FUJITSU

PRIMERGY BX920 S4
Server Blade

Operating Manual

November 2013

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to email: manuals@ts.fujitsu.com.

Certified documentation
according to DIN EN ISO 9001:2008

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH www.cognitas.de

Copyright and Trademarks

Before reading this manual

For your safety

This manual contains important information for safely and correctly using this product.

Carefully read the manual before using this product. Pay particular attention to the accompanying manual "Safety Notes and Regulations" and ensure these safety notes are understood before using the product. Keep this manual and the manual "Safety Notes and Regulations" in a safe place for easy reference while using this product.

Radio interference

This product is a "Class A" ITE (Information Technology Equipment). In a domestic environment this product may cause radio interference, in which case the user may be required to take appropriate measures.   VCCI-A

Aluminum electrolytic capacitors

The aluminum electrolytic capacitors used in the product's printed circuit board assemblies and in the mouse and keyboard are limited-life components. Use of these components beyond their operating life may result in electrolyte leakage or depletion, potentially causing emission of foul odor or smoke.

As a guideline, in a normal office environment (25°C) operating life is not expected to be reached within the maintenance support period (5 years). However, operating life may be reached more quickly if, for example, the product is used in a hot environment. The customer shall bear the cost of replacing replaceable components which have exceeded their operating life. Note that these are only guidelines, and do not constitute a guarantee of trouble-free operation during the maintenance support period.

High safety use

This product has been designed and manufactured to be used in commercial and/or industrial areas as a server.

When used as visual display workplace, it must not be placed in the direct field of view to avoid incommoding reflections (applies only to TX server systems).

The device has not been designed or manufactured for uses which demand an extremely high level of safety and carry a direct and serious risk of life or body if such safety cannot be assured.

These uses include control of nuclear reactions in nuclear power plants, automatic airplane flight control, air traffic control, traffic control in mass transport systems, medical devices for life support, and missile guidance control in weapons systems (hereafter, "high safety use"). Customers should not use this product for high safety use unless measures are in place for ensuring the level of safety demanded of such use. Please consult the sales staff of Fujitsu if intending to use this product for high safety use.

Measures against momentary voltage drop

This product may be affected by a momentary voltage drop in the power supply caused by lightning. To prevent a momentary voltage drop, use of an AC uninterruptible power supply is recommended.

(This notice follows the guidelines of Voltage Dip Immunity of Personal Computer issued by JEITA, the Japan Electronics and Information Technology Industries Association.)

Technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan

Documents produced by Fujitsu may contain technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan. Documents which contain such technology should not be exported from Japan or transferred to non-residents of Japan without first obtaining authorization in accordance with the above law.

Harmonic Current Standards

This product conforms to harmonic current standard JIS C 61000-3-2.

Only for the Japanese market:
About SATA hard disk drives

The SATA version of this server supports hard disk drives with SATA / BC-SATA storage interfaces. Please note that the usage and operation conditions differ depending on the type of hard disk drive used.

Please refer to the following internet address for further information on the usage and operation conditions of each available type of hard disk drive:

http://jp.fujitsu.com/platform/server/primergy/harddisk/

Only for the Japanese market:

i Although described in this manual, some sections do not apply to the Japanese market. These options and routines include:

– CSS (Customer Self Service)

Contents

Contents

1 Introduction

The PRIMERGY BX920 S4 server blade is an Intel-based dual-socket server blade. It is ideal for use in data centers belonging to enterprises or Internet service providers, and makes an excellent large application server, terminal server for compute-intensive applications or DBMS server.

Security functions in the *BIOS Setup* protect the data on the server blade from unauthorized changes.

The server blade occupies only one bay in the PRIMERGY BX900/BX400 system unit.

> **i** You can find information about assembling, starting up and operating the system unit in the relevant operating manual.

1.1 Concept and target groups for this manual

This operating manual describes how to install, set up and operate your server blade.

This operating manual is intended for those responsible for installing the hardware and ensuring that the system runs smoothly. It contains all the information you need to put your PRIMERGY BX920 S4 server blade into operation.

To understand the various expansion options, you will need to be familiar with the fields of hardware and data transmission and you will require a basic knowledge of the underlying operating system.

1.2   Documentation overview

More information on your PRIMERGY BX920 S4 server blade can be found in the following documents:

– "ServerView Quick Start Guide"

– "Safety Notes and Regulations" manual
  " 安全上のご注意 " for the Japanese market

– "Warranty" manual
  " 保証書 " for the Japanese market

– "PRIMERGY ServerView Suite Local Service Concept - LSC" manual

– "Returning used devices" manual and "Service Desk" leaflet
  " サポート＆サービス " for the Japanese market

– PRIMERGY BX920 S4 Server Blade Upgrade and Maintenance Manual

– D3142 BIOS Setup Utility for PRIMERGY BX920 S4 Server Blade
  Reference Manual

– "LSI MegaRAID - SAS Software User Guide"

– "Modular RAID Controller / Modular SAS HBA Installation Guide"

> **i** All documentation on PRIMERGY hardware and ServerView software is available online from the Fujitsu manuals server at:
>
> – *http://manuals.ts.fujitsu.com* (global market)
> – *http://jp.fujitsu.com/platform/server/primergy/manual* (Japanese market)
>
> The complete PRIMERGY documentation set can also be downloaded as a DVD ISO image at:
>
> – *ftp://ftp.ts.fujitsu.com/images/serverview/manuals* (global market)
> – *http://jp.fujitsu.com/primergy/downloads* (Japanese market)

