
Contact the nearest Fujitsu service center about "Table 3.5 Specifying the Snapshot to Collect" when collecting a snapshot.

Note

- Collecting a snapshot takes time. Furthermore, while collecting a snapshot, you cannot collect a new snapshot.

Remarks

- The [System Event Logs] screen displays up to 3,000 events, starting with the latest ones. To check all events, collect a snapshot and download the file.

1. Click the [Collect] button.

   The snapshot collection dialog box appears.

Figure 3.4 Snapshot Collection Dialog Box

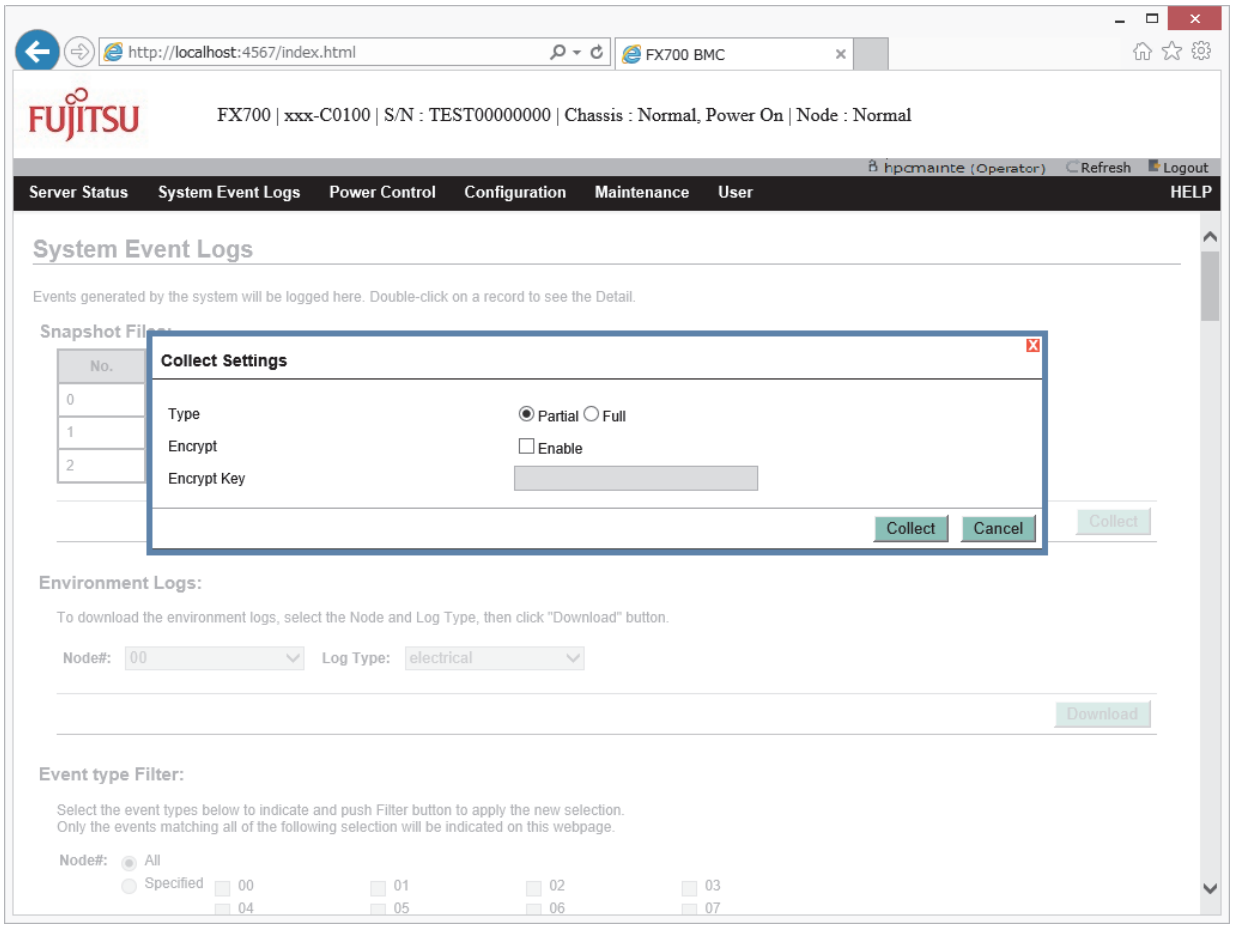


Table 3.5 Specifying the Snapshot to Collect

Input Item	Description
Type	Specify the type of collection: - Partial - Full
Encrypt	To use encryption, check the [Enable] check box.
Encrypt Key	If the [Enable] check box in [Encrypt] is checked, specify an encryption key with 1 to 63 single-byte characters, which may be or the following: ! # $ % * + , - . / : = ? @ [ ] ^ _ { } ~

2. Specify the type of collection, whether to use encryption, etc., and click the [OK] button.

   The execution result dialog box appears.

3. Click the [OK] button.

   The browser returns to the [System Event Logs] screen.

4. Under [File Path] in [Snapshot Files:], click the snapshot file to download.

Downloading an Environment Log

An environment log is used to investigate in detail a hardware failure.
Contact the nearest Fujitsu service center when downloading an environment log.

1. In [Environment Logs:], specify the environment log to download.

Table 3.6 Specifying the Environment Log to Download

Input Item	Description
Node#	Specify the node or chassis of the environment log to download.
Log Type	Specify the type of environment log to download: - electrical (Voltage/Current log of power supply parts, or PSU voltage or current-related log) - environment (Temperature log of power supply parts, or PSU temperature information log and PSU FAN information log) - inlet thermal (intake air temperature log. Only chassis can be specified)

2. Click the [Download] button.

   The environment log is downloaded, and the browser returns to the [System Event Logs] screen.

Redisplaying a List of Events According to the Specified Filter Conditions

[Logs:] on the [System Event Logs] screen displays up to 3,000 events, starting with the latest ones, from the registered event logs. Out of 3,000 events displayed from event logs in [Logs:] on the [System Event Logs] screen, you can extract the events that satisfy the specified filter conditions by using the filter function.

1. Specify filter conditions.

Table 3.7 Filter Conditions of the Event Type Filter

Input Item	Description
Node#	Specify filter conditions (Node): - All - Specified (00 to 07 and Chassis can be selected)
Status	Specify filter conditions (Status): - All - Specified (EAlarm, Alarm, Warning, Normal, and - (hyphen) can be selected)
FRU	Specify filter conditions (FRU): - All - Specified (CMU#00, CMU#01, CMU#02, CMU#03, CPUFW, IOCABLE, SSD, FANU, BMCU, PSU, BMCIF, and ENVIRONMENT can be selected)
FRUE	Specify filter conditions (FRUE): - All - Specified (CPU and MEM can be selected)

2. Click the [Filter] button.

   The list of events is redisplayed.

[Logs:] on the [System Event Logs] screen displays the following content. One page displays up to 200 events. Click the following to display the previous and next pages:
[>]: Next page
[>>]: Last page
[<]: Previous page
[<<]: First page

Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen

Display Item	Details of Display
Node #	Displays the registration places (node or chassis) of events. - 00 to 07: Node number - - (hyphen): Chassis Furthermore, icons are displayed according to [Status]. - EAlarm:  - Alarm:  - Warning:  - Normal:  - No icon if [Status] is "-" (hyphen)
Log ID	Displays log IDs in hexadecimal notation to indicate the registration order of logs.
Time Stamp	Displays the local date and time when a snapshot was collected, in the "MM/DD/YYYY hh:mm:ss" format. - MM: Month - DD: Day - YYYY: Year - hh: Hour - mm: Minute - ss: Second
Status	Indicates the severity for FRU replacement. - EAlarm: Need to immediately stop using the corresponding suspected part and immediately replace the FRU - Alarm: Need to stop using the corresponding suspected part after the job completes, and then immediately replace the FRU - Warning: Can use the corresponding suspected part but need to replace the FRU in planned maintenance - Normal: Replacement not needed

Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen *(continued)*

Display Item	Details of Display
Occurred	Displays the local date and time when an error occurred, in the "MM/DD/YYYY hh:mm:ss" format. - MM: Month - DD: Day - YYYY: Year - hh: Hour - mm: Minute - ss: Second "-" (hyphen) is displayed when an error has not occurred.
FRU (replacement unit)	Displays up to 2 suspected units per entry, in the "1st suspected unit, <return> 2nd suspected unit" format. "-" (hyphen) is displayed when there is no suspected unit. [Example] - With 1st suspected unit only: /CMU#00 - With 2nd suspected unit too: /CMU#00, /Chassis
FRUE (suspected location for replacement unit)	Displays up to 2 suspected locations among suspected units, in the "suspected location of 1st suspected unit, <return> suspected location of 2nd suspected unit" format. "-" (hyphen) is displayed when there is no suspected location. [Example] - With 1st suspected location only: /CPU#00 - With 1st and 2nd suspected locations: /CPU#00, /SBC_N#00
Msg	Displays messages.

Double-click a specific event log in [Logs:] on the [System Event Logs] screen to display details of that event in the [Detail] dialog box.

Figure 3.5 [Detail] Dialog Box

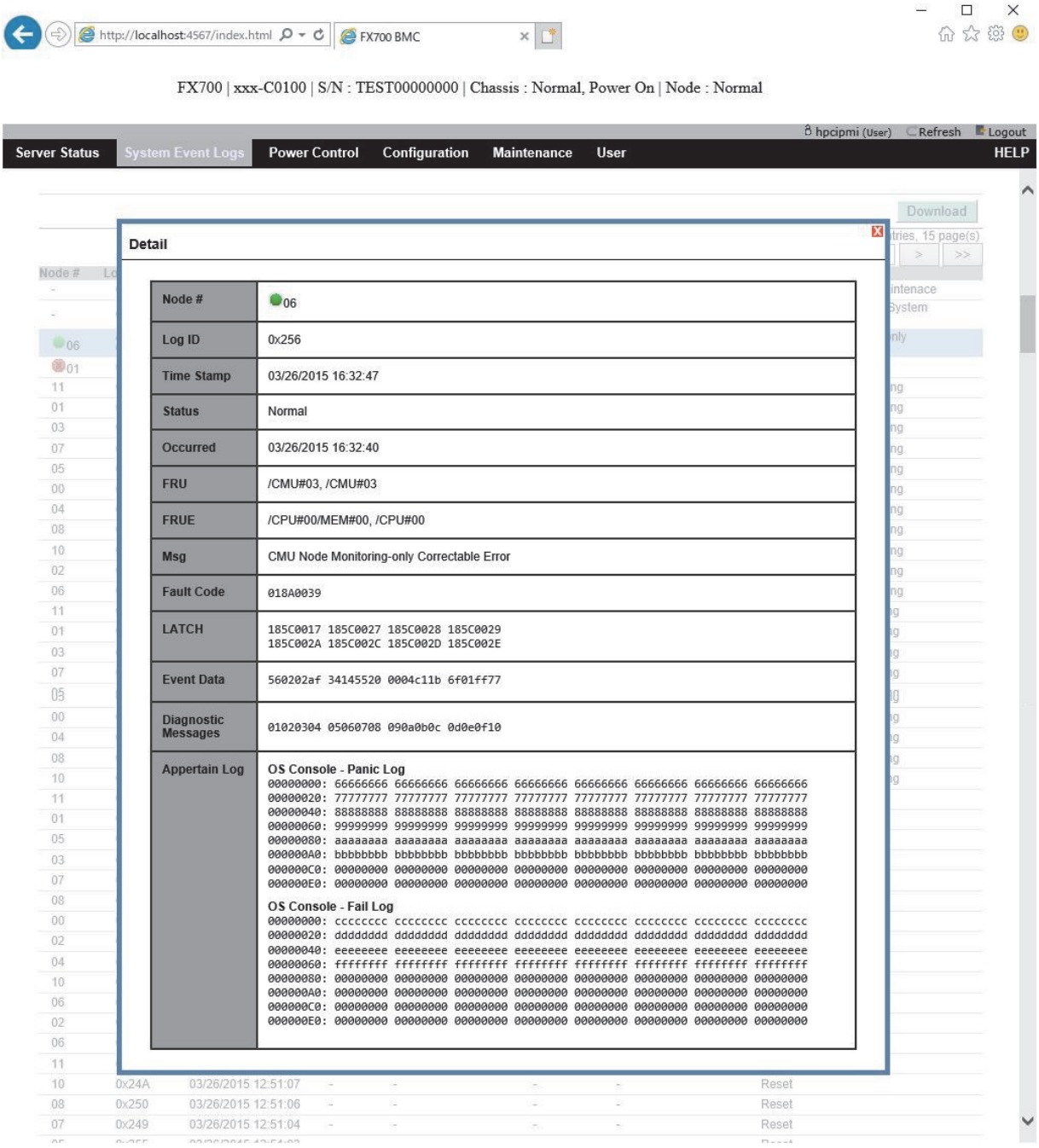


Table 3.9 Display Items in the [Detail] Dialog Box

Display Item	Details of Display
Node #	See "Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen."
Log ID	See "Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen."
Time Stamp	See "Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen."
Status	See "Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen."
Occurred	See "Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen."

Table 3.9 Display Items in the [Detail] Dialog Box *(continued)*

Display Item	Details of Display
FRU	See "Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen."
FRUE	See "Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen."
Msg	See "Table 3.8 Display Items in [Logs:] on the [System Event Logs] Screen."
Fault Code	Detail code
LATCH	Detail code
Event Data	Detail code
Diagnostic Messages	Detail code
Appertain Log	Detail code

Downloading an Event Log

You can download up to 3,000 of the latest entries, as a text file, from the registered event logs.

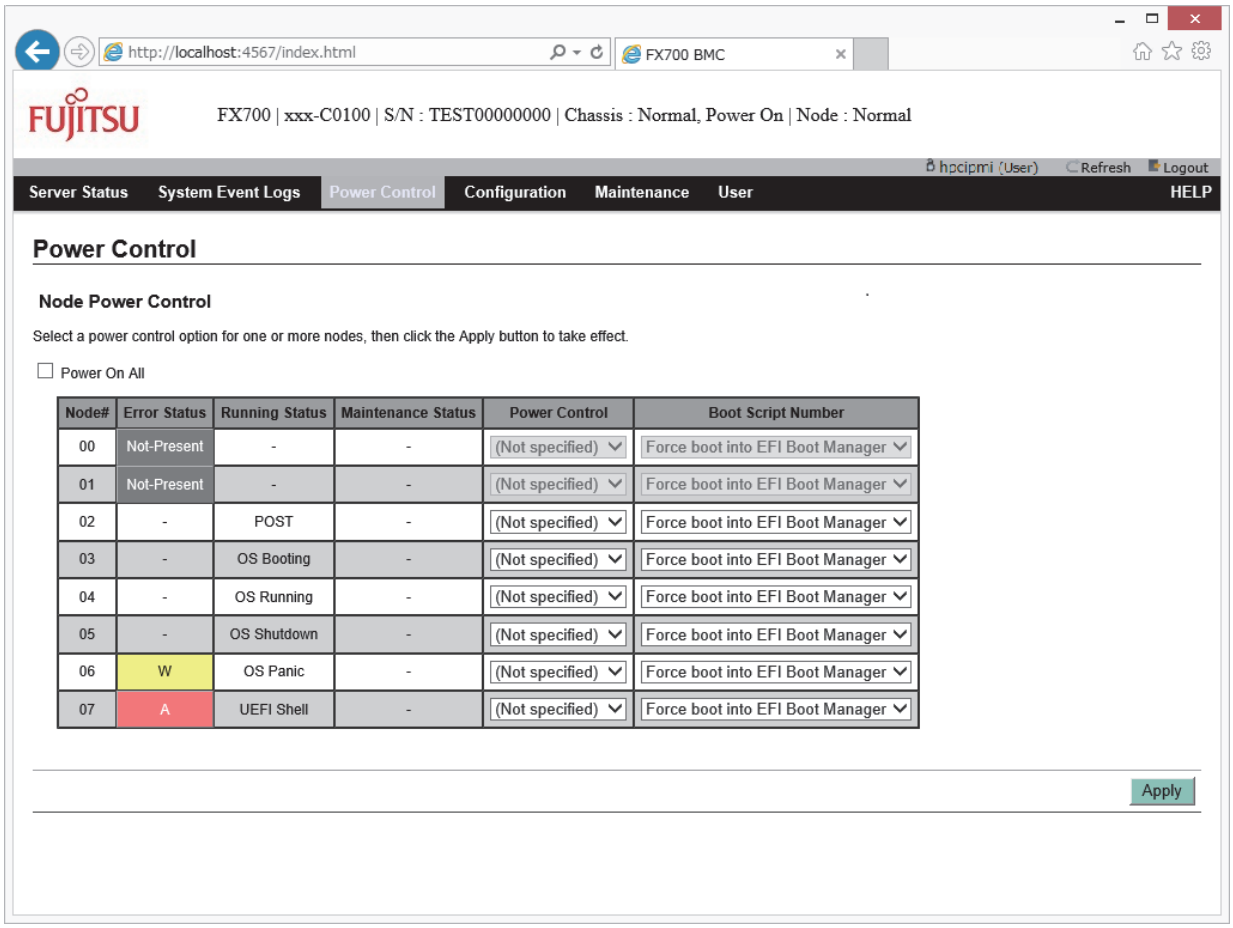
1. In [Logs:], click the [Download] button.

   The event log is downloaded, and the browser returns to the [System Event Logs] screen.

3.3 Power Control

On the [Power Control] screen, you can check and control the power supply status of nodes.

Figure 3.6 [Power Control] Screen



To check the current status (Error Status, Running Status, Maintenance Status), click the [Refresh] button to reload the screen. After the reload, the [Boot Script Number] item displays "Force boot into EFI Boot Manager."
You can perform the following operation on the [Power Control] screen.

Table 3.10 Operation Item on the [Power Control] Screen

Operation Item	Description
Apply	Change the power supply status of nodes. For the procedure, see "Changing the Power Supply Status of Nodes."

Changing the Power Supply Status of Nodes

1. Under [Power Control] and [Boot Script Number], specify power control and a boot mode, respectively, for each node.

Table 3.11 Specifying Power Control and a Boot Mode

Input Item	Description
Power On All	If the [Power On All] check box is checked, [Power On] is specified for powered-off nodes under [Power Control]. If the checked [Power On All] check box is unchecked, [Power Control] for the powered-off nodes returns to [(Not specified)].
Power Control	Specify power control for each node. **If the node has been powered off** - Power On: Issues a power-on instruction. - (Not specified): Does nothing. **If the node has been powered on** - Stop: Stops the node. - Reset: Restarts the OS on the node. - Dump Request: Issues an instruction to collect an OS dump. - OS Shutdown: Stops the OS on the node. - (Not specified): Does nothing.
Boot Script Number	Specify a boot mode for each node. - 00h: Disk boot - 01h: Not supported - 02h: For OS installation - Force boot into EFI Boot Manager: Stop at UEFI without boot - Auto select Boot Script Number: Automatically select DISK boot.

2. Click the [Apply] button.

   Confirmation dialog box appears.

3. Click the [OK] button.

   The power supply status of nodes is changed, and the browser returns to the [Power Control] screen. If the version number of the HCP firmware applied on the FX700 main unit is HCP1500 or later, the set boot mode is retained for each node after a BMC reset and even after the power cord is unplugged and replugged. To check the retained boot mode, use the Get Boot Script Number command (see "4.1 Command Tables").

   Note: The retained boot mode is also applied at the power-on time when the power button on the front panel is pressed or the Chassis Control command (see "4.1 Command Tables") is used.

The [Power Control] screen displays the following items.

Table 3.12 Display Items on the [Power Control] Screen

Display Item	Details of Display
Node#	Displays the node numbers (00 to 07).

Table 3.12 Display Items on the [Power Control] Screen *(continued)*

Display Item	Details of Display
Error Status	Displays the error status of nodes: - Normal: - (hyphen) (Normal) - ResetRequest-U: RR-U (Failure) - ResetRequest-C: RR-C (Warning) - Warning: W (Warning) - ReservedAlarm: R (Failure) - Alarm: A (Failure) - RouterEAlarm: EA (Failure) - Failure to retrieve Error Status: Unknown (Normal) - CMU not mounted: Not-Present (Not mounted) For details on background colors displayed to indicate the status, see "Table 2.6 Error Status Background and Text Colors."
Running Status	Displays the operating status of nodes: - Stop - Reset - POST - UEFI Shell - OS Booting - OS Running - OS Panic - OS Shutdown - Unknown (Failed to retrieve Running Status) - − (CMU not mounted)
Maintenance Status	Displays the maintenance status of nodes (corresponding CMUs): - On: Warm maintenance in progress - − : Other than the above - Unknown: Failed to retrieve Maintenance Status
Power Control	Displays the power control methods for nodes.
Boot Script Number	Displays the boot modes of nodes.

Remarks

- HCP 1900 or earlier
  If "00h" or "02h" is specified in [Boot Script Number] and startup fails, processing stops at UEFI.
- HCP 2000 or later
  If "00h" is specified in [Boot Script Number] and startup fails, processing stops at UEFI.
  If "02h" is specified in [Boot Script Number] and startup fails, 00h is used for startup. If startup fails even with 00h, processing stops at UEFI.
  If startup fails, the retained Boot Script Number is the number you specified when clicking the [Apply] button.

