HX2560 M1/ HX2560 M2





IPMI User's Guide



The information in this User's Manual has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates.

Fujitsu Limited reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Fujitsu Limited and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL FUJITSU LIMITED BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTA-TION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, FUJITSU LIMITED SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUD-ING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

FCC Statement: 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. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

Manual Revision 2.0 Release Date: August 16, 2013

Unless you request and receive written permission from Fujitsu Limited, you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Preface

About this User's Guide

This user guide is written for system integrators, PC technicians and knowledgeable PC users who intend to configure the IPMI settings supported by the Nuvoton WPCM450 BMC Controller embedded in serverboards. It provides detailed information on how to configure the IPMI settings supported by the WPCM450 Controller.

ho Note: Nuvoton Technology is a subsidiary of Winbond Corp.

User's Guide Organization

Chapter 1 provides an overview on the Nuvoton WPCM450 Controller. It also introduces the features and the functionality of IPMI.

Chapter 2 provides detailed instructions on how to configure the IPMI settings supported by the WPCM450 Controller.

Chapter 3 provides the answers to frequently asked questions.

Conventions Used in This User's Guide

Pay special attention to the following symbols for proper IPMI configuration.

Marning: Important information given to avoid IPMI configuration errors,

Note: Additional information given to ensure correct IPMI configuration setup.

Notes

Table of Contents

Prefa	ce3
About	: this User's Guide
User's	Guide Organization
Conve	ntions Used in This User's Guide
Chap	ter 1 Introduction
1.1	Overview of the Nuvoton WPCM450 BMC Controller 1-1
	WPCM450 DDR2 Memory Interface 1-1
	WPCM450 PCI System Interface 1-1
	IPMI Features 1-2
1.2	WPCM450 Block Diagram 1-3
1.3	Introduction to the IPMI Platform 1-3
1.4	An Important Note to the User
Chap	ter 2 Configuring the IPMI Settings
2.1	Configuring BIOS 2-1
2.2	Accessing the Remote Server via Console Redirection Using the Browser 2-4
	To Log In to the Remote Console 2-4
2.3	IPMI Main Screen
2.4	System Status
2.5	Server Health 2-7
	2.5.1 Sensor Readings 2-8
	2.5.2 Event Log2-10
2.6	Configuration2-12
	2.6.1 Configuring the Alerts Settings2-13
	2.6.2 Configuring Date and Time Settings2-15
	2.6.3 Configuring Light-Weight Directory Access Protocol (LDAP) Settings2-16
	2.6.4 Active Directory Settings2-17
	2.6.5 Configuring the RADIUS Settings2-19
	2.6.6 Configuring the Mouse Mode Settings2-20
	2.6.7 Configuring Network Settings2-21
	2.6.8 Configuring Dynamic DNS (Domain Name System) Settings2-23
	2.6.9 Configuring the Remote Session Settings2-24
	2.6.10 Configuring the SMTP Settings2-25
	2.6.11 Configuring the SSL (Secure Sockets Layer) Certification2-26
	2.6.12 Configuring Users Settings2-27

	2.6.13 Configuring Port Settings2-28
	2.6.14 IP Access Control
	2.6.15 Configuring Fan Settings2-31
2.7	Remote Control
	2.7.1 Launching Console Redirection2-33
	2.7.2 Remote Control - Server Power Control2-54
	2.7.3 Remote Control-Launch SOL2-55
2.8	Virtual Media2-57
	2.8.1 Configuring USB Floppy & Flash Device Settings2-58
	2.8.2 Configuring CD ROM Image File Settings2-59
2.9	Maintenance
	2.9.1 Maintenance - Firmware Update2-62
	2.9.2 Maintenance - Unit Reset2-64
	2.9.3 Maintenance - IKVM Reset2-65
	2.9.4 Maintenance - Factory Default2-66
	2.9.5 Maintenance - IPMI Configuration2-67
2.10	Miscellaneous2-68
	2.10.1 Miscellaneous - POST Snooping2-68
	2.10.2 Miscellaneous - UID Control2-69
Chap	ter 3 Frequently Asked Questions
3.1	Frequently Asked Questions
Арре	ndix A Introduction to SMASHA-1
A-1	Overview A-1
	How SMASH works
	SMASH Compliance Information
A-2	An Important Note to the User
A-3	Using SMASH A-3
A-4	Initiating the SMASH Protocol A-3
	To Initiate SMASH Automatically A-3
A-5	SMASH-CLP Main Screen
A-6	Using SMASH for System Management A-4
A-7	Definitions of Command VerbsA-5
A-8	SMASH Commands A-7
A-9	Standard Command Options A-8
A-10	Target Addressing A-9
	Terms Used in the Target Addressing Diagram

Notes

Chapter 1

Introduction

1.1 Overview of the Nuvoton WPCM450 BMC Controller

The Nuvoton WPCM450, a Baseboard Management Controller (BMC), supports PCI-based 2D/VGA Graphics cores via PCI interfaces, multi-media virtualization, and Keyboard/Video/ Mouse Redirection (KVMR). The WPCM450 Controller is ideal for networking management.

The WPCM450 interfaces with the host system via PCI connections to communicate with the Graphics core. It supports USB 2.0 and 1.1 for remote KVM emulation. It also provides LPC interface support to control Super IO functions. The WPCM450 is connected to the network via an external Ethernet PHY module or shared NCSI connections.

The WPCM450 communicates with onboard components via SMBus interface, PECI (Platform Environment Control Interface) buses, and General Purpose I/O ports.

WPCM450 DDR2 Memory Interface

The WPCM450 Controller supports 16-bit DDR2 memory with a speed of up to 220 MHz. The serverboard supports 128 MB of memory which is shared between the BMC and onboard graphics card. For best signal integrity, the WPCM450 provides point-to-point connections.

WPCM450 PCI System Interface

The WPCM450 provides 32-bit, 33 MHz 3.3V PCI interface, which is compliant with PCI Local Bus Specification Rev. 2.3. The PCI system interface connects to the onboard PCI Bridge and is used by the graphics controller.

IPMI Features

- 1. Remote KVM (graphics) console
- 2. Virtual Media and ISO images
- 3. Remote server power control
- 4. Remote Serial over LAN (text console)
- 5. Event Log support
- 6. Automatic Notification and Alerts (SNMP and email)
- 7. Hardware Monitoring
- 8. Overall health display on the main page
- 9. Out of band management through shared or dedicated LAN
- 10. Option to change LAN connection interface at Runtime
- 11. VLAN
- 12. RMCP & RMCP+ protocols supported
- 13. SMASH/CLP
- 14. Secure command line interface (SSH) and Telnet
- 15. WSMAN and WS-CIM
- 16. RADIUS authentication support
- 17. Secure browser interface (Secure socket layer SSL support)
- 18. Lightweight Directory Access Protocol (LDAP) supported
- 19. DCMI 1.0 support
- 20. Backup and restore the configuration file
- 21. Factory defaults from web support
- 22. Video quality settings
- 23. Record video and play
- 24. Server data/information
- 25. Preview of the remote screen on the main page
- 26. Update Firmware through browser and OS
- 27. OS-independent

1.2 WPCM450 Block Diagram

The following diagram represents a typical system setup for the WPCM450 Controller.



1.3 Introduction to the IPMI Platform

The Intelligent Platform Management Interface (IPMI) provides remote access to multiple users at different locations for networking. It also allows a system administrator to monitor system health and manage computer events remotely.

IPMI operates independently from the operating system. When used with an IPMI Management utility installed on the serverboard, the WPCM450 BMC Controller will connect the South Bridge to other onboard components, providing remote network interface via serial links. With the WPCM450 Controller and the IPMI firmware built in, the serverboard allows the user to access, monitor, diagnose, and manage a remote server via Console Redirection. It also provides remote access to multiple users from different locations for system maintenance and management.

1.4 An Important Note to the User

The graphics shown in this user's guide were based on the latest information available at the time of publishing of this guide. The IPMI screens shown on your computer may or may not look exactly like the screen shown in this user's guide.

Chapter 2

Configuring the IPMI Settings

With the Nuvoton WPCM450 BMC Controller, serverboard allow the user to access, monitor, manage and interface with multiple systems in different remote locations.

2.1 Configuring BIOS

Before configuring IPMI, follow the instructions below to configure the system BIOS settings.

Enabling COM Port for SOL (IPMI)

- 1. Press the key at bootup to enter the BIOS Setup utility.
- 2. Select *Advanced* and press <Enter> to enter the Advanced menu.
- 3. From the Advanced menu, select Super IO Configuration and press <Enter>.
- 4. From the Super IO Configuration menu, select *Serial Port 2 Configuration* and press <Enter>.
- 5. Make sure that SOL Serial Port is enabled. If not, Select SOL Serial Port and press <Enabled>.
- 6. Make sure that Serial Port 2 Attribute is <SOL>. If not, Select Serial Port 2 Attribute and press <SOL>.



- Back to the Advanced menu. Then select Serial Port Console Redirection and press <Enter>.
- 8. Make sure that SOL Console Redirection is <Enabled>. If not, Select SOL Console Redirection and press <Enabled>.



B. Enabling All Onboard USB ports

- 1. Press the key at bootup to enter the BIOS Setup utility.
- 2. Select *Advanced* and press <Enter> to enter the Advanced menu.
- 3. Select Chipset Configuration and press <Enter>.
- 4. From the Chipset Configuration submenu, select *South Bridge* and press <Enter>.
- 5. Make sure that all *All USB Devices* are enabled. If not, Select *All USB Devices* and press <Enabled>. (This is required for KVM to work properly.)

Actio Setup Utility - Advanced PCH Information Name Stepping	Copyright (C) 2012 American M Patsburg 06 (C1 Stepping)	egatrends, Inc. Enabled/Disabled All USB Devices
2 Keyboards, 1 Mouse, 1 Point		
All USB Devices		
EHCI Controller 1 EHCI Controller 2	[Enabled] [Enabled]	
Legacy USB Support Port 60/64 Emulation EHCI Hand-off	[Enabled] [Enabled] [Disabled]	++: Select Screen 11: Select Item Enter: Select 4/-: Change Opt. F1: General Heip F2: Previous Values F3: Optimized Defaults F4: Gave a Exit ESC: Exit

C. Configuring IP and MAC Addresses using BIOS

- 1. Press the key at bootup to enter the BIOS Setup utility.
- 2. Select *IPMI* and press <Enter> to enter the IPMI menu.
- 3. From the IPMI menu, select *BMC Network Configuration* and press <Enter> to set IP and MAC addresses.

SMC Network Configuration		BIOS will set below setting to IPMI in next
LAN Channel 1		BOOT
IPMI LAN Selection	[Failover]	
IPMI Network Link Status:	Dedicated LAN	
Jpdate IPMI LAN Configuration	[NC]	
Station TP Address	010 021 078 125	
Subnet Mask	255,255,255,000	
Station MAC Address	00-25-90-9e-59-64	
Gateway IP Address	010.021.078.001	
		++: Select Screen
		↑↓: Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F2: Previous values
		F4: Save & Evit
		ESC: Exit

2.2 Accessing the Remote Server via Console Redirection Using the Browser

To Log In to the Remote Console

Once you are connected to the remote server via IPMI Console Redirection, the following IPMI Login screen will display.