> **i** For the Japanese market:
>
> Before using the product, please check for additional information that may be available under the following URL:
> *http://jp.fujitsu.com/platform/server/primergy/products/note/*

Further sources of information:

– ServerView Suite Glossary
– Manual for the monitor

– Documentation for the boards and drives
– Operating system documentation
– Information files in your operating system

1.3 Notational conventions

The following notational conventions are used in this manual:

Text in italics	indicates commands or menu items.
"Quotation marks"	indicate names of chapters and terms that are being emphasized.
►	describes activities that must be performed in the order shown.
⚠ CAUTION!	pay particular attention to texts marked with this symbol. Failure to observe this warning may endanger your life, destroy the system or lead to the loss of data.
i	indicates additional information, notes and tips.

2 Functional overview

The PRIMERGY BX920 S4 server blade is an Intel-based dual-socket server blade. It is ideal for use in data centers belonging to enterprises or Internet service providers, and makes an excellent large application server, terminal server for compute-intensive applications or DBMS server.

2.1 Features

Intel® Xeon® processor

The server blade is equipped with an Intel® Xeon® processor E5-2400 v2 family for high-speed data processing.

Customer Self Service (CSS)

The PRIMERGY Customer Self Service (CSS) concept enables you to identify and replace the affected component yourself in the case of certain error scenarios.

In the CSS concept, you can replace the following components yourself in the event of an error:

– Solid state disk drives / Hard disk drive

– Memory modules

– Expansion cards

For information on replacing these components, see the "PRIMERGY BX920 S4 Server Blade Upgrade and Maintenance Manual".

CSS indicators on the control panel of the PRIMERGY server provide you with information if a CSS event arises.

In addition, CSS errors are displayed in the ServerView Operations Manager, the server management software from Fujitsu.

In the event of errors, the ServerView Operations Manager refers you directly to the affected component and its order information in the Illustrated Spares catalog of the server in question. (This feature is not available for the Japanese market.)

| i | Further information on the CSS concept is provided in the "PRIMERGY ServerView Suite Local Service Concept - LSC" manual on the Fujitsu manuals server. |

For the latest information on optional products provided for the BX920 S4 Server Blade see the configurator of the server:

http://ts.fujitsu.com/products/standard_servers/index.html
(for the EMEA market)

http://jp.fujitsu.com/platform/server/primergy/system/
(for the Japanese market)

System board

The features of the system board are described in the Upgrade and Maintenance Manual for the hardware.

Trusted Platform Module (TPM)

A Trusted Platform Module (TPM) for safer storage of keys can be implemented as an option. This module enables programs from third party manufacturers to store key information (e.g. drive encryption using Windows Bitlocker Drive Encryption).

The TPM is activated via the BIOS system (for more information, refer to the "D3142 BIOS Setup Utility for PRIMERGY BX920 S4 Reference Manual").

⚠ **CAUTION!**

– When using the TPM, note the program descriptions provided by the third party manufacturers.

– You must also create a backup of the TPM content. To do this, follow the third party manufacturer's instructions. Without this backup, if the TPM or the system board is faulty you will not be able to access your data.

– If a failure occurs, please inform your service about the TPM activation before it takes any action, and be prepared to provide them with your backup copies of the TPM content.

Hard disk drives (HDD) / Solid state drives (SSD)

The server blade can be equipped with a maximum of two 2.5-inch HDD/SSD modules.

Each HDD/SSD module can accommodate an SAS/SATA hard disk drive or an SAS/SATA SSD drive. The module is connected to the SAS/SATA backplane wirelessly. This allows HDD/SSD modules to be plugged in or pulled out easily.

Two SAS/SATA hard disk drives or SAS/SATA SSD drives can be controlled by the onboard SAS/SATA controller.

Mixed configurations of SAS HDDs, SATA HDDs, SAS SSDs and SATA SSDs within the same logical drive (RAID array) are not supported.

If the server blade has a corresponding RAID configuration, HDD/SSD modules can also be replaced during operation.

Onboard CNA controller

A CNA controller is integrated on the system board; up to 4 x 1 Gbit/s or 2x 10 Gbit/s can be selected on the CNA controller.

For more information on configuring the controller, see section "Configuring the onboard CNA controller" on page 56.

Onboard SAS/SATA controller

A SAS/SATA controller is integrated on the system board; up to two SAS/SATA hard disk drives or SAS/SATA SSD drives can be connected to the controller. The LSI Embedded MegaRAID software (SATA Software RAID) supports RAID levels 0, 1 and 10. The SAS functionality needs to be enabled separately by using an onboard SAS enabling key.

For more information on configuring the controller, see section "Configuring the onboard SAS/SATA controller" on page 55.

SAS/SATA RAID controller

The server blade is available with the following SAS/SATA RAID controllers for operating the internal SAS/SATA hard disk drives:

– Modular RAID 5/6 controller with "MegaRAID functionality" (SAS MegaRAID) for SAS1.0 and SAS2.0

  RAID levels 0, 1, 10, 1E, 5, 50, 6 and 60 are supported for internal hard disk drive configurations. As an option, a flash backup unit (FBU) can save the memory content even if the power fails. Cache memory size of 512 Mbyte is available.

> **i** For more information on configuring the controller, see section .