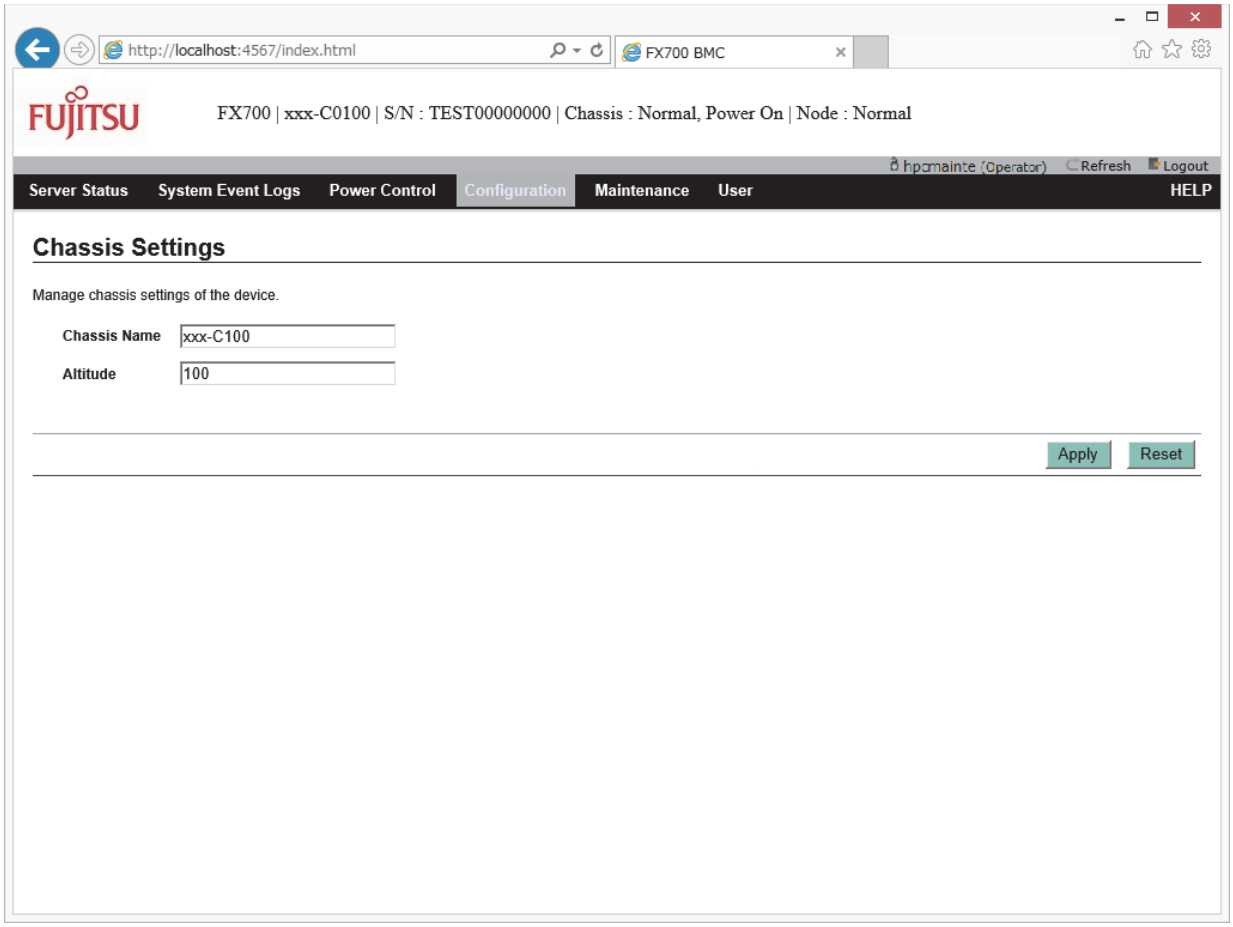
3.4 Configuration

This category provides functions related to FX700 main unit settings.

3.4.1 Chassis Settings

On the [Chassis Settings] screen, you can check and set the name and altitude of the FX700 main unit.

Figure 3.7 [Chassis Settings] Screen



You can perform the following operations on the [Chassis Settings] screen.

Table 3.13 Operation Items on the [Chassis Settings] Screen

Operation Item	Description
Apply	Change FX700 main unit information. For the procedure, see "Changing FX700 Main Unit Information."
Reset	Restore the information currently set for the FX700 main unit.

Changing FX700 Main Unit Information

1. In [Chassis Name] and [Altitude], specify the FX700 main unit name and altitude, respectively.

Table 3.14 Specifying the FX700 Main Unit Name and Altitude

Input Item	Description
Chassis Name	Specify the FX700 main unit name with 1 to 63 characters, which may be alphanumeric characters, the hyphen, or the period. Neither the hyphen nor period can be specified as the first or last character. If the original name is displayed at the input time, delete it.
Altitude	Specify an altitude between 0 and 3000. The set value will be a multiple of 100 m. If the original altitude is displayed at the input time, delete it.

2. Click the [Apply] button.

   Confirmation dialog box appears.

   Remarks

   - To restore the information currently set for the FX700 main unit, click the [Reset] button instead of the [Apply] button.

3. Click the [OK] button.

   The FX700 main unit information is changed, and the browser returns to the [Chassis Settings] screen.

The [Chassis Settings] screen displays the following items.

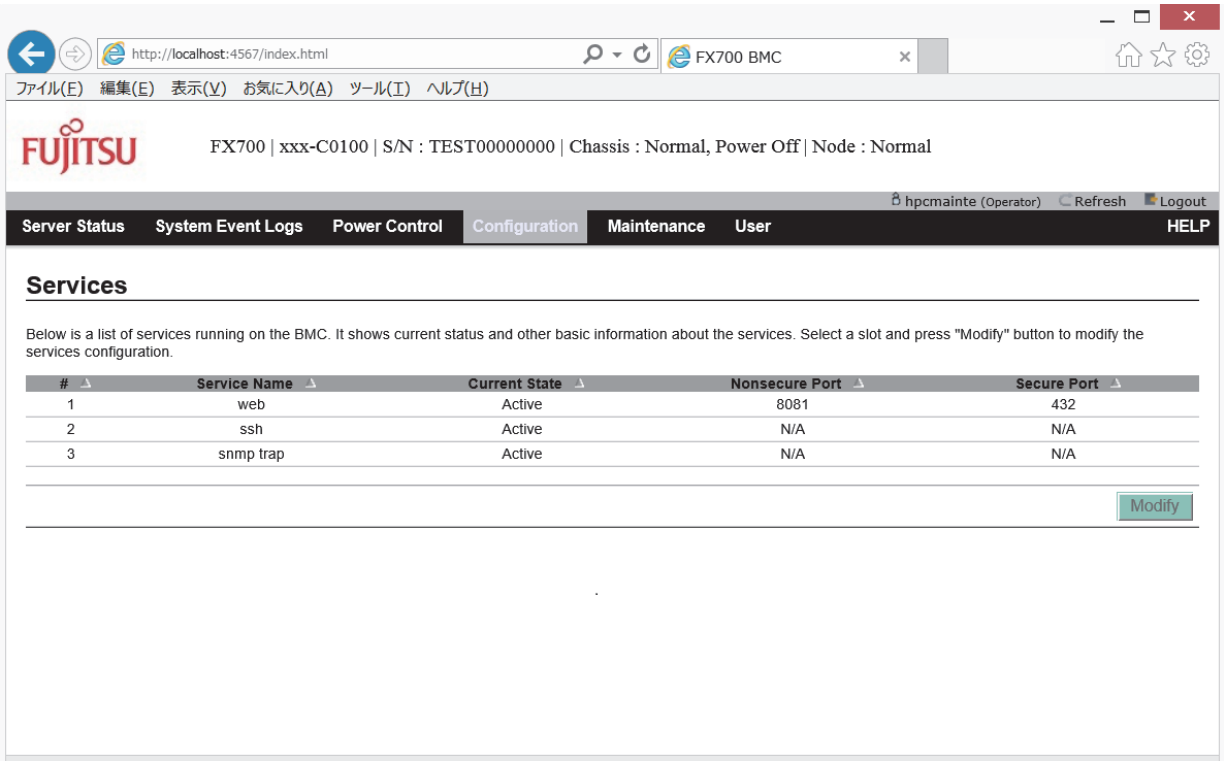
Table 3.15 Display Items on the [Chassis Settings] Screen

Display Item	Details of Display
Chassis Name	Displays the FX700 main unit name.
Altitude	Displays the altitude.

3.4.2 Services

On the [Services] screen, you can check the enable/disable setting and port number of the web, ssh, and snmp services. You can also change the port number of the web service, enable/disable the ssh service, and enable/disable the snmp service.

Figure 3.8 [Services] Screen



The [Services] screen displays the following items.

Table 3.16 Display Items on the [Services] Screen

Display Item	Details of Display
Service Name	Displays the service names.
Current Status	Displays the set status of the service: - Active: Enabled - Inactive: Disabled - N/A: No set value
Nonsecure Port	Displays the port number of the connection (only for the web service).
Secure Port	Displays the port number of the connection (only for the web service).

You can perform the following operations on the [Services] screen.

Table 3.17 Operation Items on the [Services] Screen

Operation Item	Description
Modify	- Change the port number of the web service. For the procedure, see "Changing the Port Number of the web Service." - Enable/Disable the ssh service. For the procedure, see "Enabling/Disabling the ssh Service." - Enable/Disable the snmp service and change its port number. For the procedure, see "Enabling/Disabling the snmp service."

Changing the Port Number of the web Service

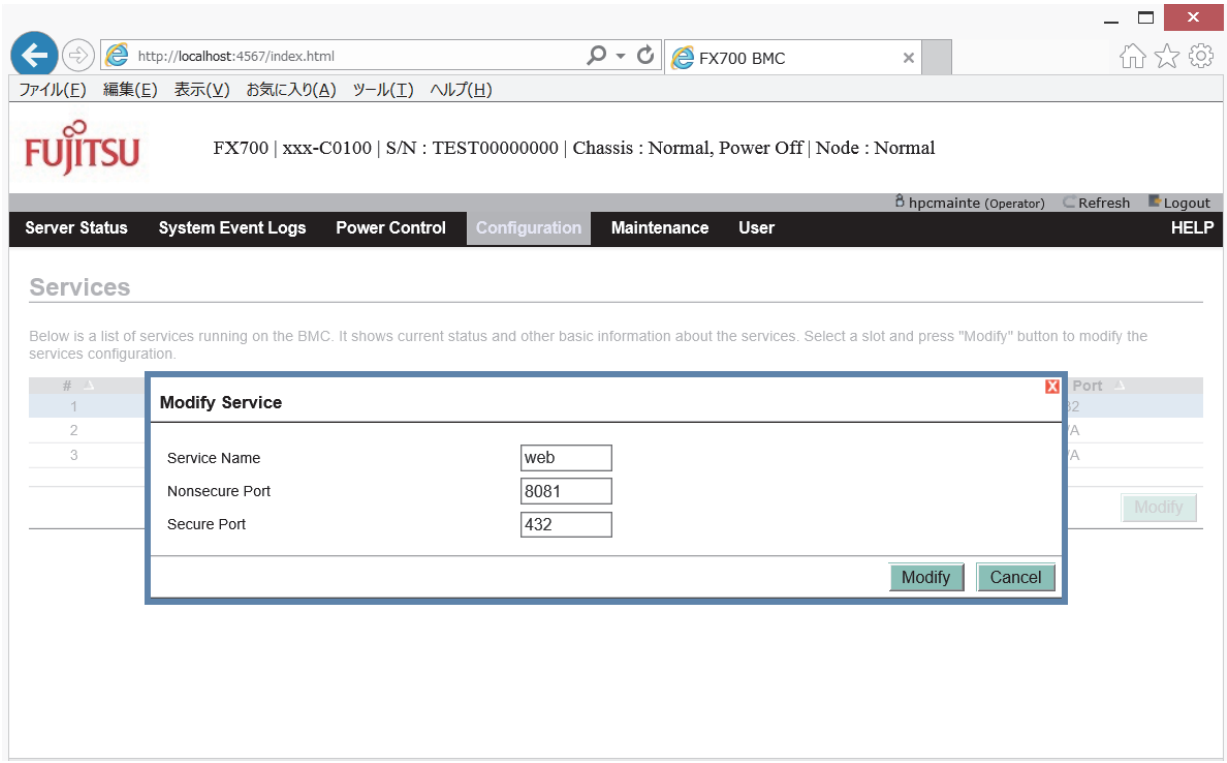
1. Select the row showing "web" under [Service Name], and click the [Modify] button.

   The dialog box for modifying the web service appears.

   Remarks

   - You can also display the dialog box for modifying the web service by double-clicking the web row.

Figure 3.9 web Service Modification Dialog Box



2. Specify the respective port numbers in [Nonsecure Port] and [Secure Port].

Table 3.18 Specifying the web Service

Display/Input Item	Description
Service Name	The name of the web service is displayed.
Nonsecure Port	Specify a port number between 1 and 65535 for the http connection. The default port number is 8031.
Secure Port	Specify a port number between 1 and 65535 for the https connection. The default port number is 432.

3. Click the [Modify] button.

   An execution confirmation dialog box appears.

4. Click the [OK] button.

   The current session is disconnected, and you are prompted on the screen to log in again.

Enabling/Disabling the ssh Service

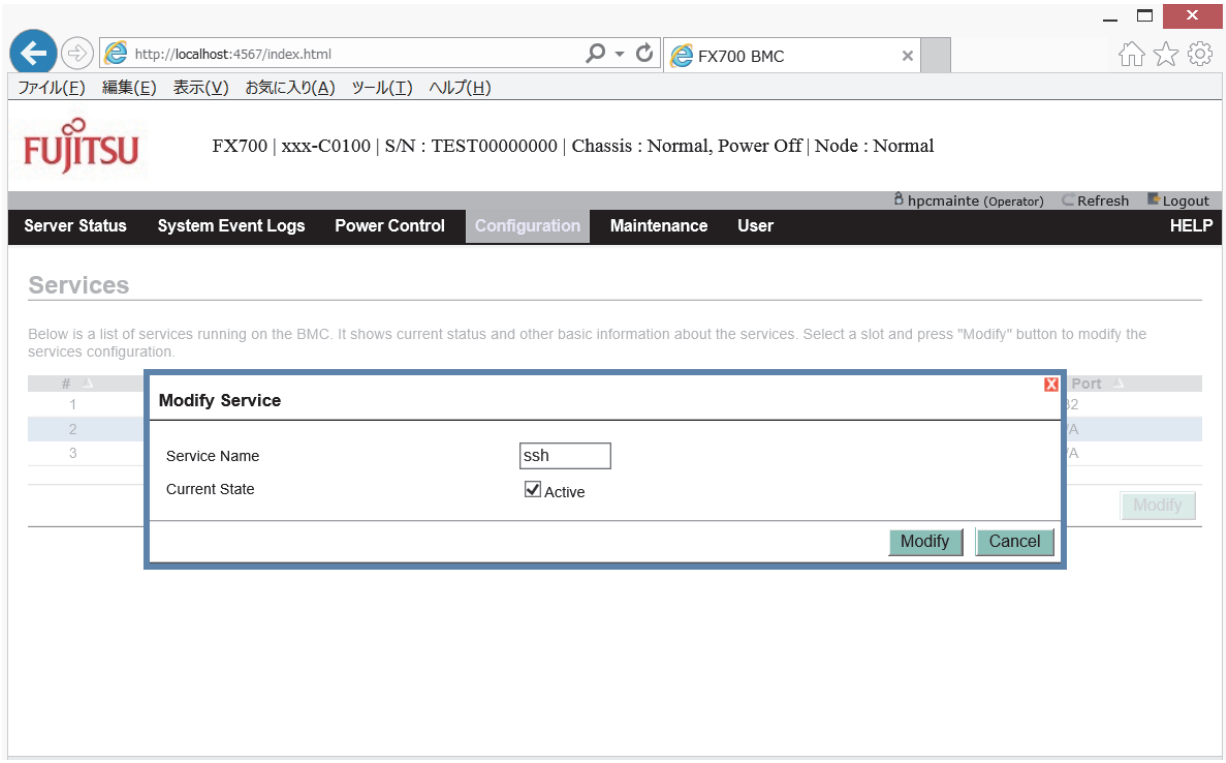
1. Select the row showing "ssh" under [Service Name], and click the [Modify] button.

   The dialog box for modifying the ssh service appears.

   Remarks

   - You can also display the dialog box for modifying the ssh service by double-clicking the ssh row.

Figure 3.10 ssh Service Modification Dialog Box



2. Specify whether to enable or disable the ssh service.

Table 3.19 Specifying the ssh Service

Display/Input Item	Description
Service Name	The name of the ssh service is displayed.
Current State	To enable the ssh service, check the [Active] check box.

3. Click the [Modify] button.

   An execution confirmation dialog box appears.

4. Click the [OK] button.

   The browser returns to the [Services] screen.

Enabling/Disabling the snmp service

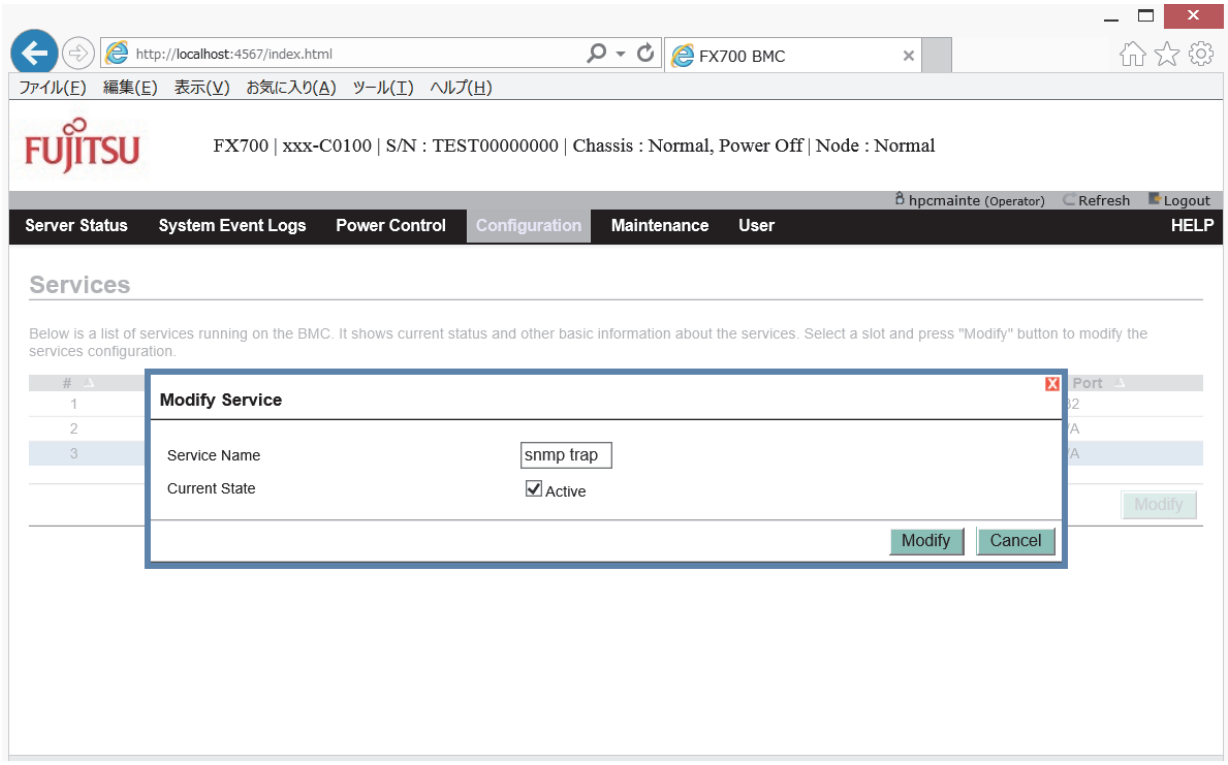
1. Select the row showing "snmp" under [Service Name], and click the [Modify] button.

   The dialog box for modifying the snmp service appears.

   Remarks

- You can also display the dialog box for modifying the snmp service by double-clicking the snmp row.

Figure 3.11 snmp Service Modification Dialog Box



2. Specify whether to enable or disable the snmp service.

Table 3.20 Specifying the snmp Service

Display/Input Item	Description
Service Name	The name of the snmp service is displayed.
Current Status	To enable the snmp service, check the [Active] check box.

3. Click the [Modify] button.

   An execution confirmation dialog box appears.