កប្បីរីវន្ស	
Please Login Username Password Login	

- 1. Enter your Username in the Username fields.
 - **Note:** The manufacturer default username and password are ADMIN/ADMIN. Once you have logged into the BMC using the manufacturer default password, be sure to change your password for security purpose.
- 2. Enter your Password in the Password box and click <Login>.
- 3. The Home Page will display as shown on the next page.

Note: The *Administrator* account cannot be deleted.

2.3 IPMI Main Screen

The IPMI Main screen displays the following information.



The IPMI Main screen displays system information, including the following:

- The Menu Bar: The menu bar on the top displays System Information, Server Health, Configuration, Remote Control, Virtual Media, Maintenance, and Miscellaneous. Click an item on the Menu Bar to access an IPMI feature and configure its settings.
- 2. The Options Window: This window displays IPMI submenu items. Click an item in this window to configure the setting.
- 3. The Main Display Area: This area displays the contents of the particular section. Click an item in this area to configure the setting.
- 4. System Health Status: This icon displays the health status of the server.
 - Green: It indicates that the server is normal.
 - Orange: At least an alert has occurred. Take proper actions to ensure system health.
 - Red: At least one critical condition has occurred. Immediate attention is required to resolve the critical condition for the server to function normally.
- 5. Language Select: From the pull-down menu, select a language.
 - English
 - Japanese

2.4 System Status

Once you've logged into the remote server, the IPMI Main scree will display.

[FUĴÎTSU			Host Identification Server: 010. User:	021.135.086 ADMIN (Adminis	rator)		Normal Refresh Logour English
	System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
12	 System System inform FRU Reading 	€ S	Summary ware Revision : 11.81 ware Build Time : 2012-1 mote Conscie Preview Refer Strategie (Strategie (Strate	0-23	IP address : 010.0 BING MAC address System LAVE MAC System LAVE MAC	21.135.086 : 00.255.00.2317t address : 00.25.90.4f19 address : 00.25.90.4f19	ka) let	
		Pe	wer Control via IPMI Ho Power On	et is currently on Power Down	Reset			

- 1. System Information: This item displays the following firmware information.
 - Firmware Revision
 - Firmware Build Time
 - IP Address
 - MAC Address
 - Preview Screen
 - Power Control: This feature allows the user to launch the remote console by clicking a preview screen.
- 2. FRU Reading: Click this item to display the following BMC FRU (Field Replaceable Unit) information.
 - FRU Device ID
 - Chassis Information
 - Board Information
 - Product Information

2.5 Server Health

This feature allows the user to set *Server Health* settings. To access *Server Health* information, follow the instructions below.

FUJÎTSU		-Host Identification Server: 010.0 User:	21.135.086 ADMIN (Adminis	trator)		Normal <mark>QRefresh@Logout</mark> English
System Serve	er Health Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
 Server Health Sensor Readings 	Server Health	ta related to the server	's health, such as ser	sor readings and the e	vent log.	
Event Log	 Senar Readings (See The event by See The eve	e the readings from the var	ious sensors g			

- 1. Click <Sensor Readings> to access information on sensor readings as shown on the next page.
- 2. Click <Event Log> to access event logs.

2.5.1 Sensor Readings

This page displays sensor readings for the remote console.



- 1. From the pull-down menu, select a sensor type (category). The options include the following.
 - All Sensors
 - Temperature Sensors
 - Voltage Sensors
 - Fan Sensors
 - Physical Secrity
 - Power Supply
 - OEM Reserved:

- 2. A senor color that is displayed in front of an sensor indicates the status of the sensor.
 - Green: It indicates that the sensor reading is normal. The system functions normally.
 - Amber: There is an alert on the sensor reading. Attention is needed to ensure that the system is functioning properly.
 - Red: One or more sensors have reached the critical state. Immediate action is needed to resolve the problem.
- Name of the Sensor: This column displays the names of the sensors that are currently active in system monitoring, including system temperature, CPU temperature, fan speeds, CPU core voltages, +3.3Vcc, and +12V voltage monitoring.
- 4. Status: This column indicates the status of each sensor reading.
- 5. Reading: This column indicates the reading of each sensor.
- 6. Refresh: Click this item to refresh the page.
- 7. Show Thresholds: Click this item to display senor thresholds.

2.5.2 Event Log

This page displays a record of critical system monitoring events. The event log indicates the time when a critical condition had occurred and when this condition was resolved. You can choose a specific event category from the pull-down menu to display events included in this category.

FUJITSU	_		User:	ADMIN (Adminis	trator)		Winning Neitesing Colout Lingisi
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Server H	ealth 🔵 E	Event Log					
Sensor R	eadings						
D Event Lo	,	Below is a table of the ev	ants from the system's er	vent log. You can choose a	category from the pull-dov	wn box to	
			sort show by choose g and				
	s	select an event log categor	ć				
		Sensor-Specific Events	~				Event Log:0 event entri
		Clear Event Lon					

- 1. Event Category: From the pull-down menu, select an event category to display.
 - Sensor-Specific Events: These event logs are generated by the BMC if the sensor's reading reaches the threshold.
 - BIOS-Generated Events: These event logs are generated by the BIOS and logged to the BMC.
 - System Management Software Events: These events logs are generated by the OS, application software, etc., and logged to the BMC.
 - All Events: This category includes all the above event logs.

In addition to the events listed on the previous page, it is normal to see boot-up and shutdown events generated by the installed system software (OS). The table below lists examples of these types of events.

Sensor Type	Event
OS Boot	A: boot completed
	C: boot completed
	PXE boot completed
	Diagnostic boot completed
	CD-ROM boot completed
	ROM boot completed
	Boot completed - boot device not specified
OS Stop/Shut-	Stop during OS load/initialization, Unexpected error during
down	system startup, Stopped waiting for input or power cycle/
	reset
	Run-time stop (a.k.a 'core dump', 'blue screen')
	OS graceful stop (system powered up, but normal OS opera-
	tion has shut down and system is awaiting reset pushbutton,
	power cycle or other external input)

2.6 Configuration

This feature allows the user to configure various network settings. When you click the *Configuration* icon on the menu bar, the following screen will display.

าปุ๊กรบ			Host Identification Server: 010. User:	n 021.135.086 ADMIN (Adminis	trator)		NormalQRefreshQLogout English
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
 Configuration Alerts 	⊜ c	onfiguration	nure various settings, s	uch as alerts, users, o	network etc.		
Date and Time		 Alerts : Add, edit or Date and Time : Conr 	remove alert destinations figure Date and Time Setting	18			
 Active Directory 		LDAP : Check the bo Active Directory : Co	x below to enable LDAP au infigure settings to authenti	theritication and enter the r cate and access the Active	equired information to acc a Directory server	eas the LDAP server. Press	the Save button to save your changes.
RADIUS		 RADIUS : Configure : Nouse mode : Config Network : See the M 	settings to authenticate and pure the mouse mode for re AC address or charge orth	access the RADIUS serve mote console work settions, including dur	r. namic and static IP assistor	and a	
Network		Dynamic DNS : Conf Remote Session : Co	igure dynamic update prope infigure Remote session se	nties for Dynamic DNS tings for virtual media			
Dynamic DNS		 SMTP : Configure the SSL Certificate : The organization of the Updated but 	e SMTP email server dates for the default certif	icate and private key are sl	town below. To upload a r	rew SSL certificate, use the	Browse button to navigate to the certificate and
SMTP		Users : Add, edit, or Port : Configure the p	remove users port number of the services				
SSL Certification		P Access Control :) Fan Mode : Configur	Add, edit or remove IP acce e the fan mode	ss rules			
Users Port							
IP Access Control	Ic						
Fan Mode							

This section allows the user to configure the following settings.

- Alerts: Use this item to configure alert destination settings.
- Date & Time
- LDAP: Use this item to configure LDAP (Lightweight Directory Access Protocol) settings for authentication and access to the LDAP server.
- Active Directory: Use this item to configure the settings for authentication and access to the Active Directory server.
- RADIUS: Use this item to configure the settings for authentication and access to the Radius server.
- Mouse mode
- Network
- Dynamic DNS
- Remote Session
- SMTP
- SSL Certificate

- Users
- Port
- IP Access Control
- Fan Mode

2.6.1 Configuring the Alerts Settings

This feature allows the user to configure *Alert* settings. When you click the <Alerts> icon in the menu bar, the following screen will display.

lem Serve	r Health Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Configuration	List of Alerts					
Alerts						
Date and Time	Below is a list of the co configure it, or Send Te	infigured alert destinations. You ist Alert to send a test alert to the	can select an alert and pres	is the Modify button to		
LDAP						
A stars Discussion						Alert Table:
Active Directory	Alert No. :	۵	lert Level :		Destination Ad	ktress :
RADIUS	1	1	Disable All		000.000.000.000	8 NULL
	2		Disable All		000.000.000.000	8 NULL
Mouse Mode	3)	Disable All		000.000.000.000	& NULL
	4		Disable All		000.000.000.000	8 NULL
Network	5	1	Disable All		000.000.000.000	8 NULL
0	6	1	Disable All		000.000.000.000	8 NULL
Dynamic DNS	7	1	Disable All		000.000.000.000	& NULL
Remote Session	8		Disable All		000.000.000.000	8 NULL
	9	1	Disable All		000.000.000.000	& NULL
SMTP	10	1	Disable All		000.000.000.000	8 NULL
SSL Certification	Modify Send	Test Alert Delete				
) Users	A A	▲ ▲				
Port						
P Access Control						

To setup an alert or to modify an alert setting, do the following.

- 1. Click <Alerts> to activate the alert submenu.
- 2. Click <Modify> to configure or modify the settings of an alert.
- 3. Send Test Alert is used to check if the alerts have been set and sent out correctly.
- 4. Click <Delete> to delete an alert.

To Setup an Alert

System Serv	er Health Configurati	on Remote Contro	Virtual Media	Maintenance	Miscellaneous	
Configuration	S Modify Alert					
Alerts						
Date and Time	Enter the inform	don for the alert below and pro	as Save.			
C LDAP						
Active Directory	Event Severity:	Nisable All				
RADIUS	Destination IP: 0	00.000.000.000				
Mouse Mode	Subject:	ULL				
Network	Message:	ULL				
Dynamic DNS	Save Can	el				
Remote Session	•					
SMTP						
SSL Certification						
S Users						
Port						
IP Access Control						
Can Hodo	-					

Follow the steps below to setup an alert.

- 1. Select *Alerts* from the window on the left.
- 2. Select Alert Severity.