Slots for expansion cards

The server blade supports two optional mezzanine cards. This enables Fibre Channel connections, Infiniband connections and/or additional Ethernet connections to be implemented.

The following mezzanine cards are available for the server blade:

– 1 Gbit/s Ethernet mezzanine card with 4 ports

– 6 Gbit/s SAS HBA mezzanine card

– 6 Gbit/s SAS expander mezzanine card

– 6 Gbit/s SAS RAID mezzanine card

– 8 Gbit/s Fiber channel mezzanine card with 2 ports

– 10 Gbit/s Ethernet mezzanine card with 2 ports

– 10 Gbit/s CNA mezzanine card with 2 ports

– 40-Gbit/s Infiniband mezzanine card with 2 ports

– 56-Gbit/s Infiniband mezzanine card with 2 ports

> **i** If a server blade is configured with one or two mezzanine cards, this does not exclude other configurations for any of the other server blades in a system unit.
>
> If you want to install mezzanine cards in server blades, the system unit must be fitted with the corresponding Fibre Channel, SAS, Infiniband and/or Ethernet connection blades. You can find detailed information about the equipping rules for connection blades in the operating manual for the system unit.
>
> Mezzanine cards may only be installed and removed by authorized, qualified personnel. The procedure is described in the PRIMERGY BX920 S4 server blade Upgrade and Maintenance Manual.

USB flash module (UFM)

A UFM (USB flash module) can also be configured.

Graphics controller

The server blade has an onboard graphics controller (integrated in the iRMC controller). A monitor can be connected via the Y-cable on the front of the server blade.

| **i** | For peripherals like keyboard, mouse, display, optical drive, etc. Advanced Video Redirection and Virtual Media connection by iRMC is recommended. |

External ports

The server blade has the following ports on the front:

– One USB port

– One port for a special Y-cable , with 2 USB ports and one VGA port.

High level of availability and data security

When memory data is accessed, 1-bit errors are identified in the main memory and automatically corrected with the error correcting code (ECC) method.

ASR&R (Automatic Server Reconfiguration and Restart) restarts the system in the event of an error and automatically "hides" the defective system components.

The PDA (Prefailure Detection and Analyzing) technology from Fujitsu Technology Solutions analyzes and monitors all components that are critical for system reliability.

iRMC with integrated management LAN connector

| **i** | The server blade can use iRMC Advanced Video Redirection and Virtual Media as a standard function. Therefore, the license key to the option is unnecessary. |

The iRMC (**i**ntegrated **R**emote **M**anagement **C**ontroller) is a Baseboard Management Controller (BMC) with integrated management LAN connector and expanded functionality that was previously only available with additional plug-in cards. In this way, the iRMC enables complete control of PRIMERGY servers, regardless of system status, and thus particularly the control of PRIMERGY servers that are in the "out-of-band" system status.

Major functions supported by the iRMC include the following:

● Browser access via iRMC's own web server

- Secure communication (SSH, SSL)

- Power Management for the managed server (depending on its system status)

- Power Consumption Management

- Connecting virtual drives as remote storage

- Text-based and graphic console bypass (Advanced Video Redirection)

- Virtual Media

- Command Line Interface (CLI)

- Simple, interactive or script-based iRMC configuration

- Customer Self Service (CSS)

- iRMC's own user management

- Multi-computer, global iRMC user administration using an LDAP Directory Service

- Automatic network configuration via DNS / DHCP

- Power supply of the iRMC via the system standby supply

- Full-coverage alarm management

- System Event Log (SEL) reading and processing

- IPMI support

- CIM / WS-MAN support

- Internal Event Log for user login/logout auditing

More information about the iRMC can be found in the "iRMC S4 - integrated Remote Management Controller" user guide (on the Fujitsu manual server under *Industry Standard Servers - Software - ServerView Suite - Out-Of-Band Management*).

Server management

Server management is implemented using the ServerView Operations Manager supplied and the PDA (Prefailure Detection and Analysis) technology from Fujitsu. PDA reports the threat of a system error or overload at an early stage, allowing preventive measures to be taken.

The ServerView Operations Manager enables the management of all PRIMERGY servers in the network via a central console. The ServerView Operations Manager supports the following functions:

● Round-the-clock monitoring, regardless of server status

● High-performance, graphical console bypass (AVR) protected by HTTPS/SSL (128 bit)

● Virtual Media via USB

● Remote power on

● Temperature monitoring of the CPU and the surrounding area

● Detailed status and error reports for processors and main memory

● Watchdog timer for Automatic Server Reconfiguration and Restart (ASR&R) in the event that memory modules or processors fail

● Power monitoring

● End-of-life monitoring of fans with prompt notification before failure

● Watchdog timer for monitoring the operating system with ASR&R

Further information on the ServerView Operations Manager is provided in the associated documentation.

ServerView Installation Manager

You can configure the PRIMERGY server quickly and precisely with the ServerView Installation Manager software provided. User-guided menus are available for installing the server operating system (for further details see section "Configuring the Server Blade" on page 52).

Service and support

PRIMERGY servers are service-friendly and modular, thus enabling quick and simple maintenance. The two redundant hot-pluggable management blades of the system unit, with independent LAN and COM ports for management, enable comprehensive remote administration of the server blade. Together, they allow remote diagnosis for system analysis, remote configuration and remote restart, even in the case of operating system failure or hardware errors.

2.2 Server specification

This section explains the specifications for the server blade. The specifications for this server blade are liable to be updated without any notice. Please be forewarned.

