EXPRESSSCOPE Engine 2
User's Guide

3rd Edition Dec, 2007

TRADEMARKS AND PATENTS

Microsoft, Windows and Windows Vista are registered trademarks of Microsoft Corporation in the United States and other countries.
Firefox is registered trademarks of the Mozilla Foundation.
Java is registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

NOTES

(1) No part of this manual may be reproduced in any form without the prior written permission of NEC Corporation.
(2) The contents of this User’s Guide may be revised without prior notice.
(3) The contents of this User's Guide shall not be copied or altered without the prior written permission of NEC Corporation.
(4) All efforts have been made to ensure the accuracy of all information in this User's Guide. If you notice any part unclear, incorrect, or omitted in this User's Guide, contact the sales agent where you purchased this product.
(5) NEC assumes no liability arising from the use of this product, nor any liability for incidental or consequential damages arising from the use of this User's Guide regardless of Item (4).

ABOUT THIS USER' S GUIDE

This User's Guide provides the instructions for properly using the EXPRESSSCOPE Engine 2. Please keep this document at hand for a quick reference and use it when you encounter any questions or troubles while using the EXPRESSSCOPE Engine 2 for remote control, monitoring, and management of the host system.

Table of Contents

SYMBOLS

The following symbols are used throughout this manual.

Items to be observed or points to be noted when using this product.

Items to be checked when using this product or software.

Information useful or convenient for you.

Example of troubles occurred.

PREFACE

The EXPRESSSCOPE Engine 2 enables you to monitor the operating status of the host system (power supplies, fans, temperature and so forth), to operate the host system's keyboard, video, and mouse (KVM) from a remote console* and to access to CD-ROM/Floppy disk drives on a remote site*. The EXPRESSSCOPE Engine 2 is enabled by a system management LSI called "BMC (Baseboard Management Controller)" and thus referred to as the "BMC" hereinafter in this User's Guide.
*The Remote KVM and Remote Media functions are optional.

1. Overview

The host system comes standard with the BMC (system management LSI) and a management LAN port dedicated to the BMC. By connecting the management LAN port to your network, you can monitor and control the host system from a remote site via a Web browser and Telnet/SSH client.

With the optional N8115-03 Remote KVM and Media License, you can operate the host system's KVM (keyboard, video, and mouse) from a remote console and access CD-ROM/DVD-ROM/floppy disk drives and USB memory in a remote site.

2. Configuring the Host System

This chapter describes about the settings necessary to configure the BMC in the host system.

DEFAULT NETWORK SETTINGS

The BMC's default network settings are as follows:

IP Address:	**192.168.1.1**
User Name:	**administrator**
Password:	**(None)**

- Connect the management LAN port to the private network on which the default IP address "192.168.1.1"is reachable. If the default IP address is not reachable on the network, assign a new IP address to the management LAN by using the BIOS Setup Utility or NEC EXPRESSBUILDER in the host system. Refer to "Management LAN Settings" in the next page for the settings.

For security reasons, change the above default settings (IP address, User Name, and Password) to the ones appropriate in your network environment. Refer to "Network Configuration" in the "Chapter 5: Using Remote Management" for details.

- The remote management function is disabled by default. (In some systems, the remote management function is enabled by default.) So, enable necessary settings by using BIOS Setup Utility or NEC EXPRESSBUILDER. Refer to "Management LAN Settings" in the next page for the settings.

MANAGEMENT LAN SETTINGS

You can configure basic setting of management LAN settings of BMC for remote management using Web server function and command line interface of BMC by using BIOS Setup Utility or NEC EXPRESSBUILDER.

Settings by BIOS Setup Utility

This section describes about the settings of management LAN settings of BMC by using BIOS Setup Utility.

Press the F2 key during POST(Power on Self test) or displaying logo immediately after power on or reset the host system to enter the BIOS Setup Utility. And select [Server]-[BMC LAN Configuration].

You can configure following items on the BMC LAN configuration menu of the BIOS Setup Utility. After the configuration, execute [Exit]-[Save Changes] to apply change of the configuration. Please refer to the User's Guide of your host system for more details.

Shared BMC LAN

Select [Enabled] to share a system LAN port with BMC LAN. If you use a management LAN port for the BMC, select [Disabled]. The management LAN port is not available when this setting is set [Enabled]. (Default setting is [Disabled]. In some systems, this menu is not supported. Please refer to the User's Guide of your host system for more details.)

IP Address

If DHCP is not used to automatically obtain an IP address, enter the BMC's IP address.
If DHCP has been used, an automatically obtained IP address will appear.
(Default setting is 192.168.1.1.)

Subnet Mask

If DHCP is not used to automatically obtain a subnet mask IP address, enter the subnet mask of your management LAN.
If DHCP has been used, an automatically obtained subnet mask IP address will appear. (Default setting is 255.255.255.0.)

Default Gateway

If DHCP is not used to automatically obtain a default gateway IP address, enter the default gateway of your management LAN.
If DHCP has been used, an automatically obtained default gateway will appear.
(Default setting is 0.0.0.0.)

DHCP

If you want to obtain an IP address, choose [Enabled].
If you want to manually configure an IP address, choose [Disabled].
(Default setting is [Disabled](*).)

Web Interface:

HTTP Interface

Select [Enabled] to use the Web Server function using the HTTP. If not, select [Disabled]. (Default setting is [Disabled](*).)

HTTP Port Number

Specify the HTTP port number. (Default setting is 80.)

HTTPS Interface

Select [Enabled] to use the Web Server function using the HTTPS(SSL). If not, select [Disabled]. (Default setting is [Disabled](*).)

HTTPS Port Number

Specify the HTTPS(SSL)port number. (Default setting is 443.)

Command Line Interface:

Telnet

Select [Enabled] to use the Command Line Interface using telnet. If not, select [Disabled]. (Default setting is [Disabled](*).)

Telnet Port Number

Specify the BMC's Telnet port number. (Default setting is 23.)

SSH

Select [Enabled] to use the Command Line Interface using SSH. If not, select [Disabled]. (Default setting is [Disabled](*).)

SSH Port Number

Specify the BMC's SSH port number. (Default setting is 22.)

Clear BMC Configuration

The BMC Configuration will be cleared. Please use this function when you forgot your user name and password, etc. for remote management via a Web browser and command line interface. This function will be executed when you select "YES" on confirmation menu which appears after pressing the "Enter" key. This menu invokes the BMC configuration clear operation after selecting the "YES".

- **These BMC Management LAN-related settings of BMC are not changed to default settings by executing the "Load Setup Default" of BIOS Setup Utility. (Execute the "Clear BMC Configuration" to set default settings to the BMC Management LAN settings.)**
- **It typically takes about several tens of seconds to complete initialization by the "Clear BMC Configuration".**

The Clear BMC Configuration also deletes the settings for DianaScope (a software application bundled for remote management). Be sure to perform a backup for the DianaScope settings before you change the BMC settings.

* In some systems, the default settings are [Enabled] for DCHP, HTTP, HTTPS, Telnet, and/or SSH. Please refer to the User's Guide of your host system for more details.

Settings by NEC EXPRESSBUILDER

This section describes configuration for management LAN settings of BMC by using NEC EXPRESSBUILDER.

Start the NEC EXPRESSBUILDER DVD-ROM in the host system, and select [Tool]-[System Management]. Following settings are enabled.

Setup for BMC Web Server

Server

Obtain an IP address automatically (DHCP)

If you want to obtain an IP address, select [Enable].
If you want to manually configure an IP address, select [Disable].
(Default setting is [Disable] (*).)

IP Address

If DHCP is not used to automatically obtain an IP address, enter the BMC's IP address.
If DHCP has been used, an automatically obtained IP address will appear.
(Default setting is 192.168.1.1.)

Subnet Mask

If DHCP is not used to automatically obtain a subnet mask IP address, enter the subnet mask of your management LAN.
If DHCP has been used, an automatically obtained subnet mask IP address will appear. (Default setting is 255.255.255.0.)

Default Gateway

If DHCP is not used to automatically obtain a default gateway IP address, enter the default gateway of your management LAN.
If DHCP has been used, an automatically obtained default gateway will appear..
(Default setting is 0.0.0.0.)

Connection Setting

HTTP

Select [Enable] to use the Web Server function using the HTTP. If not, select [Disable]. (Default setting is [Disable] (*).)

HTTP TCP Port Number:

Enter the TCP port number used for HTTP connection on your management LAN.
(Default setting is 80.)

HTTPS

Select [Enable] to use the Web Server function using the HTTPS(SSL). If not, select [Disable]. (Default setting is [Disable] (*).)

HTTPS TCP Port Number:

Enter the TCP port number used for HTTPS connection on your management LAN.
(Default setting is 443.)

Telnet

Select [Enable] to use the Command Line Interface using telnet. If not, select [Disable]. (Default setting is [Disable] (*).)

Telnet Port Number

Enter the TCP port number used for telnet connection on your management LAN .
(Default setting is 23.)

SSH

Select [Enable] to use the Command Line Interface using SSH. If not, select [Disable]. (Default setting is [Disable] (*).)

SSH Port Number

Enter the TCP port number used for SSH connection on your management LAN. (Default setting is 22.)

Confirm that you have entered correct information, and select [OK] and press “Enter” key for registration.

LAN Port Setting

Shared BMC LAN

Select [Enable] to share a system LAN port with BMC LAN. If you use a management LAN port for the BMC, select [Disable]. The management LAN port is not available when this setting is set [Enable]. (Default setting is [Disable])

This menu appears for the system which supports this function. Please confirm the presence of this function on the [BMC LAN Configuration] of the BIOS Setup Utility for the support of this function. Please refer to the User's Guide of your host system for more details.

Confirm that you have entered correct information, and select [OK] and press “Enter” key for registration.

Clear BMC Configuration

The BMC Configuration will be cleared. Please use this function when you forgot your user name and password, etc. for remote management via a Web browser and command line interface. This function will be executed when you press "Enter"("Execute") key on confirmation menu which appears after selecting this menu and pressing "Enter" key.

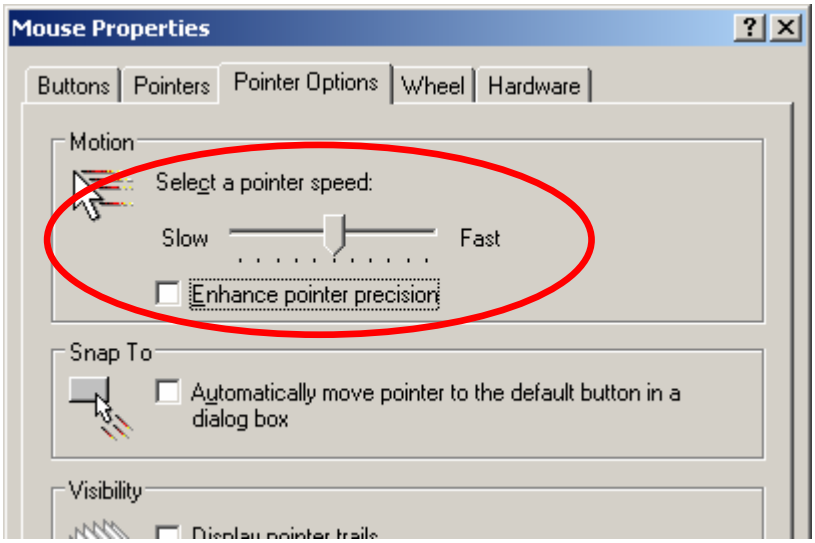
It typically takes about several tens of seconds to complete initialization by the "Clear BMC Configuration".

The Clear BMC Configuration also deletes the settings for DianaScope (a software application bundled for remote management). Be sure to perform a backup for the DianaScope settings before you change the BMC settings.

* In some systems, the default settings are [Enable] for DCHP, HTTP, HTTPS, Telnet, and/or SSH. Each default setting is same as the BIOS Setup Utility’s one. Please refer to the User's Guide of your host system for more details.

MOUSE PROPERTIES SETTINGS

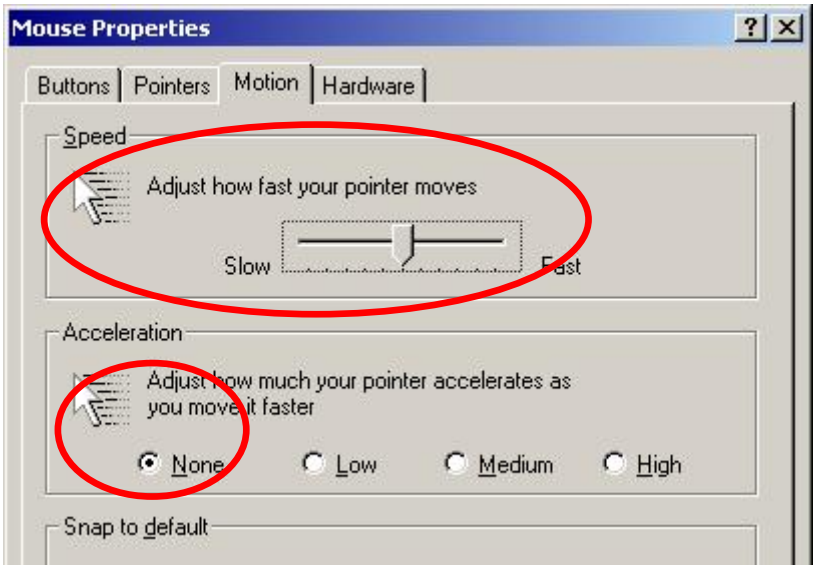
If the host system runs Windows Server 2003, go to [Mouse properties]–[Pointer Options]–[Motion] and clear the check box for “Enhance pointer precision.”
If you cannot move your mouse pointer down to the right bottom of the host server screen from a remote console, adjust your pointer speed in “Select a pointer speed.”



Notice

It is necessary to set "SETTING MOUSE PROPERTIES" in Windows Server 2003 in each user account.