3. Enter the SNMP Trap receiver IP address to use SNMP. For further guidance on typical inquiries relating to SNMP, see the table below.

ltem	Answer
SNMP version number	SNMP version 2.
The IPMI item you need to con- figure so the SNMP manager can receive the SNMP trap	The alert LAN destination address (see #3 under 2.6.1) must be set to the same IP in as the SNMP manager.
Can I query for detailed informa- tion on the MIB "Event" trap items?	Detailed queries are not possible because event mapping is based only on sensor type, event type, and sensor offset.
A list of trap items generated for my platform	No standard list of event traps exist because the PEF (Platform Event Filter) table is OEM customizable.

4. Enter the email address to send the alert to, then configure the SMTP settings (see section 2.6.10)

- 5. Enter the subject line of the alert.
- 6. Enter a message for the alert.
- 7. Click <Save> to save the settings.

2.6.2 Configuring Date and Time Settings

This feature allows the user to configure the time and date settings for the host server and the client computer. When you click the <Time and Date> icon in the Options window, the following screen will display.

FUJITSU			-Host Identification Server: 010.1 User:	1 121.135.086 ADMIN (Administr	ator)		Normat <mark>QRefresh@Logout</mark> English
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Configuration	•	Date & Time					
Alerts							
Date and Time		Here you can view and	modify the device's date and	time			
DIDAP							
Active Directory	-	Time Zone:	UTC+00:00				
C RADIUS		NTP Enable	O NTP Enabl	e 💿 NTP Disable			
Mouse Mode	-	Primary NTP Server:	localhost				
Network		Secondary NTP Server.	127.0.0.1				
Dynamic DNS	-	Date:	November N	12 • 2012 •]		
Remote Session		Time: (hh:mm:ss)	17 :	19 : 00			
SMTP		Daylight Saving Tim	e				
SSL Certification		Refresh	re				
Users							
Port							
IP Access Contr	ol						
Fan Mode							

The user can either set the date & time setting manually or use the *NTP Server* setting to set date & time. Follow the instructions below to set Date/Time settings.

- Note: Time zone is enabled when NTP is selected. The options are UTC -12:00 hr. ~ +12:00 hr.
- 1. Click *Date/Time* on the left to set the date/time settings.
- 2. Select the time zone.
- 3. Check this item for NTP settings.
- 4. Enter the IP address for the primary NTP server.
- 5. Enter the IP address for the secondary NTP server.
- 6. Enter the date.
- 7. Enter the time in hh/mm/ss format.

Click *Refresh* to change the date/time settings.

Click Save to save the entries.

2.6.3 Configuring Light-Weight Directory Access Protocol (LDAP) Settings

This feature allows the user to configure the *Light-Weight Directory Access Protocol* (LDAP) settings. When you click <LDAP> in the Options window, the following screen will display.

FUĴÎTSU			Host Identification Server: 010.0 User:	n 021.135.086 ADMIN (Adminis	trator)		Ø Normal Refresh Logout Eng
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Configuratio	a 🔁 L	DAP Settings					
Alerts							
Date and Tir	ne	Check the box below to Press the Save button t	enable LDAP authentication o save your changes.	and enter the required inf	ormation to access the LDA	P server.	
C LDAP							
Active Direc	tory						
RADIUS		Enable LDAP Authe	ntication 1 over SSI				
S Mouse Mod		Port	0				
Network		P Address	000.000.00	0.000			
Dynamic DN	s	and Password					
Remote Ses	sion	Bearchbase					
SMTP							
SSL Certific	ation	Save					
S Users							
Port							
IP Access C	ontrol						
Fan Mode							

Follow the steps below to configure the LDAP settings.

- 1. Check the enable box to enable LDAP Authentication and LDAP Authentication over SSL support.
- 2. Enter a port number for the LDAP server.
- 3. Enter an IP Address for the LDAP server.
- 4. Enter a Bind Password for the LDAP server.
- 5. Enter a Bind DN value in the field. (The bind DN is the user or the LDAP server that is permitted to do search in the LDAP directory within a defined search base.)
- 6. Enter a SearchBase value in the field. (The SearchBase is the directory that allows the external user to search data.)
- 7. After entering the information in the fields, click <Save> to save the information you've entered.

2.6.4 Active Directory Settings

This page displays a list of role groups and their Group IDs, Group Names, Domains and Network Privilege settings. When you click the <Active Directory> icon in the Options window, the following screen will display.

ມງິກຽບ			Host Identification Server: 010.021.135 User: ADMIN	.086 (Administrator)	Sormal Refresh Logout English
ystem	Server Health	Configuration	Remote Control	Virtual Media Maintenance	Miscellaneous
Configuration		Active Directory S	Settings		
Alerts		To enable or configure the	e Active Directory server, ple	ase click here	
Date and Time					
D LDAP		The list below shows the select the name in the list	e current list of configured Role at and press Delete Role Group	e Groups. If you would like to delete or modify a or Modify Role Group. To add a new Role Grou	role group, p. select an
Active Directory		unconfigured slot and p	ress Add Role Group.		
S RADIUS					Number of configured role groups: 0
Mouse Mode		Role Group ID ©	Group Name	Group Domain ©	Network Privilege :
		1	~	~	Reserved
Network		2	12	~	Reserved
		3	100	~	Reserved
Dynamic DNS		4	~	~	Reserved
Remote Session		ь	10	~	Reserved
SMTP					
SSL Certification					
🕤 Users					
Port		Add Hole Group	Moany Role Group	Lielete Köle Group	
IP Access Contro	н	T	Ī	T	
Fan Mode					

- 1. Click <HERE> to enable or configure the Active Directory server. See the next page for enabling or configuring Active Directory instructions.
- 2. Select a group and click <Add> to add a role group.
- 3. Select a group and click <Modify> to modify a role group.
- 4. Select a group and click <Delete> to delete a role group.

Configuring the Active Directory Settings

This feature allows the user to configure the *Advanced Active Directory* settings. When you click <Here> on the screen shown on the previous page, the following screen will display.

System Server H Configuration Configuration Alerts Date and Time LDAP Active Directory RADIUS	Configuration Remo Configuration Remo Check the box below to enable Acts Active Directory enable Acts Active Directory contents the S Gradie Acts Directory ActiveDirectory activeDir	te Control Virtue ed Settings • Directory suthentication ave button to save your ch	al Media and enter the requi	Maintenance	Miscellaneous	
Configuration Alerts Date and Time LDAP Active Directory RADIUS	Active Directory - Advanc Check the box below to enable Active Active Directory server. Press the S Enable Active Directory Authentit Active Directory Authentities	ed Settings	and enter the requi	ired information to acce	ss the	
Alerts Date and Time LDAP Active Directory RADIUS	Check the box below to enable Active Active Directory server. Press the S	e Directory authentication ave button to save your ch ation	and enter the requi anges.	ired information to acce	ss the	
 Date and Time LDAP Active Directory RADIUS 	Check the box below to enable Activ Active Directory server. Press the S	e Directory authentication ave button to save your ch	and enter the requi	ired information to acce	ss the	
LDAP Active Directory RADIUS	Enable Active Directory Authentic	ation				
 Active Directory RADIUS 	Enable Active Directory Authentic	ation				
RADIUS	Active Directory Author/Section or					
	Active Directory Addrenic address	ver SSL				
S Mouse Mode	Port User Domain Name	389				
S Network	Time Out	0				
Dynamic DNS	Domain Controller Server Address1	0.0.0.0				
Remote Session	Domain Controller Server Address2	0.0.0.0				
SMTP	Domain Controller Server Address3	0.0.0.0				
SSL Certification	Save Cancel					
S Users						
Port						
IP Access Control						
Fan Mode						

- 1. Check the <Enable> box to enable *Active Directory* authentication support. Then, Enter the values in the fields below.
- 2. Enter User Domain Name in the field.
- 3. Enter Time Out value in the field to set the time limit for a user to stay logging-in.
- 4. Enter <Controller Server Address1>.
- 5. Enter <Controller Server Address2>.
- 6. Enter <Controller Server Address3>.

After entering the information, click <Save> to save the settings.

2.6.5 Configuring the RADIUS Settings

This feature allows the user to configure *Radius Option* settings. When you click <RADIUS>in the Options Window, the following screen will display.

FUĴÎTSU	_		Server: 010.021 User: AD	135.086 MIN (Administrator	Σ	🥥 No	rmat <mark>@Refresh@Logout</mark> English
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Configuration	٢	RADIUS Setting	gs				
Alerts							
Date and Time		Check the box below the Save button to s	w to enable RADIUS and enter save your changes.	the required information to a	ccess the RADIUS server.	Press	
D LDAP							
Active Directo	*	Enable RADIUS					
PRADIUS		Port	0				
Mouse Mode		IP Address	0.0.0.0				
Network		Secret					
Dynamic DNS		Save					
Remote Sessi	m						
SMTP							
SSL Certificati	on						
Users							
Port							
IP Access Con	trol						
Fan Mode							

- 1. Check the <Enable> box to enable *Radius* support. Enter the information in the fields below to configure *Radius* settings.
- 2. Enter the port number for the Radius server.
- 3. Enter the IP address of the Radius server.
- 4. Enter a (secret) password for the user to access the Radius server

After entering the information in the fields, click <Save> to save the information you've entered.

2.6.6 Configuring the Mouse Mode Settings

This feature allows the user to configure the *Mouse Mode* settings. When you click the <Mouse Mode> icon in the Options Window, the following screen will display.

	_		User: ADM	IN (Administrator)		
System Si	erver Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Configuration	N	louse Mode Sett	ing				
Alerts							
Date and Time		Select the mouse mode	o use from the options belo	w and press the Save but	an.		
S LOAP							
Active Directory		Current Mouse Mode	IS ABSOLUTE.				
S RADIUS		Set Mode to Absolute	(Windows, Ubuntu, RH6	x later)			
Di Mouse Mode		Set Mode to Relative I Single Mouse Mode	Rest of the Linux)				
Network	_	Saua					
Dynamic DNS	_	Jure					
Remote Session							
SMTP							
SSL Certification							
S Users							
Dert O							
IP Access Control							
Ean Mode							

- 1. This item displays the current Mouse Mode setting. To select a proper Mouse Mode setting, click the proper radio button as shown below.
 - Check the radio button to set the mouse mode to *Absolute Mode* for the Windows OS. (This is the default setting.)
 - Check the radio button to set the mouse mode to *Relative Mode* for the Linux/ Unix OS.
 - Single Mouse Mode: Check this radio button to use single mouse mode.
 - After entering the information, click "Save" to save the settings.



2.6.7 Configuring Network Settings

This feature allows you to configure the network settings. When you click the <Network> icon in the Options Window, the following screen will display.