System Board

System board type	D3142-B100
Chipset	Intel® C600

Processor

Processor quantity and type	2x Intel® Xeon® processor E5-2400 v2 product family

Memory modules configuration

Memory slots	12 slots in total; 6 slots per CPU
Memory slot type	DIMM (DDR3): LRDIMM, RDIMM
Memory capacity (min. - max.)	4 GB - 768 GB
Memory protection	Advanced ECC; Memory Scrubbing, SDDC (Chipkill™); Memory Mirroring support; Hot-spare memory support
Memory notes	Memory Mirroring with identical modules in both channel pairs of a bank (2 modules per bank), Rank sparing or Performance Mode with the spare rank module having identical or larger memory capacity than all the other ranks on the same channel

Interfaces

USB connectors	4 x USB 2.0 (1x front , 2x front via Y-cable, 1x internal)
Graphics (15-pin)	1 x VGA via Y-cable (front)

Onboard or integrated controllers

RAID Controller	Modular RAID 5/6 controller with "MegaRAID functionality" (SAS MegaRAID) for SAS1.0 and SAS2.0. RAID levels 0, 1, 10, 1E, 5, 50, 6 and 60 are supported for internal hard disk drive configurations.
SAS/SATA Controller	A 6-port SAS/SATA controller is integrated on the system board; up to two SAS or SATA drives can be connected to the controller. The LSI Embedded MegaRAID software (SATA Software RAID) supports RAID levels 0, 1 and 10. The SAS functionality needs to be enabled separately by using onboard SAS enabling key.
CNA Controller	The CNA controller is integrated on the system board; up to 4 x 1 Gbit/s or 2x 10 Gbit/s can be selected on the CNA controller.
Remote Management Controller	Integrated Remote Management Controller (iRMC S4), 8 MB video memory, IPMI 2.0 compatible
Trusted Platform Module (TPM)	Infineon / 1.2 (option)

Disk drives

Drive configuration	2x 2.5-inch SAS/SATA HDD/SSD modules

Operating panel

Operating buttons	On/off button
	ID button
Status LEDs	Power indicator (orange / yellow / green)
	ID indicator (blue)
	Global error indicator (orange)
	CSS indicator (yellow)
	I/O indicator: fabric 1 (green)
	I/O indicator: fabric 2 (green)
	I/O indicator: fabric 3/4 (green)

Dimensions / Weight

Width	45 mm
Depth	508 mm
Height	210.5 mm (1 bay in the system unit)
Weight	Max. 5.3 kg
Weight notes	Weight may vary depending on actual configuration

Ambient conditions

Environment class 3K2 Environment class 2K2	EN 60721 / IEC 721 Part 3-3 EN 60721 / IEC 721 Part 3-2
Temperature:	
Operation (3K2)	5°C ... 35°C
Transport (2K2)	-20°C ... 60°C
Humidity	10% ... 85% (non condensing)

Condensation during operation must be avoided!

Electrical specifications

Power consumption	409 W (full configuration)
Thermal dissipation	1.472 kJ/h

Compliance with regulations and standards

Product safety and ergonomics	
International	IEC 60950-1 2ed; am1
Europe	
Safety	EN 60950-1 2ed.; am1 EN 50371 EN 50392
Ergonomics	ISO 9241-3 EN 2941-3 EK1-ITB2000:2013
USA / Canada	CSA-C22.2 No. 60950-1-07 2ed. UL 60950-1 2ed.
Taiwan	CNS 14336
China	GB 4943
Electromagnetic compatibility	
International	CISPR 22
Europe	EN 55022 Class A EN 55024 EN 61000-3-2 EN 61000-3-3 ETSI 300386
USA / Canada	47CFR part 15 Class A / ICES-003
Taiwan	CNS 13438 Class A
China	GB 9245 / GB 17625
Japan	VCCI Class A / JEITA
Korea	KN 22 / KN 24
CE marking to EU directives	Low Voltage Directive 2006/95/EC Electromagnetic compatibility 2004/108/EC

Certification

Product safety approved with the system unit	
Global	CB
Germany	GS, CE
USA/Canada	CSA_{US}/CSA_C
Japan	VCCI
China/Taiwan	BSMI

3 Installation steps, overview

This chapter contains an overview of the steps necessary to install your Server Blade. The cross-references take you to the sections containing more detailed information on the relevant installation step:

▶ First read the chapter "Important information" on page 27, particularly the section "Safety instructions".

▶ Unpack the Server Blade, check the contents of the package for visible transport damage and check whether the items delivered correspond to the details on the delivery note (see section "Unpacking the server blade" on page 38).

▶ Transport the server blade to the place where you want to set it up.

▶ Make sure that you have all necessary manuals (see page 10); print out the PDF files if required.

▶ Install the server blade in your system unit (see section "Installing the server blade in the system unit" on page 38).

▶ Familiarize yourself with the controls and indicators on the front of the server blade (see chapter "Starting up and operation" on page 47).

▶ Install the operating system and applications on the server blade.

When doing so, you have the following options:

– *Clone the server blade from a remote image server using the ServerView Deployment Manager. Cloning the ServerView Deployment Manager from a remote image server.*

This procedure is recommended if the following conditions are met:

– ServerView Deployment Manager software is available.
– You have a suitable clone image.
– A Deployment Server and LAN connection are available.