If the host system runs Windows 2000 Server, go to [Mouse Properties]-[Motion]-[Acceleration] and select the check box for "None".
If you cannot move your mouse pointer down to the right bottom of the host server screen from a remote console, go to [Speed] and adjust how fast your pointer moves.



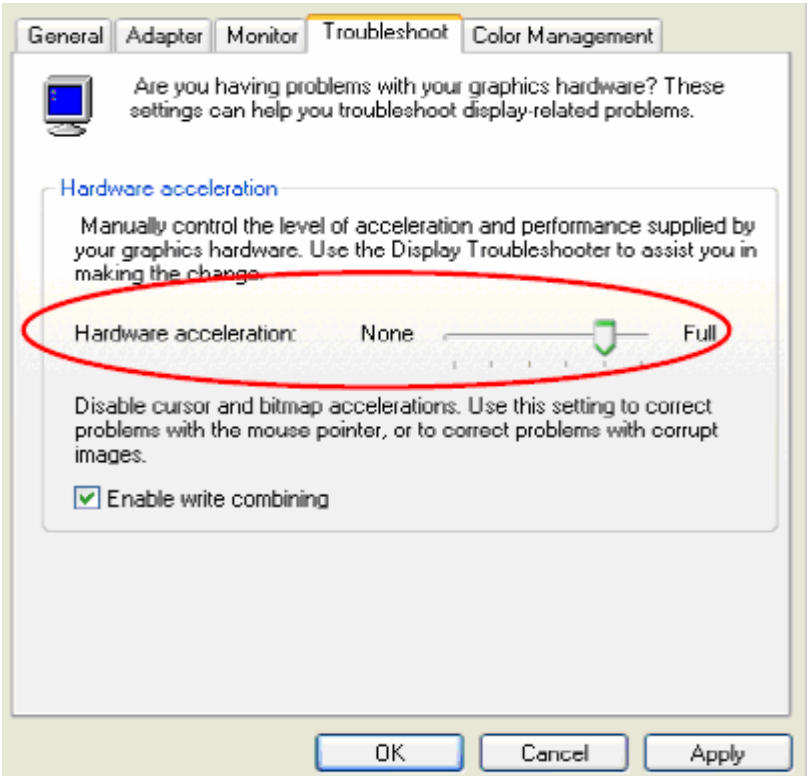
It is necessary to set "SETTING MOUSE PROPERTIES" in Windows 2000 Server in each user account.

If the host system runs Linux, set "Movement" for setting of the mouse on desktop environments (GNOME etc.) to become the following set values when confirming it by 'xset q'.

```
Pointer Control:
 acceleration: 1/1      threshold: 1
```

HARDWARE ACCELERATION SETTINGS

If the host system runs Windows, Right-click your desktop screen, select the list of context, and go to [Properties]-[Troubleshoot].
In the "Hardware acceleration" box, the pointer has to point to one scale down from "Full."
Press the "Apply" button.



Please execute "SETTING HARDWARE ACCESLERATION" after installing the graphics accelerator driver. To execute the setting change, the Administrator authority is needed.

If the host system runs Linux, open a command prompt and run this command.

Command: xset [m (ouse)] [acceleration] [threshold]
>xset m 1 1

3. Configuring a Management PC

This chapter describes the settings necessary for the remote management PC that will be connected to the host system.

SETTING YOUR BROWSER

Configure the following settings:

- Enable SSL.
- Allow Java Script execution.
- Allow Java execution.
- Accept Cookies.

For Internet Explorer, all the following settings must be enabled by [Internet Options] - [Security] function. Please customize your security level or add the BMC's IP address to a zone where all the following settings are enabled, if you can not use EXPRESSSCOPE Engine 2's functions.

- ActiveX controls and plug-ins
  - Run ActiveX controls and plug-ins
  - Script ActiveX controls marked safe for scripting
- Scripting
  - Active scripting
- Miscellaneous
  - Allow META REFRESH

SUPPORTED BROWSERS

The following browsers are supported by Windows XP and Windows Server 2003:

- Microsoft Internet Explorer 6.0
- Microsoft Internet Explorer 7.0
- Firefox 2.0

The following browsers are supported by Windows Vista:

- Microsoft Internet Explorer 7.0
- Firefox 2.0

The following browser is supported by Red Hat Enterprise Linux WS(version 4) and Red Hat Desktop(version 4):

- Firefox 2.0

It’s recommended that a browser be applied the latest service pack and the security patch. When you use Firefox, Set it so as not to display another tab even if the link is clicked.

J2SE RUNTIME ENVIRONMENT

The management PC requires Java2 Runtime Environment (JRE), Standard Edition 5.0 or 6.0.

You can download the latest JRE (Java Runtime Environment) at:
http://www.java.com/en/download/

JRE is available free of charge from Sun Microsystems, Inc. For security reasons, you are recommended to use the latest JRE update.

If the management PC runs Windows XP, remote media function may not work. You need to apply Service Pack 2.

If the management PC runs Linux, you can't install operating system to the host system with the Express Setup of NEC EXPRESSBUILDER by using remote media. Please don't choose [Os installation] from NEC EXPRESSBUILDER Boot selection menu.

4. Networking

TCP/IP PORTS

The BMC uses the TCP/IP ports listed below. If you use the BMC in a firewall environment, you need to allocate the port numbers (shown in the right column) to the individual non-block ports.

Module name	Port #	Protocol	Direction	Module name	Port #
Remote Media	5901(*5)	TCP	⇔	BMC	Dynamic
Web browser / Remote KVM Console	Dynamic(*1)	TCP	⇔	BMC	80(*2)
Web browser / Remote KVM Console (SSL)	Dynamic(*1)	TCP	⇔	BMC	443(*2)
Telnet client	Dynamic(*1)	TCP	⇔	BMC	23(*3)
SSH client	Dynamic(*1)	TCP	⇔	BMC	22(*3)
SMTP server	25(*4)	TCP	⇔	BMC	Dynamic
TFTP server	69	UDP	⇔	BMC	Dynamic

*1 The Dynamic ports are dynamically allocated ports and usually ranged from 1024 to 65535.

*2 Go to [Configuration]-[Web Server] to change the port number. (Refer to the Chapter 5)

*3 Go to [Configuration]-[Miscellaneous] to change the port number. (Refer to the Chapter 5)

*4 Go to [Configuration]-[E-Mail Alert] to change the port number. (Refer to the Chapter 5)

*5 Go to [Preference] on Remote media window to change the port number. (Refer to the Chapter 5)

5. Using Remote Management

OVERVIEW

The BMC Web Server function allows you to control the host system's power and KVM from a remote console via a Web browser.

Part of the above function is implemented by Java Applet.

CONNECTING TO THE WEB SERVER

Access the following URL from the Web browser on the remote management PC:

http://BMC_HostPort
Or
https://BMC_HostPort

The "BMC_HostPort" URL includes the BMC's IP address or host name and a colon followed by a port number for HTTP or HTTPS connection: e.g. 192.168.1.1:80 If the port number is 80 for HTTP or 443 for HTTPS (default), you may omit the port number.

- **If DHCP is disabled and you use the web server, assign a new IP address to the management LAN by using the BIOS Setup Utility or NEC EXPRESSBUILDER. Refer to "Management LAN Settings" in the "Chapter 2: Configuring the Host System".**
- **If you configure the management LAN settings through the network, Web browser, connect the management LAN port to the private network on which the default IP address "192.168.1.1" is reachable. Configure network settings according to your network environment. Refer to "Configuration" in the "Chapter 5: Using Remote Management". Connect the management LAN port to your management LAN.**

For security reasons, you are recommended to use HTTPS (SSL) connection. For better communication performance, use HTTP on a secured network.

When you connect via SSL, security warning messages may appear.

Please connect to the BMC with a web browser only when you login to the BMC if you use HTTPS. Keeping the login page displayed on a web browser may obstruct other client's connection.

LOGIN AND LOGOUT

Login

When the login page appears, enter the user name and password, and then click [Login].

If you log in for the first time, use the following default user name and password.

Default user name: administrator
Default password: none (enter no password)

Notice

The password is not set by default. Make sure to set a password immediately after you log in.
For security reasons, it is recommended that you change the default user name.
For information regarding configuration and modification, refer to "Configuration" of the "Chapter 5: Using Remote Management".

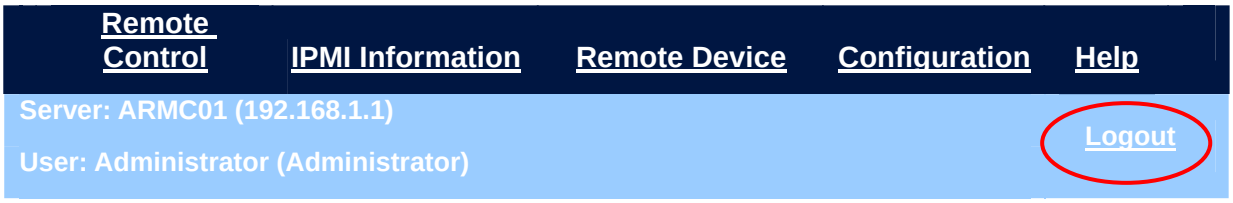
Notice

Only a single user may log in. Once the first user logs in, other users cannot access from any other browsers.

You may see a security warning dialogue after you log in. Read the message and click "Run." If you are not sure about the information, select "Cancel."

Logout

Click "Logout" in the upper right corner of the window. When a confirmation dialog appears, click [OK] to log out.



After you log out, you return to the login page. Besides, all the remote device windows that were opened during login will be closed.

Notice

If you have closed a browser without the following above step for logout, you cannot log in for the next one minute. Try to log in again after one minute.

LANGUAGE SELECTION

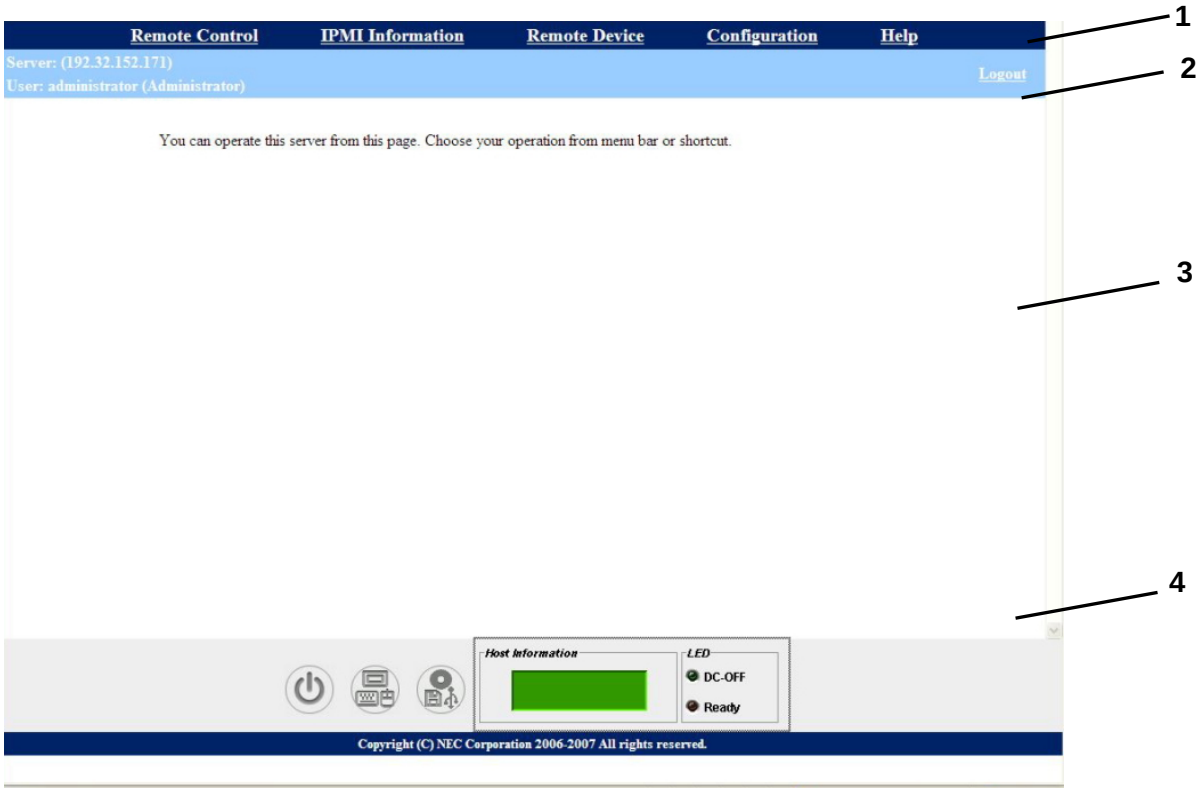
In the login page, you can select English or Japanese as a language displayed during your operation.

Click “English” in the upper right or “Japanese” beneath it.

Notice

You can select the display language only in the login page. If you want to change the language after login, log out once and change the language in the login page.

MAIN WINDOW



1 The Menu bar shows menus offered by the BMC

2 The BMC's host name and IP address
The current user's name and status
Click "Logout" to log out.

3 Content changes depending on the option you select in the Menu bar.

4 The Server Panel shows the status of the host system and shortcuts to the Remote Control page and the Remote Device page.

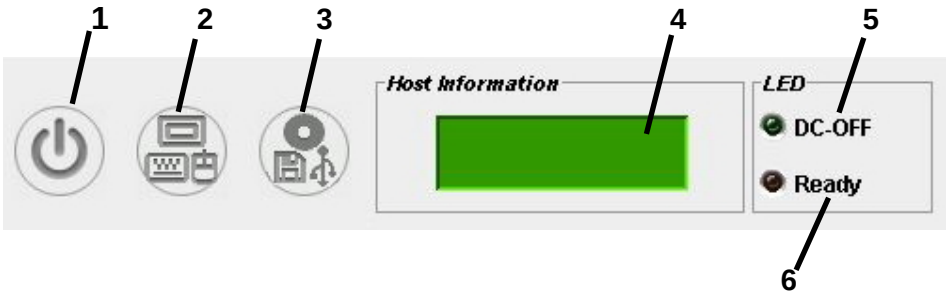
Notice

Do not use the "Reload" button in your browser after login.