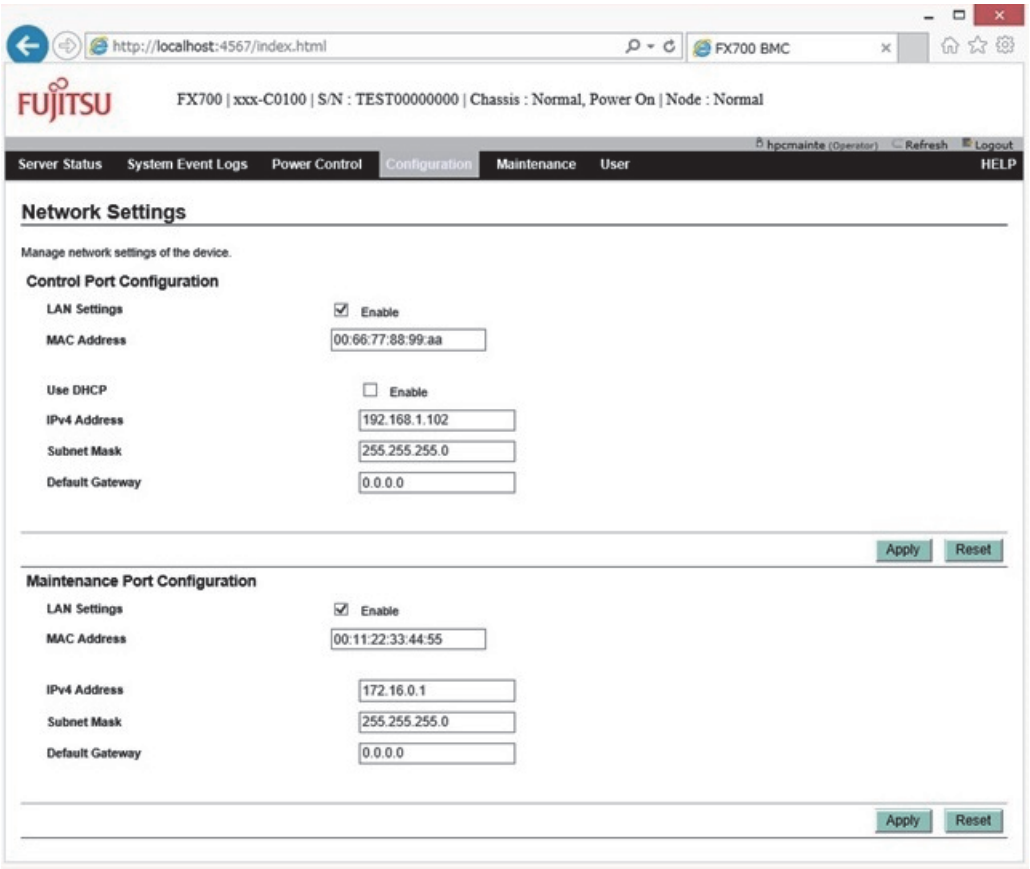
4. Click the [OK] button.

   The browser returns to the [Services] screen.

3.4.3 Network Settings

On the [Network Settings] screen, you can check and change network settings.

Figure 3.12 [Network Settings] Screen



You can perform the following operations on the [Network Settings] screen.

Table 3.21 Operation Items on the [Network Settings] Screen

Operation Item	Description
Apply	Change network information. For the procedure, see "Changing Network Information."
Reset	Restore the currently set network information.

Changing Network Information

1. Specify each of the items under [Control Port Configuration] or [Maintenance Port Configuration].

   Note

   - Change the items under either [Control Port Configuration] or [Maintenance Port Configuration]. The items of both ports cannot be changed at the same time.
   - Set the Default Gateway only under either [Control Port Configuration] or [Maintenance Port Configuration].

Table 3.22 Specifying Network Information

Display/Input Item	Description
LAN Settings	To enable the port, check the [Enable] check box.

Table 3.22 Specifying Network Information *(continued)*

Display/Input Item	Description
MAC Address	The MAC address is displayed.
Use DHCP (Control port only)(*1)	To enable DHCP, check the [Enable] check box.
IPv4 Address	Specify an IP address in the xxx.xxx.xxx.xxx format. xxx is a value between 0 and 255.
Subnet Mask	Specify a subnet mask in the xxx.xxx.xxx.xxx format. xxx is a value between 0 and 255.
Default Gateway	Specify the default gateway IP address in the xxx.xxx.xxx.xxx format. xxx is a value between 0 and 255.

*1 The Use DHCP item is not displayed by HCP1600 or earlier.

2. Click the [Apply] button.

   An execution confirmation dialog box appears.

   Remarks

   - To restore the currently set network information, click the [Reset] button instead of the [Apply] button.

3. Click the [OK] button.

   The current session is disconnected, and you are prompted on the screen to log in again.

The [Network Settings] screen displays the following items.

Table 3.23 Display Items on the [Network Settings] Screen

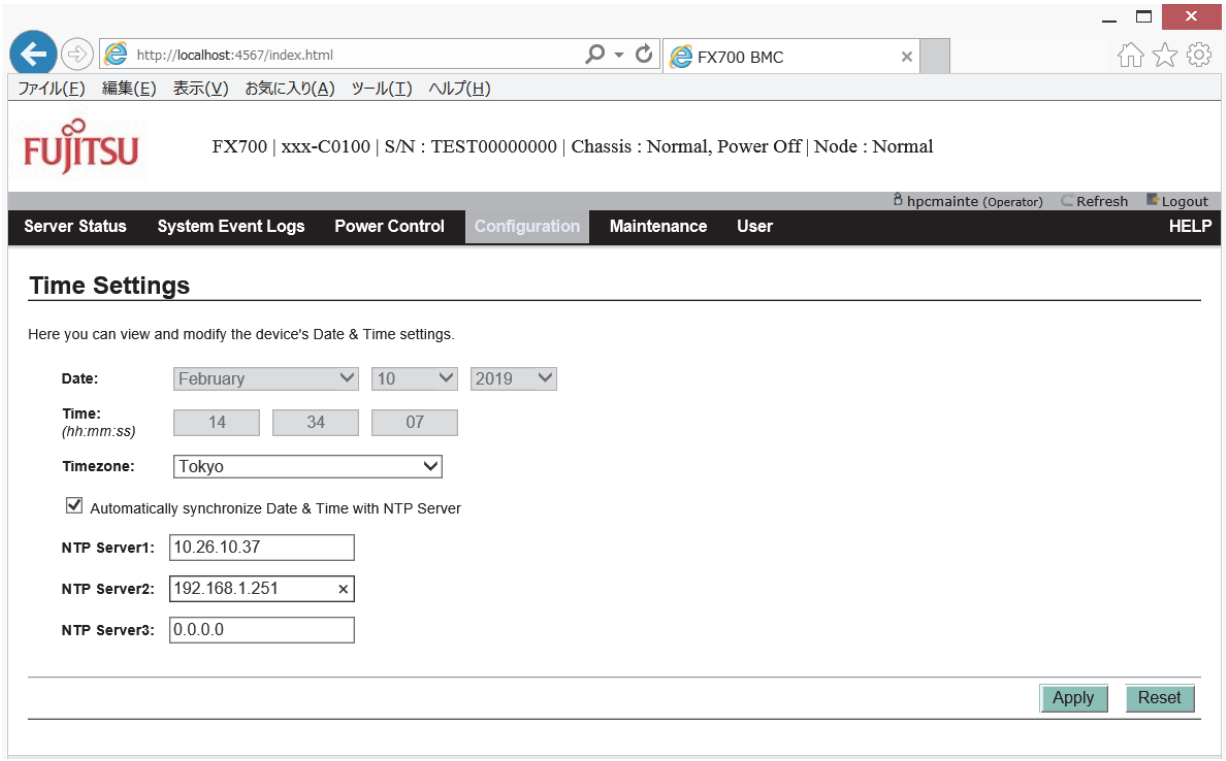
Display Item	Details of Display
LAN Settings	Indicates whether the port is enabled or disabled. If the port is enabled, the [Enable] check box is checked.
MAC Address	Displays the MAC address.
Use DHCP (Control port only)(*1)	Indicates whether the DHCP is enabled or disabled. If DHCP is enabled, the [Enable] check box is checked.
IPv4 Address	Displays the IP address.
Subnet Mask	Displays the subnet mask.
Default Gateway	Displays the default gateway IP address.

*1 The Use DHCP item is not displayed by HCP1600 or earlier.

3.4.4 Time Settings

On the [Time Settings] screen, you can check and change the set date and time of the FX700 main unit.

Figure 3.13 [Time Settings] Screen



You can perform the following operations on the [Time Settings] screen.

Table 3.24 Operation Items on the [Time Settings] Screen

Operation Item	Description
Apply	Change date and time setting information. For the procedure, see "Changing Date and Time Setting Information."
Reset	Restore the currently set date and time setting information.

Changing Date and Time Setting Information

1. Specify each item, such as [Date:], [Time:], and [Timezone:].

Table 3.25 Specifying Date and Time Setting Information

Input Item	Description
Date:	Specify the date in the order of month, day, and year.
Time:	Specify the time in the order of hour, minute, and second.
Timezone:	Specify the time zone.
Automatically synchronize Date & Time with NTP Server	To set automatic synchronization with the NTP server, check the check box. [NTP Server1:] to [NTP Server3:] are displayed when the check box is checked.
NTP Server1:	Specify the IP address of the NTP server. If no NTP server has been configured, specify "0.0.0.0".
NTP Server2:	
NTP Server3:	

2. Click the [Apply] button.

Confirmation dialog box appears.

Remarks

- To restore the currently set date and time setting information, click the [Reset] button instead of the [Apply] button.

3. Click the [OK] button.

   The date and time information is set, and the browser returns to the [Time Settings] screen.

The [Time Settings] screen displays the following items.

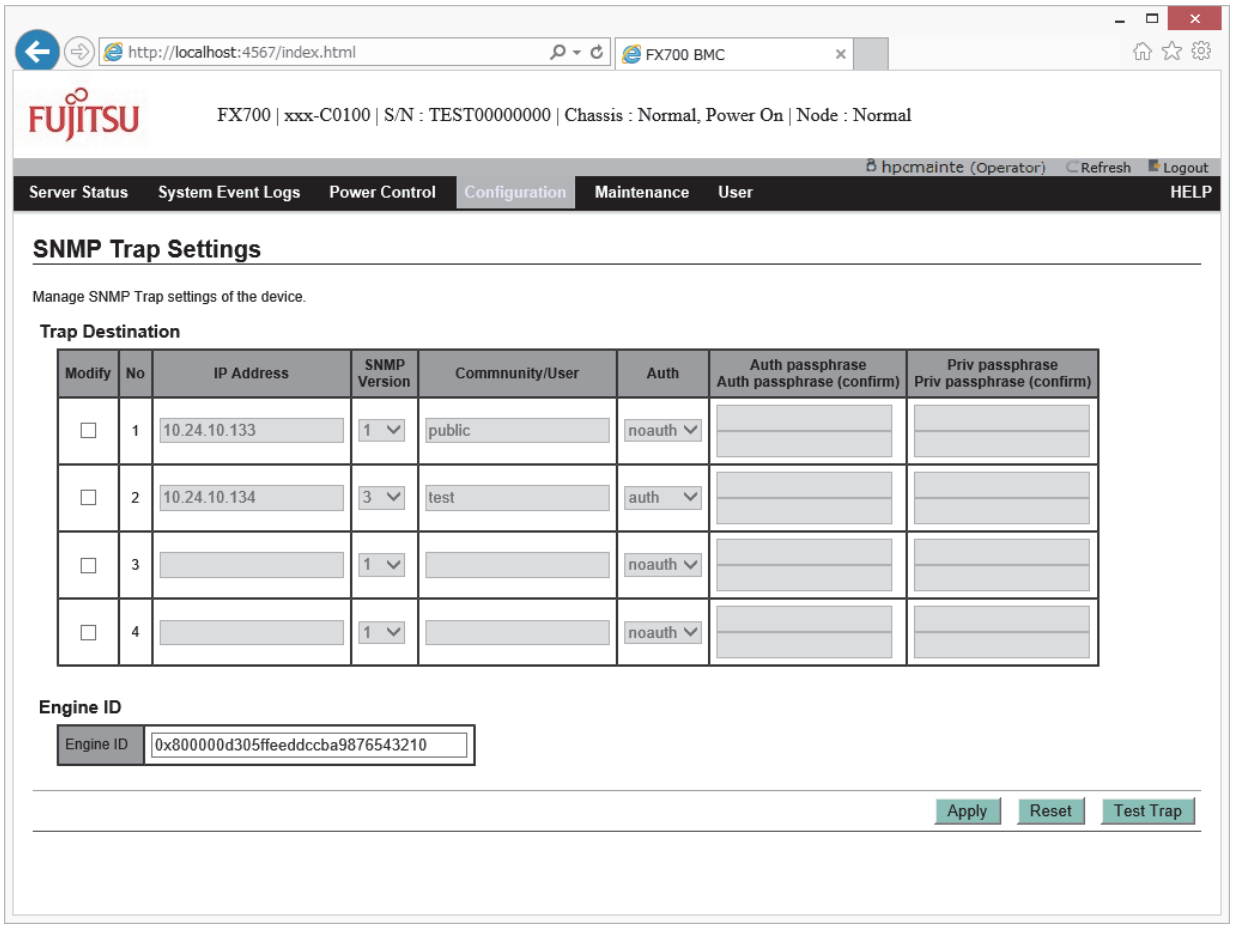
Table 3.26 Display Items on the [Time Settings] Screen

Display Item	Details of Display
Date:	Displays the date in the order of month, day, and year.
Time:	Displays the time in the order of hour, minute, and second.
Timezone:	Displays the time zone.
Automatically synchronize Date & Time with NTP Server	Shows a checked check box if automatic synchronization with the NTP server is set. Furthermore, [NTP Server1:] to [NTP Server3:] would be displayed.
NTP Server1:	Displays the IP address of the NTP server.
NTP Server2:	
NTP Server3:	

3.4.5 SNMP Trap Settings

On the [SNMP Trap Settings] screen, you can check and change SNMP trap settings.

Figure 3.14 [SNMP Trap Settings] Screen



You can perform the following operations on the [SNMP Trap Settings] screen.

Table 3.27 Operation Items on the [SNMP Trap Settings] Screen

Operation Item	Description
Apply	Change SNMP trap setting information. For the procedure, see "Changing SNMP Trap Setting Information."
Reset	Restores the currently set SNMP trap information.
Test Trap	Send a test trap to all of the set trap destinations. For the procedure, see "Sending a Test Trap."

Changing SNMP Trap Setting Information

1. To change the setting information for a trap destination, check its check box.
2. Specify each item, such as [Community/User], [IP Address], and [SNMP Version].

Table 3.28 Specifying SNMP Trap Setting Information

Input Item	Description
IP Address	Specify the IP address of an SNMP trap destination in the xxx.xxx.xxx.xxx format. xxx is a value between 0 and 255.

Table 3.28 Specifying SNMP Trap Setting Information *(continued)*

Input Item	Description
SNMP Version	Specify the SNMP version.
Community/User	- For SNMPv1 and SNMPv2, specify an SNMP community string consisting of 1 to 32 characters. - For SNMP v3, specify a user name consisting of 1 to 32 characters. - Only alphanumeric characters are allowed.
Auth	Specify a security level. - noauth: Do not use the authentication function. - auth: Use the authentication function. - priv: Use the authentication and privacy functions (data encryption).
Auth passphrase	If "auth" or "priv" is specified in [Auth], specify an authentication password consisting of 8 to 32 characters, which may be alphanumeric or the following: ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ |
Auth passphrase (confirm)	Specify the same authentication password as in [Auth passphrase].
Priv passphrase	If "priv" is specified in [Auth], specify an encryption password consisting of 8 to 32 characters, which may be alphanumeric or the following: ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ |
Priv passphrase (confirm)	Specify the same encryption password as in [Priv passphrase].

Table 3.28 Specifying SNMP Trap Setting Information *(continued)*

Input Item	Description
Engine ID	Specify a hexadecimal number with up to 32 characters and "0x" at the beginning. In other words, in accordance with SNMPv3 specifications, specify "0x" + "enterprise number with leading 1 bit" (8 hexadecimal digits) + "format value" + "unique value" (up to 20 hexadecimal digits). Enterprise number This refers to a private enterprise number of the Internet Assigned Numbers Authority (IANA). For example, if the enterprise number is 211 (0x000000d3 in hexadecimal), specify "0x800000d3" (with a leading 1 bit). Format value Specify "03" or "05". Unique value The unique value varies depending on the format value. - For "03": Specify the MAC address. We recommend using the MAC address (12 digits excluding the colon (:)) of the control port. You can check the MAC address from the BMC webpage at [Configuration] - [Network Settings]. - For "05": Specify an arbitrary unique value with a hexadecimal number of up to 20 digits. - Do not set any alphabetic letter that is not a hexadecimal digit. An example of input is shown below. - When specifying the MAC address 1A:2B:3C:4D:5E:6F (for example), enter "0x800000d3031a2b3c4d5e6f". - When specifying the arbitrary value 0xffeeddccba9876543210 (for example), enter "0x800000d305ffeeddccba9876543210".

Remarks

- To disable existing SNMP trap setting information, delete its IP address.

3. Click the [Apply] button.

   Confirmation dialog box appears.

   Remarks

   - To restore the currently set SNMP trap setting information, click the [Reset] button instead of the [Apply] button.

4. Click the [OK] button.

   The SNMP trap setting information is changed, and the browser returns to the [SNMP Trap Settings] screen.

Sending a Test Trap

1. Click the [Test Trap] button.

Confirmation dialog box appears.

2. Click the [OK] button.

   A test trap is sent to all of the set trap destinations.

The [SNMP Trap Settings] screen displays the following items.

Table 3.29 Display Items on the [SNMP Trap Settings] Screen

Display Item	Description
IP Address	Displays the IP addresses of SNMP trap destinations.
SNMP Version	Displays the SNMP version.
Community/User	Displays an SNMP community string when the version is SNMPv1 or SNMPv2, and displays a user name when it is SNMPv3.
Auth	Displays security levels. - noauth: Do not use the authentication function. - auth: Use the authentication function. - priv: Use the authentication and privacy functions (data encryption).
Auth passphrase	Displays an authentication password if "auth" or "priv" is specified in [Auth].
Auth passphrase (confirm)	
Priv passphrase	Displays an encryption password if "priv" is specified in [Auth].
Priv passphrase (confirm)	
Engine ID	Displays engine IDs.

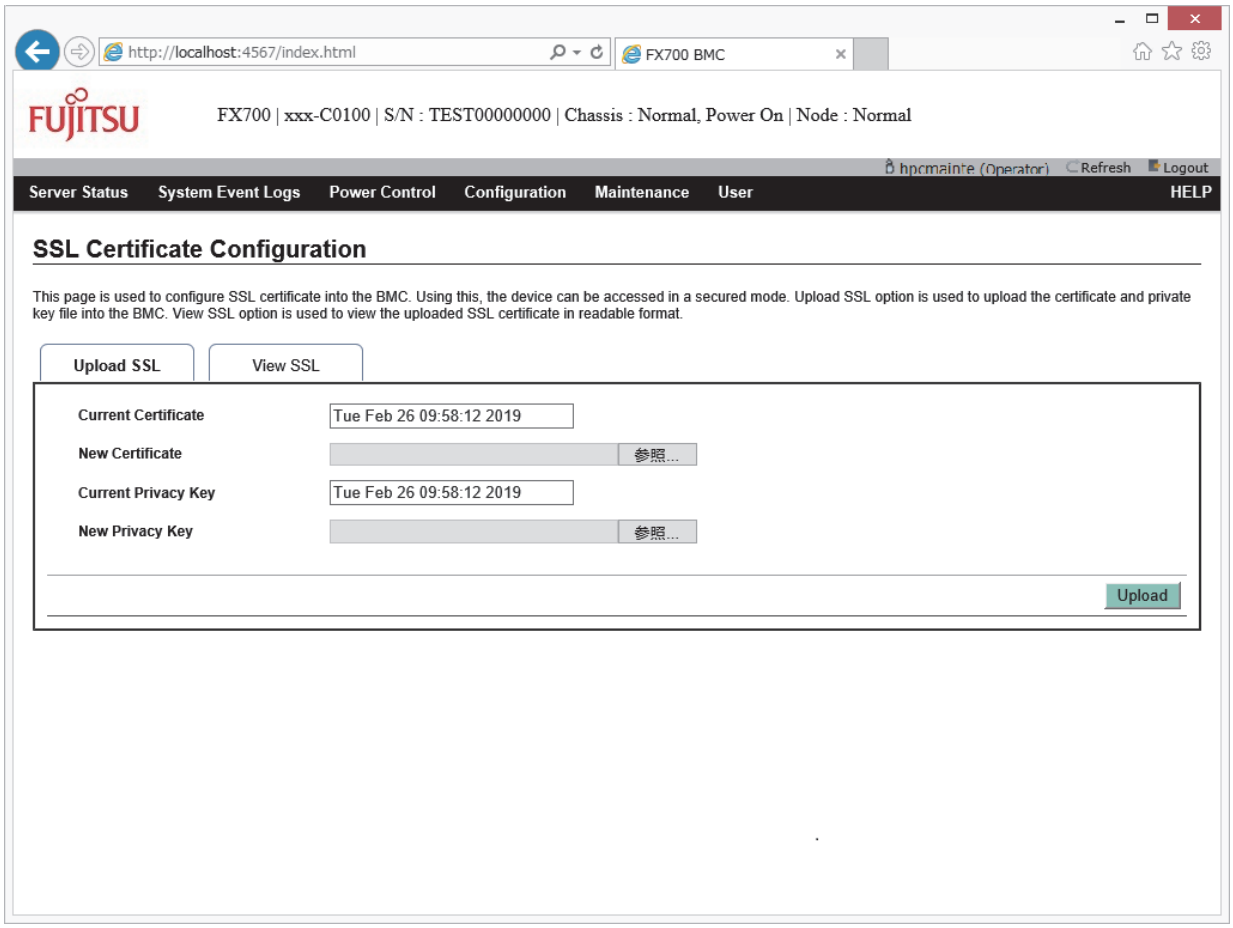
3.4.6 SSL Certificate Configuration

On the [SSL Certificate Configuration] screen, you can check the registered contents of an installed SSL certificate. You can also upload the SSL certificate issued by an external agency.

Note

- The default status does not allow https connection to the BMC. https connection is allowed when the BMC has uploaded an SSL certificate through an http connection.

Figure 3.15 [Upload SSL] Tab on the [SSL Certificate Configuration] Screen



You can perform the following operations on the [Upload SSL] tab on the [SSL Certificate Configuration] screen.

Table 3.30 Operation Items on the [Upload SSL] Tab on the [SSL Certificate Configuration] Screen

Operation Item	Description
Upload	Upload an SSL certificate. For the procedure, see "Uploading an SSL certificate."