Γ	FUJITSU			Host Id Ser	entification ver: 010.021 ier: ADI	135.086 JIN (Administrato	r)		🔘 Norr	nal <mark>ØRefresh@Logout</mark> Englis	h 🔽
	System	Server Health	Configuratio	on Rem	ote Control	Virtual Media	Maintenance	Miscella	neous		
	Configuration		Network Sett	ings							^
	Alerts										
	Date and Time		You can view an or manually conf	id modify the netw igure one.	ork settings on	this page. Select whether	to obtain an IP address aut	omatically			
	C LDAP										
	Active Director		MAC Address	00-25-90-21-3	I1-fc						
\sim	E RADIUS		Hostname								
	Mouse Mode		O Obtain an IP a	ddress automat	cally (use DH	CP)					
പ	A Network		 Use the follow 	ing IP address							
ভা	1.	-	IPv4 Setting	010 001 10]					
	Dynamic DNS		IP Address	010.021.13	5.086						
	Remote Session	n	Subnet Mask	255.255.255	5.000						
	SMTP		Gateway	010.021.13	5.001						
~	SSL Certificatio	n	DNS Server IP	000.000.000	0.000						
(3)-	Users		IPv6 Setting								
\sim			IPv6 Address								
	D Port		● Add IP ● I	Delete IP 🗹 Au	no Configurat	ion					
	IP Access Cont	rol	OHCPv6 Stat	eless O DHC	Pv6 Stateful						
	E Fan Mode		Address List								
			IPv6 Address L	ist -	(*					
			DNS Server IP								
			DUED	and sectors.							
\sim			DOID	no value							
(4)			VLAN	O enable (disable						
				VLAN ID 0							
(5)			Lan Interface	Failover 🛩							
6			RMCP Port	623	1						
\sim			- Naturade Link	Status							
			Active Interface	Dedicated							
			Dedicated								
			Status :	Connected							
			Speed :	100M							
			Duplex:	Full Duplex							
			Share								
			Status :	Connected							
			Speed :	1G							
			Duplex:	Full Duplex							
			Fano								

To configure *Network* settings, follow the instructions below.

- Enter the MAC address for the network server. You can also check the first radio button to obtain an IP address automatically by using DHCP (Dynamic Host Configuration Protocol) or check the second radio button to setup the IP address by manually entering the information in the fields below. (Note: DHCP is the default setting.)
- 2. To set the IP address using the IPv4 format, enter proper information in the following fields.
 - IP address

- Subnet Mask
- (Default) Gateway
- DNS Server IP
- 3. To set the IP address using the IPv6 format, enter an IPv6 Address in the field. Enter a DNS Server IP and DUID (unit ID) in the boxes below.
- 4. Check this box to enable Virtual LAN support, and enter the VLAN ID in the field.

5. LAN Interface

This feature allows the user to select the port to be used for IPMI out-of-band communication.

- The default setting is Failover, which will allow IPMI to be connected from either the shared LAN port (LAN1/0) or the dedicated IPMI LAN port. Precedence is given to the Dedicated LAN port over the shared LAN port.
- Select <Dedicated LAN> for IPMI to connect through the IPMI Dedicated LAN port at all time.
- Select *Shared LAN* for IPMI to connect through the LAN port on the board.

6. <u>RMCP Port</u>

This feature allows the user to select the desired RMCP (Remote Mail Checking Protocol) port based on his configuration. The default port is 623.

After entering all fields above, click <Save> to save the Network settings.

2.6.8 Configuring Dynamic DNS (Domain Name System) Settings

This feature allows you to configure DNS settings. When you click the Dynamic DNS icon in the Options Window, the following screen will display.

FUJIISU		Server: 010.021.135 User: ADMIN	.086 (Administrator)		Wormal Refrest Logout English
System Server	Health Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
Configuration Active Directory Active D	Configure Dyr Configure Oyam O Dynamic Upda O Dynamic Upda Dynamic DHS Ser BMC Histham E soable TSIG A TSIG kay File (*) TSIG, prode File (*) Sere	emic DNS upde properties. (* - spiton e Enable © Dynamic Upd te Enable © Dynamic Upd thenitication	al fest(s)) alte Disable 一〇一〇一〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇		

- 1. Click the <Enable> radio button to enable Dynamic DNS update support. Click Disable to disable Dynamic DNS update support. (**Default**: Disable)
- 2. Enter the IP address of your Dynamic DNS (Domain Name System) server.
- 3. Enter the name of the BMC (Baseboard Management Controller) Host Server.
- 4. Check the box to enable TSIG Authentication support, and browse the files to select the *TSIG.key* file. (This item is optional.)
- 5. Browse the files to select the *TSIG.private* file. (This item is optional.)

After entering the required information in the fields, click <Save> to save the information you have entered.

2.6.9 Configuring the Remote Session Settings

This feature allows the user to enable or disable encryption support on IKVM, or to select the Virtual Media Attach mode for console redirection. When you click the Remote Session in the menu bar, the following screen displays.



- This item displays the current Virtual Media Attached mode. To change the Virtual Media Attached mode, select the desired setting from the list below.
 - Auto Attach (Default): Select this mode to automatically enable virtual media support and make it available for remote access. Virtual devices will only be shown in the operating systems and the BIOS when a device or an ISO image is connected through the virtual media wizard.
 - Attach: Select this mode to activate a virtual media and make it available for remote access. A virtual device will always be seen in the system BIOS even when it is not active.
 - Detach: Select this mode to disable virtual media for remote access.

After making selection, click <Save> to save the settings.
2.6.10 Configuring the SMTP Settings

This feature allows the user to configure SMTP (Simple Mail Transfer Protocol) settings for email transmission through the network. When you click the <SMTP> icon in the Options window, the following screen will display.

FUĴĨTSU		Hos	Viser: ADMIN	6 (Administrator)]	Normal Refresh Logout English
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
 Configuration Alerts Date and Time 	SMT	P Setting	the SMTP Mail server below	and press the Save buttor	s.	
 LDAP Active Directory 	► SMTP	SSL Auth:				
RADIUS	SMTP	port Number: 0				
Network	SMTP	Password:	Ĺ			
 Dynamic DNS Remote Session 	Sav	e				
SMTP						
Dusers						
 Port IP Access Control 	k					
Fan Mode						

To configure SMTP settings, follow the instructions below.

1. Check the box to enable SMTP SSL Authentication support. Once SMTP SSL Authentication is enabled, enter information in the fields below.



Note: SHA2 and RSA 2048 bit SSL supported.

- Enter the IP address for the SMTP (Simple Mail Transfer Protocol) Mail server. The SMTP port number will be displayed.
- 3. Enter the user name for your SMTP Mail server. (Optional)
- 4. Enter the user password for your SMTP Mail server. (Optional) The status of the sender's address will be displayed.

After entering the information above, click <Save> to save the settings.

2.6.11 Configuring the SSL (Secure Sockets Layer) Certification

This feature displays the default certificate and private keys. It also allows the user to upload a new SSL certificate. When you click the <SSL> icon in the Options window, the following screen will display.

FUĴĨTSU	_	S	ierver: 010.021.135.08 User: ADMIN	6 (Administrator)		Normal Refresh Logout Englis
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
Configuration	a S	SL Upload				
Alerts						
Date and Time		The dates for the default of Browse button to navigate	certificate and private key a to the certificate and pre-	are shown below. To uplo as the Upload button.	ad a new SSL certificate,	use the
C LDAP						
Active Directory	0					
S RADIUS		Certification Valid From Certification Valid Until	2012年4月1. 2014年4月1.	28 11:19:39 28 11:19:39		
Mouse Mode		New SSL Certificate		参照		
S Network		New Private Key	-	●城.		
Dynamic DNS		Unload				
Remote Session		opioad				
SMTP						
SSL Certificatio	n					
S Users						
Port						
IP Access Cont	rol					
S Fan Mode						

1. To enter a new SSL Certificate, enter a new certificate in the field. You can also browse the data base to select a new certificate.



Note: SHA2 and RSA 2048 bit SSL supported.

- 2. Enter a new Private Key in the field, if desired. You can also browse the data base to select a new key.
- 3. After entering the new SSL certificate or/and a new private key, press <Upload> to upload the certificate and private key to the server.

2.6.12 Configuring Users Settings

This page displays information on the current users. It also allows you to add, delete or modify user information. When you click the <Users> icon in the Options window, the following screen will display.

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous					
Configuration	a u	Jser List									
Alerts											
Date and Time		The list below shows the current list of configured users. If you would like to delete or modify a user, select their name in the list and press Delete User or Modify User. To add a new user, select an unconfigured slot and press									
DLDAP		Add User.									
Active Directory						Numbe	of configured users: 10				
RADIUS		User ID ÷		User Name ÷	Net	twork Privilege :					
		1		Anonymous	R	eserved					
Mouse Mode		2		ADMIN	Ad	iministrator					
		3		~	R	eserved					
Network		4		10	R	eserved					
O Description		5		~	R	eserved					
Dynamic Dws		6		~	R	eserved					
Remote Session		7		~	R	eserved					
		8		~	R	eserved					
SMTP		9		~	R	eserved					
SSL Certification		10		~	К	eserved					
Users	-	Add User Mor	fify User Delete	User							
Dort O		Ī	T í	T							
IP Access Contro	ol										

1. This item lists current user information, including User ID, User name and Network Privilege settings. Network privilege settings are shown below.

Function	User	Operator	Administrator
System Information	Full Access	Full Access	Full Access
Chassis Locator Control	View Only	Full Access	Full Access
FRU Reading	Full Access	Full Access	Full Access
Sensor Readings	Full Access	Full Access	Full Access
Event Log	View Only	Full Access	Full Access
Alert	No	View Only	Full Access
LDAP	No	View Only	Full Access
Mouse Mode	No	Full Access	Full Access
Network	No	View Only	Full Access
Remote Session	No	View Only	Full Access
SMTP	No	View Only	Full Access
SSL	No	View Only	Full Access
Users	No	View Only	Full Access
Event Action	No	View Only	Full Access
Power Control	View Only	Full Access	Full Access
KVM	View Only	Full Access	Full Access
F/W Update	View Only	View Only	Full Access
SDR Update	View Only	View Only	Full Access
Logout	Full Access	Full Access	Full Access

- 2. This item displays the number of the users that are set up for the network. The maximum of 10 user profiles can be made.
- 3. To add a new user to the network, click <Add User>. When prompted, select an empty slot from the users list to add an user.
- To modify the information or the status of a user, click <Modify User>. When prompted, using the arrow keys, select a user from the users list to modify the user information.
- 5. To delete a user from the network, click <Delete User>. When prompted, using the arrow keys, select a user from the users list to delete it from the list.

2.6.13 Configuring Port Settings

This page allows you to configure port settings. When you click the <Port> icon in the Options window, the following screen will display.

FUĴĨTSU		Host Identification Server: 010.021.135.0 User: ADMIN)86 (Administrator)]	Normal <u>Refresh Logout</u> English
System	Server Health Configu	ration Remote Control	Virtual Media	Maintenance	Miscellaneous
System Configuration Configuration Alerts Date and Time LDAP LDAP LDAP LDAP LDAP LDAP LDAP LDAP	Server Health Configur Port Settin Nere you ca Web SRL port HVML server po VML and server po Save	Remote Control g a contigure the port number 80 443 5500 cont 623	Virtusi Media	Meintenance	Miscellanous
 Users Port IP Access Control Fan Mode 	1 1				

- 1. Web Port: Enter the desired web port number.
- 2. Web SSL Port: Enter the Web SSL port number.
- 3. IKVM Port: Enter the desired IKVM port number.
- 4. Virtual Media Port: Enter the desired virtual media port number.