SERVER PANEL

The Server Panel displays the status of the host system and shortcuts to the Power Control page and the Remote Device page.

Control Panel Functions



1 Shortcut icon for the Power Control menu

2 Shortcut icon for the Remote KVM menu

3 Shortcut icon for the Remote Device menu

4 Virtual LCD that displays the status of the host system

5 Power LED indicator that shows the power status of the host system

6 Status LED indicator that shows the status of the host system

Tips

Refer to User's Guide of the system for the message displayed in the Virtual LCD.

MENU BAR

How to use each menu provided in the Menu bar is described below.

Remote Control

Click “Remote Control” in the Menu bar. You will see the following icons. Select a function and click the icon.

Notice **Using the above functions when the operating system is running may cause the loss of data in the host system.**

Power ON

Power on the host system

Forced Power OFF

Perform a forced power shutdown

Power Cycle

Perform a forced power shutdown and power on the host system again

System Reset

Reset your host system

OS Shutdown

Perform OS shutdown
(Your operating system must be set to shut down when you power off the host system.)

Tips **The above OS Shutdown menu is equivalent to pressing the POWER switch when the power of the host system is on.**

Dump

Perform OS memory dump.

Tips **The above Dump menu is equivalent to pressing the DUMP switch on the host system.**

Chassis Identify

The UID (Unit ID) LED on the host system flashes.
“Chassis Identify” icon changes into “Stop Identification” icon while executing chassis identification (while the UID LED is flashing).

Click the "Stop Identification" icon to turn off the UID LED when you would like to stop the chassis identification.

If the UID LED is not mounted into the host system, the “Chassis Identify” function is not executed.

Please refer to the User’s Guide of your host system for the description of the UID LED.

IPMI Information

The IPMI Information includes system event logs (SEL), sensor data records (SDR), field replaceable units (FRU) information and Management Controller (MC) Information. By selecting the IPMI Information menu, you can confirm the IPMI information and following actions.

By clicking "Backup IPMI Information" icon in the IPMI information page, you can backup the IPMI information of the host system.

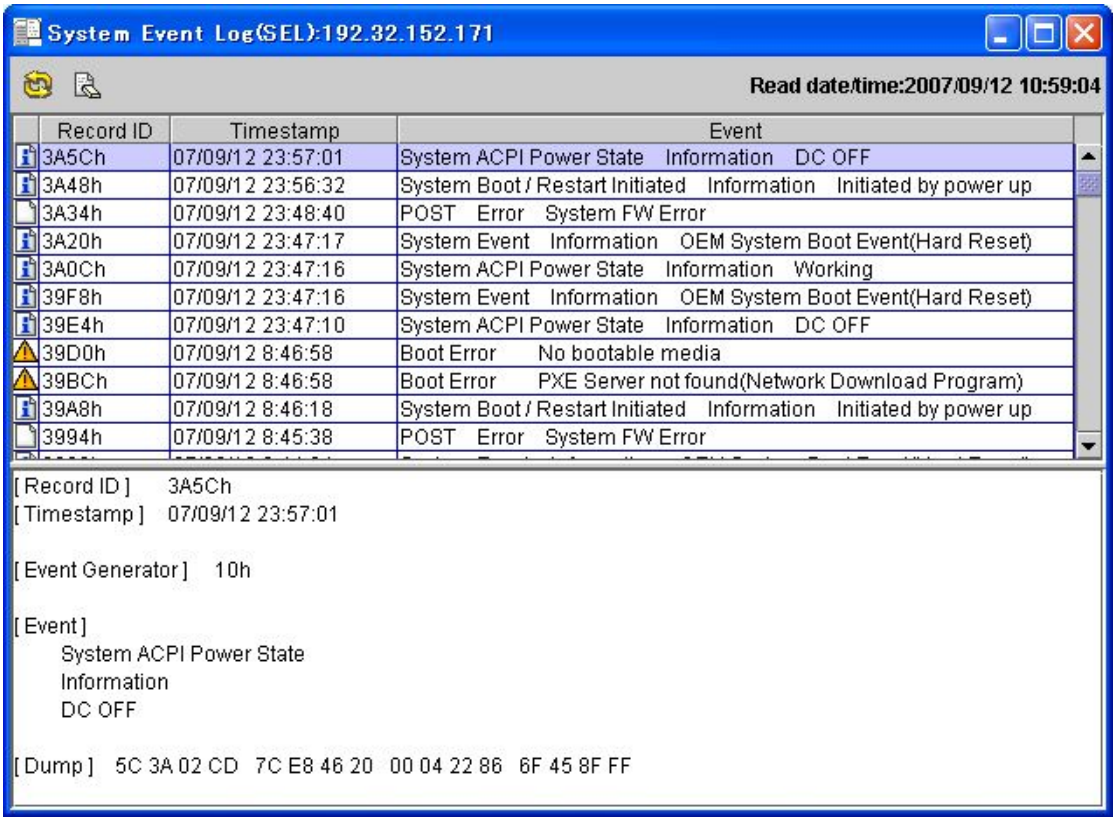
And also, by clicking "System Environment" icon in the IPMI information page, you can check the system environment status (temperature, voltage, fan, power, power supply unit, HDD) of the host system.

By confirming these information, you can examine failures and events in the host system and identify a component that needs to be replaced.

System Event Logs (SEL)

In the Menu bar, click “IPMI Information.” The following six icons will appear:

Click “SEL Information” to collect system event logs via the BMC. The System Event Logs (SEL) window will appear as follows:



A list of event logs appears above in the window. The detail of the event entry that you select in the list is shown below in the window.

Click [] to reload event logs via the BMC and display the most updated information.

The date when SEL information was read at the end is displayed “Read date/time”

Clearing SEL information

Click [] to delete the SEL information in the BMC. When a confirmation message appears, click [Yes] if you agree. If not, click [No] so that the SEL information will not be deleted.

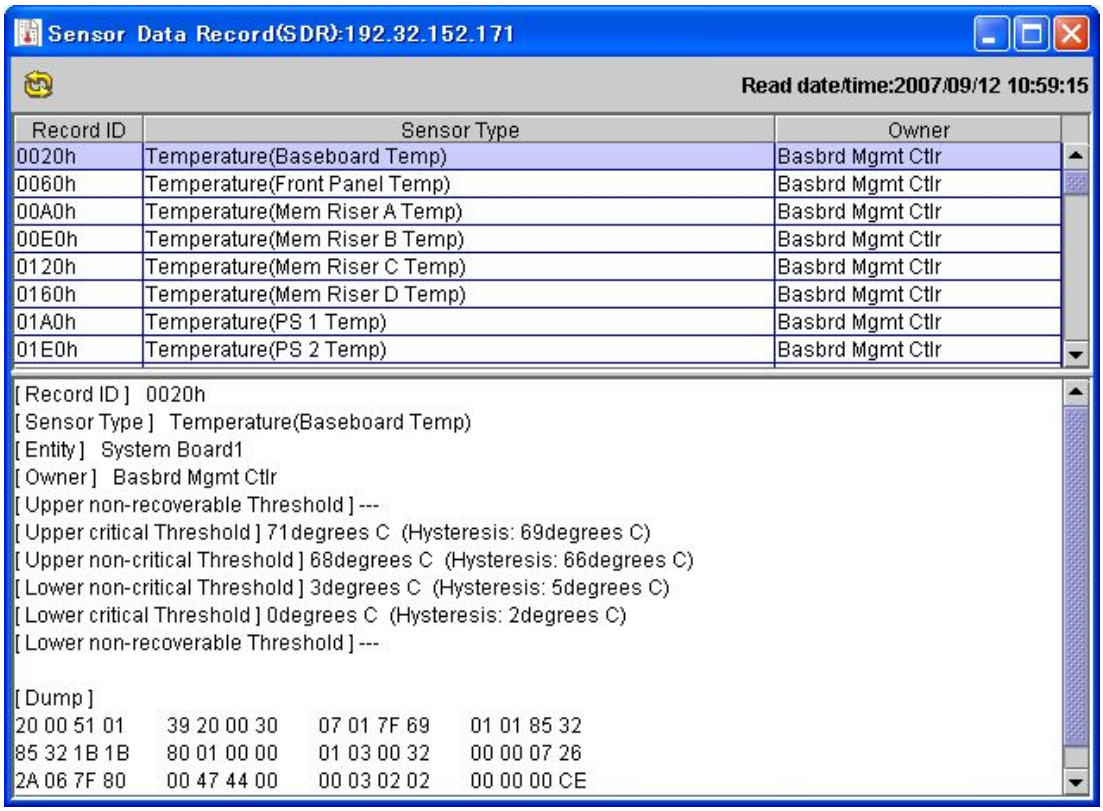
To delete SEL Information, you must log in as a user with an administrative account.
Otherwise, the Delete icon ([]) does not appear.

If you use NEC ESMPRO/Agent, you do not have to use the above Delete function, as NEC ESMPRO/Agent manages SEL Information for you.

Sensor Data Records (SDR)

In the Menu bar, click “IPMI Information.” The following six icons will appear:

Click “SDR Information” to load sensor data records via the BMC. The Sensor Data Record (SDR) window will appear as follows:



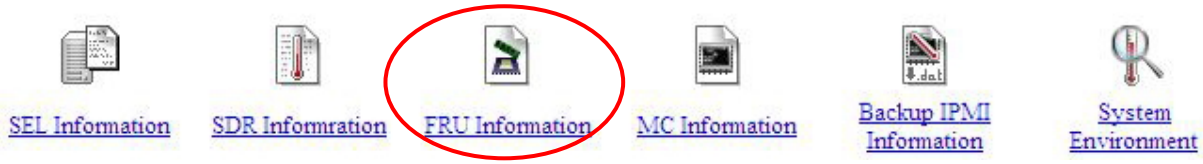
A list of sensor data records appears above in the window. The detail of the record entry that you select in the list is shown below in the window.

Tips

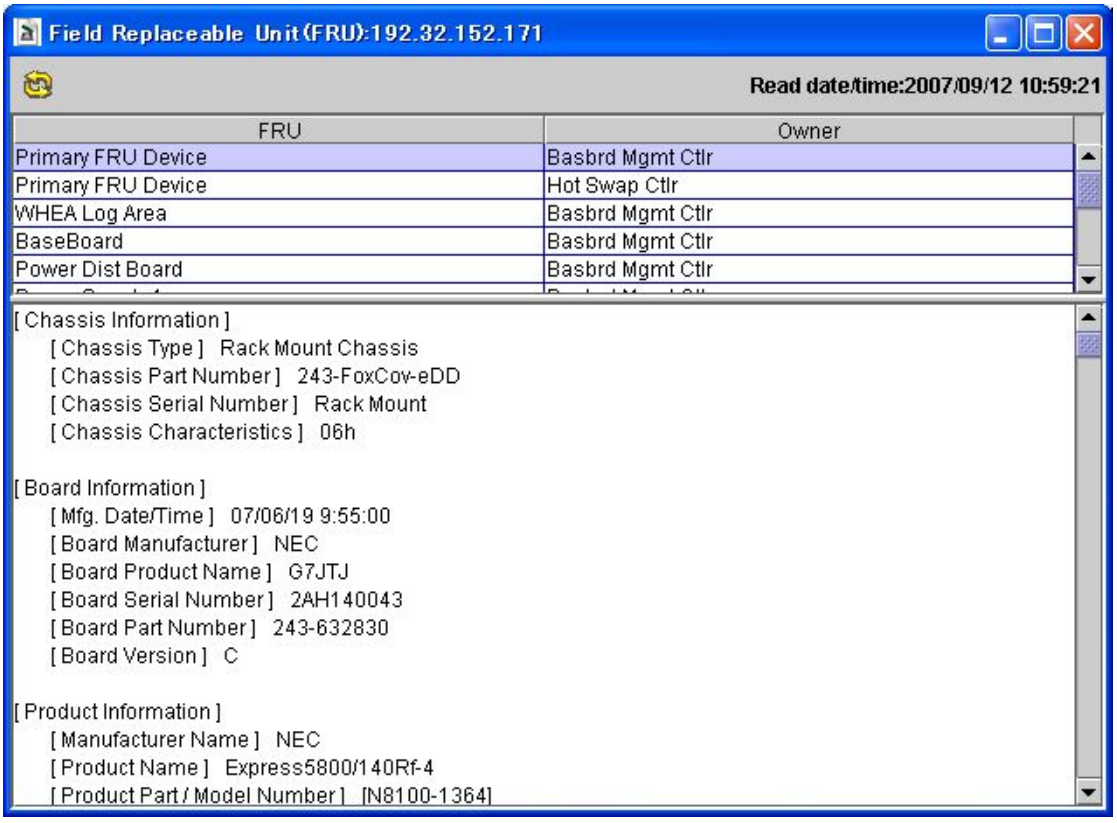
The SDR refers to information defined for each sensor in the host system. The BMC monitors individual sensors based on these definitions.