Uploading an SSL certificate

1. Click the [Upload SSL] tab, and specify files in [New Certificate] and [New Privacy Key].

Table 3.31 Display Items on the [Upload SSL] Tab

Display/Input Item	Description
Current Certificate	The timestamp of the file with the currently applied certificate is displayed.
New Certificate	Specify the file of the certificate to upload (extension: .pem).
Current Privacy Key	The timestamp of the file with the private key used for the currently applied certificate is displayed.
New Privacy Key	Specify the file of the private key used for the certificate to upload (extension: .pem).

2. Click the [Upload] button.

   Confirmation dialog box appears.

3. Click the [OK] button.

   You are logged out in order to apply the uploaded SSL certificate.

The [View SSL] tab on the [SSL Certificate Configuration] screen displays the following content.

Figure 3.16 [View SSL] Tab on the [SSL Certificate Configuration] Screen

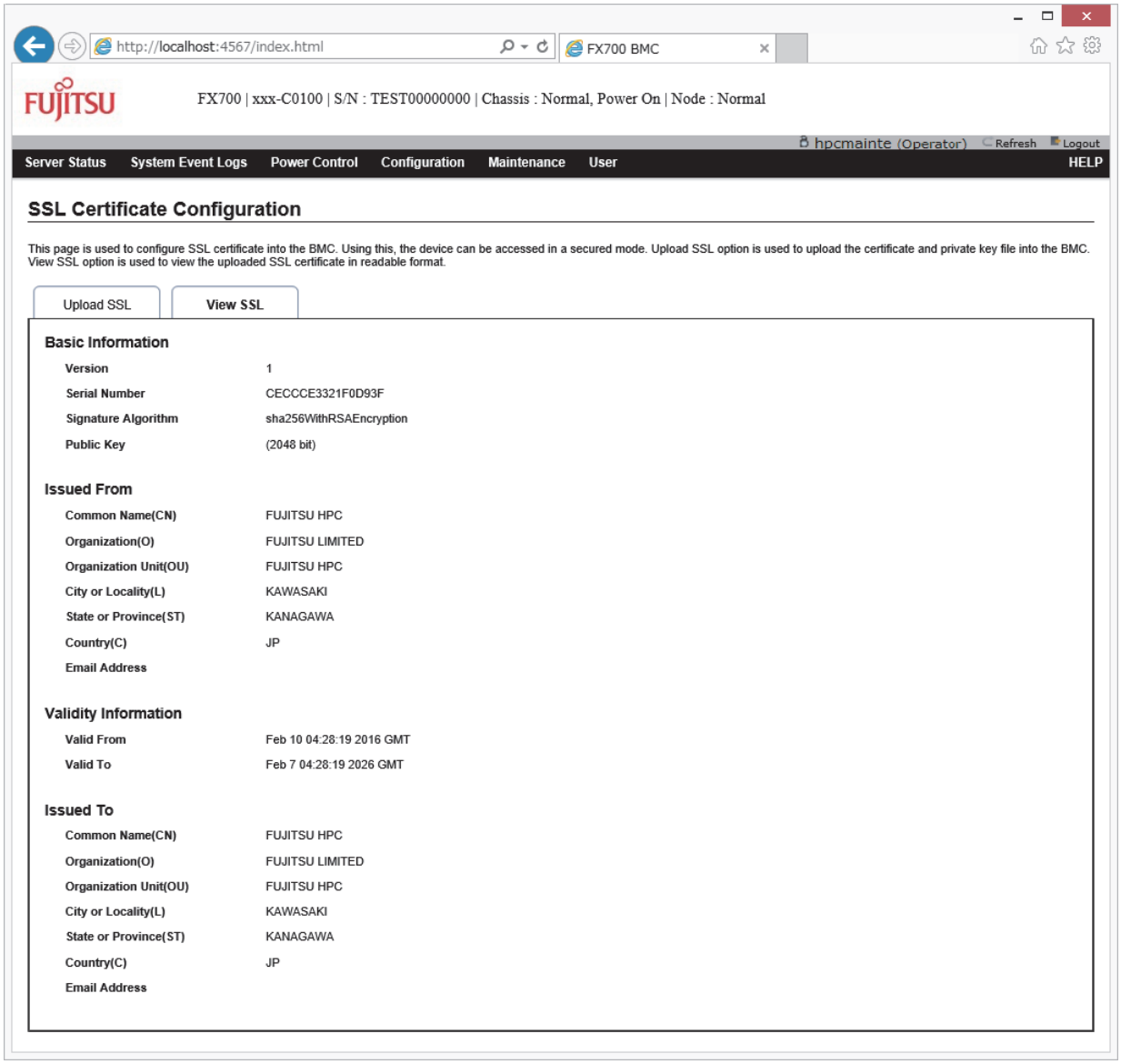


Table 3.32 Display Items on the [View SSL] Tab on the [SSL Certificate Configuration] Screen

Display Item	Description
Basic Information	Displays basic information on X.509: - Version: Version - Serial Number: Serial number - Signature Algorithm: Public key algorithm - Public Key: Public key of the issuance requester
Issued From	Displays information on the issuance requester: - Common Name (CN): Site name - Organization (O): Department name - Organization Unit (OU): Organization name - City or Locality (L): Name of a city, town, or village - State or Province (ST): Prefecture name - Country (C): Country name - Email Address: E-mail address
Validity Information	Displays validity period information: - Valid From: Start of the validity period - Valid To: End of the validity period
Issued To	Displays information on the issuer: - Common Name (CN): Site name - Organization (O): Department name - Organization Unit (OU): Organization name - City or Locality (L): Name of a city, town, or village - State or Province (ST): Prefecture name - Country (C): Country name - Email Address: E-mail address

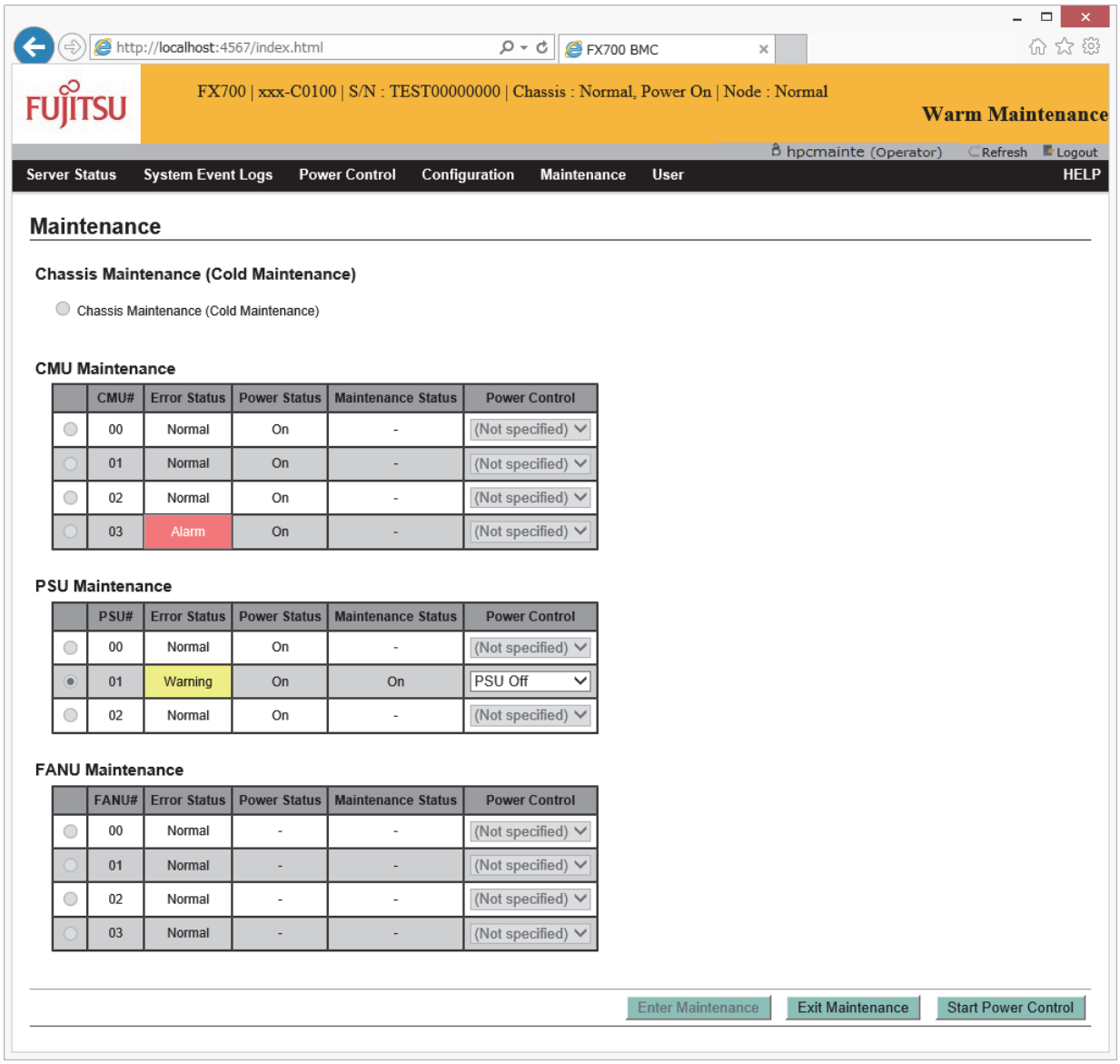
3.5 Maintenance

This category provides functions related to FX700 main unit maintenance.

3.5.1 Maintenance

On the [Maintenance] screen, the entire FX700 main unit or individual FRUs are placed in or released from the maintenance state during the replacement of maintenance parts.

Figure 3.17 [Maintenance] Screen



You can perform the following operations on the [Maintenance] screen.

Table 3.33 Operation Items on the [Maintenance] Screen

Operation Item	Description
Enter Maintenance	Enter the maintenance state. For the procedure, see "Entering the Maintenance State."
Exit Maintenance	Release the maintenance state. For the procedure, see "Releasing the Maintenance State."
Power Control	Execute the power operation instruction of the CMU or PSU in the maintenance state. For the procedure, see "Executing a Power Operation."

Entering the Maintenance State

1. To place the FX700 main unit or a FRU in the maintenance state, click its radio button.

Note

- You can click only one of the following radio buttons to place the corresponding component in the maintenance state: [Chassis Maintenance (Cold Maintenance)], [CMU Maintenance], [PSU Maintenance], and [FANU Maintenance].
- To replace parts with the system stopped, select [Chassis Maintenance (Cold Maintenance)]. To hot-swap a FRU while the node is operating, select the radio button of the FRU.

2. When selecting the [CMU Maintenance] or [PSU Maintenance] radio button, specify a power operation in [Power Control] as required.

Table 3.34 Operations in [Power Control]

Input Item	Description
CMU Maintenance	Specify a power operation for the CMU: - Both Node Off - Both Node On - (Not Specified)
PSU Maintenance	Specify a power operation for the PSU: - PSU Off - PSU On - (Not Specified)

Note

- If a failure occurs in the FANU, maintenance mode cannot be set for the CMU. For this reason, replace the FANU first. For details, see "4.1.3 Precaution on Maintenance Mode" in the *FUJITSU Supercomputer PRIMEHPC FX700 Upgrade and Maintenance Manual*.

3. Click the [Enter Maintenance] button.

   Enter the maintenance state.

Executing a Power Operation

1. Referring to "Entering the Maintenance State," enter the maintenance state.
2. Click the [Start Power Control] button.

   A confirmation dialog box appears.

3. Click the [OK] button.

   The power operation is executed.

Releasing the Maintenance State

1. After maintenance work, click the [Refresh] button to update the screen display.
2. Click the [Exit Maintenance] button.

   The maintenance state is released.

The [Maintenance] screen displays the following items.

Table 3.35 Display Items in [CMU Maintenance] on the [Maintenance] Screen

Display Item	Details of Display
CMU#	Displays the CMU numbers.
Error Status	Displays the failure status of the CMUs: - Normal - Warning - Alarm - EAlarm - Not-Present - Unknown (Failed to retrieve Error Status)
Power Status	Displays the power supply status of the CMUs: - On - Off - Unknown (Failed to retrieve Power Status)
Maintenance Status	Displays the set status of maintenance: - On: Warm maintenance in progress - − : Other than the above - Unknown: Failed to retrieve Maintenance Status
Power Control	Displays the power operation instruction for the CMU that is set to the maintenance state.

Table 3.36 Display Items in [PSU Maintenance] on the [Maintenance] Screen

Display Item	Details of Display
PSU#	Displays the PSU numbers.
Error Status	Displays the failure status of the PSUs: - Normal - Warning - Alarm - EAlarm - Not-Present - Unknown (Failed to retrieve Error Status)
Power Status	Displays the power supply status of the PSUs: - On - Off - Unknown (Failed to retrieve Power Status)
Maintenance Status	Displays the set status of maintenance: - On: Warm maintenance in progress - − : Other than the above - Unknown: Failed to retrieve Maintenance Status
Power Control	Displays the power operation instruction for the PSU that is set to the maintenance state.

Table 3.37 Display Item of [FANU Maintenance] in [Maintenance] Screen

Display Item	Details of Display
FANU#	Displays the FANU numbers.
Error Status	Displays the failure status of the FANUs: - Normal - Alarm - Not-Present - Unknown (Failed to retrieve Error Status)
Power Status	- (Not used)
Maintenance Status	Displays the set status of maintenance: - On: Warm maintenance in progress - − : Other than the above - Unknown: Failed to retrieve Maintenance Status
Power Control	- (Not used)

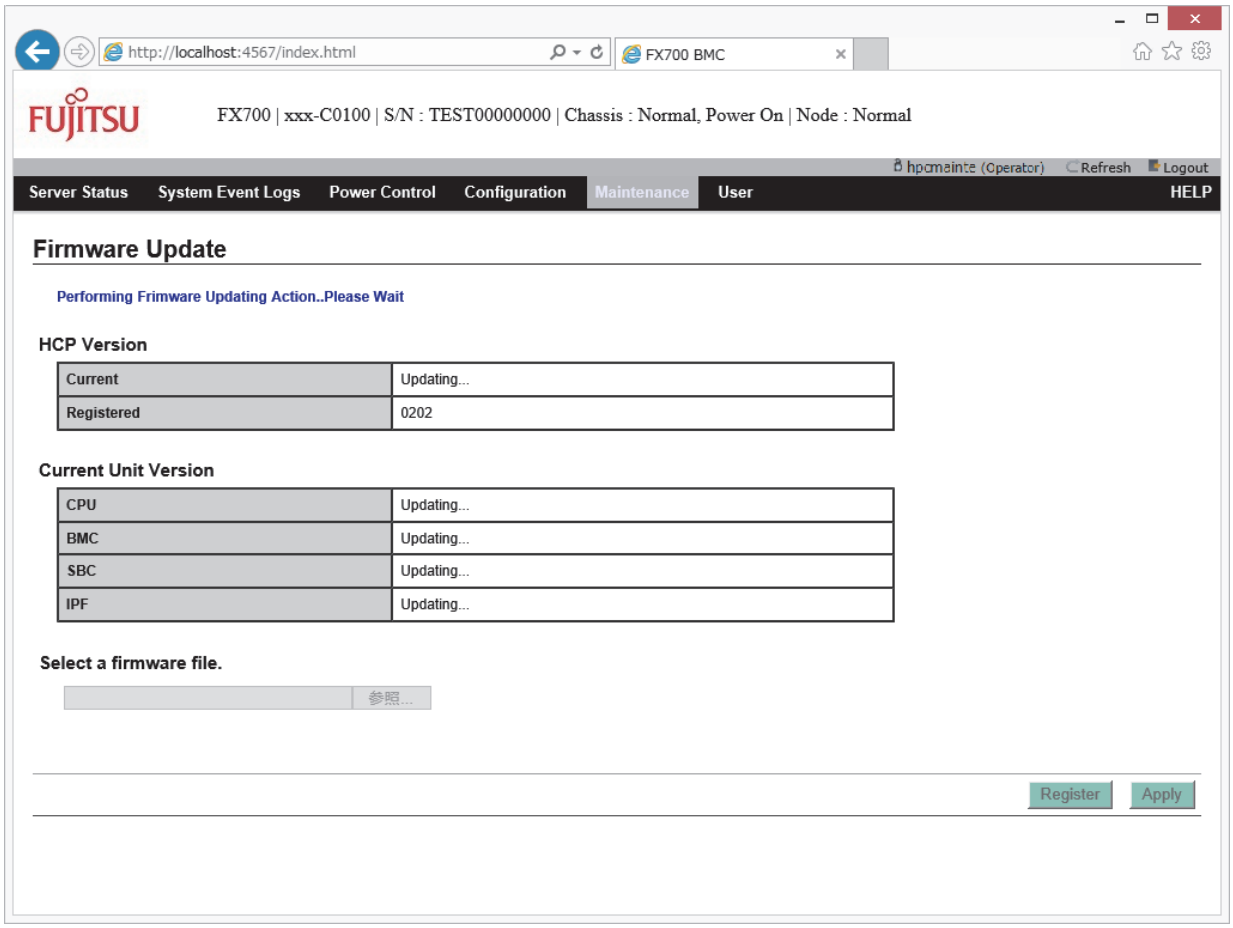
3.5.2 Firmware Update

On the [Firmware Update] screen, you can check the HCP firmware applied to the FX700 main unit and the version applied to each unit. You can also apply HCP firmware to the FX700 main unit.

Remarks

Before starting the firmware update, confirm that the running status of all nodes is "Stop."

Figure 3.18 [Firmware Update] Screen



You can perform the following operations on the [Firmware Update] screen.

Table 3.38 Operation Items on the [Firmware Update] Screen

Operation Item	Description
Register	Register HCP firmware. For the procedure, see "Registering HCP Firmware."
Apply	Apply the registered HCP firmware to the FX700 main unit. For the procedure, see "Applying HCP Firmware."

Registering HCP Firmware

HCP firmware is available online.

- For the Japanese market:
  https://www.fujitsu.com/jp/products/computing/servers/supercomputer/downloads/
- For the global market:
  https://www.fujitsu.com/global/products/computing/servers/supercomputer/documents/

1. In [Select a firmware file.], specify the HCP firmware file to be registered.
2. Click the [Register] button.

   Confirmation dialog box appears.
3. Click the [OK] button.

The HCP firmware is registered, and the browser returns to the [Firmware Update] screen.

Applying HCP Firmware

1. Referring to "Registering HCP Firmware," register HCP firmware.
2. Click the [Apply] button.

   Confirmation dialog box appears.

3. Click the [OK] button.

   The session is disconnected, and you are logged out in order to apply the HCP firmware.

   Note

   If an error message appears, try the operation again according to the contents of the message. For details, see "4.2.3 Precaution During Updates" in the *FUJITSU Supercomputer PRIMEHPC FX700 Upgrade and Maintenance Manual* (C120-0090EN).

Confirming HCP Firmware Application

Confirm that the integrated version number of the HCP firmware in the [Current] field of [HCP Version] has been updated.

1. The firmware update takes approximately 20 minutes. During that period, the Web GUI session is disconnected several times.
2. The update has completed when the integrated version number of the HCP firmware in the [Current] field of [HCP Version] is the same as the registered HCP version.

The [Firmware Update] screen displays the following items.

Table 3.39 Display Items on the [Firmware Update] Screen

Display Item	Details of Display
Current	Displays the integrated version number of the applied HCP firmware that is running.
Registered	Displays the integrated version number of the registered HCP firmware that can be applied.
CPU	Displays the version number of the firmware applied to the CPU.
BMC	Displays the version number of the firmware applied to BMC.
SBC	Displays the version number of the firmware applied to SBC.
IPF	Displays the version number of the firmware applied to IPF.

Note

- If firmware application fails, try again starting with the HCP firmware registration procedure.

3.5.3 CPU Feature Settings

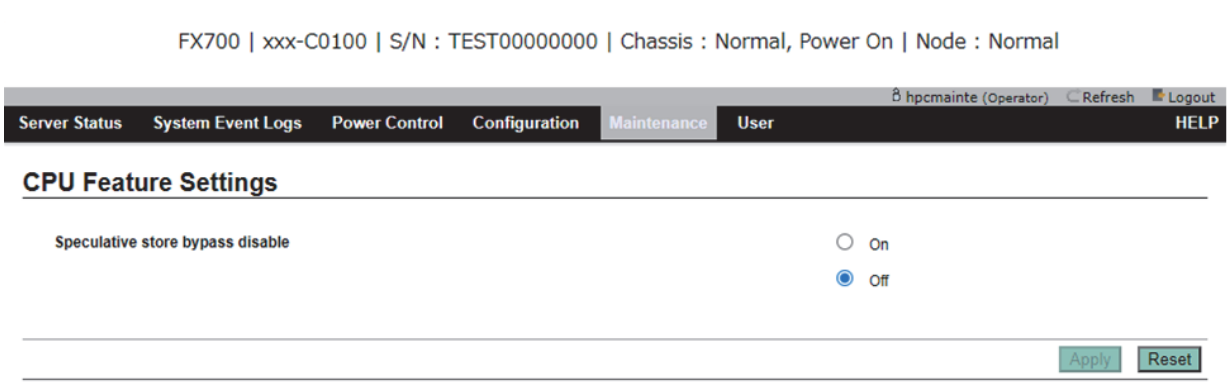
On the [CPU Feature Settings] screen, you can check and set the Speculative store bypass disable (SSBD). Setting the Speculative store bypass disable (SSBD) to On may have an impact on performance, depending on the customer's operating environment. Check in advance in your environment before applying the setting.