– *Remote installation with ServerView Installation Manager*

This installation method is recommended if you have a LAN connection and a DHCP server (Deployment Server) available, but the cloning requirements are not met.

– *Local installation with or without ServerView Installation Manager*

Local installation is the least convenient method. It is only recommended if the requirements for remote installation and cloning are not met.

If you want to install an operating system that is not supported by *ServerView Installation Manager*, you can of course install it directly without *ServerView Installation Manager*.

| i | For more information about installing the server remotely or locally, please refer to the "ServerView Installation Manager" user guide. You can find a description of how to clone server blades in the ServerView Deployment Manager user guide (on the Fujitsu manuals server under *Industry Standard Servers - Software - ServerView Suite - Server Installation and Deployment*). |

4 Important information

This chapter provides safety instructions which you must observe when handling your server.

4.1 Safety instructions

| i | The following safety instructions are also provided in the manual "Safety Notes and Regulations" or " 安全上のご注意 ". |

This device meets the relevant safety regulations for IT equipment. If you have any questions about whether you can install the server in the intended environment, please contact your sales outlet or our customer service team.

CAUTION!

● The actions described in this manual shall be performed by technical specialists. A technical specialist is a person who is trained to install the server including hardware and software.

● Repairs to the device that do not relate to CSS failures shall be performed by service personnel. Please note that unauthorized interference with the system will void the warranty and exempt the manufacturer from all liability.

● Any failure to observe the guidelines in this manual, and any improper repairs could expose the user to risks (electric shock, energy hazards, fire hazards) or damage the equipment.

● Before installing/removing internal options to/from the server, turn off the server, all peripheral devices, and any other connected devices. Also unplug all power cords from the power outlet. Failure to do so can cause electric shock.

Before starting up

⚠ **CAUTION!**

● During installation and before operating the device, observe the instructions on environmental conditions for your device (see "Server specification" on page 20).

● If the server has been moved from a cold environment, condensation may form both inside and on the outside of the machine.

Wait until the server has acclimatized to room temperature and is absolutely dry before starting it up. Material damage may be caused to the server if this requirement is not met.

● Only transport the server in the original packaging or in packaging that protects it from impacts and jolts.

Installation and operation

⚠ **CAUTION!**

● The device may only be operated in a maximum ambient temperature of 35°C.

● If the device is integrated in an installation that receives power from an industrial (public) power supply network with the IEC309 connector, the (public) power supply protection must comply with the requirements for non-industrial (public) power supply networks for the type A connector.

● The On/Off button or the main power switch (if there is one) does not disconnect the device from the mains voltage. To completely disconnect it, you must remove all the power plugs from the power outlets.

● Data cables must be adequately shielded to avoid interference.

● Do not connect or disconnect any data transmission cables during a thunderstorm (lightning hazard).

● Make sure that no objects (e.g. bracelets or paper clips) fall into or liquids spill into the device (risk of electric shock or short circuit).

CAUTION!

- In emergencies (e.g. damaged casing, control elements or power cable, penetration of liquids or foreign bodies), switch off the device immediately, unplug it from the grounded power outlets, and contact your customer service center.

- Proper operation of the device (in accordance with IEC 60950-1/EN 60950-1) is only ensured if the casing is fully assembled and the rear covers for the installation bays are in place (electric shock, cooling, fire protection, interference suppression).

- Install only system extensions that satisfy the requirements and rules governing safety, electromagnetic compatibility, and telecommunications terminal equipment. If you install other extensions, you may damage the system or violate these safety regulations. You can find out which system extensions are suitable from the customer service center or your sales outlet.

- The components marked with a warning label (e.g. lightning symbol) may only be opened, removed or exchanged by authorized, qualified personnel. Exception: CSS components can be replaced.

- If you cause a defect on the device by installing or exchanging system extensions, the warranty will be invalidated.

- Only set the resolutions and refresh rates specified in the operating manual for your monitor. Otherwise, you may damage the monitor. If you are in any doubt, contact your sales outlet or customer service center.

Batteries

⚠ **CAUTION!**

● Incorrect replacement of batteries may lead to a risk of explosion. The batteries may only be replaced with identical batteries or with a type recommended by the manufacturer (refer to the "PRIMERGY BX920 S4 Server Blade Upgrade and Maintenance Manual").

● Do not throw batteries into the trash can.

● Batteries must be disposed of in accordance with local regulations concerning special waste.

● Replace the lithium battery on the system board in accordance with the instructions in the "PRIMERGY BX920 S4 Server Blade Upgrade and Maintenance Manual".

● All batteries containing pollutants are marked with a symbol (a crossed-out garbage can). In addition, the marking is provided with the chemical symbol of the heavy metal decisive for the classification as a pollutant:

Cd Cadmium
Hg Mercury
Pb Lead

Working with CDs/DVDs/BDs and optical drives

When working with devices with optical drives, these instructions must be followed.

⚠ **CAUTION!**

● Only use CDs/DVDs/BDs that are in perfect condition, in order to prevent data loss, equipment damage and injury.

● Check each CD/DVD/BD for damage, cracks, breakages etc. before inserting it in the drive.

Note that any additional labels applied may change the mechanical properties of a CD/DVD/BD and cause imbalance.

Damaged and imbalanced CDs/DVDs/BDs can break at high drive speeds (data loss).

Under certain circumstances, sharp CD/DVD/BD fragments can pierce the cover of the optical drive (equipment damage) and can fly out of the device (danger of injury, particularly to uncovered body parts such as the face or neck).