Field Replaceable Units (FRU) information

In the Menu bar, click “IPMI Information.” The following six icons will appear:



Click “FRU Information” to load Field Replaceable Unit information via the BMC. The Field Replaceable Unit (FRU) window will appear as follows:

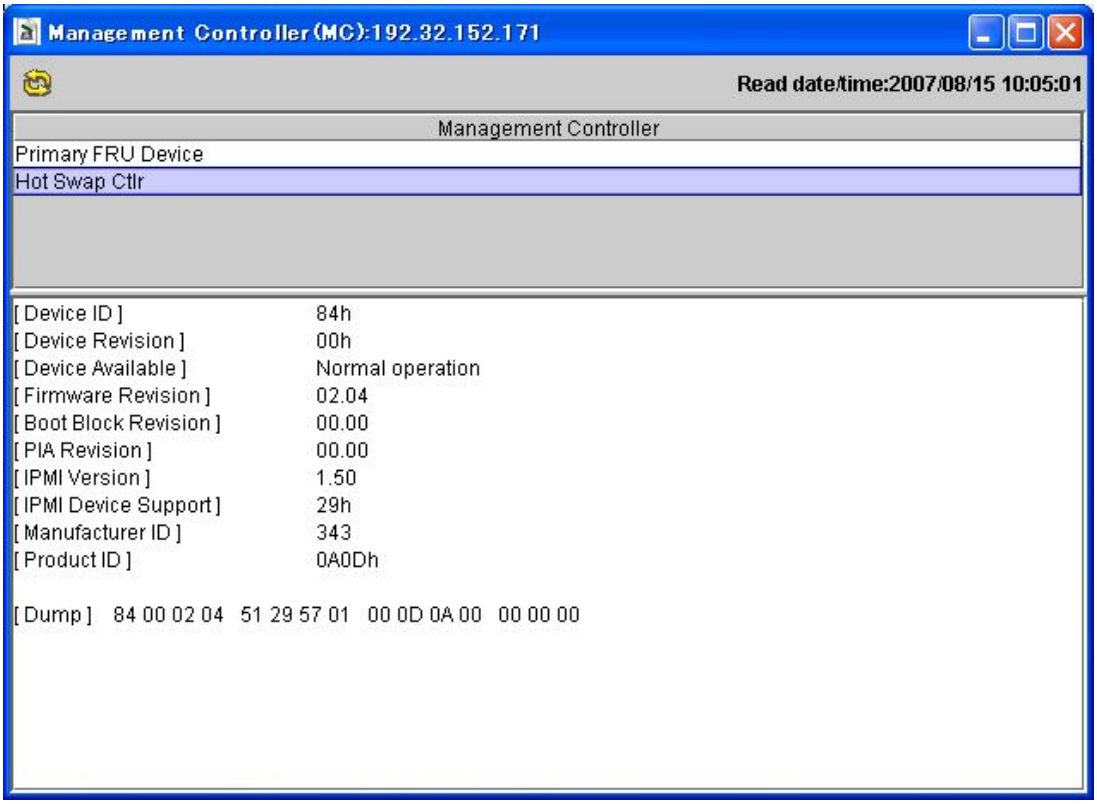


A list of field replaceable units appears above in the window. The detail of the unit entry that you select in the list is shown below in the window.

Management Controller (MC) Information

In the Menu bar, click “IPMI Information.” The following six icons will appear:

Click “MC Information” to collect management controller information via the BMC. The Management Controller (MC) Information window will appear as follows:

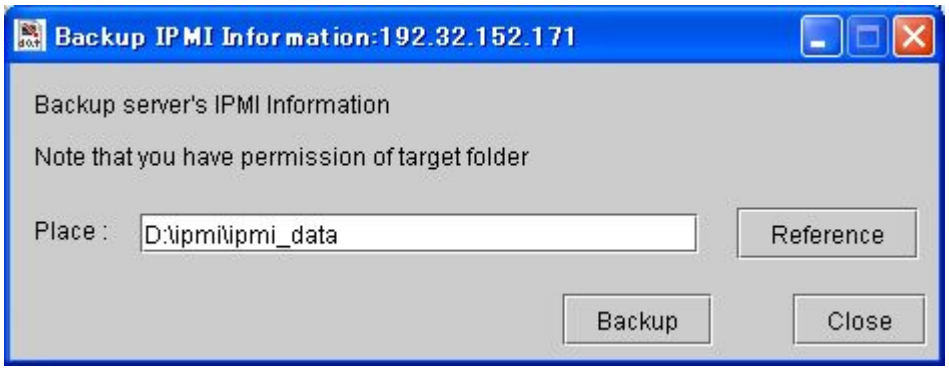


A list of Management Controller (MC) appears above in the window. The detail of the MC that you select in the list is shown below in the window.

Backup IPMI Information

In the Menu bar, click “IPMI Information.” The following six icons will appear:

Click “Backup IPMI Information” to backup the IPMI information of the host system. The Backup IPMI Information window will appear as follows: And you can backup IPMI Information to the specified file.



You can view the Back Up data you saved with server management software (ESRAS Utility and Off-line Maintenance Utility).

System Environment

In the Menu bar, click “IPMI Information.” The following six icons will appear:

Click “System Environment” to retrieve the system environment status (temperature, voltage, fan, power, power supply unit, HDD) from the BMC and to display items (temperature, voltage, fan, power, power supply unit, HDD) of the status. The System Environment window will appear as follows:

Displays system environment status of the target system. Reload

Sensor	Status	Current Reading
Temperature [Hide]		
Baseboard Temp	OK	40 degree C
Front Panel Temp	Critical	31 degree C
Mem Riser A Temp	OK	36 degree C
PS 1 Temp	OK	32 degree C
PS 2 Temp	OK	32 degree C
SAS BP Temp	OK	31 degree C
Voltage [Show]		
Fan [Show]		
Power [Show]		
Power Supply Unit [Show]		
HDD [Show]		

Reload

When [Show] of each item is clicked, information of the item is displayed, By pushing "Reload" button, you can reload the current system environment status of the host system.

When [Hide] of each item which displays its information is clicked, the information of the item is not displayed.

Initial state of the window when you login the BMC Web server, is that all the items of the status do not display there information.

Tips

The item not supported by the host system is not displayed for each item (temperature, voltage, fan, power, power supply unit, HDD) of the system environment status. Moreover, the item supported with the host system might not be displayed according to a state of a power supply and mounting such as a device of the system either.

Remote Device

The Remote Device menu allows you to start the Remote KVM function, Remote Media function and register the license required for using this function.

To use the Remote Device menu, you must log in as a user with an administrative account

If the host system runs VMware, the mouse function of Remote KVM Console and Remote Media function are not supported.

License Registration

Click “Remote Device” in the Menu bar. You will see the following icons. Click “License Registration” to go to the License Registration page.

In the License Registration page, you can confirm your license registration status (shown in the license registration form above). If your license has not been registered yet, enter the license key provided in the optional N8115-03 Remote KVM and Media License, and click the “Register” button.

After the registration, confirm that your license has been registered.

If you fail to enter a correct license key, the Remote Device menu will not function even if a valid license key has already been registered.

To use the Remote Device menu after registration, you must first log out and log in again.

Remote KVM Console

The BMC features the Remote KVM Console function that allows you to display the screen of the host system in the remote Web browser. With this function, you have full access to the host system from the management PC using the remote keyboard, video, and mouse.

To use the Remote KVM Console function, the “Remote KVM and Media License” is required. Refer to the “License Registration” section.

You cannot use the host system's KVM from two or more remote management PCs at the same time.

The Remote KVM Console function supports the following display resolutions:

-1600	×	1200 pixels,	256 colors, 16-bit color
-1280	×	1024 pixels,	256 colors, 16-bit color
-1152	×	864 pixels,	256 colors, 16-bit color, 24-bit color
-1024	×	768 pixels,	256 colors, 16-bit color, 24-bit color, 32-bit color
- 800	×	600 pixels,	256 colors, 16-bit color, 24-bit color, 32-bit color
- 640	×	480 pixels,	256 colors, 16-bit color, 24-bit color, 32-bit color

Do not set any resolution other than those above, or the Remote KVM Console cannot display correctly.

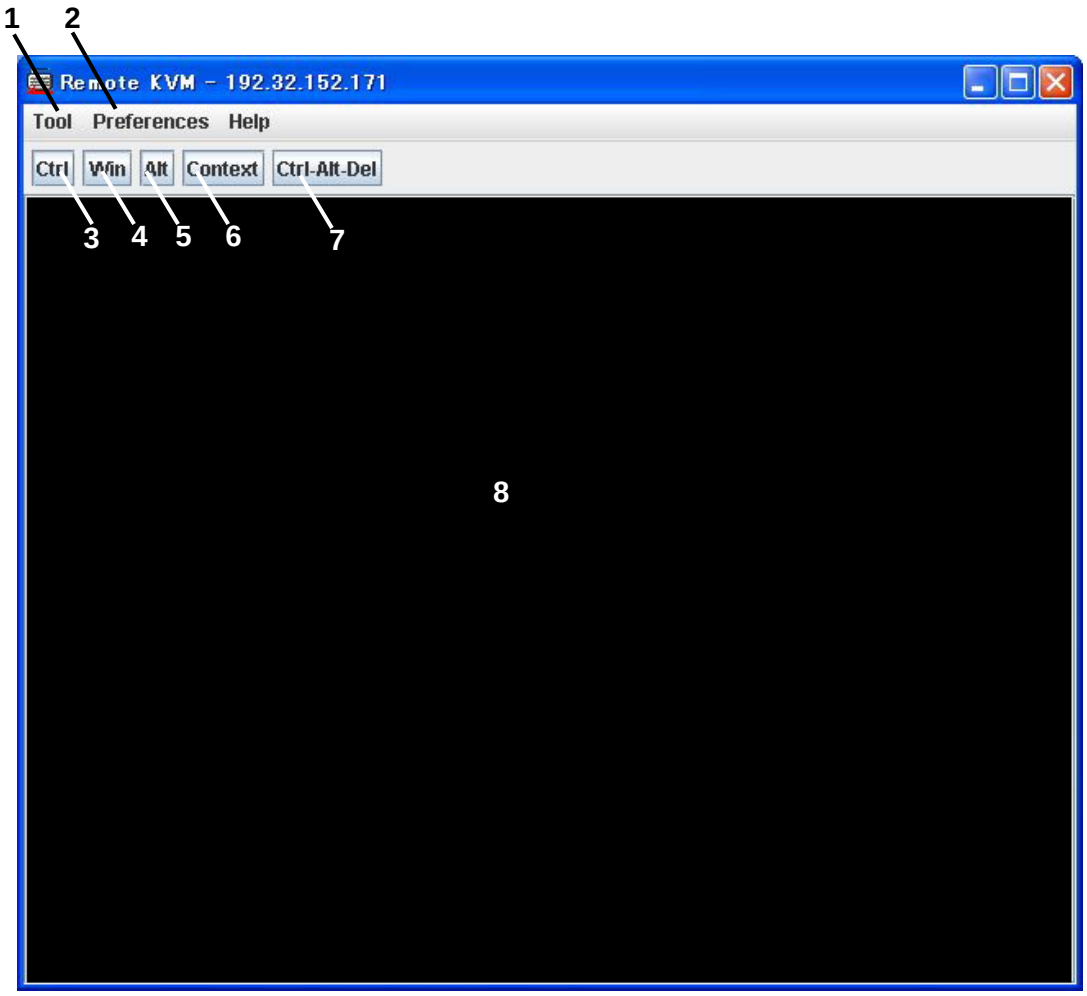
The BMC enables the Remote KVM Console function by controlling video, keyboard, and mouse signals in the host system and allows remote management, regardless of the OS status in the host system (during POST and OS boot/operation, including DOS and other text mode OS's, and at the event of panic).

Starting up Remote KVM Console

Click "Remote Device" in the Menu bar. You will see the following icons. Click "Remote KVM" to go to the Remote KVM Console window.

When you log on to the BMC from the host system, do not access the Remote KVM Console from a Web browser in the host system. You will not be able to use keyboard and mouse.

Remote KVM Console Window



1 Tools: start Software Keyboard or perform Refresh Screen

2 Preferences: change the remote console settings

3-7 Specific Key Icons

8 Displays the host system's screen

Notice **When you use the Remote KVM Console function, the keyboard LED indicator on the management PC does not synchronize with the one on the host system.**

Specific Key Icons

Use the following four specific key icons in the Remote KVM Console window. (Pressing the same keys on the remote keyboard is not effective.)

Ctrl key	Ctrl (raised "Up" state) Ctrl ("Pressed" state)	Toggles whenever clicked.
Windows key	Win (raised "Up" state) Win ("Pressed" state)	Toggles whenever clicked.
Alt key	Alt (raised "Up" state) Alt ("Pressed" state)	Toggles whenever clicked.

Context [ ] key 

Ctrl-Alt-Del key 

Software Keyboard

Click [Tools]-[Keyboard]. The Software Keyboard panel appears. The specific keys toggle whenever you click them.

Refresh Screen

Click [Tools]-[Refresh Screen]. The Remote KVM Console screen will be refreshed. Refresh your screen when the screen display is garbled.

Change properties

Click [Preferences] to change the following settings:

Keyboard

Set Keyboard language. Select the keyboard language of the management PC.

Mouse

Cursor Mode

The mouse cursor displayed on the remote KVM console screen can be selected. Select [Single] when you display only the cursor of host system. Select [Dual] when you display the cursors of management PC and host system.

Coordinate Mode

You can change the mode for sending mouse cursor coordinates from the remote management PC to the host system. [Absolute] or [Relative] can be selected.

[Absolute]: Send the raw x and y coordinates of the mouse pointer to the host system.
[Relative]: Send the relative coordinates of the previous mouse pointer position to the host system.

Before open the login page of EXPRESSSCOPE Engine, you should match the key board language of the management PC with the host system.