Remarks

Before changing the setting of the Speculative store bypass disable, confirm that the running status of all

nodes is "Stop."

Figure 3.19 [CPU Feature Settings] Screen



You can perform the following operations on the [CPU Feature Settings] screen.

Table 3.40 Operation Items on the [CPU Feature Settings] Screen

Operation Item	Description
Apply	Change the Speculative store bypass disable. For the procedure, see "Changing the Speculative store bypass disable."
Reset	Restore the current setting.

Changing the Speculative store bypass disable

1. **Specify On or Off in [Speculative store bypass disable].**

Table 3.41 Specifying the Speculative store bypass disable

Display/Input Item	Description
Speculative store bypass disable	Specify On/Off for the setting.

2. **Click the [Apply] button.**

   An execution confirmation dialog box appears.

   Remarks

   - To restore the current setting, click the [Reset] button instead of the [Apply] button.

3. **Click the [OK] button.**

   The Speculative store bypass disable is set, and the browser returns to the [CPU Feature Settings] screen.

   The [CPU Feature Settings] screen displays the following items.

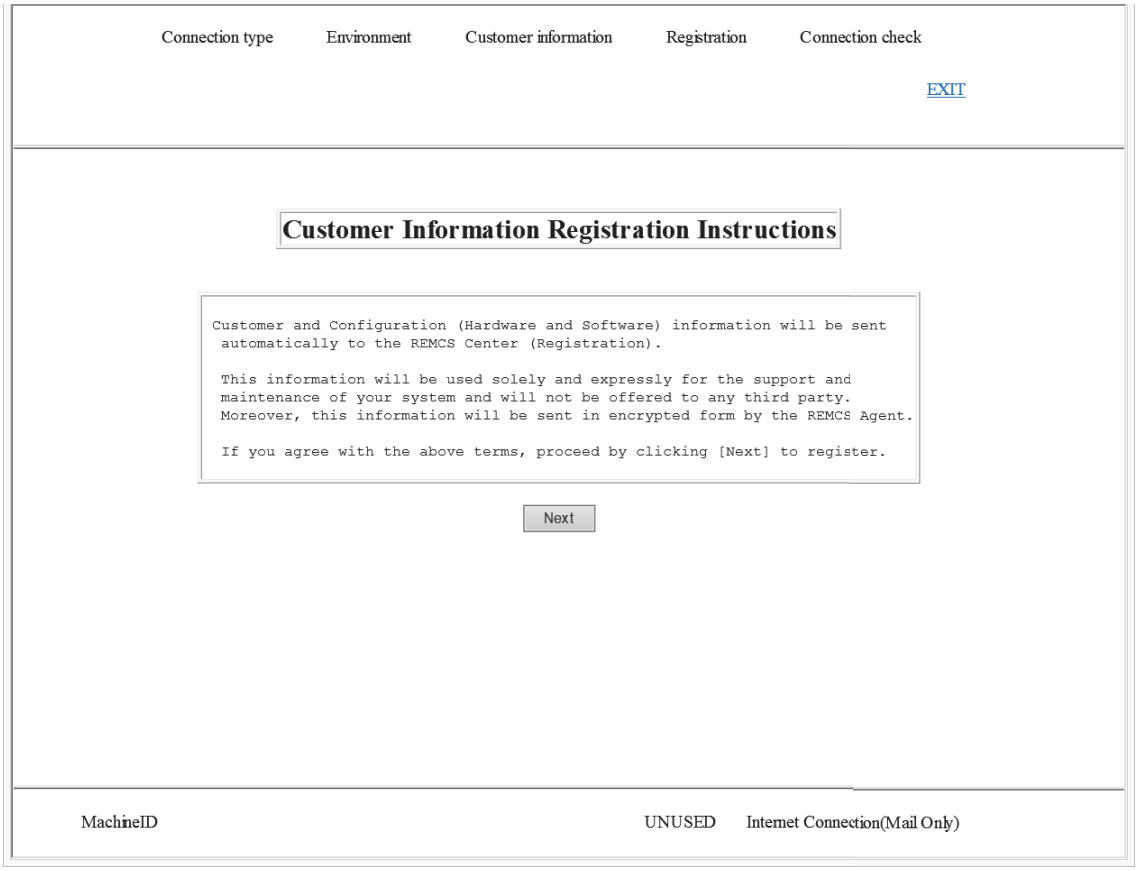
Table 3.42 Display Items on the [CPU Feature Settings] Screen

Display/Input Item	Description
Speculative store bypass disable	The current On/Off setting is displayed.

3.5.4 REMCS

Select this menu to display the [REMCS] screen. For details on settings, see "A.1 REMCS Settings."

Figure 3.20 [REMCS] Screen



3.5.5 REMCS Detail Setup

Select this menu to display the [REMCS Detail] screen. For details on settings, see "A.2 REMCS Detail Setup."

Figure 3.21 [REMCS Detail] Screen

3.6 User

This category provides functions to display and change user registration information.

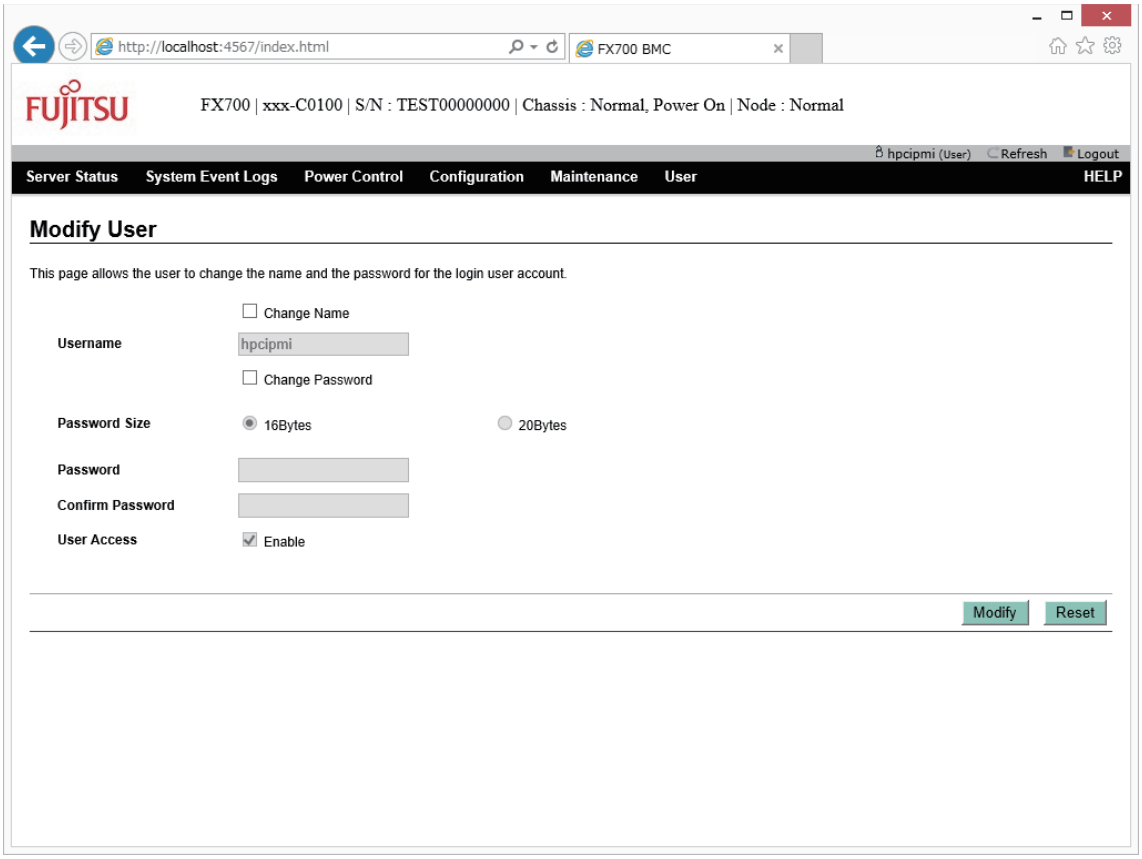
3.6.1 Modify User

On the [Modify User] screen, you can check and change the registered information on the login user.

Remarks

- The [Modify User] screen appears at the time of login with an Operator/User authority account.

Figure 3.22 [Modify User] Screen



You can perform the following operations on the [Modify User] screen.

Table 3.43 Operation Items on the [Modify User] Screen

Operation Item	Description
Modify	Change the registered information on the login user. For the procedure, see "Changing Registered User Information ([Modify User] Screen)."
Reset	Restore the registered information currently set for the user.

Changing Registered User Information ([Modify User] Screen)

Note

- [User Access] cannot be changed.

Table 3.44 Changing Registered User Information ([Modify User] Screen)

Input/Display Item	Description
Change Name	To change the user name, check the [Change Name] check box.
UserName	Specify a new user name with 1 to 16 characters. If the original user name is displayed at the input time, delete it.
Password Size	To change the password, specify a password length by clicking [16 Bytes] or [20 Bytes]. If the [20 Bytes] radio button is selected, lanplus connection using IPMI communication will be required.

Table 3.44 Changing Registered User Information ([Modify User] Screen) *(continued)*

Input/Display Item	Description
Password	- Specify a password with 7 or more characters. - If the [16 Bytes] radio button is selected in [Password Size], the maximum password length is 15 characters. If the [20 Bytes] radio button is selected, the maximum password length is 19 characters.
Confirm Password	Specify the same password as in [Password].
User Access	The [Enable] check box is shown as checked.

1. Click the [Modify] button.

   Confirmation dialog box appears.

2. Click the [OK] button.

   The browser returns to the [Modify User] screen.

   Remarks

   If the user name has been changed, the current session is disconnected, and you are prompted on the screen to log in again.

The [Modify User] screen displays the following items.

Table 3.45 Display Items on the [Modify User] Screen

Display Item	Details of Display
Username	Displays the user name.
User Access	Displays the user access status as Enabled.

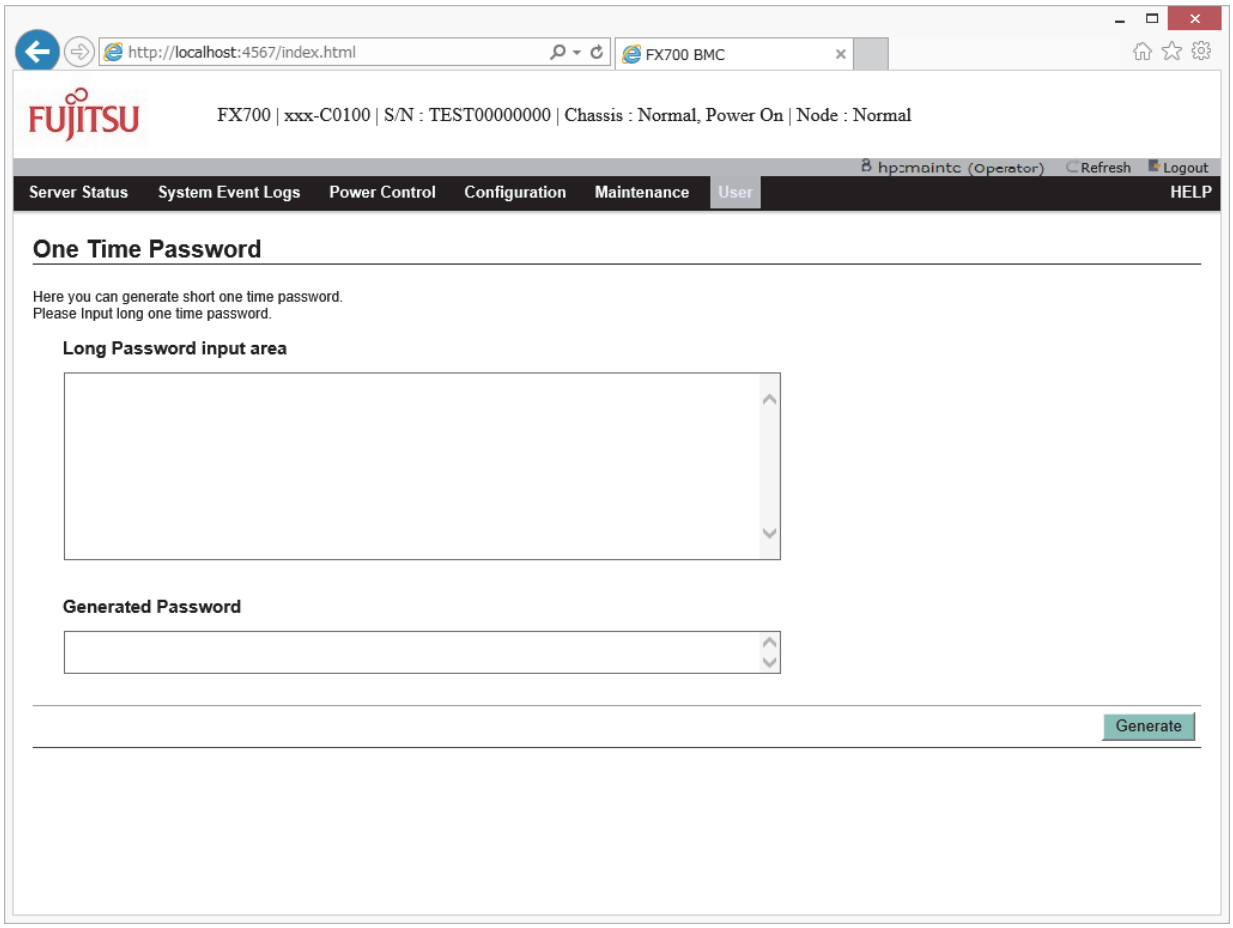
3.6.2 One Time Password

On the [One Time Password] screen, you can issue a short password for temporary login with root authority to the BMC firmware.

Note

- To issue a short password, the password issued by the person with long-password issuing authority is required. Contact the nearest Fujitsu service center.

Figure 3.23 [One Time Password] Screen



You can perform the following operations on the [One Time Password] screen.

Table 3.46 Operation Items on the [One Time Password] Screen

Operation Item	Description
Generate	Issue a short password. For the procedure, see "Issuing a Short Password."

Issuing a Short Password

Only the personnel in charge of maintenance use this function. Do not allow users with Operator authority to use it.

1. In [Long Password input area], enter the password issued by the person with long-password issuing authority, and click the [Generate] button.

   A short password is issued and displayed in [Generated Password].

Table 3.47 Issuing a Short Password

Input Item	Description
Long Password input area	Specify the password issued by the person with long-password issuing authority.

Chapter 4 Command Support (IPMI)

This chapter describes the requests (commands) received by the BMC, command functions, and request/response data formats.
Commands entered by the management client are transmitted to the BMC via LAN.

Note

Only the commands described in this chapter are supported. Operation is not guaranteed when an unsupported command is entered.

4.1 Command Tables

This section describes the standard commands.

Remarks

A response is always sent to the interface of a received request.

4.1.1 IPMI Standard Command Table

This section shows a list of IPMI standard commands.

Table 4.1 Chassis Device Commands

Command	Synchronization	CMD	Privilege	Target(*1)	
				Chassis	Node
Get Chassis Status	Synchronous	01h	User	Supported	Supported
Chassis Control	Asynchronous	02h	User	Supported	Supported

*1 Target for the issued command

How to Specify the Target

You can specify the target with the -t option in the ipmi command.

```
-t <target>
```

Options you can specify for the target

- 0x20 Chassis
- 0x30 Node#0
- 0x32 Node#1
- 0x34 Node#2
- 0x36 Node#3
- 0x38 Node#4
- 0x3a Node#5

- 0x3c Node#6
- 0x3e Node#7

4.1.2 Get Chassis Status (NetFN:00h, CMD:01h)

When issued to each node (Node#0 to Node#7), this command returns the power supply status of each node. On the other hand, when issued to the chassis-BMC, the command returns the power supply status of the chassis (PSU/FAN).

Table 4.2 Get Chassis Status Format

	Byte	Data Field
Request Data	-	-
Response Data	1	Completion Code
	2	Current Power Status [7] reserved [6:5] power restore policy 00B = Maintain Power Off state after power supply resumes. [4] power control fault 1b = Unexpected power supply state 0b = Normal [3] power fault 1b = Power failure detected 0b = Normal [2] 1b = Shutdown due to interlock state 0b = Not in interlock state [1] Power overload 1b = Shutdown due to power overload state 0b = Not in power overload state [0] Power is on 1b = System power is on 0b = System power is off
	3	Last Power Event [7:5] reserved [4] 1b = Power is on (due to IPMI command) [3] 1b = Power down (due to power failure) [2] 1b = Power down (due to power interlock state) [1] 1b = Power down (due to power overload state) [0] 1b = AC failed
	4	Misc. Chassis State [7:4] reserved [6] 1b = Chassis Identify command supported [5:4] Chassis LED State 00b = Off 01b = On (definite time) 10b = On (indefinite) 11b = reserved [3] 1b = FAN failure detected [2] 1b = Drive failure detected [1] 1b = Button disabled from forced chassis power-off/reset [0] 1b = Chassis intrusion active
	(5)	Front Panel Button Capabilities and disable/enable status (Option)

4.1.3 Chassis Control (NetFN:00h, CMD:02h)

Use the command to power on/off nodes.
This command only issues power-on/off instructions, and the power-on/off processing is executed separately.
If the destination is the chassis, "Not supported" (Completion Code: C1h) is the response.

Table 4.3 Chassis Control Format

	Byte	Data Field
Request Data	1	[7:4] reserved [3:0] chassis control 0h = Power down 1h = Power up 2h = Power cycle (Not supported) 3h = Hard reset 4h = Pulse Diagnostic Interrupt 5h = Initiate a soft-shutdown 6h-Fh = reserved
Response Data	1	Completion Code

4.1.4 OEM Command Table

This section shows a list of OEM commands.

Table 4.4 OEM Commands

NetFn = OEM(34h)

Command	Synchronization	CMD	Privilege	Target(*1)		Interface
				Chassis	Node	
Set Boot Script Number	Synchronous	2Eh	User	-	Supported	LAN
Get Boot Script Number	Synchronous	4Fh	User	-	Supported	LAN

4.1.5 Set Boot Script Number (NetFN: 34h, CMD: 2Eh)

This command sets the boot script number for a node.

Table 4.5 Set Boot Script Number Format

	Byte	Data Field
Request Data	1	Boot Script Number 00h = Disk boot 01h = Not supported 02h = For OS installation 80h = Stop at UEFI without boot FFh = Automatically select DISK boot.
Response Data	1	Completion Code

4.1.6 Get Boot Script Number (NetFN: 34h, CMD: 4Fh)

The response is the set boot script number at "Node."

Table 4.6 Get Boot Script Number Format

	Byte	Data Field
Request Data	-	-
Response Data	1	Completion Code
	2	Boot Script Number 00h = Disk boot 01h = Not supported 02h = For OS installation 80h = Stop at UEFI without boot FFh = Automatically select DISK boot.

Appendix A REMCS

This appendix describes REMCS settings.

A.1 REMCS Settings

CAUTION

Customer Information Entry

If you register customer information with the REMCS center, a "registration completion" notification (sent by e-mail and by letter in an envelope) will be issued to the customer. To avoid problems with the customer, be sure to check with the customer before entering any customer information.

A.1.1 Preparing the Environment

This section describes the environment and conditions required for connecting to the REMCS center and starting services.

A.1.1.1 Conditions for Connecting to the REMCS Center

The following conditions must be met to connect the customer's device to the REMCS center.

■ For Internet Connection

- The customer's device is in an environment that can connect to the Internet.
- E-mail can be sent via the Internet.

Note

- Permission to send e-mails via the Internet may be required, depending on the customer's network environment. For details, check with the customer's network administrator.

Remarks

- The customer needs to prepare security mechanisms, such as a firewall, as required.

A.1.1.2 Preparing Settings

■ Preparing Network-Related Information

The network-related information shown in Table A.1 is required for making the settings for the customer's device and setting up the REMCS agent.

Note

- The contents of the settings depend on the network environment used by the customer.

Table A.1 For Internet Connection

Item		Description
System (device) settings		
1	IP address	IP address of the device - Subnet mask - Default gateway
2	Domain name system (DNS)	Settings of the DNS server used for resolving network computer names (host names) - Host name and domain name of the device - IP address of the DNS server
REMCS agent settings		
1	Mail (SMTP) server	Host name and domain name (or IP address) of the mail server used when the REMCS agent sends an e-mail
2	E-mail address for communication	E-mail address used when the REMCS agent sends an e-mail
3	E-mail address for the administrator	E-mail address used when the center provides the customer with information

■ Other

- IP address or FQDN of the mail server used
- E-mail address of the sender (Permission to send e-mails to addresses outside the company is required.)

Remarks

- Ask the customer to obtain the sender's e-mail address.

A.1.2 Configuring REMCS

Start configuring REMCS when the REMCS center connection environment is ready.