After configuring the port settings, click <Save> to save the settings.

2.6.14 IP Access Control

This page displays an IP Access Control table, which will allow you to add, modify and delete an IP Access rule, an IP Address/Mask setting or an IP access policy.



- Check this box to configure IP Access Control settings. (The default setting is Accept.)
- 2. Rule Number: This column lists the number of IP Access Control rules.
- 3. IP Address/Mask: This column displays IP Address/Mask settings.
- 4. Policy: This column displays the status of an IP Access policy.

5. Number of Access Rules: This displays the maximum number of IP Access rules you can set for the system.

บ)๊ทรบ			Server: 010.021.135.08 User: ADMIN	(Administrator)		Normal Refresh U.o.	gout English
system	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Configuration	⊜ A	dd Rule					
Alerts							
Date and Time		Enter the information for	the access rule below and	press save button.			
⇒ LDAP							
Active Directory	R	ule No 1					
S RADIUS	P	olicy ACCE	PT M				
Mouse Mode		Save Cancor	PT				
Network							
Dynamic DNS							
Remote Session							
SMTP							
SSL Certification							
Users							
Port							
IP Access Control	k						
E Fan Mode							

Modifying IP Access Rules

When you select an item and click <Modify>, the Add Rule submenu will display as shown below.

To modify a rule, enter the information needed for the following items:

- IP Address/Mask: This item allows you to grant access to a specific IP address or a range of IP addresses. For example, if you wanted to specify a range of IP addresses from 192.168.0.1 to 192.168.0.126, you would enter 192.168.0.1/25.
- Policy: Select Accept to allow access for the IP address(es) entered above. Select Drop to deny access.

2.6.15 Configuring Fan Settings

This page allows you to configure fan mode settings. When you click the <Fan Mode> icon in the Options window, the following screen will display.



- 1. This item displays the current fan mode setting.
- 2. Check this radio button to use the standard fan speed setting for power-saving.
- 3. Check this button to use the full speed setting for optimal system performance.
- 4. Check this button to use the optimal fan speed setting which will adjust the fan speed by balancing the needs between system performance and power saving.

After configuring the fan speed setting, click <Save> to save the entry.

2.7 Remote Control

This section allows the user to carry out activities and perform operations on a remote server via remote access.



To launch remote console or to change to power settings of the remote console, follow the instructions below.

- Click "(Launch) Console Redirection" to launch Console Redirection and configure the settings of the remote server. For more details on Console Redirection, please refer to "Launching Console Redirection" on the next page.
- 2. Click "Power Control" to display and configure the power settings of the remote console, including the following settings.
 - Reset Server
 - Power Off Server-Immediately
 - Power Off Server-Orderly Shutdown
 - Power On Server
 - Power Cycle Server

Once you have clicked the desired power setting, click "Perform Action" to change the power setting of the server.

3. Click "Launch SOL" to launch SOL (Serial Over LAN) console and manage the remote server.

2.7.1 Launching Console Redirection

This feature allows you to launch Console Redirection via IKVM (keyboard, video/monitor, mouse) support. When you click <(Launch) Console Redirection> in the Options window, the following screen will display.



- Click <Launch Console> on the Console Redirection screen to launch the remote console via Java or Active X (for the Internet Explorer). If it is blocked by the IE due to security reasons, click on the top of the menu bar and select <Download File>.
- 2. A screen will display to indicate that Java is launching.
- 3. When the warning screen as shown above displays, click <Run> to launch the remote console.

2.7.1.1 Console Redirection - Virtual Device

This feature allows you to configure Virtual Device settings for your console redirection. When you click the <Virtual Device> icon in the Menu bar, the video settings of the remote console will display as shown below.



- 1. Click <Virtual Media> to configure virtual device settings of a server at a remote site via Console Redirection.
- Click <Virtual Storage> to select a device you want to connect to the remote server as a virtual device. When you click on this item, the screen as shown below displays.

You can connect Floppy, USB Flash, CD-ROM, DVD ROM or ISO images using this feature.

🛃 Java iKVM Viewer v1.57 r8 [172.31.2.10] - Resolution 752 X 413 - FPS 0
Virtual Media Record Macro Options User List Capture Exit
Virtual Storage 1.2 r2
Settings for Device 1
Logical Drive Type Image File Name and Full Path No Select Open Image
Refresh Plug in Plug Out OK
Connection Status History

Virtual Keyboard

1. Click the <Virtual Keyboard> to use the onscreen Keyboard.

x c v b n m

z

2:

alt

Û

ctrl

2. The screen above shows the Virtual Keyboard in English. Click a key on the keyboard for your BMC connection.

e :	ers BVD Verse	u v1.57 (6	[172.31.2.1	0] - 11deo O	dy - Recolut	ia 1074 X J	91 - 115 X	,												E = 🔀
1	mar Markala – Brancha – Br	ard Macro	 Optione 	UnerList	Copure Da									Wine	Sows Se Edition	erver 2003				
English keyb esc F1 F2 F3 F							ar d F	5 F	6 F	7 F	8	F9	F10	F11 F12		psc	sll) (k	Dau	3
		1	2	3	4	5	б	7	8	9	0	-	=	+	ins	< 1	nlk	1	* -]
	H	Ħ	q	w	e	r	t	у	u	i	0	р]] /	del	∕ Ŧ	~	1	1 +	
			a	s	d	f	g	h	i	k	1	:	1	-			+		→ ·	

1

.

alt

Û

🏞 🗐 ctrl

1

 $\leftarrow \downarrow \rightarrow$

1

4

ins del

Ŧ

2.7.1.2. Console Redirection - Recording

This feature allows you to record media displays for your console redirection. When you click the Record icon in the Menu bar, Record settings will be shown below.



- 1. Click <Record> to use the recording features for your remote server. The features include the following.
- 2. Click <Start Recording> to start video recording from your remote server.
- 3. Click <Stop Recording> to stop video recording from your remote server.

2.7.1.3. Console Redirection - Recording

This feature allows you to record the media displays. Click <Record> in the Menu bar to enable virtual media recording support.

1	Virtual Mec	Macro Op	tions User List	Capture	Exit			
Ũ							5	
~			Save					
(2)			Save et al 3½ Flop Local D DVD-RM New Vo DVD Data (F: New Vo Data (F: New Vo Tech_W	My Com py (A:) sk (C:) M Drive (D lume (E:) lume (G:) hiter_Bac	puter ;;) kup on 'Super-twfs' (2;)			/ er 2003
			Files of Type	: Lavi			-	
3								
9						Save	Cancel	

- 1. Click <Record> to enable media recording support. Click <Start Recording> to start recording.
- 2. From the pull-down menu, select the location where you want to save the recording.
- 3. Enter the filename and click <Save> to save the recording.

2.7.1.4. Console Redirection - Macro

This feature allows you to configure Macro settings for your console redirection. When you click the <Macro> icon in the Menu bar, the macro settings screen will display as shown below.



Click <Macro> to configure the Macro settings for your remote server. The features include the following.

- Hold Right ALT Key: This item performs the same function as holding down the <Right Alt> key.
- Hold Left ALT Key: This item performs the same function as holding down the <Left Alt> key.
- Right Windows Key: This item performs the same function as you pressing the <Right Windows> key. Right click this item to select <Hold Down> or <Press & Release> for the Right Windows key.
- Left Windows Key: This item performs the same function as pressing the <Left Windows> key. Right click this item to select <Press Down> or <Press & Release> for the <Left Windows> key.
- **Macro:** Click this item to activate a pull-down submenu. The Macro Hotkey submenu includes the following items as shown on the next page.

Click <Macro Hotkeys> to display the Macro Hotkey pop-up submenu. The hot keys include the following:

Virtual Media Record Macro Options User List Capture Exit
🗆 Hold Right Alt Key
Hold Left Alt Key
Right Window Key ▶
Left Window Key 🕨
Macro > Ctri+Alt+Dei
Alt+Tab
Alt+Esc
Ctri+Esc
Alt+Space
Alt+Enter /indows
Alt+typhen e Merent
All+F4 Windows Server 2003
Alt+PrntScrn Clereprise Edition
PrnfScrn 033 Microsoft Corporation Microsoft
F1
Alt+E1 SC01-Alt-Delete to begin.
Pause key combination at startum helins keen yeur
computer secure. For more information, click Help. [Herb]
L1380

- CTRL + ALT + Del
- ALT + Tab
- ALT + Esc
- Ctrl + Esc
- ALT + Space
- ALT + Enter
- ALT + Hyphen
- ALT + F4
- ALT + Prnt Scrn
- Prnt Scrn
- F1
- Alt + F1
- Pause

2.7.1.5 Console Redirection - Options

This feature allows you to configure *Options* settings for your console redirection. When you click the <Options> icon in the Menu bar, the Options menu will display as shown below.



- 1. Click <Options> to activate the pull-down menu to configure Options settings.
- 2. The options menu allows you to configure the following settings.
 - Hotkey
 - Preference
 - Full-Screen Mode
 - OSD UI Style
 - Keyboard Mouse Hotplug

2.7.1.5.1 Console Redirection - Options: Hotkey Settings

This feature allows you to configure Hotkey settings for your console redirection. When you click the <Options-Hotkey> icon in the Menu bar, the Hotkey menu will display as shown below.

🚳 Java iKVM Viewer v1.57 r8 [1]	72.31.2.10] - Resolution 1024 X 768 - FPS 54
Virtual Media Record Macro	Options User List Capture Exit
	Hotkey Settings
	Preference Hotkey Settings
	Full-Screen Mode
	OSD UI Style
	Keyboard Mouse Hotplug
🙆 Hotkey Settings	
Hotkey Settings	
action	Hotkeys2
Adjust Mouse	F1
Exit Remote Location	F2
Full-Screen Mode	F3
Refresh screen	F4 E5
Toggle Mouse Display	F6
Toggle UI Display	F7
Korboard Monitor	
Reyboard Monitor	
Start Stop	Assign Close Default
1 3	(4) (5)

To assign a hotkey for an action, follow the steps below.

- 1. Click <Start>.
- 2. Enter the hotkey of your choice (-it can be a single word or a combination).
- 3. Click <Stop>.
- 4. Select an item from the action list and click <Assign>.
- 5. Click <Close> to exit.

2.7.1.5.2. Console Redirection - Options: Preference (-Display)

This feature allows you to configure Video Recording Preference settings for your console redirection. When you click the <Preference> icon in the Menu bar, the Preference menu will display as shown below.



To configure the preference settings for video recording, please follow the instructions below.