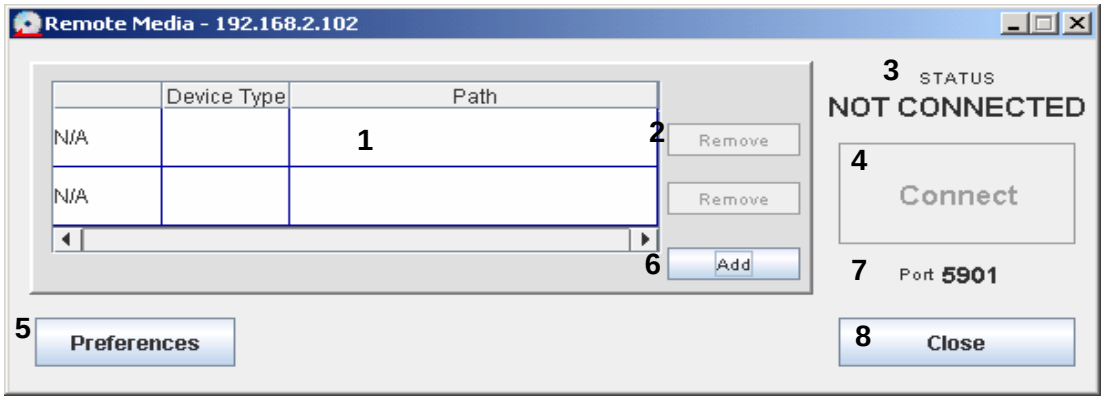
Remote Media

The Remote Media function enables CD/DVD-ROM/floppy disk drives, ISO image files, and USB memory in the management PC to be recognized as virtual media drives in the host system, allowing you to connect the devices independent of the operation system status in the host system.

Starting the Remote Media Function

Click “Remote Media” in the Menu bar. You will see the following icons. Click “Remote Media” to go to the Remote Media window.

Remote Media Window



1 Lists registered devices (floppy disk drive, CD/DVD-ROM drive, ISO image, and USB memory)

2 Removes the registered device. You cannot remove when the connection status is “CONNECTED.”

3 Displays the connection status for the registered devices and host system.

NOT CONNECTED --- The registered devices are not connected to the host system.

CONNECTED --- The registered devices are connected to the host system.

ERROR --- An error has occurred. Check your network status and the media drives on the management PC.

4 Connects or disconnects the registered devices to and from the host system.

5 Opens the Preference window.

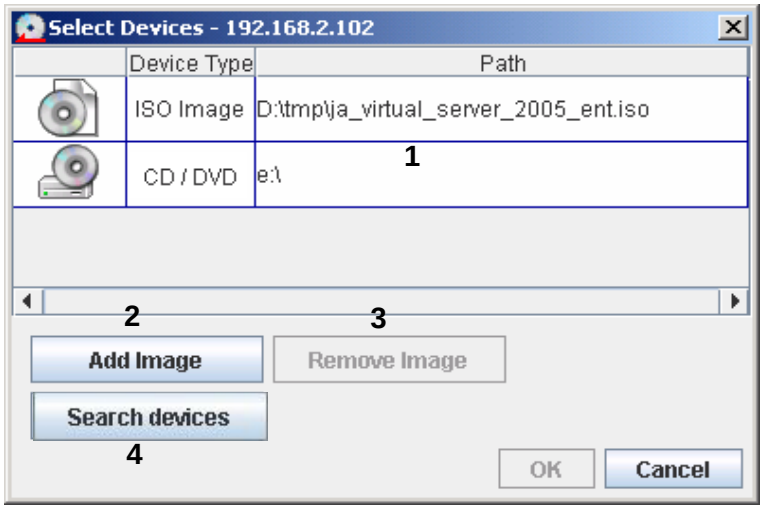
6 Opens the Select Devices window.

7 Shows the port number used for the communication between the management PC and the host system. To change the port number, go to the Preference window.

8 Closes the Remote Media window. When the connection status is “CONNECTED,” the remote media devices remain connected until you log out.

Select Devices Window

Click the Add button in the Remote Media window. You will see the Select Devices window as below:



1 Lists the remote media devices recognized on the management PC. When a medium is not inserted to a drive, the drive is not recognized. Press “Search device” after inserting a medium.

2 Adds the ISO image file you selected to the above list (1).

3 Deletes the ISO image file you selected from the above list (1).

4 Searches again for the drive connected to the management PC.

Following icons are displayed for recognized device.

	Floppy disk drive		ISO image
	CD/DVD-ROM drive		Storage Device (USB memory)

Notice **If any other application is being used in a remote media device on the management PC, the drive cannot be connected and displayed in the “Select Devices” window.**

Tips **Hard disk drive is also recognized as “Storage Device” unless connection is not supported. Please confirm whether the selected device is not Hard disk drive.**

USB memory which supports multi partition cannot be recognized.

If management PC runs Linux, some devices may not be recognized.
If problem occurs, execute with root authority user.

How to Connect the Remote Media Devices

Follow the procedure below to connect the remote media devices to the host system properly. If you do not connect them properly, the host system may not recognize the remote media devices.

1 Confirm the connection status is “NOT CONNECTED” in the Remote Media window, and click the Add button. The Select Devices window will open.

2 Select a drive or ISO image file you want to add to the Remote Media window. When a medium is not inserted to a drive, the drive is not recognized. Press “Search device” after inserting a medium.

3 If the inserted medium starts running automatically, stop the software. If the CD/DVD-ROM drive’s access LED is illuminated, wait until it turns off.

4 When you add the ISO image file, press the “Add Image” button and select the ISO image file in the Select Devices window.

5 Press "OK" to close the Select Devices window after selecting the device and ISO image file. The Remote Media window shows the device and ISO image file that you have added.

6 Click “Connection” in the Remote Media window. The connection status turns to “CONNECTED” in a few seconds.

7 After a few seconds, the host system will recognize the added device as a virtual media drive. If the host system runs Linux, mount the drive manually.

8 The host system can access the remote device in the management PC via network, as it accesses other locally connected devices.

If you press the "Connect" button, all registered devices are connected.

You cannot register the same type of devices in the Remote Media window.
You can select following devices.

FD	**+ CD/DVD**
FD	**+ ISO image**
FD	**+ USB memory**
CD/DVD	**+ FD**
CD/DVD	**+ USB memory**

When the connection status is “CONNECTED” (the host system is connected to the management PC) , you cannot use other functions (“Add”, ”Remove” and “Preference”). To change the connection status to “NOT CONNECTED,” click the “Disconnect” button to disconnect the remote media devices once.

The floppy disk drive’s access LED indicator may remain illuminated after the drive is connected to the host system.

After you click the “Connect” button, it takes a few seconds until the host system recognizes the remote media devices.

Connect remote media in advance while the system is off, or connect it while the operating system is already running. Don't connect remote media while POST is running because it may make the system unstable.

How to Disconnect the Remote Media Devices

Follow the procedure below to disconnect the remote media devices from the host system properly. If you do not disconnect them properly, the drives may not be used until you log in again.

If you host system runs Windows Server 2003:

1 Follow the Unplug or Eject Hardware message to disconnect the remote media devices.

2 Confirm the CD/DVD-ROM drive’s access LED indicator is off.

3 Click the “Disconnect” button if the connection status is “CONNECTED” in the Remote Media window. After a few seconds, The status turns to “NOT CONNECTED”.

4 The remote devices have been disconnected.

If your host system runs Windows 2000 Server:

1 The remote devices may not appear in [Unplug or Eject Hardware] window.

2 Confirm the CD/DVD -ROM drive’s access LED indicator is off.

3 Click the “Disconnect” button if the connection status is “CONNECTED” in the Remote Media window. After a few seconds. The status turns to “NOT CONNECTED”.

4 The remote devices have been disconnected.

If your host system runs Linux:

1 Close an application using the remote media device, if any.

2 Confirm the CD/DVD -ROM drive’s access LED indicator is off.

3 Remove the remote media device.

4 Click the “Disconnect” button if the connection status is “CONNECTED” in the Remote Media window. After a few seconds, The status turns to “NOT CONNECTED”.

5 The remote devices have been disconnected.

Important Instructions for Using the Remote Media Devices

Important Notes:

- **If the host system features a built-in USB floppy disk drive and external USB floppy disk drive, the host system may not recognize a remote floppy disk drive as an "A" drive. If you need to have it recognized as an "A" drive, remove drives from the host system’s USB floppy disk drive..**
- **If you select "Connect" and "Disconnect" when the CD/DVD-ROM is being accessed, the host system cannot recognize the CD/DVD-ROM drive. Make sure you select "Connect" and "Disconnect" after the access LED indicator turns off.**
- **If you need to change the CD/DVD-ROM while the drive is connected, disconnect the CD/DVD-ROM drive in the Remote Media window, change the CD/DVD-ROM, and connect the drive again.**
- **If you access the CD/DVD-ROM in the management PC after disconnecting the drive to replace the CD/DVD-ROM, the host system cannot recognize the replacement of the CD/DVD-ROM.**
- **You cannot format a floppy disk in the remote floppy disk drive connected using the Remote Media function. Use a formatted floppy disk.**
- **The remote floppy disk dive or USB memory is recognized as a "USB KEY" in the BIOS Setup Utility.**
- **If the host system runs Linux, the drive whose device type is "FDD" is recognized as a USB Disk in a SCSI device by the operating system.**
- **You can’t boot the host system from the remote USB memory. Please use remote USB memory after operating system runs.**
- **You have to set firewall to enable the port (5901:tcp) used for the communication with the host system.**
- **If the management PC runs Windows Vista, execute Web browser as Administrator privilege.**

  Click the Web browser program file with right button on your mouse, and select “execute as Administrator”.
- **In the Select Device Window, USB memory which supports multi partition can’t be recognized.**
- **Please do NOT power off and reset the host system while the Remote Media is working.**

Configuration

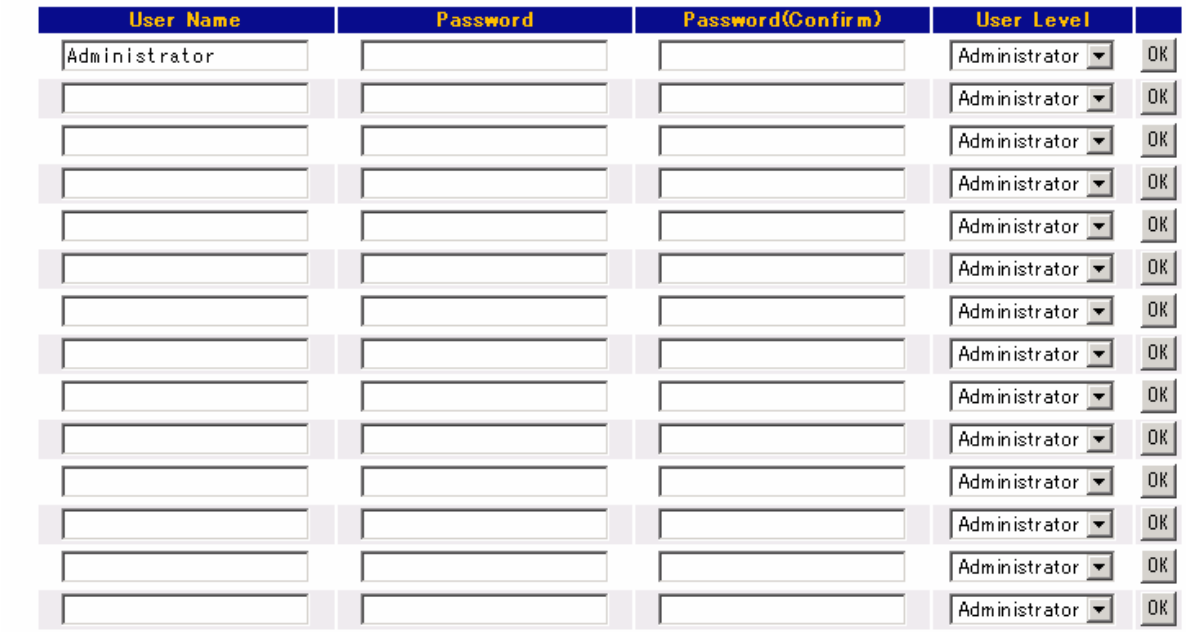
To configure the BMC settings, click “Configuration” in the Menu bar. You will see the following icons. Select a function and click the icon.

User

You can configure user accounts in the Configuration page below.
The page shows a list of current users.

Notice **A password does not appear in the Password column.**

Notice **A user name can contain up to 15 alphanumeric characters, including “- (minus)” and “_ (underscore).” The password accepts up to 19 ASCII characters, except for “ (space)”, ““(quotation marks)”, “?”, “=”.**



To change or add a user account, enter a user name and password, select a user level, and click [OK].

The default setting for this user account's configuration is that only the user of the first line is set. In this case, only following account is available for the default setting.

User Name	:	Administrator
Password	:	(None)
User Level	:	Administrator

If you want to delete a user account, delete the user name and click [OK].

User Level

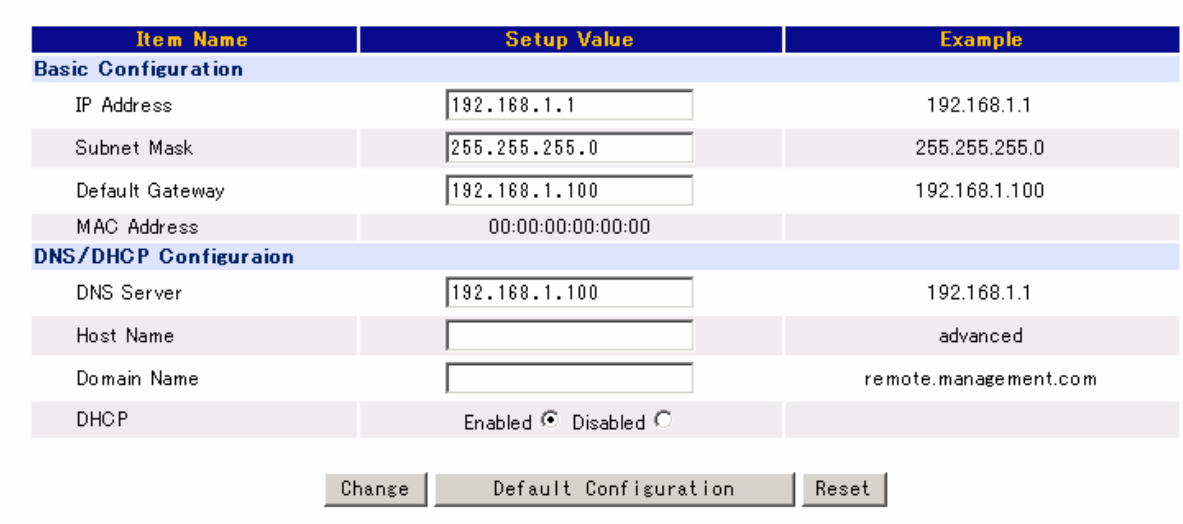
Administrators:
Users who have an administrative account and are allowed to perform any operation

Operators:
Users who are entitled to operate the system but are not allowed to change settings and use the Remote Device menu

Users:
General users who are only allowed to access the IPMI Information

Network Configuration

You can configure basic network settings (e.g. the BMC IP address).