1. Log in to the Web GUI, and select [Maintenance] - [REMCS] to open the REMCS menu.

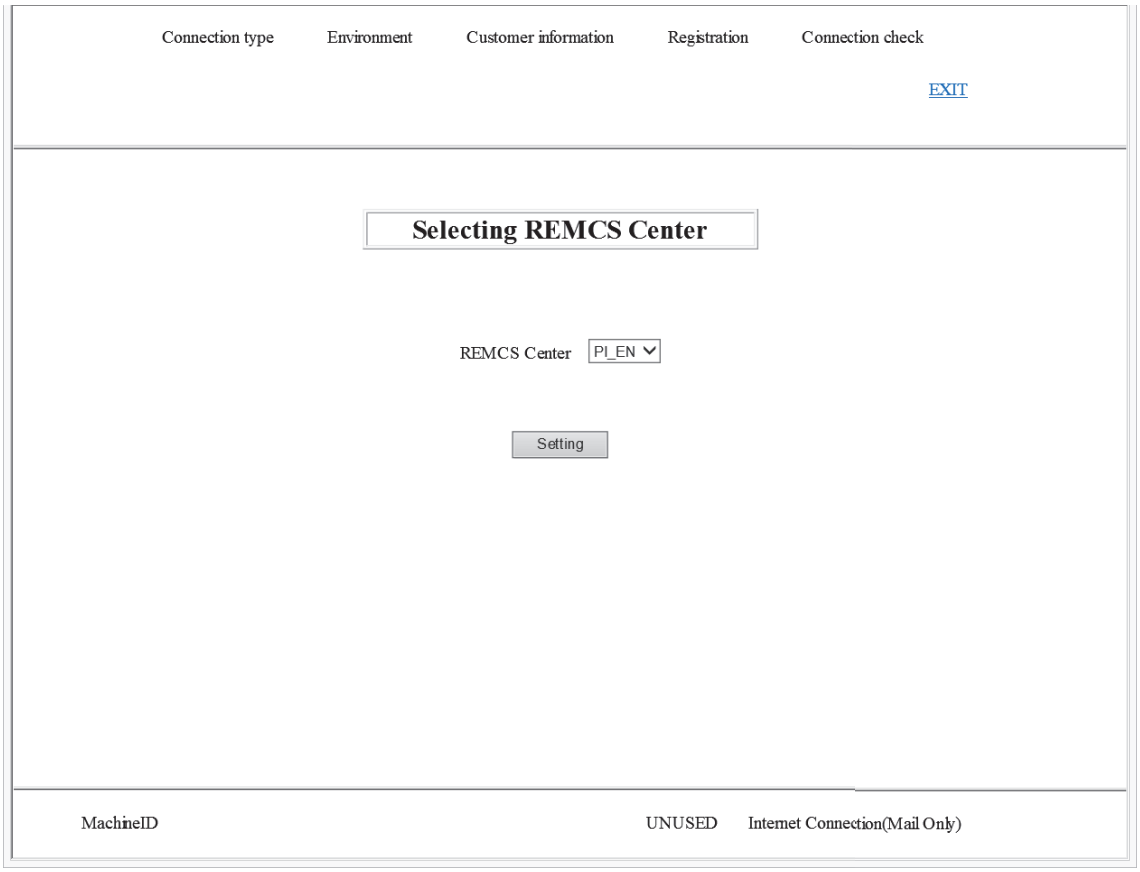
   If REMCS settings have not been completed, the [Customer Information Registration Instructions] screen shown in Figure A.1 appears.

Figure A.1 [Customer Information Registration Instructions] Screen

2. Confirm that the model name and serial number matches the contents displayed in [MachineID] at the bottom left of the [Customer Information Registration Instructions] screen. Then, click the [Next] button.

   The [Selecting REMCS Center] screen appears.

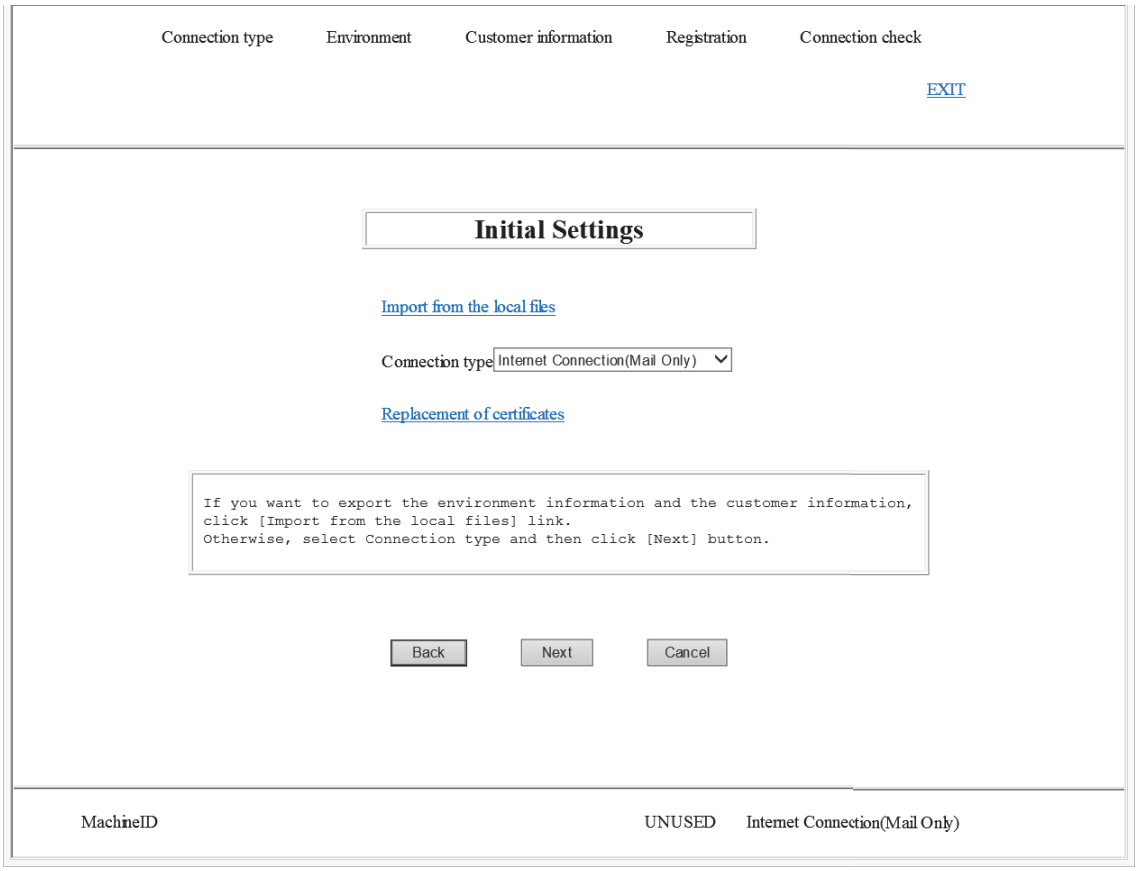
Figure A.2 [Selecting REMCS Center] Screen



3. Select from [REMCS Center] on the [Selecting REMCS Center] screen, and click the [Setting] button.

   The [Initial Settings] screen appears.

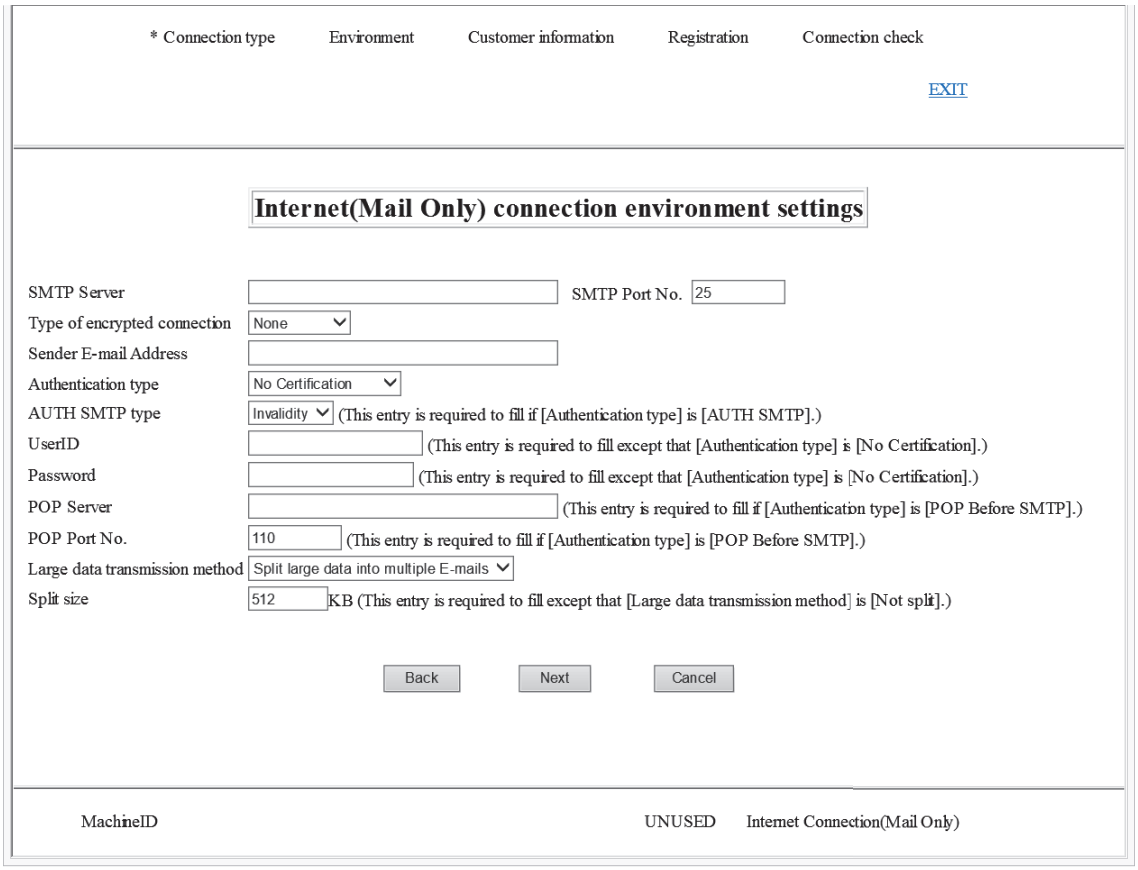
Figure A.3 [Initial Settings] Screen



4. Select [Internet Connection(Mail Only)] in [Connection type], and click the [Next] button.

   The [Internet(Mail Only) connection environment settings] screen appears.

Figure A.4 [Internet Connection environment settings] Screen



5. Specify information for sending e-mails.

Table A.2 Information Specified on the [Internet(Mail Only) connection environment settings] Screen

Input Item	Input Required?	Description
SMTP Server	Yes	Specify the SMTP server name or IP address with up to 128 single-byte alphanumeric characters.
Sender E-mail Address	Yes	Specify the sender's e-mail address with up to 128 single-byte alphanumeric characters.
Authentication type	-	Select an authentication type from the following: - No Certification - POP Before SMTP - AUTH SMTP
AUTH SMTP type(*1)	-	Select the AUTH SMTP type from the following: - AUTO (Default) - CRAM-MD5 - PLAIN - LOGIN
UserID	Conditional(*2)	Specify the user ID for the authentication server with up to 64 single-byte alphanumeric characters.

Table A.2 Information Specified on the [Internet(Mail Only) connection environment settings] Screen *(continued)*

Input Item	Input Required?	Description
Password	Conditional(*2)	Specify the password for the authentication server with up to 64 single-byte alphanumeric characters. "*" (asterisk) is displayed for every specified character.
POP Server	Conditional(*3)	Specify the POP server name or IP address with up to 128 single-byte alphanumeric characters.
Large data transmission method(*4)	-	Select a large data transmission method from the following: - No split - Split large data into multiple E-mails - Split event (Default)
Split size	Conditional(*5)	Specify the division size with up to 3 single-byte digits. - If [Split large data into multiple E-mails] is selected in [Large data transmission method], specify a value between 10 and 100 KB. The default is 64 KB. - If [Split event] is selected in [Large data transmission method], specify a value between 64 and 512 KB. The default is 512 KB.
Encryption type(*4)	-	Select an encryption type from the following: - S/MIME format (Default) - Conventional format Conventionally, encryption is performed during REMCS file format creation. Instead, REMCS supports the generally used S/MIME encrypted e-mail method.

*1 Valid only when [AUTH SMTP] is selected in [Authentication type]

*2 Required when anything other than [No Certification] is selected in [Authentication type]

*3 Required when [POP Before SMTP] is selected in [Authentication type]

*4 The selectable encryption types change as follows according to the large data transmission method:

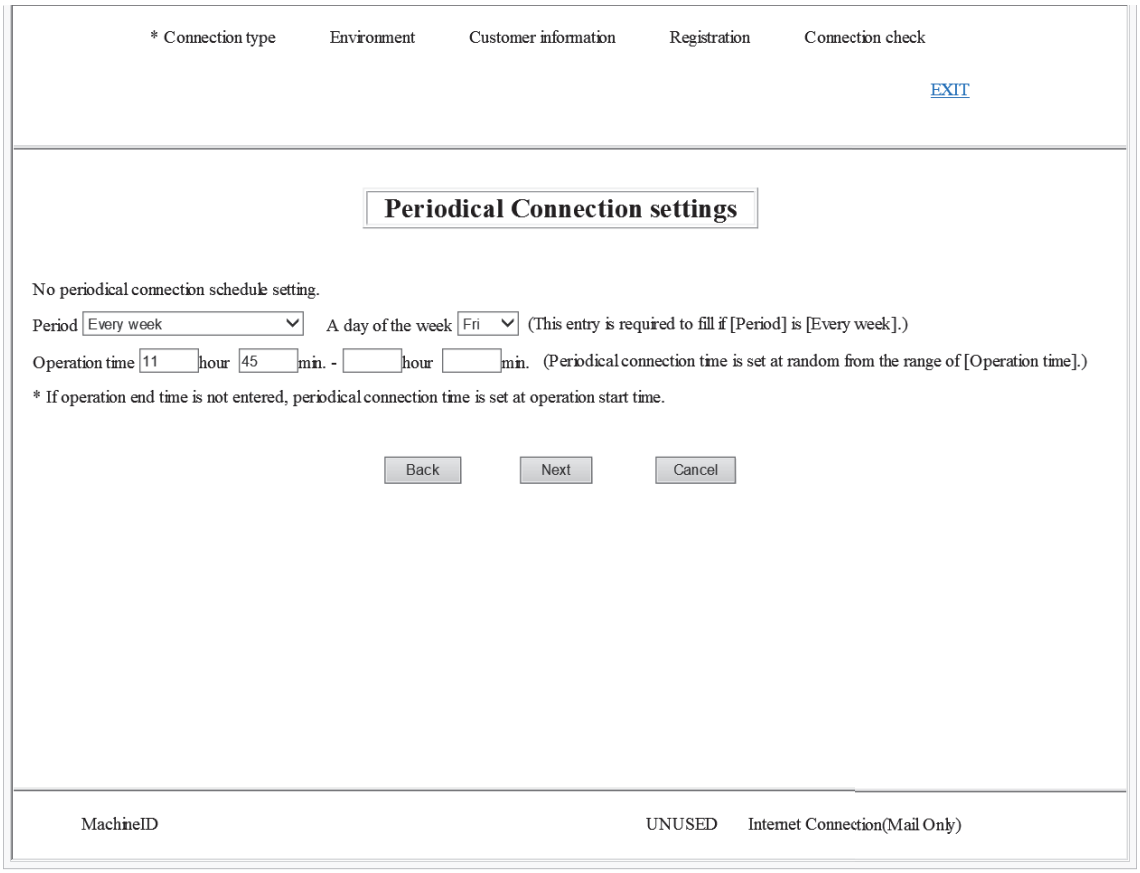
- No split: Both formats selectable
- Split large data into multiple E-mails: Conventional format only
- Split event: Both formats selectable

*5 Required when [No split] is selected in [Large data transmission method]

6. Click the [Next] button.

   The [Periodical Connection settings] screen appears.

Figure A.5 [Periodical Connection settings] Screen



7. Specify the periodical connection schedule.

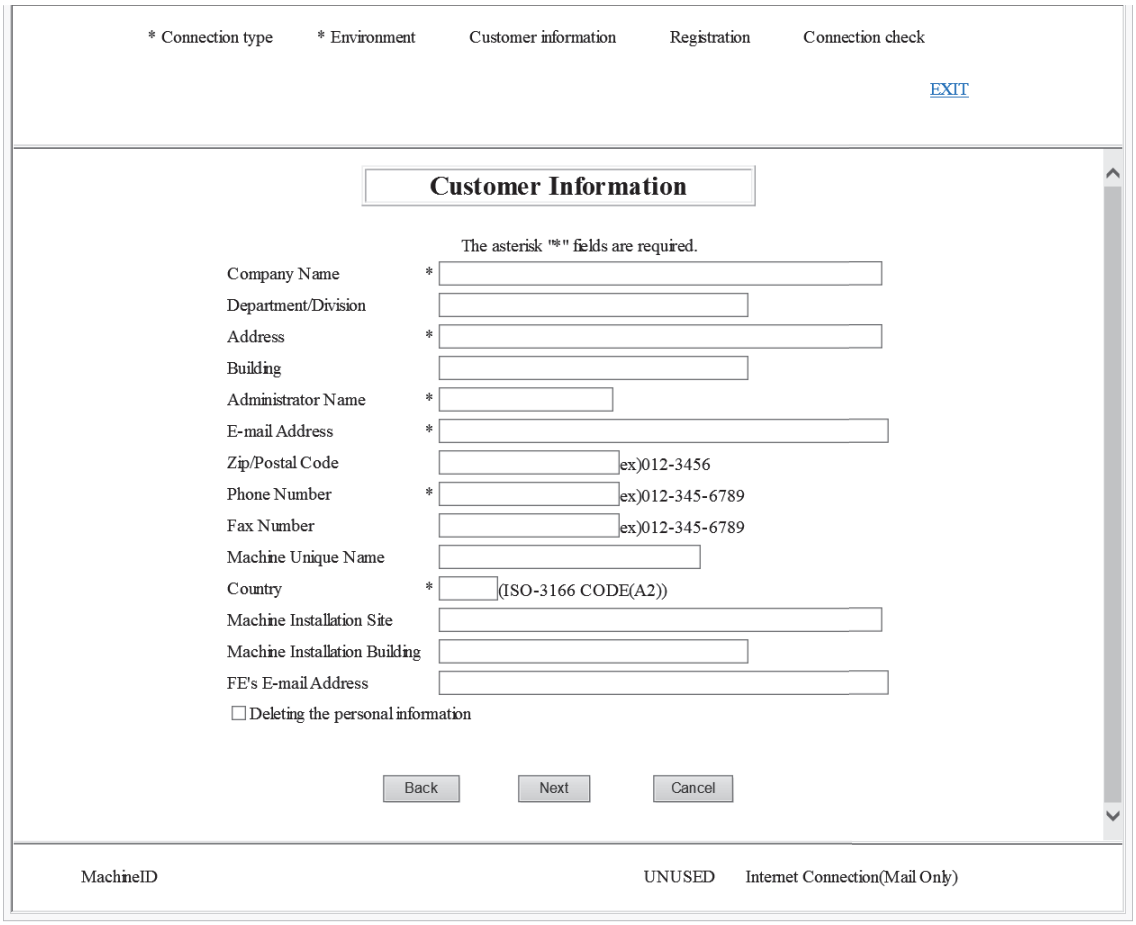
Table A.3 Information Specified on the [Periodical Connection settings] Screen

Input Item	Input Required?	Description
Period	-	Select a schedule from the following: - Weekly - Daily - Daily (except Sundays) - Daily (except weekends) - Once a week
A day of the week	-	If [Weekly] or [Once a week] is selected in [Schedule], specify a day of the week between [Sunday] and [Saturday].
Operation time (start) hour	Yes	Specify a single-byte number between 0 and 23 for the hour of the operation start time.
Operation time (start) min.	Yes	Specify a single-byte number between 0 and 59 for the minute of the operation start time.
Operation time (end) hour	Yes	Specify a single-byte number between 0 and 23 for the hour of the operation end time.
Operation time (end) min.	Yes	Specify a single-byte number between 0 and 59 for the minute of the operation end time.

8. Click the [Next] button.

   The [Customer Information] screen appears.

Figure A.6 [Customer Information] Screen



9. Specify customer information.

Table A.4 Information Specified on the [Customer Information] Screen

Input Item	Input Required?	Description
Company name	Yes	Specify the company name with up to 60 characters.
Department/Division	No	Specify the customer's department/division name with up to 40 characters.
Address	Yes	Specify the customer's address with up to 60 characters.
Building	No	Specify the building name of the customer's office with up to 40 characters.
Administrator Name	Yes	Specify the name of the customer's server administrator with up to 40 characters.
E-mail Address	Yes	Specify the e-mail address of the customer's server administrator with single-byte alphanumeric characters.