- 1. Click <Preference> to invoke the Preference submenu which includes Display, Input, Language Setting, Window and Video Stream Control settings.
- 2. Click <Display> to configure Video Display features.
- Check this box to enable Auto Stop support, which will allow the video recording to be automatically turned off after recording of certain period of time. After <Enable auto stop> is checked, enter the number of minutes upon which your video recording will be automatically turned-off.
- 4. Use the slider on the Display Scale to set the appropriate scale setting for your video display from Low (25) to High (100).
- 5. To ensure the best image quality, select <High Color> for heavier network traffic connections; select <Low Color> for lighter network traffic.
- 6. Click <OK> to save the recording preference settings or click <Cancel> to cancel the selection.

2.7.1.5.3. Console Redirection - Options: Preference (-Input)

This feature allows you to configure Video Recording input settings for your console redirection. Click <Input> in the menu bar to activate the Input submenu.



To configure Video Input settings, follow the instructions below.

- 1. Click <Preference> to invoke the Options submenu.
- 2. From the Options submenu, click <Input> to invoke the *Input* page to configure mouse and keyboard settings.
- Check <Enable Mouse Input> to enable mouse support so that you can use the mouse as an input device. Once mouse support is enabled, set a proper mode for your console redirection.
 - Select Absolute Mode if you have the Windows OS
 - Select *Relative Mouse* for the Linux OS.
- 4. Select *Enable Keyboard Input* to enable keyboard support so that you can use soft keyboard as an input device. From the *Keyboard layout* pull-down menu, select the right language setting for your soft keyboard.
- 5. Use the slider on the *Repeat Key Timeout* scale to select the appropriate timeout settings for repeat keystrokes from Oms to 1000ms (micro-second).
- 6. Click <Save> to save the keyboard setting or click <Cancel> to cancel it.

2.7.1.5.4. Console Redirection - Options: Preference (-Language Settings)

This feature allows you to configure Language settings for your console redirection. Click <Options> in the Menu bar to activate the Preference menu.

	Virtual Media	Record	Macro	Options User List Capture Exit	
				Hotkey Settings	
1				Preference	
~				Leave Full Screen Mode	
				OSD UI Style	
				Keyboard Mouse Hotplug	
				Welcome to Windows	
				Accest 1	
				Windows Server 2003	
				- J. Enterprise Edition	
				Copyright © 1985-2003 Microsoft Corporation Microsoft	
				Press Ctrl-Alt-Delete to be	
0				Options	
(2)				Requiring this key combination at start Display Inger Language Setting Window VI	
				Language Setting	
(3				Language Setting English 🔻	
<u> </u>					
G				OK Cancel	
4					

To select the correct language setting for your console, follow the steps below.

- 1. Select *Options* from the Menu bar. From the pull-down menu, select *Preference*.
- 2. Click <Language Setting>.
- From the Language Setting pop-up menu, select the language you want to use for your console redirection. The language options include English, Chinese (Traditional), Japanese, German, French, Spanish, Korean, and Italian.
- 4. Once you have selected a language setting, click <OK> to use the language.

2.7.1.5.5. Console Redirection - Options: Preference (-Window)

This feature allows you to configure Window settings for your console redirection. Click <Options> in the Menu bar to activate the Preference menu.



To select the correct Window settings for your console redirection, follow the instructions below.

- 1. Select Options from the Menu bar. From the pull-down menu, select Preference.
- 2. Click <Window>.
- Check <Auto Re-size Window> for the system to reset the size of your display window. (If you do not wish your display window to be re-sized automatically, leave the box blank.)
- 4. Click <OK> to save the window settings.

2.7.1.5.6. Console Redirection - Options: Preference (-Video Stream Control)

This feature allows you to configure Window settings for your console redirection. Click <Options> in the Menu bar to activate the Preference menu.



To select the correct Video Stream Control settings for your console redirection, follow the instructions below.

- 1. Select <Options> from the Menu bar. From the pull-down menu, select Preference.
- 2. Click <Video Stream Control>.
- Check <Enable Flow Control> to provide support for video flow control. Once the Flow Control support is enabled, select the proper speed for video streaming from the pull-down menu. The speed settings listed below.

🖌 Enat	ble Flow Control	
Speed	256K Cable/DSL 💌]
	256K Cable/DSL	1
	T1	
	T2	

- 256K Cable/DSL
- T1
- T2
- 4. Click <OK> to save the Video Stream Control setting.

2.7.1.5.7. Console Redirection - Options: Full Screen Mode

This feature allows you to configure Window settings for your console redirection. Click <Options> in the Menu bar to activate the submenu. From the pull-down menu, select *Full Screen Mode*.

🕌 Java iKVM Viewer v1.57 r8 [1	72.31.2.1	0] - Resolut	tion 102	24 X 768 - FP
Overlage North Nacro	Options	User List	Captur	e Exit
	Hotkey S	ettings		
	Preferen	се		
2	Full-Scre	en Mode		
	OSD UI S	tyle		
	Keyboard	l Mouse Hot	plug	

• To Use a Full Screen Display

To set a full screen display for your console redirection, follow the instructions below.

- 1. Select <Options> from the menu bar to activate the submenu.
- 2. Select <Full Screen Mode> from the pull-down menu. Then, press <Enter>. A fullscreen display will appear.



- To Leave the Full Screen Display
- 3. To leave the full screen display, click <Options> to activate its submenu.
- 4. From the pull-down submenu, select <Leave Full Screen> and press <Enter>.

2.7.1.5.8 Console Redirection - Options: OSD UI Style

This feature allows you to configure OSD (On-screen Display) UI (User-Interface) Style settings for your console redirection. To configure the OSD UI settings, follow the steps below.



- From the Options pull-down menu, click <OSD UI Style> to display the OSD UI Style screen as shown below. This screen provides shortcuts to the main features provided by the firmware for your console redirection.
- 2. Click an <OSD UI_Style> icon to change the settings listed on the next page.



The OSD UI Style Screen Close-up



- 1. Move OSD UI Screen: Click this icon to move the OSD UI Screen to a new location on the display.
- 2. Hotkey Settings: Click this icon to access the Hotkeys submenu and change the settings.
- 3. Virtual Media: Click this item to access the Virtual Media submenu and configure the settings.
- 4. Virtual Keyboard: Click this item to access the Virtual Keyboard submenu and use your virtual (soft) keyboard.
- 5. **Preferences submenu:** Click this item to access the References submenu as indicated in the previous sections.
- 6. **Full Screen Mode:** Click this item to change the size of your display window to the full screen mode.
- 7. Exit Remote Console: Click this item to exit from the remote connection.
- 8. Users List: Click this item to display the user list.
- 9. Change Toolbar Display: Click this item to change the toolbar display format.
- 10. Hotplug Keyboard/Mouse: Click this item to hotplug keyboard and mouse.
- 11. Macro: Click this item to enable Macro support and use Macro features.
- 12. Video Recording: Click this item to access the Video Recording submenu and to use video recording.
- 13. **Image Size:** This item displays the image size in pixel.
- 14. IP Address: This item displays the IP Address of IPMI.





- 1. Click <Options> on the menu bar to invoke the pull-down submenu.
- Click <Keyboard/Mouse Hotplug> from the pull-down menu to enable keyboard/ mouse hotplug support for your console redirection.

2.7.1.6 Console Redirection - User List

This feature allows you to access the user list. To configure User List settings, follow the instructions below.

🕌 Java iKVM 🛚	/iewer v1	.57 r8 [1	72.31.2.	10] - Video (Only - Res	olution 1024 >	(768 - FPS 30
1 Virtual Media	Record	Macro	Options	Þ User List	Capture	Exit	
_							
	酱 User I	List					
	User List	1					
		Session I	D	UserN	lame	IP Add	dress
			229380/	ADMIN	A	172.31.1.36	
		Ť	245762	ADMIN	— —	172.31.1.36	
	action						
							Close
						l	
		(2)		(3)	(4)

- 1. From the menu bar, click <User List> to display the User List screen as shown above.
- 2. Session ID: This item displays the current session ID#.
- 3. User Name: This item displays the name(s) of the user(s).
- 4. IP Address: This item displays the IP Address of the client server.

2.7.1.7 Console Redirection - Capture

This feature allows you to capture the screen displayed on your remote console.



- 1. Click "Capture" in the Menu bar. The Capture submenu will display as shown above
- 2. From the pull-down menu, select "Full Screen" video display for your remote console.

2.7.1.8 Console Redirection - Exit



1. To exit from Console Redirection, click <Exit>.



- 2. At the prompt- "Are you sure?", click <Yes> to exit from remote redirection.
- 3. Click <No> to return to the current session.

2.7.2 Remote Control - Server Power Control

This feature allows the user to check power state and perform remote power control.



- 1. Click <Reset Server> and press <Perform Action> to reset the host server.
- 2. Click <Power Off Server Immediately> and press <Perform Action> to power off the remote server immediately.
- Click <Power Off Server Orderly Shutdown> and press <Perform Action> to power off and shutdown the remote server orderly.
- 4. Click <Power On Server> and press <Perform Action> to power on the remote server.
- 5. Click <Power Cycle Server> and press <Perform Action> to reset the power cycle of the remote server.

2.7.3 Remote Control-Launch SOL

This feature allows you to launch the remote console by using SOL (Serial over LAN). This feature provides serial port connections over LAN to allow the user to access a host server via Console Redirection. It also allows a system administrator to monitor and manage a server from a remote site. To launch SOL, follow the instructions below.

	FUĴĨTSU		Hos	t Identification Server: 010.021.135.08 User: ADMIN	6 (Administrator)]	Normal <mark>@Refresh@Logout</mark> English M
	System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
]•- 2)•-	Remote Control Console Redre Console Redre Power Control Launch SOL		DL Console Press the buttor to laure Laurech SOL	ch the SOL console and mai	age the server remotely.		

- 1. Click <Launch SOL> in the left Options window to enable SOL (Serial Over LAN) support.
- 2. Click the <Launch SOL> button to launch SOL. After SOL is launched, the following screen will display as shown on the next page.



Launching SOL

- You can select a Baud Rate (bps) from the pull-down menu as your SOL transfer rate. The options are listed below. Make sure that the Baud Rate selected here matches the Baud Rate set in the BIOS.
 - 9600 bps (bit-per-second)
 - 19200 bps
 - 38400 bps
 - 57600 bps
 - 115200 bps
 - Manufacture Default.
- 2. Once you've selected the Baud rate, press <Start> to start the session.
- 3. You can also press <Stop> to stop SOL connection.

2.8 Virtual Media

This feature allows you to upload and share images via the BMC (Baseboard Management Controller). These images will be emulated to the host server as USB applications. To follow the Virtual Media settings, follow the instructions below.



- 1. Click <Virtual Media> to configure virtual media settings for your remote console, including Floppy Disk and CD-ROM image settings.
- Click <Floppy Disk> on the Options Window to configure the floppy disk settings for your console redirection. The Floppy Disk screen will display as shown on the next page.
- 3. Click <CD-ROM Image> to configure CD-ROM image settings for your console redirection. When you click on this item, the screen on Page 2-59 displays.

2.8.1 Configuring USB Floppy & Flash Device Settings

To configure CD ROM image files for sharing, follow the instructions below.