Basic Configuration

IP Address

If DHCP is not used to automatically obtain an IP address, enter the BMC's IP address.
If DHCP has been used, an automatically obtained IP address will appear.

Subnet Mask

If DHCP is not used to automatically obtain a subnet mask IP address, enter the subnet mask of your management LAN.
If DHCP has been used, an automatically obtained subnet mask IP address will appear.

Default Gateway

If DHCP is not used to automatically obtain a default gateway IP address, enter the default gateway of your management LAN.
If DHCP has been used, an automatically obtained default gateway will appear.

MAC Address

The MAC address of your management LAN port will appear.

Notice

If you change an IP address, enter a new address and click [Change]. Your session is disconnected after the setting was changed. Close the window once, and enter the new IP address (or host name) in the browser to log in.

DNS/DHCP Configuration

DNS Server

If DHCP is not used to automatically obtain a DNS server IP address, enter the DNS server IP address of your management LAN.
If DHCP has been used, an automatically obtained DNS server IP address will appear.

Host Name

Enter the BMC's host name.

Domain Name

Enter the domain name of the network to which the BMC belongs to

DHCP

If you want to obtain an IP address, choose [Enabled].
If you want to manually configure an IP address, choose [Disabled].

The BMC's host name and domain name cannot be identical to those of the operating system in the host system because the BMC uses a separate LAN controller independent from the operating system. If the BMC belongs to a different network domain, you can use the same host name.

If you enable the DHCP function in the environment where DHCP is not supported, you will not be able to communicate with the BMC. To resume the communication, Configure network settings such as an IP address by using the BIOS Setup Utility or NEC EXPRESSBUILDER. Refer to "Management LAN Settings" in the "Chapter 2: Configuring the Host System".

When it is not possible to communicate with the BMC even if you operate the above-mentioned, please configure the network settings such as IP address and enabling HTTP and/or HTTPS once again after clearing all the BMC settings, Refer to the Troubleshooting for how to clear.

[Change] button:

All changes you have made in this page will be written into the BMC.

[Default Configuration] button:

The setup values you have entered will be changed to the BMC's default values. Click [Change] to return the BMC network settings back to default.

[Reset] button:

All setup values you have entered in this page will be cleared.

Default Values

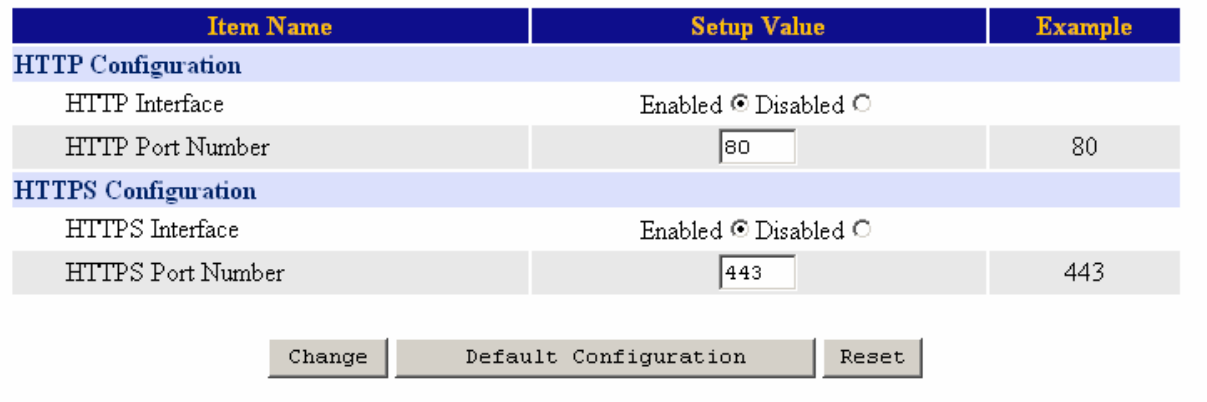
The BMC's default network values are as follows.

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
Default Gateway : 0.0.0.0
DNS Server : 0.0.0.0
Host Name : (none)
Domain Name : (none)
DHCP : [Disabled] *

* In some systems, this default setting is [Enabled]. This default setting is same as one of the BIOS Setup Utility. Please refer to the User's Guild of your host system and "Management LAN Settings" in the "Chapter2: Configuring the Host System".

Web Server Configuration

You can configure the BMC Web server settings



HTTP Configuration

HTTP Interface

Select [Enabled] to use the Web Server function using the HTTP port. If not, select [Disabled].

HTTP Port Number

Specify the HTTP port number.

HTTPS Configuration

HTTPS Interface

Select [Enabled] to use the Web Server function using the HTTPS(SSL) port. If not, select [Disabled].

HTTPS Port Number

Specify the HTTPS(SSL)port number.

Notice

Once you disable the HTTP Interface or the HTTPS interface which is used by the BMC Web Server, you cannot connect to the BMC via a Web browser. To enable the BMC Web Server again, refer to "Management LAN Settings" in the "Chapter 2: Configuring the Host System".

Notice

If you change the HTTP and HTTPS(SSL) port numbers, your session will be disconnected.

Close the window once, enter new port numbers in a browser, and log in again.

[Change] button:

All changes you have made in this page will be written into the BMC.

[Default Configuration] button:

The setup values you have entered will be changed to the BMC’s default values. Click [Change] to return the BMC Web Server settings back to default.

[Reset] button:

The setup values you have entered in this page will be cleared.

Default Values

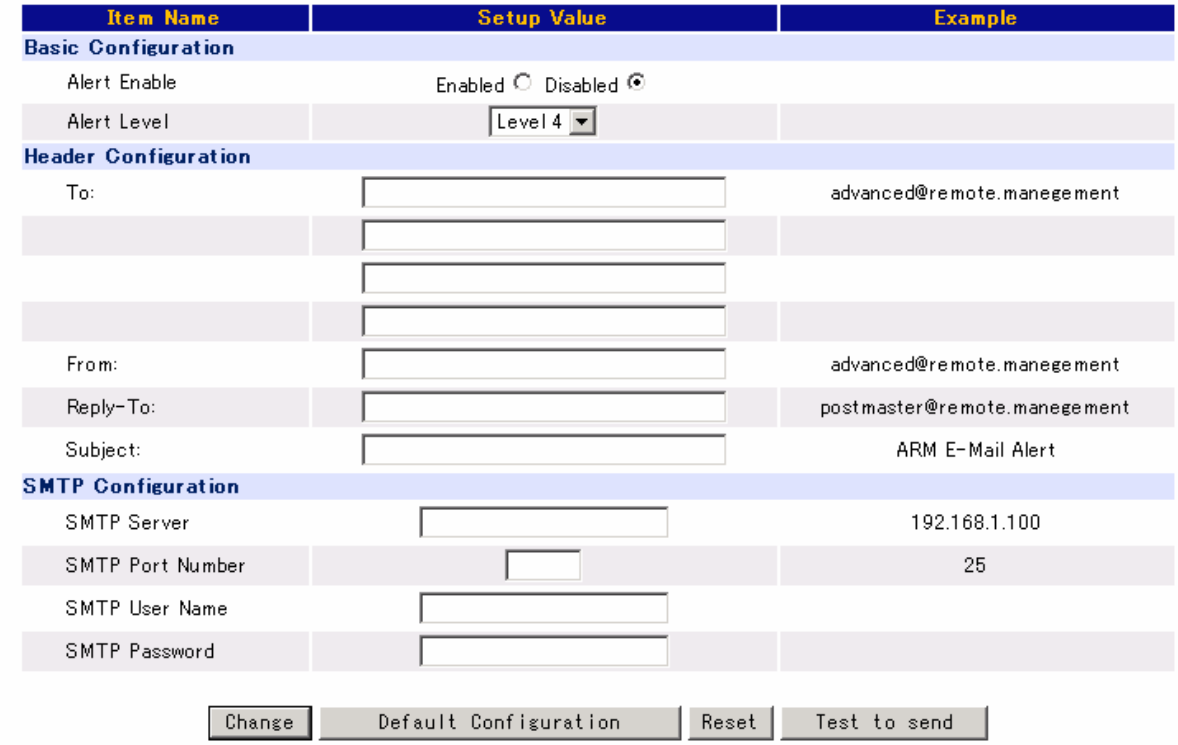
The BMC's default Web Server values are as follows.

HTTP Interface	: [Disabled]	*
HTTP Port Number	: 80	
HTTPS Interface	: [Disabled]	*
HTTPS Port Number	: 443	

* In some systems, this default setting is "Enabled". This default setting is same as one of the BIOS Setup Utility. Please refer to the User's Guild of your host system and "Management LAN Settings" in the "Chapter2: Configuring the Host System".

E-Mail Alert Configuration

You can configure the E-Mail alert settings.



Basic Configuration

Alert Enable

Select [Enabled] to use the E-mail alert function. If not, select [Disabled].

Alert Level

Select an alert level from the six severity levels below:.

Level1: Non-recoverable
Level2: Level1+Critical
Level3: Level2+Non-critical
Level4: Level3+OK
Level5: Level4+Information
Level6: Level5+Monitoring

Notice

Some systems may alert you to the identical event at different severity levels.

Tips

The field of "X-Priority: " will change in the alert mail header, depending on the severity of the event.

Non-recoverable/Critical	**X-Priority: 1**
Non-critical	**X-Priority: 3**
OK/Information/Monitoring	**X-Priority: 5**

Header Configuration

To:
Specify up to four destination addresses to alert.

From:
Specify the “From: ” field for alert mails.

Reply-To:
Specify the “Reply-To: ” field for alert mails.

Subject:
Specify the “Subject: ” field for alert mails.

Specify a reachable address in the “Reply-To: ” field.

You can use ASCII characters except for ‘+’, ‘”’, ‘?’, ‘=’, ‘<’, and ‘>’ in the Subject field.

SMTP Server Configuration

SMTP Server
Specify an IP address or DNS host name as a SMTP server address.

SMTP Port Number
Specify the SMTP server’s port number.

SMTP User Name
Specify a SMTP user name for SMTP authentication.

SMTP Password
Specify a SMTP password for SMTP authentication.

Without the SMTP user name and SMTP password, SMTP authentication is not enabled.

[Change] button:

All changes you have made in this page will be written into the BMC.

[Default Configuration] button:

The setup values you have entered will be changed to the BMC’s default values. Click [Change] to return the BMC E-mail alert settings back to default.

[Reset] button:

All setup values you have entered in this page will be cleared.

[Test to send] button:

A test mail will be sent according to the current setting.

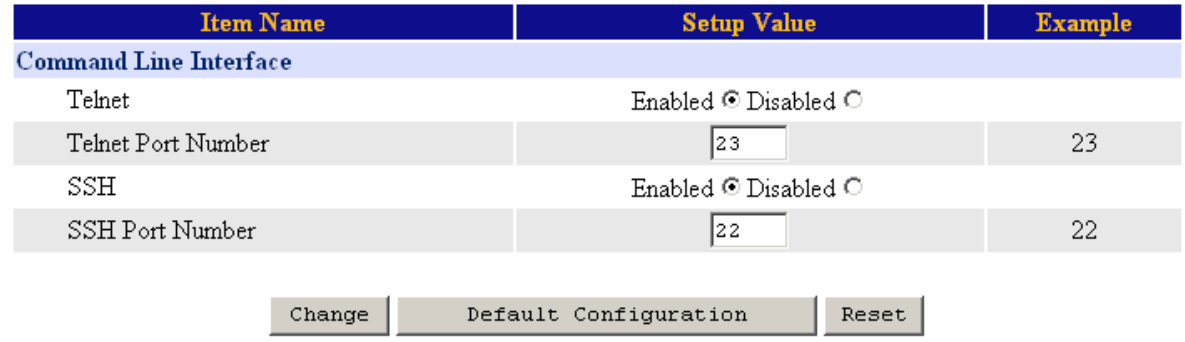
Default Values

The BMC's default E-Mail Alert values are as follows.

Alert Enable	: [Disabled]	
Alert Level	: Level4	
To:	: (none)	(All of the four places)
From:	: (none)	
Reply-To:	: (none)	
Subject:	: (none)	
SMTP Server	: 0.0.0.0	
SMTP Port Number	: 25	
SMTP User Name	: (none)	
SMTP Password	: (none)	

Other Configuration

You can configure the settings for the BMC's Command Line Interface.



Command Line Interface

Telnet
Select [Enabled] to use the Command Line Interface using telnet. If not, select [Disabled].

Telnet Port Number
Specify the BMC's Telnet port number.

SSH
Select [Enabled] to use the Command Line Interface using SSH. If not, select [Disabled].

SSH Port Number
Specify the BMC's SSH port number.

[Change] button:

All changes you have made in this page will be written into the BMC.

[Default Configuration] button:

The setup values you have entered will be changed to the BMC's default values. Click [Change] to return the settings for the BMC Command Line Interface back to default.

[Reset] button:

All setup values you have entered in this page will be cleared.

Default Values

The BMC's default Command Line Interface values are as follows.