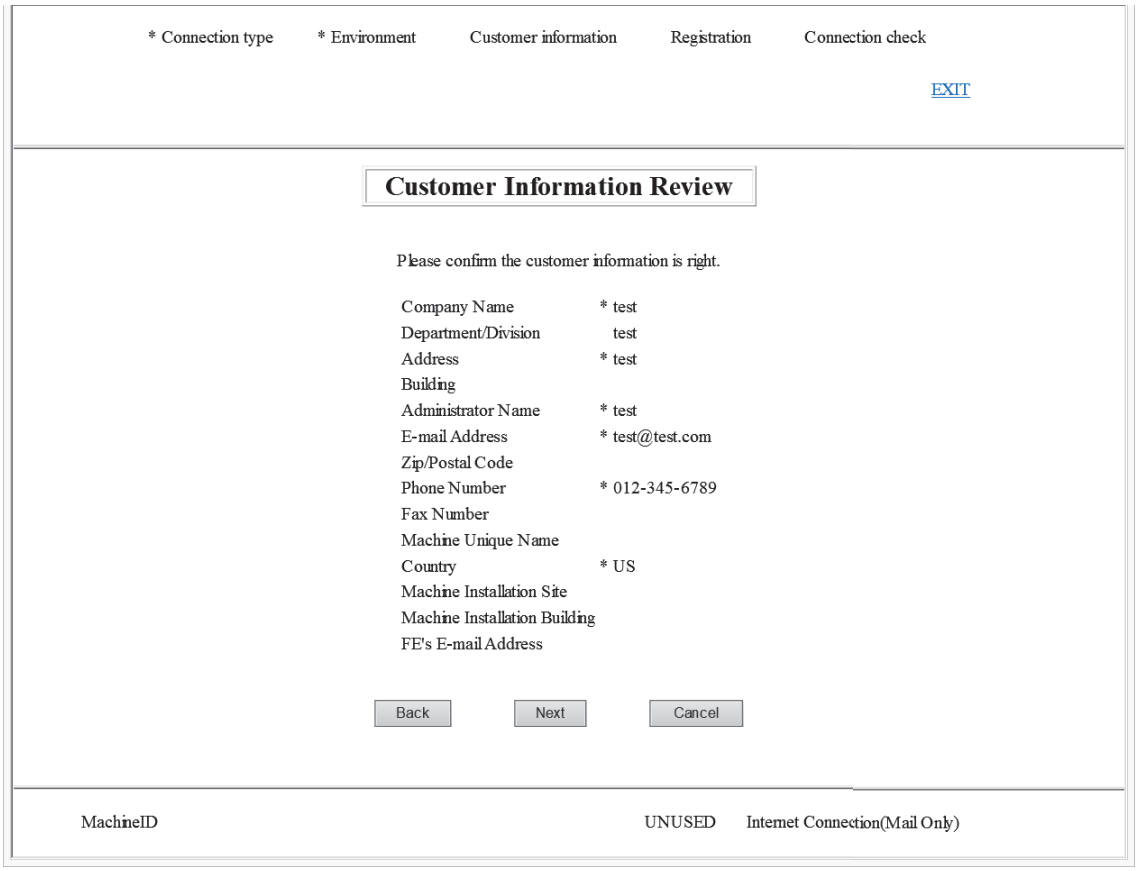
Table A.4 Information Specified on the [Customer Information] Screen *(continued)*

Input Item	Input Required?	Description
Zip/Postal	No	Specify the zip/postal code of the customer's office address with single-byte digits and a hyphen (-). The number of characters that can be specified corresponds to the device installation location in the country. The number is defined in the definition file. If not defined in the definition file, the number of characters that can be specified is 10.
Telephone Number	Yes	Specify the customer's telephone number with single-byte digits and a hyphen (-).
FAX Number	No	Specify the customer's fax number with single-byte digits and a hyphen (-).
Machine Unique Name	No	Specify the customer-specific name with up to 32 single-byte alphanumeric characters. We recommend specifying the rack number assigned to the FX700 system.
Country	Yes	Specify the country name with 2 alphabetic characters. If specified with lowercase characters, those characters are converted to uppercase characters. Specify 99 for an unspecified country.
Machine Installation Site	No	Specify the machine installation site with up to 60 characters.
Machine Installation Building	No	Specify the building name of the machine installation site with up to 40 characters.
FE's E-mail Address	No	Specify the FE's e-mail address with single-byte alphanumeric characters.
Deleting the personal information	No	To delete personal information with [Deleting the personal information] from the [FE operation] menu, check the check box. If checked, [Deleting the personal information] deletes the following customer information: - Administrator name - E-mail address - Telephone number - FAX number - FE's e-mail address For details on [Deleting the personal information], see "A.2.6 Deleting the Personal Information."

10. Click the [Next] button.

    The [Customer Information Review] screen appears.

Figure A.7 [Customer Information Review] Screen



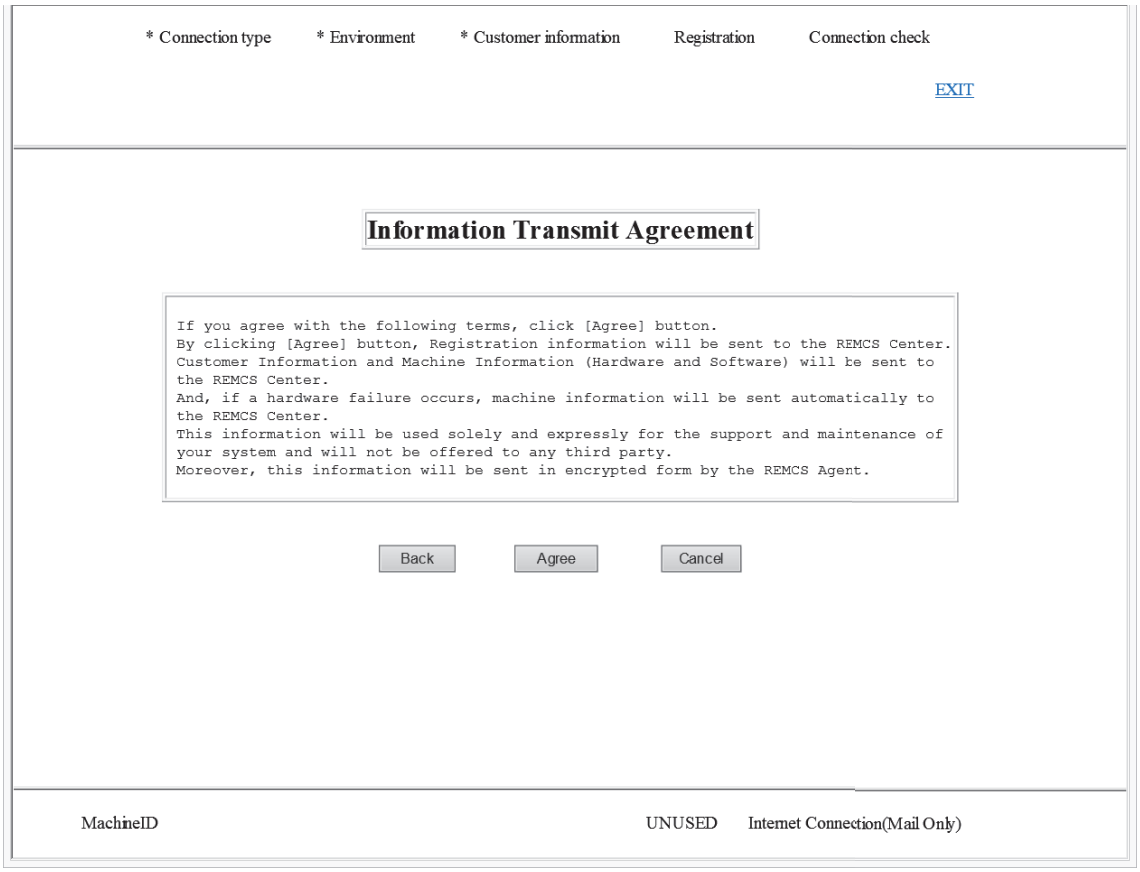
11. Confirm there is no error in the customer information, and click the [Next] button.

    The [Information Transmit Agreement] screen appears.

    Remarks

    - If the customer information has an error, click the [Back] button to return to the [Customer Information] screen, and correct the customer information.

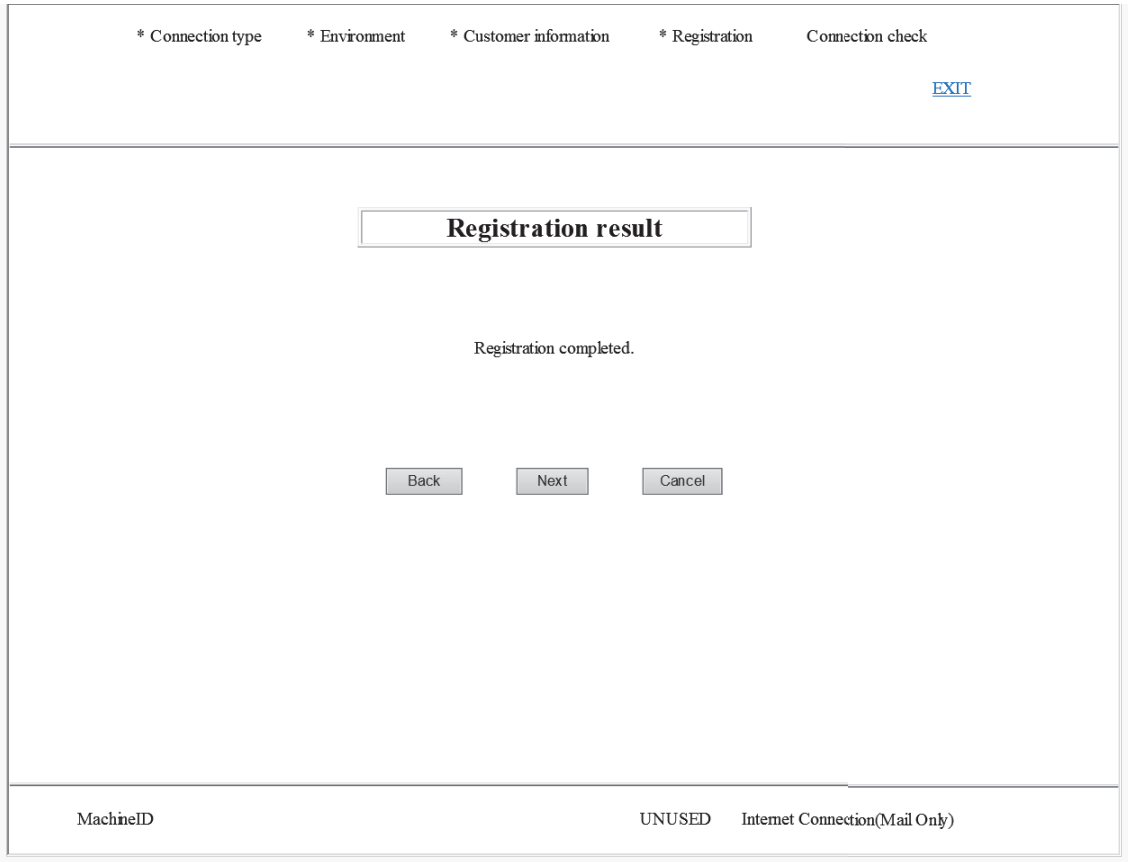
Figure A.8 [Information Transmit Agreement] Screen



12. Confirm that the environment allows e-mail sending before clicking the [Agree] button.

    The entered information is sent to the REMCS center, and the [Registration result] screen appears.

Figure A.9 [Registration result] Screen



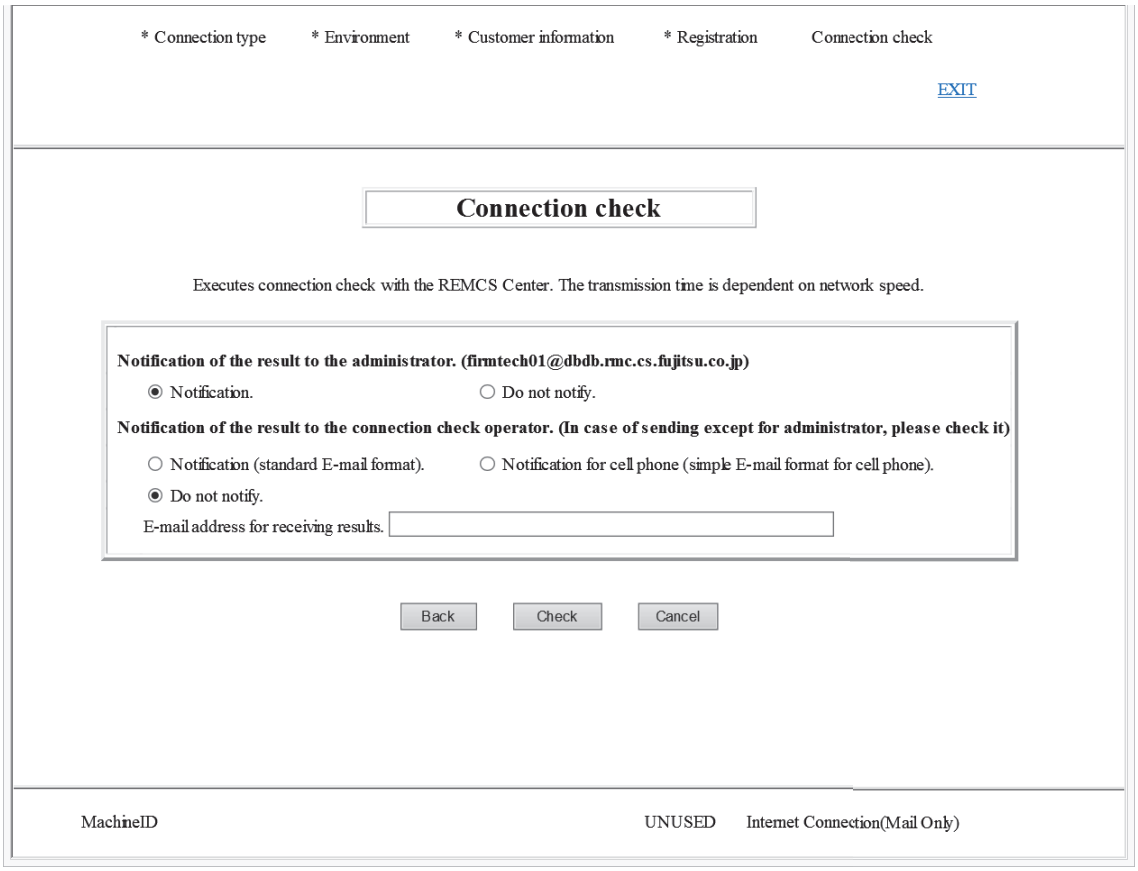
13. Confirm that the registration was successful, and click the [Next] button.

    The [Connection check] screen appears.

    Remarks

    - If registration fails, click the [Back] button, and correct the information.

Figure A.10 [Connection check] Screen



14. Specify the send destination for the connection check result.

Table A.5 Information Specified on the [Connection check] Screen

Input Item	Input Required?	Description
Notification of the result to the administrator(*1)	-	Specify whether the customer's administrator needs to be notified of the result. The default is that [Notification] is selected.
E-mail address of the administrator(*2)	No	Specify the e-mail address of the customer 's server administrator with up to 60 single-byte alphanumeric characters. If specification of [E-mail address of the administrator] is omitted even though [Notification] is selected for [Notification of the result to the administrator], the result notification is sent to the e-mail address registered with the REMCS center.
Notification of the result to the connection check operator.(In case of sending except for administrator, please check it)	-	Specify whether the person who performed the work needs to be notified of the result. The default is that [Do not notify] is selected.

Table A.5 Information Specified on the [Connection check] Screen *(continued)*

Input Item	Input Required?	Description
E-mail address for receiving results	Conditional(*3)	Using up to 60 single-byte alphanumeric characters, specify the e-mail address of the person who performed the work.

*1 If the personal information has not been deleted, this item displays the e-mail address of the customer's server administrator as specified in [E-mail Address] on the [Customer Information] screen.

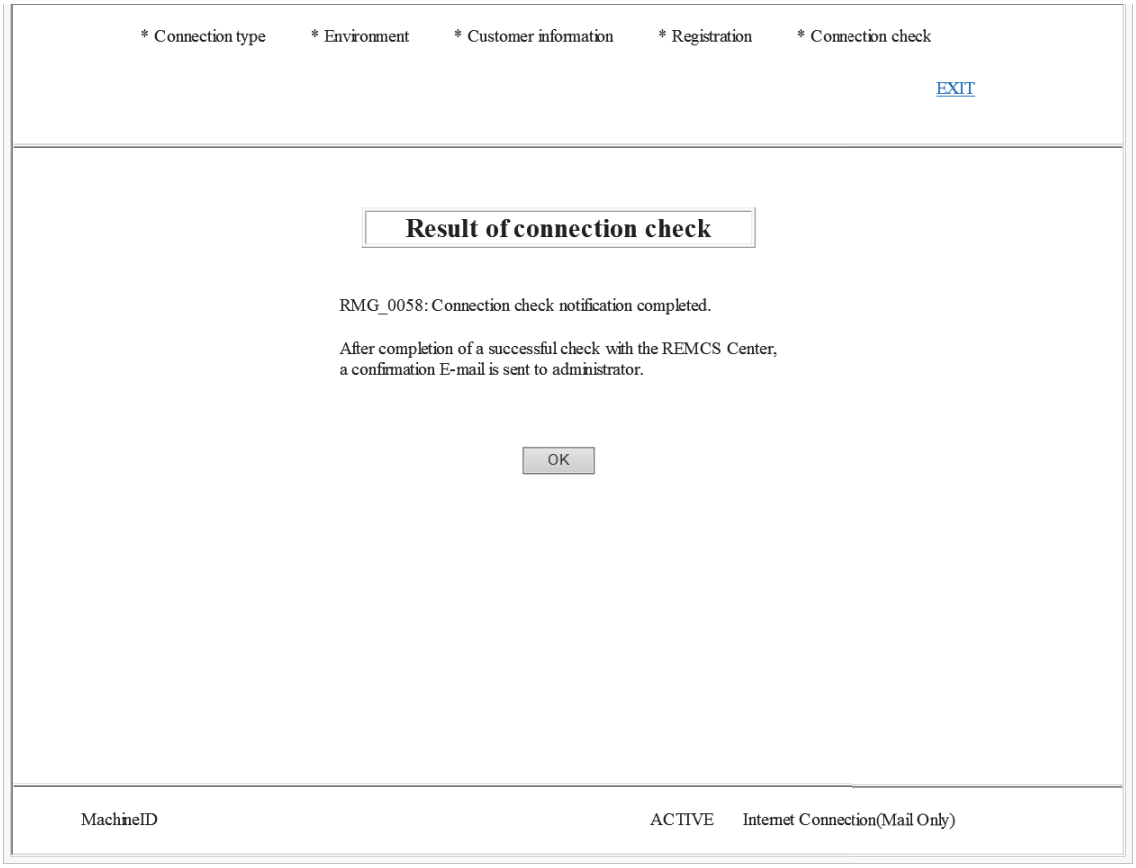
*2 This is displayed only if the personal information has been deleted by [Deleting the personal information] from the [FE operation] menu.

*3 Input is required if [Notification] is selected for [Notification of the result to the connection check operator].

15. Click the [Check] button.

    The [Result of connection check] screen appears.

Figure A.11 [Result of connection check] Screen



16. Click the [OK] button.

    The browser returns to the [Selecting REMCS Center] screen.

A.2 REMCS Detail Setup

Log in to the Web GUI, and select [Maintenance] - [REMCS Detail Setup] to display the [REMCS FE

menu] screen.
Execute a detailed REMCS setup from the [FE operation] menu on the [REMCS FE menu] screen.
By selecting appropriately from the menu on the [FE operation menu] screen, you can select the REMCS center, switch the display language between Japanese and English, configure detailed environment settings, delete personal information, etc.

A.2.1 REMCS FE Menu (Initial Screen)

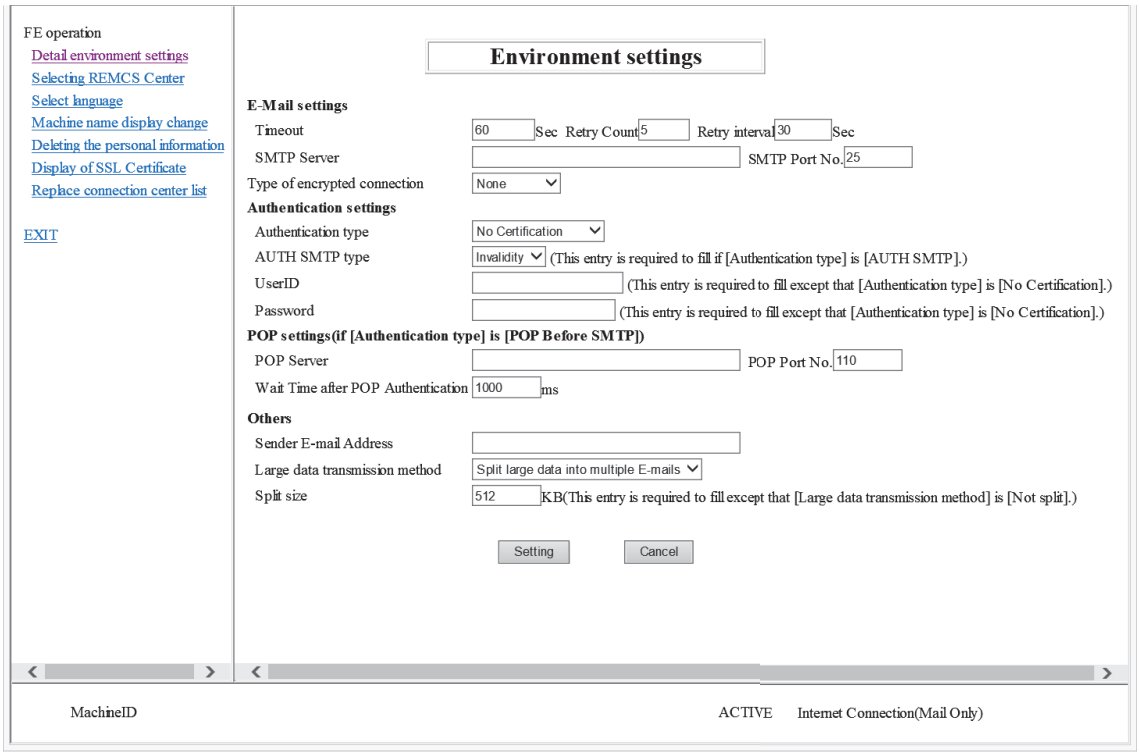
Figure A.12 shows the initial screen for the [REMCS FE menu] screen.