● High humidity and airborne dust levels are to be avoided. Electric shocks and/or server failures may be caused by liquids such as water, or metallic items, such as paper clips, entering a drive.

● Shocks and vibrations are also to be avoided.

● Do not insert any objects other than the specified CDs/DVDs/BDs.

● Do not pull on, press hard, or otherwise handle the CD/DVD/BD tray roughly.

● Do not disassemble the optical drive.

● Before use, clean the optical disk tray using a soft, dry cloth.

● As a precaution, remove disks from the optical drive when the drive is not to be used for a long time. Keep the optical disk tray closed to prevent foreign matter, such as dust, from entering the optical drive.

● Hold CDs/DVDs/BDs by their edges to avoid contact with the disk surface.

● Do not contaminate the CD/DVD/BD surface with fingerprints, oil, dust, etc. If dirty, clean with a soft, dry cloth, wiping from the center to the edge. Do not use benzene, thinners, water, record sprays, antistatic agents, or silicone-impregnated cloth.

● Be careful not to damage the CD/DVD/BD surface.

● Keep the CDs/DVDs/BDs away from heat sources.

● Do not bend or place heavy objects on CDs/DVDs/BDs.

● Do not write with ballpoint pen or pencil on the label (printed) side.

● Do not attach stickers or similar to the label side. Doing so may cause rotational eccentricity and abnormal vibrations.

● When a CD/DVD/BD is moved from a cold place to a warm place, moisture condensation on the CD/DVD/BD surface can cause data read errors. In this case, wipe the CD/DVD/BD with a soft, dry cloth then let it air dry. Do not dry the CD/DVD/BD using devices such as a hair dryer.

- To avoid dust, damage, and deformation, keep the CD/DVD/BD in its case whenever it is not in use.

- Do not store CDs/DVDs/BDs at high temperatures. Areas exposed to prolonged direct sunlight or near heating appliances are to be avoided.

| i | You can prevent damage from the optical drive and the CDs/DVDs/BDs, as well as premature wear of the disks, by observing the following suggestions: |

- Only insert disks in the drive when needed and remove them after use.
- Store the disks in suitable sleeves.
- Protect the disks from exposure to heat and direct sunlight.

Laser information

The optical drive complies with IEC 60825-1 laser class 1.

⚠ **CAUTION!**

The optical drive contains a light-emitting diode (LED), which under certain circumstances produces a laser beam stronger than laser class 1. Looking directly at this beam is dangerous.

Never remove parts of the optical drive casing!

Modules with Electrostatic-Sensitive Devices

Modules with electrostatic-sensitive devices are identified by the following sticker:
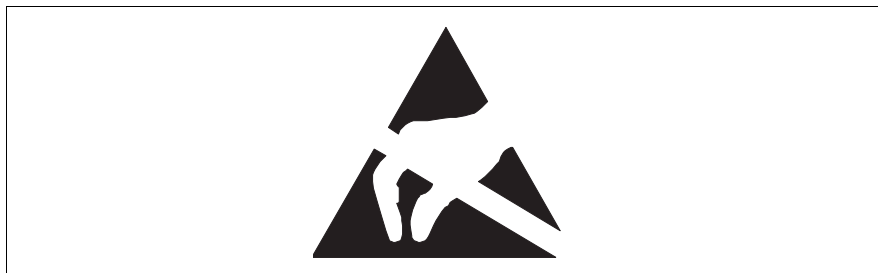

Figure 1: ESD label

When you handle components fitted with ESDs, you must always observe the following points:

- Switch off the system and remove the power plugs from the power outlets before installing or removing components with ESDs.

- You must always discharge static build-up (e.g. by touching a grounded object) before working with such components.

- Any devices or tools that are used must be free of electrostatic charge.

- Wear a suitable grounding cable that connects you to the external chassis of the system unit.

- Always hold components with ESDs at the edges or at the points marked green (touch points).

- Do not touch any connectors or conduction paths on an ESD.

- Place all the components on a pad which is free of electrostatic charge.

| i | For a detailed description of how to handle ESD components, see the relevant European or international standards (EN 61340-5-1, ANSI/ESD S20.20). |

Other important information:

- During cleaning, observe the instructions in section "Cleaning the Server Blade" on page 59.

- Keep this operating manual and the other documentation (such as the Upgrade and Maintenance Manual, documentation DVD) close to the device. All documentation must be included if the equipment is passed on to a third party.

4.2   CE conformity

The system complies with the requirements of the EC directives 2004/108/EC regarding "Electromagnetic Compatibility" and 2006/95/EC "Low Voltage Directive". This is indicated by the CE marking (CE = Communauté Européenne).

4.3   FCC class A device

⚠ **Warning!**

This is a class A product, which may cause radio interference in a domestic environment. If this is the case, the user may be required to take adequate measures.

4.4   Transporting the Server Blade

⚠ **CAUTION!**

Only transport the server blade in its original packaging or in suitable packaging which protects it from knocks and jolts.

For the Japanese market it is not required to transport the device in its original packaging.

Do not unpack the server blade until it is at its installation location.

4.5   Notes on installation in the system unit

⚠ **CAUTION!**

Beware of the energy hazard at the midplane contacts of the system unit. A short circuit on these contacts may damage the system.