- 4. USB Floppy & Flash Status displays the status of a USB floppy or a flash device.
- 5. CDROM & ISO Status displays the status of a CDROM or an ISO device.
- 6. Click <Refresh Status> to refresh the USB floppy or the flash device.
- Click <Browse> to select an image file from your data base for your console redirection.
- 8. After you've selected your image file, click <Upload> to upload your image file to the server.

2.8.2 Configuring CD ROM Image File Settings

To configure CD ROM image files for sharing, follow the instructions below.

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
 Virtual Media Floppy Disk 		nage on Windows	s Share			
CD-ROM Ima	30	This option allows you to image will be emulated to	share a CD-ROM image ov the host as USB device.	er a Windows Share with	a maximum size of 4.7GB.	This
		ISB Floppy&Flash Status DROM&ISO Status	No disk emulation No disk emulation	n set. n set.		
		Refresh Status				
		ath to image				
		assword (optional)				
		Save Mount	Umount			

- 9. Click <CD-ROM Image File> to invoke the <Image on Windows Share> screen as shown above. The following items will display.
- USB Floppy & Flash Status indicates the status of a USB floppy or a flash device.
- CD ROM & ISO Status indicates the status of a CD-ROM or an ISO device.
- 10. Click <Refresh Status> to refresh USB Floppy/Flash and CD ROM/ISO devices.
- 11. Enter the *Share Host* server for your console redirection.
- 12. In the Path to Image field, enter the path to the CD-ROM image file for sharing.
- 13. In the *Users (Optional)* field, specify the users that have access to the CD-ROM image files. (This item is optional).
- 14. In the Password (Optional) field, enter your user password. (Optional.)
- 15. To *mount* an image file, follow the steps below.
 - 1. Click <Save>.
 - 2. Click <Mount>.

- 3. To *unmount* an image file, follow the steps below.
 - 1. Click <Unmount>.
 - 2. Click <Save>.

CDROM&ISO Status	There is a disk mounted.		
Refresh Status			
Share host	192.168.1.187		
Path to image	\av\cd.iso	share folder\image name	
User (optional)	user		
Password (optional)			
2.9 Maintenance

Use this feature to manage and configure IPMI device settings.

System Server Health Configuration Remote Control Virtual Media Maintenance Misscellaneous Maintenance Use these pages to maintain the IPMI device, such as update firmware or resef the IPMI device. Maintenance Use these pages to maintain the IPMI device, such as update firmware or resef the IPMI device. Maintenance Maintenance Maintenance Muscellaneous Muscellane	ะบุ๊มารบ	Hos	Server: 010.021.135.08 User: ADMIN	6 (Administrator)]	Normal Refresh Logout English
Image: System Event Log System Event Log	System Server	Health Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
	Maintenance Firmware Update Unit Reset Unit Reset Factory Default IPAII Configuration System Event Log	Maintenance Use these pages to maint Firmware Update : R Unit Rest: Restor II KrWA Rest: Restor Factory Default : Res PMI Configuration : 2 System Event Log : 7	tain the IPMI device, suc erform firmware update MII Device virtual media, IKVM keyboan et PMI to Factory defaults are or rebad IPMI configur ricu can turn onloff sysem i	th as update firmware of 1 & mouse settings. PMI connection w ation. wvent log on this page.	or reset the IPMI device il be reset.	e.

Click the <Maintenance> icon in the menu bar to invoke the *Maintenance* main screen as shown above. The *Maintenance* menu includes the following items.

- **Firmware Update:** Click this item to update the remote server's BMC firmware. The Firmware Update screen is shown in the next section.
- Unit Reset: Click this item to reboot the BMC (IPMI) controller.
- IKVM Reset: Click this item to reset the IKVM setting.
- Factory Default: Click this item to restore IPMI to the factory default settings.
- **IPMI Configuration**: Click this item to save IPMI configuration settings to a file or to load IPMI configuration settings from a file.

2.9.1 Maintenance - Firmware Update

	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
Maintenance		irmuara Lindata				
Eirmwara Hod	ato					
S linit Report		Press Enter Update Mo	ie to put the device in a spec	ial mode that allows firmw	are update.	
O HORE Reset		Please note that once y	ou enter update mode the de	vice will reset if the updat	e process is canceled.	
Castan Data						
Factory Defaul		Enter Update Mod	2			
Dipwi Conngura	luon					
System Event	Log					
	パージからのメッヤー	Ĩ				
Web						
Web	Are you sure to	enter update mode? You	will not be able to perform	any other tasks until fir	mware upgrade is comple	te and the device is rebooted.
Web	Are you sure to	enter update mode? You	will not be able to perform	any other tasks until fir キャンセル	mware upgrade is comple	te and the device is rebooted.
Web	Are you sure to	enter update mode? You	will not be able to perform	any other tasks until fir	mware uperade is comple	te and the device is rebooted.
	Are you sure to	enter update mode? You	will not be able to perform	any other tasks until fir	mware uperade is comple	te and the device is rebooted
Web 2	Are you sure to	enter update mode? You	will not be able to perform	any other tasks until fir	mware upgrade is comple	te and the device is rebooted

Firmware Update

To update IPMI Firmware, follow the instructions below.

- 1. Click <Firmware Update> in the Options Window.
- Click <Enter Update Mode> to enter the update mode. A warning message will display.



Warning: Once the server is in the firmware update mode, the device will be reset, and the server will reboot even if you cancel firmware updating.

- 3. Click <OK> to update your IPMI firmware. Once you've clicked OK to update the firmware, the *Firmware Upload* screen will display as shown on the next page.
- 4. Click <Cancel> to cancel firmware updates.

Once you have clicked <OK> to update the IPMI Firmware, the following Firmware Upload screen will display as shown below.



- 5. Enter the name of the firmware you wish to upload. You can also select a firmware from the pull-down menu to upload.
- 6. Click <Upload Firmware> to upload the selected firmware to the host server.



- **Warning!** To properly update your firmware, do not interrupt the process until the process is completed. Once it is completed, the system will automatically reboot, and you will need to login to the server again.
- 7. Click <Cancel> to abort firmware uploading.

2.9.2 Maintenance - Unit Reset

Use this feature to reset the IPMI device.

ะบุј๊กรบ		- Hos	Server: 010.021.135.00 User: ADMIN	86 (Administrator)		Normal <mark>QRefresh@L</mark>	ogout English
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Maintenan	ce 🌍 U	Init Reset					
🕤 Firmware L	Update						
😌 Unit Reset	1	Click on the reset button	to reboot the IPMI device.				
IKVM Rese	t						
Factory Del	fault	Reset					
IPMI Config	guration						
System Eve	ent Log						

2.9.3 Maintenance - IKVM Reset

This feature allows you to reset IKVM. It will reset virtual media, IKVM keyboard and mouse.

FUĴĨTSU		Hos	t Identification Server: 010.021.135.0 User: ADMIN	86 (Administrator)]	Normal Refrest	Logout English
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Maintenance	NI 🕒	VM Reset					
Firmware Up	date						
Unit Reset		Click on the reset button	to reset virtual media, IKVI	/ keyboard & mouse.			
🔵 IKVM Reset							
Factory Defa	ult	Reset					
IPMI Configure	ration						
System Even	nt Log						

To reset these devices, follow the instructions below.

- 1. Click the Maintenance icon in the menu bar, the Maintenance Main page will display as shown above.
- 2. Click "IKVM Reset" in the Options Window to enable Unit-Reset support
- 3. Press the "Reset" button to reset virtual media, keyboard and mouse devices.

2.9.4 Maintenance - Factory Default

This feature allows the user to restore IPMI to factory default settings.

FUĴĨTSU		Hos	t Identification Server: 010.021.135.08 User: ADMIN	6 (Administrator)]	Normal Refresh Logout Engl	ish 🛉
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	
Maintenance	:e 😑 Fi	actory Default					
Firmware U	Ipdate						
Unit Reset		Click on the restore butt	on to reset IPMI to Factory d	efaults settings. IPMI conne	ection will be reset.		
S IKVM Reset							
S Factory Def	fault	Restore					
IPMI Config	uration						
System Eve	ent Log						

- 1. Click the Maintenance icon in the menu bar, the Maintenance Main page will display as shown above.
- 2. Click "Factory Default" in the Options Window to enable default setting support
- 3. Press the "Restore" button to restore the IPMI settings to the factory default settings.

2.9.5 Maintenance - IPMI Configuration

This feature allows the user to save IPMI configuration settings. To save the IPMI configuration settings, follow the instructions below.



- 1. From the top menu bar, select *Maintenance*.
- 2. Select IPMI Configuration on the left of the screen.
- 3. Click Save to save the IPMI Configuration settings.
- 4. From the Reload pull-down menu, select an IPMI Configuration setting to reload.
- 5. Click *Reload* to reload the IPMI Configuration Setting.

2.10 Miscellaneous

This feature allows the user to perform various network activities including POST (Power-On-Self Test) code query and turning-on/-off UID control. To query POST codes or to turn on/off UID control, follow the instructions below.

FUJ๊ITSU		Hos	t Identification Server: 010.021.135.08 User: ADMIN	36 (Administrator)		⊗ Normal <mark>⊘Refresh@Logout</mark> English ▼
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
Miscellaneous Post Snooping UID Control	• M Us	iscellaneous e these pages to perfor • Pest Snooping : Oue • UD Control : You ca	irm various features, su	ich as query the post s	nsopling code.	

2.10.1 Miscellaneous - POST Snooping

- 1. Click <Post Snooping> in the Options window. The *Post Snooping* screen will display as shown above.
- 2. Click <Refresh> to query the POST Snooping code for BIOS LPC Port80.

	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
S Miscellaneo	B 😑 Pi	ost Snooping				
😔 Post Snoopin	g					
UID Control		This page displays curr	ent BIOS post code.			
	P	ost Snooping: 00				
		Refresh				

2.10.2 Miscellaneous - UID Control

This feature allows the user to turn-on or turn-off UID (Unit Identification) control. To turn on or off UID control, follow the instructions below.



- 1. Click <UID Control> in the *Options* window. The <UID Control> screen will display as shown above. It will also show the current UID Control status.
- 2. Click <Turn On> to turn on UID control.
- 3. Click <Turn Off> to turn off UID control.
- 4. Click <Save> to save the setting.

Notes

Chapter 3

Frequently Asked Questions

3.1 Frequently Asked Questions

A. Question: If I am using a firewall for my network connections, which ports should I open so that I can access my IPMI connection?

Answer: In order to access your IPMI connection behind a firewall, please open the following ports:

HTTP: 80 (TCP) HTTPS: 443 (TCP) IPMI: 623 (UDP) Remote console: 5900 (TCP) Virtual media: 623 (TCP) SMASH: 22 (TCP) WS-MAN: 8889 (TCP)

B. Question: My system seems to function properly; however, the IPMI event log indicates that my voltage and temperatures are beyond the limits. Why?

Answer: It is not a normal condition. Make sure that there is no other device accessing the I²C bus. If another device accesses the I²C bus frequently, it might cause a collision with the BMC when this device accesses the I²C bus. When you see this error, please uninstall Im_sensors in the Linux.