Telnet	: [Disabled] *
Telnet Port Number	: 23
SSH	: [Disabled] *
SSH Port Number	: 22

* In some systems, this default setting is [Enabled] depending on the model. This default setting is same as one of the BIOS Setup Utility. Please refer to the User's Guild of your host system and "Management LAN Settings" in the "Chapter2: Configuring the Host System".

Help

Refer to HELP for supplementary information that is not provided in this User’s Guide.
You can also confirm the BMC firmware revision here.

6. Command Line Interface

OVERVIEW

With the BMC Command Line Interface, you can control the host system from a remote Telnet/SSH client. The BMC supports Telnet and SSH (Version 2) protocol.

CONNECTING TO BMC

Access the BMC IP address or DNS host name from Telnet /SSH client on the remote management PC.

To use Command Line Interface, you need to change the configuration of the command line interface (Telnet and/or SSH) to be enabled by any of the setting of the BIOS Setup Utility or NEC EXPRESSBUILDER or Web browser. For using the BIOS Setup Utility or NEC EXPRESSBUILDER, refer to the "Management LAN Settings" in the "Chapter 2: Configuring the Host System". For using Web browser, you need to login with Web browser and change the value of [Configurations]-[Other Configuration]- [Command Line Interface] - [Telnet] and/or [SSH] to be [Enabled].

You can change the BMC's Telnet/SSH port number by using the BIOS Setup Utility, NEC EXPRESSBUILDER or a web browser. The default settings are as follows:

Telnet:	**23**
SSH:	**22**

The BMC only supports the SSH protocol version 2. Any SSH client supporting version 1 cannot be connected to the BMC. Use the client supporting the version 2.

A security warning messages regarding your server certificate may be displayed when you access the BMC from a SSH client.

LOGIN AND LOGOUT

Login

Enter your user name and password at login prompt. A command prompt will be displayed after login.

The user account is common to the one for a remote management function via web browser.

The number of users who can log in the system using the command line interface at the same time is three users or less. Therefore, you cannot log in the system when other three users have been logging in the system using Telnet/SSH clients via the command line interface. Check whether other three users are logging in the system, if you cannot log in via the command line interface.

Only a single user among users who are using the command line interface or DianaScope(a software application bundled for remote management) can use a character-based remote console via the command line interface or DianaScope. Once the first user uses the character-based remote console, other users cannot use any character-based remote console from any Telnet/SSH clients or DianaScope Manager. Check whether another user is using a character-based remote console, if you cannot use a character-based remote console.

Logout

Enter the “exit**”** command at the command prompt. The Telnet/SSH client will be disconnected from the BMC after logout.

BASIC COMMANDS

This section describes about basic commands to use them as the command line interface. These basic commands manage the host system by using the concept of verb (command) and target (Managed Element) proposed by DMTF (Distributed Management Task Force).

Each basic command functions to a specified target. The target points the managed element by address path much like the path to a file in a file system.

Both absolute path, which is started from "/", and relative path are available for pointing the target. Specifically, "." and ".." are supported. The "." means the current default target and the ".." means the parent target.

Each basic command functions to the current default target when the <target>, which is an argument pointing a target for the command, is not specified to the basic command. The current default target can be changed by the cd command. The current default target is "/"(root) when the command line interface session is started.

Help string, command syntax, of each command appears when "-h" option is specified as the <options> of the command. The argument placed between "[" and "]" is omissible.

The user must have an account as the following user level to use the basic commands:

- **cd, exit, help, show and version can be use under an account as all user levels.**
- **stop, start and reset are needed an account as operator or administrator user level to use these commands.**
- **set and load are needed an account as administrator user level to use these commands.**

cd

Syntax:

cd [<options>] [<target>]

Description:

The cd command changes the current default target to the target specified by the <target> argument. The cd command without any argument displays the current default target.

exit

Syntax:

exit [<options>]

Description:

The exit command terminates and logs out the user session.

help

Syntax:

help [<options>] [<help topics>]

Description:

A target, <target> and/or a basic command, <command>, can be specified for the <help topics>.

The help command displays the help string for the specified target when only <target> argument is specified.

The help command displays the help string for specified basic command related to the specified target when both <target> and <command> arguments are specified.

The help command displays the help string for specified basic command related to the current default target when only <command> argument is specified.

This command displays "Unsupported Command" message when the specified target does not support the specified command or the host system does not support the specified target.

load

Syntax:

load -source <URI> -oemnecfiletype csr [<options>] [<destinationtarget>]

Description:

The load command is used to take a BMC firmware binary image from a specific source location (specified as a <URI>) and place it at the specified target (specified as <distinationtarget>). The BMC firmware binary image downloads using TFTP from the specified location and programs flash ROM in the BMC with the image.

The options -source <URI> and -oemnecfiletype csr MUST be specified except when -h is specified as the <options>.

The expected format for the <URI> is //<TFTP Server's IP Address>/<path>/<filename>.

The valid targets as the <distinationtarget> for the load is only /system1/firmware.

It is needed that the TFTP server is prepared in advance to use the load command for BMC firmware update. At first, please place the BMC firmware to the specific location of the TFTP server. And then, please download the BMC firmware from the TFTP server to the BMC using the load command. A successful firmware upload typically takes typically several minutes.

Please use the load command ONLY when it is directed with the other documents of our company for BMC firmware update. Besides, please do NOT use the load command for any other purpose.

reset

Syntax:

reset [<options>] [<target>]

Description:

The reset command performs a hardware reset on the <target>.

/system1 and /map1 are available for the <target> of the reset command.
For /system1, the host system is reset. For /map1, the BMC is reset.

set

Syntax:

set [<options>] [<target>] <propertyname>=<value>

Description:

The set command is used to set the value of one or more properties of target specified by the <target>. The command accepts a target specified by the <target> and series of <propertyname>=<value> pairs which is will try and apply. The <propertyname> means a name of property set by the command. The <value> means a new value set by the command.

One or more <propertyname>=<value> pairs can be specified by delimiting between each pair in space.

The set command requires <propertyname>=<value> command line argument except when -h is specified as the <options>.

show

Syntax:

show [<options>] [<target>] [<properties>]

Description:

The show command is used to display information about the target specified by the <target> argument.

The command displays the target specified by the <target> as the first line of the information. It displays the current default target in the first line if <target> is not specified.

The default behavior of the command for the target specified by the <target> is as follows. The command display targets which are contained by the specified target after the "Targets" string. The command displays properties which are contained by the specified target after the "Properties" string. The properties are displayed in the form of property=value. The command displays basic commands(verbs) and special extended commands which are available for the specified target after the "Verbs" string.

The command displays the property specified by the <properties> in the form of property=value if the <properties> is specified. The command displays all properties which are contained by the specified target if the <properties> is not specified.

There is -display <arg values> option which can be specified by the <options> for the

show command. The option can control the type of information that is displayed about the target specified by the <target>. Valid option argument values as the <arg values> for this option include "targets", "properties", "verbs", and "all". The option argument values can select the above "Targets", "Properties" and "Verbs" information that is displayed. “all” displays the whole. The default for the -display option control is "all".

start

Syntax:

start [<options>] [<target>]

Description:

/system1 and /system1/console1 are available for the target of the start command.

The start command performs a power on to the host system if /system1 is specified by the <target>.

The start command starts a character-based remote console if /system1/console1 is specified by the <target>.

stop

Syntax:

stop [<options>] [<target>]

Description:

The stop command performs an OS shutdown request (normal power off request) or a forced power off request.

/system1 is available for the target of the stop command. The stop command with no option as the <options> performs an OS shutdown request (normal power off request) to the host system if /system1 is specified by the <target>. The command with -f (or -force) as the <options> performs a forced power off request to the host system if /system1 is specified by the <target>.

version

Syntax:

version [<options>]

Description:

The version command is used to display the version of the command line protocol specification which is supported.

REMOTE CONTROL

You can perform remote control of the host system at the command prompt.

The user must have an account as operator or administrator for remote control.

Performing remote control when the operating system is running may cause the loss of data in the host system.

Power ON

Enter the following command at the command prompt.

```
start /system1
```

Forced Power OFF

Enter the following command at the command prompt.

```
stop -force /system1
  Or
stop -f /system1
```

OS Shutdown

Enter the following command at the command prompt.

```
stop /system1
```

The above OS shutdown is equivalent to pressing the POWER switch when the power of the host system is on. Your operating system must be set to shut down when you power off the system.

System Reset

Enter the following command at the command prompt.

```
reset /system1
```

If you perform a system reset when the power of the host system is off, the system will be powered on.

Remote Console

To start a character-based remote console, enter the following command at the command prompt.

```
start /system1/console1
```

To return from the character-based remote console to the command interface session, enter the **<ESC>stop** keys (<ESC>key, <s>key, <t>key, <o>key and <p>key) during the character-based remote console.

To use a character-based remote console, set appropriate settings for the console redirection function of the host system's serial port on the BIOS Setup Utility in advance.

Especially, please use the following items by the following setting:

- **BIOS Redirection Port : Serial Port B**
- **Baud Rate : 19.2K**
- **Flow Control: CTS/RTS**
- **Terminal Type: PC ANSI**

For the system BIOS Setup Utility, please refer to the User's Guide of your host system.

Only a single user among users who are using the command line interface or DianaScope(a software application bundled for remote management) can use a character-based remote console via the command line interface or DianaScope. Once the first user uses the character-based remote console, other users cannot use any character-based remote console from any Telnet/SSH clients or DianaScope Manager. Check whether another user is using a character-based remote console, if you cannot use a character-based remote console.

Chassis Identify

You can control the UID (Unit ID) LED on the host system for chassis identify through the command line interface.

The user must have an account as administrator for flashing or turning off the UID LED because of using the set command for flashing or turning off it.

Flashing UID LED

Enter the following command at the command prompt.

```
set /system1/led1 enabledstate=enabled
```

Turning off UID LED

Enter the following command at the command prompt.

```
set /system1/led1 enabledstate=disabled
```

State confirmation of UID LED

Enter the following command at the command prompt.

```
show /system1/led1
```

You can confirm the state of the UID LED by value of enabledstate of the "Properties" which is displayed by the command.

enabledstate=enabled : UID LED is flashing.
enabledstate=disabled : UID LED is turned off.

If the UID LED is not mounted into the host system, the “Chassis Identify” function is not executed.
Please refer to the User’s Guide of your host system for the description of the UID LED.

VIEWING SYSTEM EVENT LOG

To move the current default target to /map1/log1, enter the following command at the command prompt:

```
cd /map1/log1
```

Here, to confirm the total number of system event log records, enter the following command: The "Targets" section reported by the following command indicates the "record<N>" target(s): <N> means any value between 1 and the total number of the system event log records.

```
show
```

Next, when the following command is input, information of a specific record is displayed at "Properties" section: Here, <n> means record number which you would like to confirm.

```
show record<n>
```

For example, enter the following command when you would like to confirm the number 2 record:

```
show record2
```

The example of displaying information in this case is shown below.

```
record2
Targets
Properties
   number=2
   date=12/20/2004
   time=15:22:05
   sensordescription= Baseboard 12v
   eventdescription= Upper Critical-going high
   eventdirection=Assertion
Verbs
   cd
   version
   exit
   show
   reset
   oemnec
   help
```

USER SETTINGS

This section describes about how to confirm and modify the user account through the command line interface. To move the current default target to /map1/accounts, enter the following command at the command prompt.

```
cd /map1/accoutns
```

Next, to move the current default target to an user target which you would like to confirm or(and) modify, enter the following command at the command prompt. <N> means the any value between 1 and 13 for the following command: Therefore you can select a user between user1 and user13. The <N> corresponds to an order from the list of user accounts top on the user account configuration page through a Web browser. Refer to the “User” of the “Configuration” in the “Chapter 5: Using Remote Management” “Menu Bar”.

```
cd user<N>
```

Enter the following command, if you would like to confirm the information which the selected user has as its properties.

```
show
```

Enter the following command if you would like to modify a property of the selected user.

```
set <Property name>=<New value>
```

The properties which the selected user target contains are as follows:

- **username**

  This corresponds to a user name (login name). It becomes effective at next login if you change it.

- **password**

  This is the user password (only can be changed). "password=" is displayed but the password setting, value of this property, is not displayed when this property is displayed. It becomes effective at next login if you change it.

- **group**

  This specifies the user level. The valid values for this property are "User", "Operator" and "Administrator". It becomes effective at next login if you change it.

A user name can contain up to 15 alphanumeric characters, including “- (minus)” and “_ (underscore).” The password accepts up to 19 ASCII characters, except for “ (space)”, ““(quotation marks)”, “?”, “=”.

NETWORK SETTINGS

This section describes about how to confirm and modify the network setting through the command line interface. To move the current default target to /map1/nip1, enter the following command at the command prompt:

```
cd /map1/nic1
```

Enter the following command, if you would like to confirm information of the network setting as properties of the network target which is /map1/nip1.

```
show
```

Enter the following command if you would like to modify a property of the network target.

```
set <Property name>=<New value>
```

The properties which the network target contains are as follows:

- **networkaddress**

  This specifies the IP address for the network (NIC). This is the dynamic setting.

- **oemnec_mask**

  This specifies the subnet mask for the network (NIC). This is the dynamic setting.

- **oemnec_gateway**

  This specifies the default gateway IP address for the network (NIC). This is the dynamic setting.

- **oemnec_dhcp_enable**

  This specifies whether DHCP is enabled for the network (NIC). Note that, the valid values for this property are "TRUE" and "FALSE". "TRUE" means that the DHCP is enabled. "FALSE" means that the DHCP is disabled. This is the dynamic setting.

SPECIAL EXTENDED COMMANDS

This section describes about the special extended command which can do state acquisition (powerstate, lampstate) and interrupt generation for OS dump (nmidump). The special extended commands use the syntaxes different from the basic command's ones.

State Acquisition

You can acquire the state of the system at the command prompt:

Commands to acquire the state are executable in all user levels.