4.6 Environmental protection

Environmentally-friendly product design and development

This product has been designed in accordance with the Fujitsu standard for "environmentally friendly product design and development". This means that key factors such as durability, selection and labeling of materials, emissions, packaging, ease of dismantling and recycling have been taken into account.

This saves resources and thus reduces the harm done to the environment. Further information can be found at:

– *http://ts.fujitsu.com/products/standard_servers/index.html* (for the EMEA market)
– *http://jp.fujitsu.com/platform/server/primergy/concept/* (for the Japanese market)

Energy-saving information

Devices that do not need to be constantly switched on should be switched off until they are needed as well as during long breaks and after completion of work.

Packaging information

This packaging information doesn't apply to the Japanese market.

Do not throw away the packaging. You may need it later for transporting the system. If possible, the equipment should only be transported in its original packaging.

Information on handling consumables

Please dispose of printer consumables and batteries in accordance with the applicable national regulations.

In accordance with EU directives, batteries must not be disposed of with unsorted domestic waste. They can be returned free of charge to the manufacturer, dealer or an authorized agent for recycling or disposal.

All batteries containing pollutants are marked with a symbol (a crossed-out garbage can). They are also marked with the chemical symbol for the heavy metal that causes them to be categorized as containing pollutants:

Cd Cadmium
Hg Mercury
Pb Lead

Labels on plastic casing parts

Please avoid sticking your own labels on plastic parts wherever possible, since this makes it difficult to recycle them.

Returns, recycling and disposal

Please handle returns, recycling and disposal in accordance with local regulations.

The device must not be disposed of with domestic waste. This device is labeled in compliance with European directive 2002/96/EC on waste electrical and electronic equipment (WEEE).

This directive sets the framework for returning and recycling used equipment and is valid across the EU. When returning your used device, please use the return and collection systems available to you. Further information can be found at *http://ts.fujitsu.com/recycling*.

Details regarding the return and recycling of devices and consumables within Europe can also be found in the "Returning used devices" manual, via your local Fujitsu branch or from our recycling center in Paderborn:

Fujitsu Technology Solutions
Recycling Center
D-33106 Paderborn

Tel.   +49 5251 525 1410
Fax   +49 5251 525 32 1410

5 Hardware installation

⚠ **CAUTION!**

● Follow the safety instructions in the chapter "Important information" on page 27.

● Do not expose the server to extreme environmental conditions (see "Ambient conditions" on page 22). Protect the server from dust, humidity and heat.

● Make sure that the server is acclimatized for the time indicated in this table before putting it into operation.

Temperature difference (°C)	Minimum acclimatization time (hours)
5	3
10	5
15	7
20	8
25	9
30	10

Table 1: Acclimatization time

In the table "Acclimatization time", the temperature difference refers to the difference between the operating environment temperature and the temperature to which the server was exposed previously (outside, transport or storage temperature).

5.1 Unpacking the server blade

⚠ **CAUTION!**

Follow the safety instructions in chapter "Important information" on page 27.

Do not unpack the server blade until it is at its installation location.

► Transport the server blade to the place where you want to set it up.

► Unpack all individual parts.

Keep the original packaging in case you want to transport the server blade again (applies only to EMEA market).

► Check the delivery for any damage during transport.

► Check whether the items delivered match the details on the delivery note.

The product name and serial number of the product can be found on the ID card (see section "ID card" on page 50).

► Notify your supplier immediately in case you discover that the items delivered do not correspond to the delivery note.

5.2 Installing the server blade in the system unit

⚠ **CAUTION!**

● Note the safety instructions and the information on handling electrostatically sensitive devices in section "Safety instructions" on page 27.

● Note the population rules for power supply units and fan modules to ensure sufficient cooling of the system. You will find more detailed information on this in the operating manual for the system unit.

Removing the dummy module

Any unused slots on the front of the system unit are fitted with appropriate dummy modules to comply with electromagnetic compatibility (EMC) regulations and to ensure sufficient cooling of the system components.

To add a server blade, you must first remove a dummy module from the relevant slot.
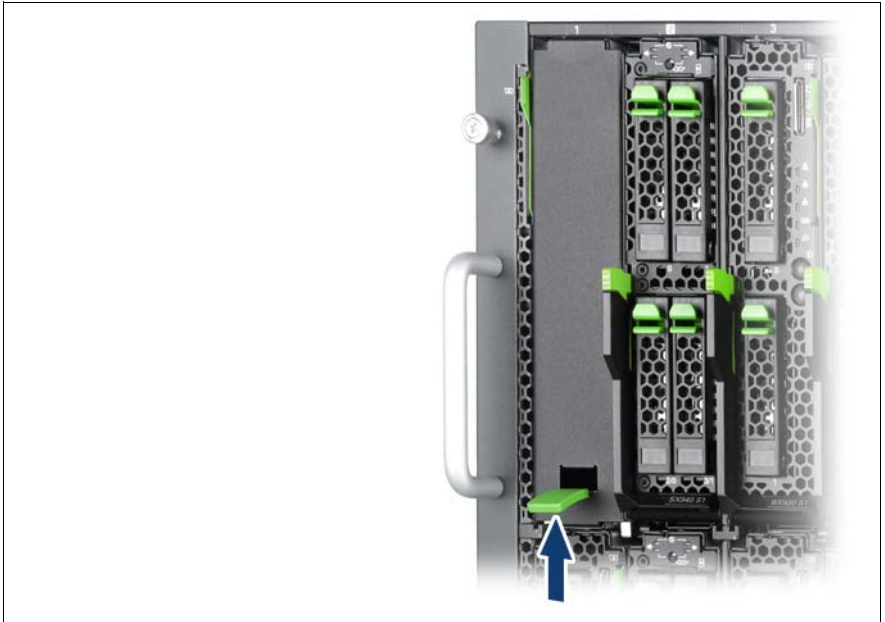
Figure 2: Removing the server blade dummy module

► Pull up the handle of the dummy module (arrow) to unlock it.