Figure A.12 REMCS FE Menu (Initial Screen)

A.2.2 Detail Environment Settings

Select [Detail environment settings] from the [FE operation] menu to display the [Environment settings] screen shown in Figure A.13.

Figure A.13 Detail Environment Settings



Specify the content shown in Table A.6 on the [Environment settings] screen.

Table A.6 Information Specified on the [Environment settings] Screen

Input Item	Input Required?	Description
E-Mail settings		
Timeout	Yes	Specify the e-mail timeout time (seconds) with up to 4 single-byte digits. You can specify a value between 60 and 3600.
Retry Count	Yes	Specify the e-mail retry count with up to 2 single-byte digits.
Retry interval	Yes	Specify the e-mail retry interval with up to 3 single-byte digits. You can specify a value between 1 and 600.
SMTP Server	Yes	Specify the SMTP server name or IP address with up to 128 single-byte alphanumeric characters.
SMPT Port No.	Yes	Specify the port number of the SMTP server with up to 5 single-byte digits. You can specify a value between 1 and 65535. The default is to use 25 (Well Known Port).
Type of encrypted connection	-	Select the type of encrypted connection for SMTP over SSL from the following when the definition file (RMG_Menu.def) has the display setting: - None (Default) - STARTTLS - SSL/TLS
Authentication settings		

Table A.6 Information Specified on the [Environment settings] Screen *(continued)*

Input Item	Input Required?	Description
Authentication type	-	Select an authentication type from the following: - No Certification - POP Before SMTP - AUTH SMTP
AUTH SMTP type(*1)	-	Select the AUTH SMTP authentication mechanism from the following: - AUTO (Default) - CRAM-MD5 - PLAIN - LOGIN
UserID	Conditional(*2)	Specify the user ID for the authentication server with up to 64 single-byte alphanumeric characters.
Password	Conditional(*2)	Specify the password for the authentication server with up to 64 single-byte alphanumeric characters. "*" (asterisk) is displayed for every specified character.
POP settings (if [Authentication type] is [POP Before SMTP])		
POP Server	Conditional(*3)	Specify the POP server name or IP address with up to 128 single-byte alphanumeric characters.
POP Port No.	Yes	Specify the port number of the POP3 authentication server with up to 5 single-byte digits. You can specify a value between 1 and 65535. The default is to use 110 (Well Known Port).
Wait Time after POP Authentication	Yes	Using up to 5 single-byte digits, specify the wait time (in milliseconds) until e-mail transfer begins after POP3 authentication. You can specify a value between 0 and 30000. The recommended value is 10000 milliseconds.
Others		
Sender E-mail Address	Yes	Specify the sender's e-mail address with up to 128 single-byte alphanumeric characters.
Large data transmission method(*4)	-	Select a large data transmission method from the following: - No split - Split large data into multiple E-mails - Split event (Default)

Table A.6 Information Specified on the [Environment settings] Screen *(continued)*

Input Item	Input Required?	Description
Split size	Conditional(*5)	Specify the division size with up to 3 single-byte digits. - If [Split large data into multiple E-mails] is selected in [Large data transmission method], specify a value between 10 and 100 KB. The default is 64 KB. - If [Split event] is selected in [Large data transmission method], specify a value between 64 and 512 KB. The default is 512 KB.

*1 Valid only when [AUTH SMTP] is selected in [Authentication type]

*2 Required when anything other than [No Certification] is selected in [Authentication type]

*3 Required when [POP Before SMTP] is selected in [Authentication type]

*4 The selectable encryption types change as follows according to the large data transmission method:

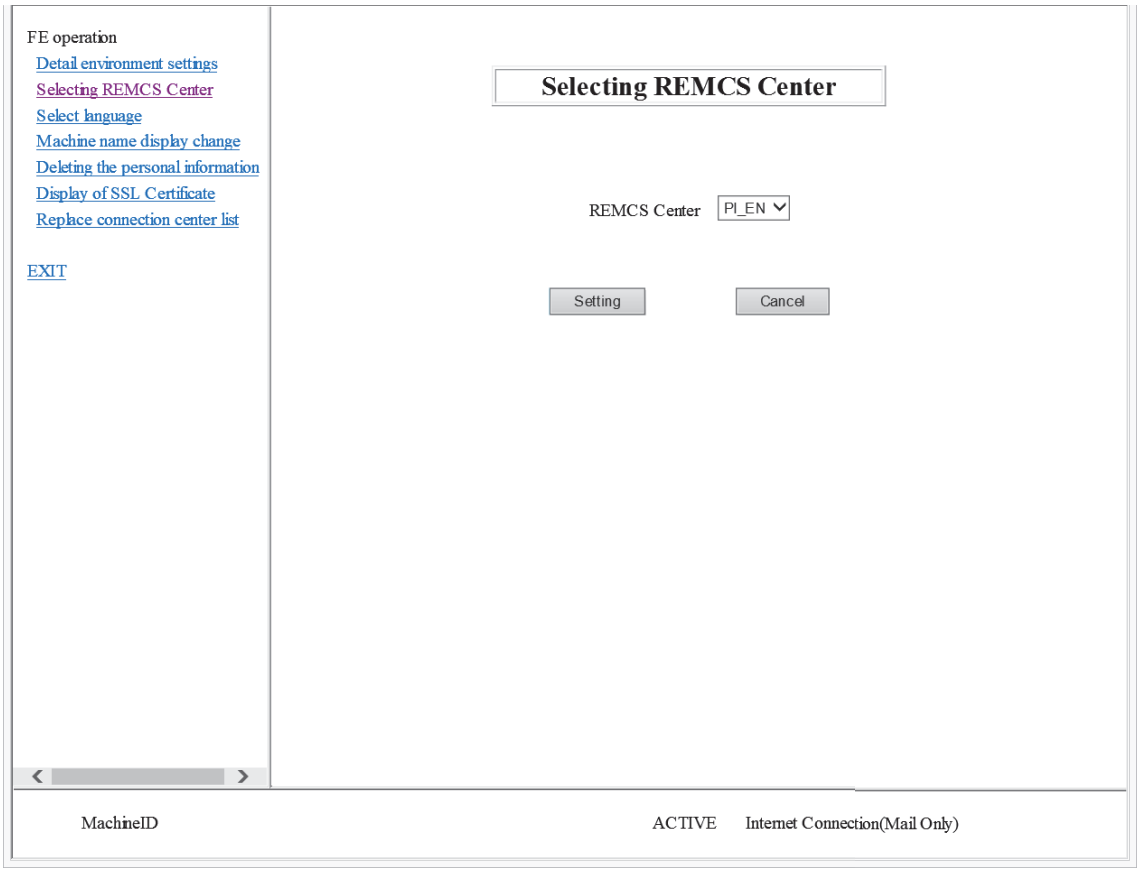
- No split: Both formats selectable
- Split large data into multiple E-mails: Conventional format only
- Split event: Both formats selectable

*5 Required when [No split] is selected in [Large data transmission method]

A.2.3 Selecting REMCS Center

Select [Selecting REMCS Center] from the [FE operation] menu to display the [Selecting REMCS Center] screen shown in Figure A.14.
Select from [REMCS Center] on the [Selecting REMCS Center] screen.

Figure A.14 Selecting REMCS Center



A.2.4 Select Language

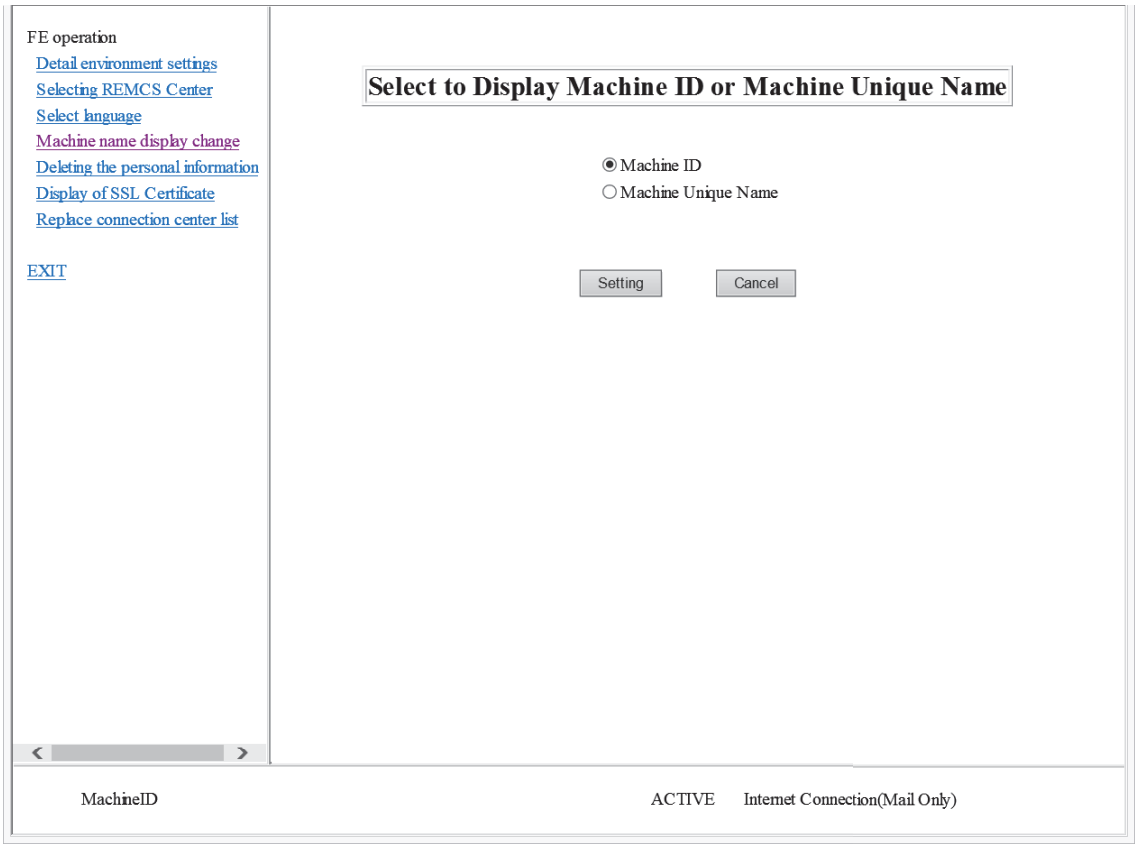
Select [Select language] from the [FE operation] menu to display the [Select language (Japanese or English)] screen shown in Figure A.15.
Specify the display language on the [Select language (Japanese or English)] screen.

Figure A.15 Select Language (Japanese or English)

A.2.5 Machine Name Display Change

Select [Machine name display change] from the [FE operation] menu to display the [Select to Display Machine ID or Machine Unique Name] screen shown in Figure A.16.
Specify on the [Select to Display Machine ID or Machine Unique Name] screen whether the machine name shown in the status display frame is a machine ID or machine unique name.

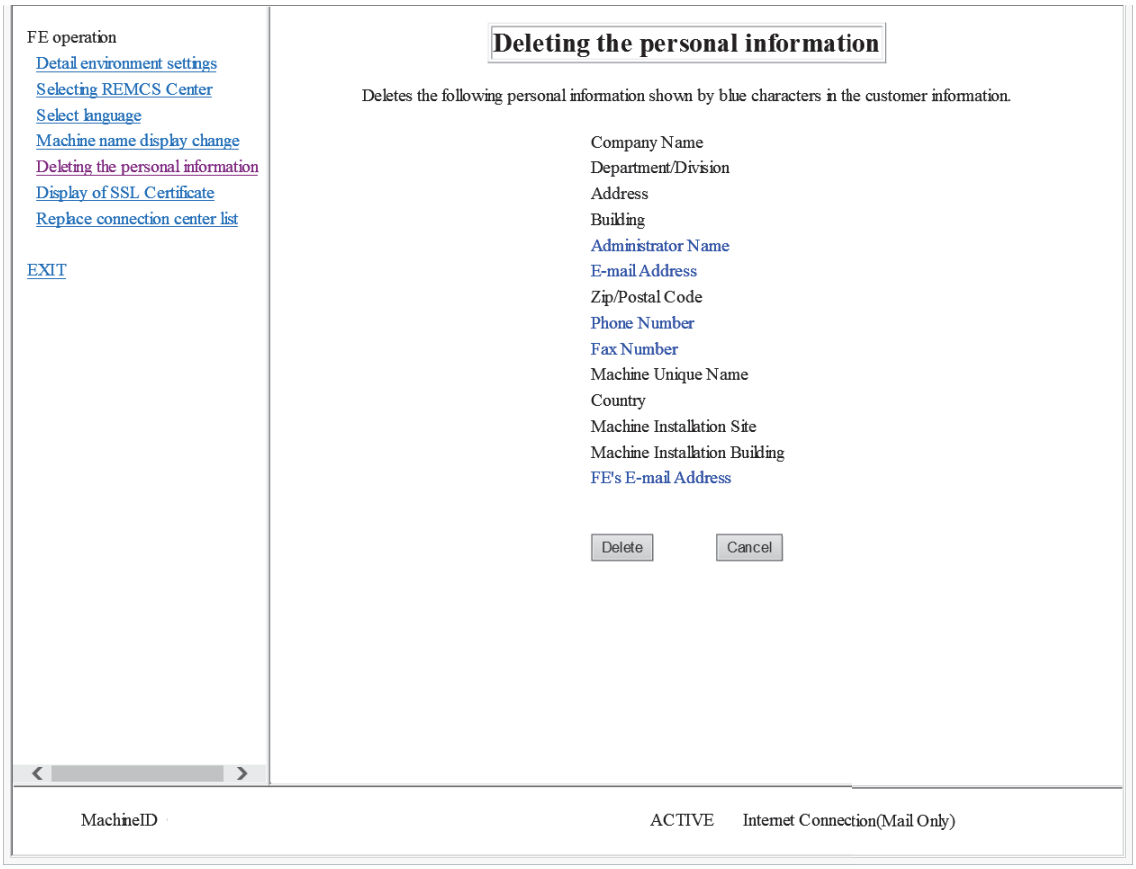
Figure A.16 Select to Display Machine ID or Machine Unique Name



A.2.6 Deleting the Personal Information

Select [Deleting the personal information] from the [FE operation] menu to display the [Deleting the personal information] screen shown in Figure A.17.
To delete the personal information included in customer information, click [Delete] on the [Deleting the personal information] screen.

Figure A.17 Deleting the Personal Information

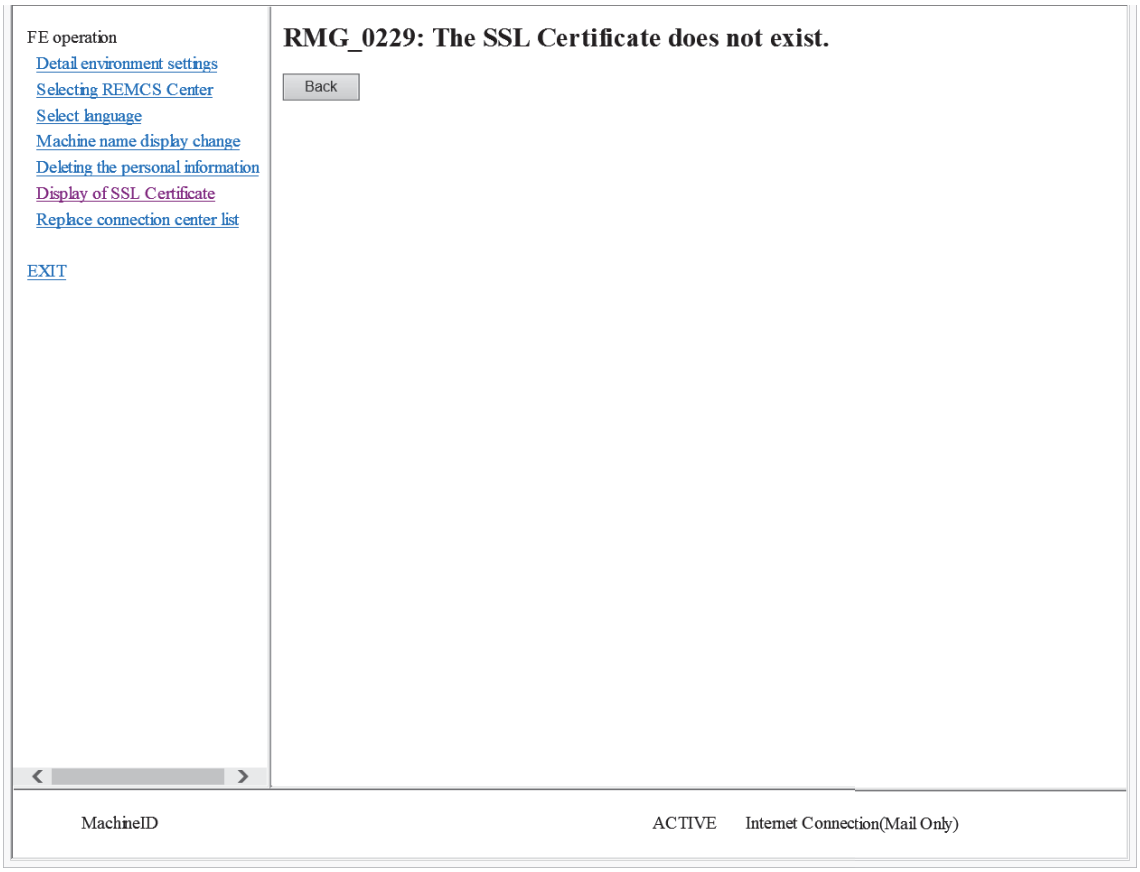


A.2.7 Display of SSL Certificate

Select [Display of SSL Certificate] from the [FE operation] menu to display the [Display of certificate] screen shown in Figure A.18 and Figure A.19.
If the SSL certificate exists, Figure A.18 appears. If the SSL certificate does not exist, Figure A.19 appears.

Figure A.18 Display of Certificate

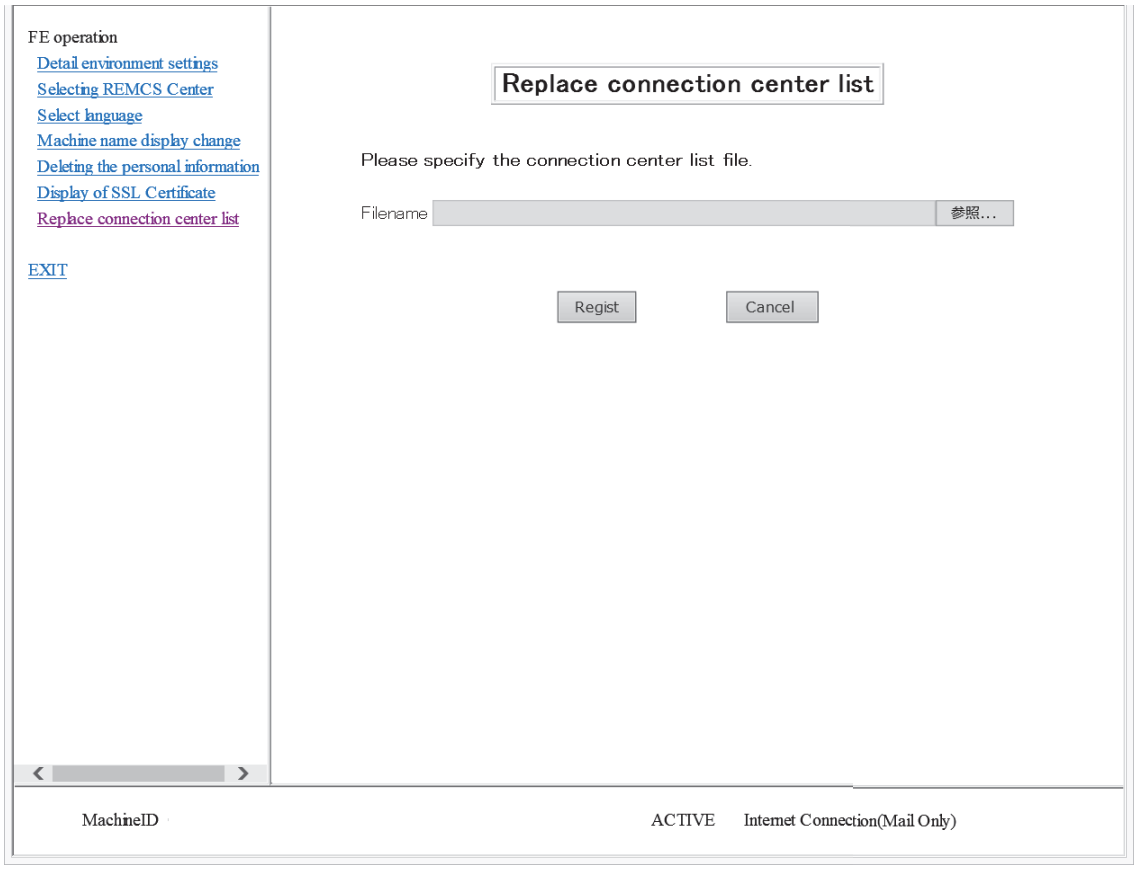
Figure A.19 Display When the SSL Certificate Does Not Exist

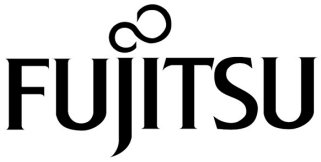


A.2.8 Replace Connection Center List

Select [Replace connection center list] from the [FE operation] menu to display the [Replace connection center list] screen shown in Figure A.20.
Specify and register the destination REMCS center list file on the [Replace connection center list] screen.

Figure A.20 Replace Connection Center List




FUJITSU