State acquisition commands (powerstate, lampstate) are executable only when current default target is "/"(root).

Enter the following command, if the current default target is not "/"(root).

```
cd /
```

Power State acquisition

Enter the following command at the command prompt:

```
powerstate
```

One of the following responses is returned according to the power state.

power on
System power is on.

power off
System power is off.

Status LED State acquisition

Enter the following command at the command prompt:

```
lampstate -statuslamp
```

One of the following responses is returned according to the STATUS LED state.

off
STATUS LED is turned off.

green on
STATUS LED lights in green.

green blink
STATUS LED is blinking in green.

amber on
STATUS LED lights in amber.

amber blink
STATUS LED is blinking in amber.

red on
STATUS LED lights in red.

red blink
STATUS LED is blinking in red.

The state of the STATUS LED and the meaning are different according to the system. Refer to the User's Guide of the system for details.

Interrupt Generation for OS Dump

You can generate the interrupt, NMI(non-maskable interrupt), for OS dump by entering following command at the command prompt.

```
nmidump /system1
```

The user must have an account as operator or administrator for executing the nmidump command.

The above command behavior is equivalent to pressing the DUMP switch on the host system.

OTHERS

Confirmation of BMC firmware revision

You can confirm the BMC firmware revision through the command line interface by entering following the basic command at the command prompt.

```
show /map1/firmware
```

In this case, the BMC firmware revision is appeared at the right side of "fwversion=" string.

You can also confirm the BMC firmware revision at the "Revision Information" of the Help page when you log in the system through web browser.

7. Troubleshooting

ERROR MESSAGES

Fatal errors

No	Error Message	What to do
1	Fatal error. JavaVM quits.	Try logging in again. If the same message continues to appear, contact your support department.
2	A fatal software error has occurred.	Try logging in again. If the same message continues to appear, contact your support department.
3	Fatal error occurred.	Try logging in again. If the same message continues to appear, contact your support department.
4	Unexpected error occurred.	Try logging in again. If the same message continues to appear, contact your support department.

Login error

No	Error Message	What to do
1	Authentication error	Check the user name and password, and then enter them again.
2	Enter user name.	You must enter user name. Enter user name and password again.

Access privilege error

No	Error Message	What to do
1	Unauthorized operation.	Your user level is insufficient for the operation you have specified. Consult your administrator.

Network errors

No	Error Message	What to do
1	Timeout has occurred.	Check the network environment and try it again. Login Web page again then try it again.

2	The parameter from HTML is illegal.	Check the network environment and try it again. Login Web page again then try it again.
3	A network error occurred.	Check the network environment and try it again. If the same message continues to appear, contact your support department.

Remote KVM Console errors

No	Error Message	What to do
1	The parameter from HTML is illegal.	Check the network environment and try it again. Login Web page again then try it again.

System event logs (SEL) display errors

No	Error Message	What to do
1	A network error occurred, or BMC was busy. Please network connection and try again after waiting for a while.	The network may be busy. After few minutes, try again. If the error persists, contact your support department because a failure may have occurred in BMC.
2	Failed to acquire system event logs.	The network may be busy. Try again. If the error persists, contact your support department because a failure may have occurred in BMC.

Sensor data records (SDR) display error

No	Error Message	What to do
1	A network error occurred, or BMC was busy. Please network connection and try again after waiting for a while.	The network may be busy. After few minutes, try again. If the error persists, contact your support department because a failure may have occurred in BMC.

Field replaceable unit (FRU) information display error

No	Error Message	What to do
1	A network error occurred, or BMC was busy. Please network connection and try again after waiting for a while.	The network may be busy. After few minutes, try again. If the error persists, contact your support department because a failure may have occurred in BMC.

BMC configuration errors

No	Error Message	What to do
1	The user name is too long	A user name should be 15 characters or less.
2	Invalid user name	You can use only alphanumeric characters, minus sign (–), and underscore (_) for a user name.
3	Invalid Password	You can use ASCII characters except ‘ ’ (space), ‘”’, ‘?’, ‘=’ for a password. The length of a password is up to 19.
4	Passwords do not match.	Input passwords again.
5	Invalid IP address	Use numerals and periods to specify an IP address.
6	Invalid subnet mask	Use numerals and periods to specify a subnet mask.
7	Invalid default gateway	Use numerals and periods to specify a default gateway.
8	Invalid DNS server IP address	Use numerals and periods to specify the IP address of DNS server.
9	Invalid host name	You can use only alphanumeric characters, minus sign (–), and underscore (_) for a host name. A host name should be 47 characters or less.
10	Invalid domain name	You can use only alphanumeric characters, minus sign (–), and underscore (_) for a domain name. A domain name should be up to 47 characters.
11	Invalid HTTP port number	You can use only numeric value from 0 to 65535.
12	Invalid SSL port number	You can use only numeric value from 0 to 65535.
13	HTTP/SSL should not be the same.	The same port number can't do them. Specify different value.
14	Invalid To: field.	You can use only alphanumeric characters, period (.), at mark (@), minus sign (–), and underscore (_) for a To: field A To: field should be up to 47 characters.
15	Invalid From: field.	You can use only alphanumeric characters, period (.), at mark (@), minus sign (–), and underscore (_) for a From: field A From: field should be up to 47 characters.

16	Invalid Reply-To: field.	You can use only alphanumeric characters, period (.), at mark (@), minus sign (–), and underscore (_) for a Reply-To: field A Reply-To: field should be up to 47 characters.
17	Invalid Subject: field.	You can use only ASCII characters except '+', '"', '?', '=', '<', '>' up to 31 characters.
18	Invalid SMTP server address	You can specify SMTP server address as IP address consists of numerals and periods or DNS name consists of alphanumeric characters, minus sign (–), and underscore (_). If you use DNS name, the length should be up 47 characters.
19	Invalid SMTP port number.	You can use only numeric value from 0 to 65535.
20	Invalid SMTP user name.	You can use only ASCII characters except ' ' (space), '"', '?', '=', '<', '>' up to 15 characters.
21	Invalid SMTP password.	You can use only ASCII characters except ' ' (space), '"', '?', '=', '<', '>' up to 19 characters.
22	Invalid Telnet port number.	You can use only numeric value from 0 to 65535.
23	Invalid SSH port number.	You can use only numeric value from 0 to 65535.
24	Telnet/SSH port number should not be the same.	The same port number can't do them. Specify different value.

OTHERS TIPS

Should you have troubles while using the BMC for remote control, monitoring, and management of the host system, please first check the system according to the following descriptions to troubleshoot your issue prior to sending it for repair.
If you find the same issue as the one identified on your remote management PC, please follow the tips and instructions provided for each issue.

For the issues regarding your system operation, please refer to the User's Guide attached to your system.

If your issue is not described below, or should the provided instructions do not resolve your issue, please contact your service center.

The web page is not displayed on the remote management PC. Or the login prompt of the command line interface is not displayed on the PC.

☑ Is JAVA 2 Runtime Environment, Standard Edition 5.0 or 6.0 installed in your remote management PC when the web page is not displayed on the PC?
=> You need to install Java2 Runtime Environment, Standard Edition 5.0 or 6.0 in your management PC. You can download the latest JRE (Java Runtime Environment) at: http://java.com/en/download

☑ Is the network cable properly connected to the Management LAN port?
=> Confirm whether the LAN cable is connected to the Management port.

☑ Is a firewall or a gateway configured to limit the communication with the Internet?
=> A firewall or a gateway may be set to limit the communication with the Internet. Connect the LAN cross-over cable directly to the management PC and see if the issue is resolved. Make sure again whether a firewall or a gateway is limiting the communication with the Internet.

☑ Is the DHCP function enabled?
=> If you enable the DHCP function in the environment where DHCP is not supported, you will not be able to communicate with the BMC. To resume the communication, Configure network settings such as an IP address by using the BIOS Setup Utility or NEC EXPRESSBUILDER. Refer to "Management LAN Settings" in the "Chapter 2: Configuring the Host System".

=> When it is not possible to communicate with the BMC even if you operate the above-mentioned, please configure the network settings such as IP address and enabling HTTP, HTTPS, Telnet and/or SSH once again after clearing the BMC settings, Refer to the tip: "I forgot my user name and password for remote management and Command Line Interface." in this section for how to clear.

☑ Is the BMC's management LAN used in the network environment that is capable of auto-negotiation?
=> The BMC's management LAN always operates with auto-negotiation. Therefore please use the BMC's management LAN in the network environment that is capable of auto-negotiation.

The Server Panel does not open.

☑ Confirm the network environment (e.g. the fire wall setting)

☑ If the message “No Java 2 Standard Edition v 5.0 support for This APPLET” is displayed, install JRE in your remote management PC as instructed above.

☑ Internet Explorer ActiveX Update (KB912945) is already installed, but Cumulative Security Update for Internet Explorer (KB912812) is not installed yet in the remote management PC.
=> If the KB912945 alone is installed, it will affect the Java applet display. Install Cumulative Security Update for Internet Explorer (KB912812) additionally. Go to the following Microsoft website for details:
http://www.microsoft.com/technet/security/Bulletin/MS06-013.mspx

The Remote KVM icon was pressed, but the Remote KVM Console function does not start.

☑ Did you log in as a user with an administrative account?
=> To use the Remote KVM Console function, the user must log in to the BMC with an administrative account.

The remote console screen does not display the host system’s screen.

☑ Is the host system’s resolution setting appropriate?
=> You must configure the resolution setting supported by the BMC.
For supported resolutions, refer to ”Remote KVM Console” in this manual.

☑ Confirm the version of Java Runtime Environment (JRE) installed in the remote management PC.
=> If you use the JRE1.4 family, it is necessary that you update it to the JRE 5.0 family.

☑ There is a possibility not to be able to display temporarily by the network problem.
=> Execute [tool]-> [Refresh Screen] on Remote KVM console.

The mouse pointer on the host system’s screen does not synchronize with the one on the management PC screen.

☑ Change the mouse mode.
=> In the Remote KVM Console window, click [Preferences], go to [Mouse Mode], and change the mode to [Absolute Mode] or [Relative Mode]. You may have to synchronize the mouse pointers after changing the mode.

☑ Synchronize the mouse pointers
=> On the screen of the remote management PC, drag the pointer off the screen from the upper left corner of the screen, and a few seconds later, move it back to the screen from the same corner. Repeat the same step at the lower right corner.

☑ If the host system runs Linux in text mode, each mouse pointer will not synchronize.

The drive registered via Remote Media is not recognized in the host system.

☑ Try “Connect” and “Disconnect” again.

☑ Reboot host system.

I can't eject a medium from the CD-ROM drive after disconnecting Remote Media.

☑ The Remote Media disconnected properly?
=> Reconnect the CD-ROM drive and then disconnect the Remote Media following proper procedure. Or reboot the management PC.

The input mode (Caps lock, Num Lock and so forth) changes on the remote management PC after when you log in to the BMC.

☑ The input mode for the host system’s keyboard is reflected to the management PC when you log in.
=> Change the mode on the management PC, if necessary.

I forgot my user name and password for remote management and Command Line Interface.

☑ You can change all the BMC settings back to default by using the BIOS Setup Utility or NEC EXPRESSBUILDER.

Method by BIOS Setup Utility

Execute Clear BMC Configuration of the BIOS Setup Utility. Refer to “Settings by BIOS Setup Utility” of “Management LAN Settings” in the “Chapter 2: Configuring the Host System”.

Method by NEC EXPRESSBUILDER

Boot the host system from the NEC EXPRESSBUILDER DVD-ROM and execute [Tool]-[System Management]-[Clear BMC Configuration]. Utility. Refer to ”Settings by NEC EXPRESSBUILDER” of “Management LAN Settings” in the “Chapter 2: Configuring the Host System”.

Check **The above methods also deletes the settings for DianaScope (a software application bundled for remote management). Be sure to perform a backup for the DianaScope settings before you change the BMC settings.**

On the Remote KVM console, I want to change Software Keyboard language to French.

☑ You can change the Software Keyboard language from Remote KVM Console menu by taking following steps:

1. Open Login Page of EXPRESSSCOPE Engine 2 and Click [English] link, which is on the upper right of the page, and login to BMC in English mode.
2. Open Remote KVM Console Window, and select language:[French(FR)] from [Presence] -> [Keyboard] menu.
3. Enter keys from remote keyboard. If you want to use Software keyboard, open Software Keyboard panel from [Tools]-[Virtual Keyboard].

Before open the login page of EXPRESSSCOPE Engine 2, you should match the key board language of the management PC with the host system.

I can't detect all connected devices in the selected device window of the Remote Media.

☑ If the management PC runs Windows XP, You can't sometimes detect the drive. You have to apply Service Pack 2.

☑If the management PC runs Windows, the process that uses the management PC's device, such as Windows Media(R) Player, is alive, you can't sometimes detect the device.
Please check that the process (ex: wmplayer.exe) is not alive with Task manager's Process tab, and search devices again.

Internet Explorer crashes .

☑ Problem occurs if the management PC runs with following environment. Please use JRE5.0 for prevention.

OS: Windows 2003 SP2.
JRE: Java™ 2 Runtime Environment, Standard Edition 6.0.
Web browser: Internet Explorer 6.0.

Notes for Windows Vista.

☑ If the management PC runs Windows Vista, you can't https access to Web server via https using Internet Explorer 7.0.

I can not enter [CapsLock], [Scroll Lock], [Num Lock] keys on the remote KVM console.

☑ On the remote KVM console, if the management PC runs Linux, [CapsLock], [Scroll Lock], [Num Lock] keys may not be sent to the host system.
In this case, please use Software Keyboard.

The mouse pointer of the host system does not appear on the remote KVM console.

☑ If the host system runs Linux, the mouse pointer of the host system does not appear on the remote KVM console.
In this case, please follow the procedure below on the remote KVM console.

1. Change the display resolution of the host system.
2. Restart X-window.