Notes

Appendix A

Introduction to SMASH

A-1 Overview

The SMASH (System Management Architecture for Server Hardware) platform, developed by Distributed Management Task Force, Inc. (DMTF), delivers a host of architecture-based, industry-standard protocols that will allow IT professionals to simplify the task of managing multiple network systems in a data center. SMASH offers a simple, intuitive solution to manage heterogeneous servers in a web environment regardless of their differences in hardware, software, OS, or network configuration. SMASH provides the end-user and the ISV community with interoperable management technology for multi-vendor server platforms.

How SMASH works

SMASH simplifies typical SMASH scripts by reducing commands to simple verbs. Although designed to manage multi-servers as a whole, SMASH can address individual components in a specific machine by using the SSH command-line protocol. Even when multiple processors, add-on cards, logical devices, and cooling systems are installed in a server, SMASH can be directed at a particular component in the server. A manager can use a text console to access, monitor, and manage all servers that are connected to the same SSL connection. SMASH can be programmed to periodically check all sensors in all machines or monitor a particular component in a specific server at any time. By adjusting the scope of tasks and the schedules of monitoring, SMASH allows the IT professionals to effectively manage multi-system clusters, minimize power consumption, and achieve system management efficiency.



Figure 1 SMASH-CLP User Interface

SMASH Compliance Information

SMASH documented in this user's guide is developed in reference to and in compliance with the SMASH Initiative Standards based on the following DMTF documents.

- System Management Architecture for Server Hardware (SMASH) Command Line Protocol (CLP) Architecture White Paper (DSP 2001)
- SM CLP Specification (DSP 0214)
- SM ME Addressing Specifications (DSP 0215)
- SM SLP to CIM Common Mapping Specification (DSP 0216)
- Common Information Model (CIM) Infrastructure Specification (DSP0004)
- The Secure Shell (SSH) Protocol Architecture (RFC4251)
- The Secure Shell (SSH) Connection Protocol (RFC4254)

A-2 An Important Note to the User

The information included in this user's guide provides a general guideline on how to use the SMASH protocol for your system management. Instructions given in this document may or may not be applicable to your system; it depends on the configuration of the system or the environment it operates in.

A-3 Using SMASH

This section provides a general guideline on how to use SMASH for your system management in a web-based environment. Refer to the SMASH script provided below to curtail a server management protocol for your systems.



Note: The instructions listed below are applicable to both Windows and Linux systems. We use the Windows platform as our default setting.

A-4 Initiating the SMASH Protocol

There are two ways of initiating the SMASH protocol.

To Initiate SMASH Automatically

You can initiate SMASH automatically by connecting the BMC (Baseboard Management Controller) via the Secure Shell protocol (SSH) from a client machine.

To connect from a Linux machine

- 1. Use 'ssh<BMC ip address>'.
- 2. Enter the password.

To connect from other machines

- 1. Use a terminal emulator application such as *Putty*.
- 2. Enter the BMC ip address in the terminal emulator application.
- 3. Choose *ssh* as the connection type
- 4. Enter the password at the prompt.
- 5. At the prompt '#", enter <SMASH> to invoke the SMASH prompt ' > '.
- 6. If you have successfully logged in, the SMASH prompt will display.

A-5 SMASH-CLP Main Screen

After you've successfully logged in the SSL network, the SMASH Command Line Protocol Main screen will display as shown below.



Figure 2 SMASH-CLP Main Screen

A-6 Using SMASH for System Management

After you've familiarized yourself with SMASH commands, you are able to use these commands to manage your system. To properly manage your network system, be sure to follow the instructions below.

Note:

Make sure that the format of all your commands are compliant with the DMTF specification, which is "<Verb> [<option>] [<target>] [<properties>]", where:

- A Verb means a command.
- An *Option* works according to the definition of a command given in Section 7: Definitions of Command Verbs.
- A *Target* is a managed device which is also referred to in the diagram of *Target Addressing* as shown in Figure 2.1.
- **Properties** are the specific attributes that you want to assign to a target machine or to get from a target machine.

🖉 172.31.1.73 - PuTTY	
-> show /system1	
/system1	
Targets :	
fwimage1	
logs1	
memory1	
pwrmgtsvc1	
sensors1	
Properties :	
None	
Verbs :	
show	
help	
version	
->	~

Figure 3 Using SMASH for System Management

A-7 Definitions of Command Verbs

Based on the DSP Specification, each target supports its own set of verbs. These verbs allow the user to issue commands to a target system to perform certain tasks. For example, the verbs supported by the *admin* target group include: cd, help, load, dump, create, delete, exit, version and show etc.

• cd

The command verb *cd* is used to navigate to a specific target address using the SSL protocol. For example, issuing the command *cd/admin1* will direct you to the target *admin* (AdminDomain).

• show

The command verb *show* is used to display the properties and the contents of a target, a group of targets, a sub-groups of the target(s). Properties, contents, supported operations related to the target, the group of targets or their sub-targets will be displayed.

• exit

The command verb *exit* is used when you want to exit from a SMASH session or close a session.

• help

The command verb *help* is used when you want to get helpful hints or information on a context-specific item. This command has the same function as the *help option* listed for the target group.

• Version

Use the command verb version to display the CLP version used in a specific machine.

set

Use the command verb set to assign a set of values to the properties of a target machine.

• start

The command verb *start* is used to turn on the power control, to start a process, or to change an operation state from a lower level to a higher level in a system.

• stop

The command verb *stop* is used to turn off the power, to stop a process, or to change an operation state from a higher level to a lower level.

reset

The command verb *reset* is used to enable or to disable the power control of or the processes of the machine.

• delete

The command verb *delete* is used to delete or to destroy an entry or a value previously entered. It can only be used in a specific target as defined according to the SAMSHCLP Standards.

• load

The command verb *load* is used to move a binary image file from a URI source to the MAP. This command will achieve different results depending on the setting of a target system, and how the verb *load* is defined in the DSP specification used in the system.

• dump

The command verb *dump* is used to move a binary image file from the MAP to a URI source. This command will achieve different results depending on the setting of a target system, and how the verb *dump* is defined in the DSP specification implemented in the system.

• create

The command verb *create* is used to create a new address entry or a new item in the MAP. It can only be used in a specific target as defined in the SMASH profile or in MAP specifications.

A-8 SMASH Commands

The following table provides the definitions and the descriptions of SMASH commands. The most useful commands are *show* and *help*, which will provide the user with useful information on how to navigate through the SSL network connection.

Option Name	Short Form	Definition	Notes
-all	-а	Instructs a command verb to perform all tasks possible	None
-destination <uri></uri>	None	Indicates the final location of an image or selected data	URI or SM instance address
-display	-d	Selects data that the user wishes to display	This can generate multiple query results
-examine	-x	Instructs the Command Processor to examine a command for syntax or semantic errors without executing it	None
-force	-f	Instructs the verb to ignore any warn- ings triggered by default but go ahead executing the command instead	None
-help	-h	Displays all information and documenta- tion regarding the command verb	None
-keep <m[.s]< td=""><td>-k</td><td>Sets a time period to hold and keep the Job ID and the status of a command</td><td>The amount of time set to hold a command Job ID or its status can differ.</td></m[.s]<>	-k	Sets a time period to hold and keep the Job ID and the status of a command	The amount of time set to hold a command Job ID or its status can differ.
-level <n></n>	-1	Instructs the Command Processor to execute the command for the current target and for all target machines within the level specified by the user	Levels should be expressed in a nature number or "all".
-Output <args></args>	-0	Controls the format and the content of a command output. This only supports "format=clpxml" and "format=keyword"	Many variables or factors can affect the outcome of format, language, level of details of the output.
-Source <uri></uri>	None	Indicates the location of a source image or a target	URI or SM Instance Address
-Version	-V	Displays the version of the command verb	None
-Wait	-W	Instructs the Command Processor to hold the command response or query result until all spawned jobs are completed.	None

Table 1 SMASH Commands

A-9 Standard Command Options

The following table lists the standard command options.

CLP		CLP Verbs											
Option	CD	Create	delete dump exit help load show set set start Stop							version			
all										x			
destination				x									
display										x			
examine	x	x	x	x	x	x	x	x	x	x	x	x	x
force			x	x			x	x	x	x	x	x	
help	x	x	x	x	x	x	x	x	x	x	x	x	x
keep													
level										x			
Output	x	x	x	x	x	x	x	x	x	x	x	x	x
Source							x						
Version	x	x	x	x	x	x	x	x	x	x	x	x	x
Wait													

Table 2 Standard Command Option

A-10 Target Addressing

To simplified the process of SMASH command execution, a file system called Target Addressing was created as shown in the diagram below.



Figure 4 Target Addressing Diagram

Terms Used in the Target Addressing Diagram

This section provides the descriptions of the terms used in the Target Addressing Diagram above.

- "/" indicates the root of the system.
- "/system1" includes all major Targets.
- "/system1/logs1/log1" includes all senor event logs.
- "/system1/sensors1" contains the readings and information of all sensors.
- *"/system1/pwrmgtsvc1"* is used for chassis control.
- "show../logs1" allows you to issue SMASH commands for the system to perform the tasks of your choice. For example:
 - Issuing the command *"show/system1/logs1"* while you are in *"show../logs1"* will allow you to set the *Absolute* or the *Relative* target path.

Notes

Appendix B

RADIUS Setup Guidelines

This chapter provides the Radius setup guidelines for IPMI firmware.

1. Start VM with RHEL4.7.VMX and boot into the OS.

Red Hat Enterprise	e Linux
Username:	Username: root Password: paseword
Please enter your userna	

2. Check the IP address of the RADIUS server.

```
[root@server postfix]# ifconfig
          Link encap:Ethernet HWaddr 00:0C:29:D6:5E:27
inet addr:192.168.10.154 Bcast:192.168.10.255 Mask:255.255.255.0
eth0
          inet6 addr: fe80::20c:29ff:fed6:5e27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:61045 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1708 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5596983 (5.3 MiB) TX bytes:151803 (148.2 KiB)
          Interrupt:193 Base address:0x2024
10
          Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:2556 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2556 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

RX bytes:3202416 (3.0 MiB) TX bytes:3202416 (3.0 MiB)

[root@server postfix]#

3. Configure User information.

vi /etc/raddb/users

- H=4, I =4 →Administrator (Super)
- H=3, I =3 → Operator (Randy)
- H=2, I =2 → User (Tester)
- H=1, I =1 → No Access

4. Configure Client information.

5. Configure Port information.

vi /etc/raddb/radiusd.conf



6. Start RADIUS service.

```
[root@server postfix]#
[root@server postfix]#
[root@server postfix]#
Starting RADIUS server:
[ OK ]
[root@server postfix]#
```

7. Enable RADIUS in the IPMI web page.

RADIUS Settings



8. Logout ADMIN and try to login using a RADIUS account



Notes

(continued from front)

The products sold by Fujitsu Limited are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Fujitsu Limited disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Fujitsu Limited harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.