► Pull the dummy module out of the slot.

⚠ **CAUTION!**

Keep the dummy module for future use. If you remove a server blade and do not replace it with a new one, you must install a dummy module to comply with the regulations regarding electromagnetic compatibility and to ensure sufficient cooling of the system components.

Installing the dummy module

To install the dummy module, follow the same procedure as for removing it, except in reverse order.

Installing the server blade

⚠️ **CAUTION!**

Follow the safety instructions and information in section "Modules with Electrostatic-Sensitive Devices" on page 32.

Figure 3: Installing the server blade

► Open the release lever.

► Push the server blade as far as possible into the slot.

Figure 4: Locking the server blade

▶ Push the release lever up until it engages.
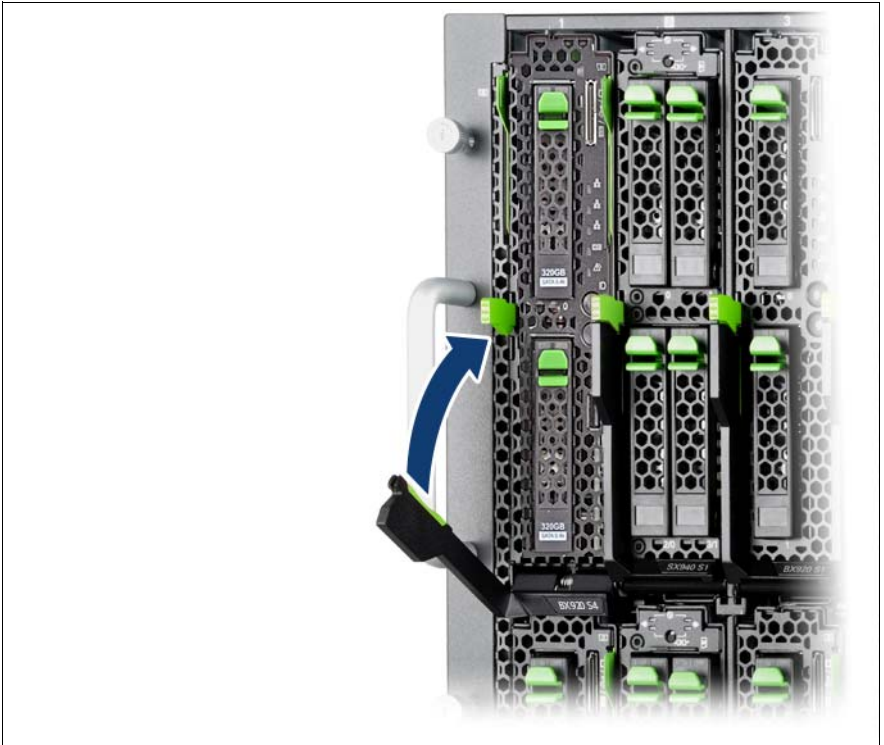
Removal is carried out in reverse order.

⚠ **CAUTION!**

If you remove a server blade and do not replace it with a new one, you must install a dummy module to comply with the regulations regarding electromagnetic compatibility and to ensure sufficient cooling of the system components.

5.3   Connecting devices

All connections that are required to operate the server blade are made via the midplane of the system unit. When the server blade is installed, midplane contacts automatically establish connections to the infrastructure modules on the rear of the system unit:

– Power supply units

– Management blade(s) for server administration

– Ethernet and/or fiber-channel connection blades for connection to a LAN or SAN

You can find information about the external ports of the system unit in the relevant operating manual.

The front of the server blade has a port for a special Y-cable, which provides 2 USB ports and 1 VGA port. An additional USB port is available on the front of the server blade.

Figure 5: Ports on the front

1	USB connector (2x)	4	Y-cable connector on the server blade
2	VGA connector	5	Front USB port
3	Plug connection to the server blade. The labeled side of the plug must face left when plugged in.		

i The Y-cable is delivered with the system unit.

5.4 Instructions for connecting/disconnecting cables

CAUTION!

Be sure to read the documentation for the peripheral devices before connecting them.

Do not connect or disconnect data cables during a thunderstorm.

When removing a cable, always hold it by the plug. Never unplug a cable by pulling at the cable itself.

Connect and disconnect the cables in the order described below.

Connecting cables

| i | For peripherals like keyboard, mouse, display, optical drive, etc. Advanced Video Redirection and Virtual Media connection by iRMC is recommended. |

► Turn off the power of the target server blade and all peripherals.

► Disconnect all power plugs of the peripherals from the grounded shockproof sockets.

► Connect the Y-cable to the server blade.

► Connect all peripherals to the connectors of the Y-cable.

► Plug all power plugs of the peripherals to the grounded shockproof sockets.

Disconnecting cables

► Turn off the target server blade.

► Turn off the all connected peripherals

► Disconnect all power plugs of the peripherals from the grounded shockproof sockets.

► Disconnect all peripherals from the Y-cable.

► Disconnect the Y-cable from the server blade.

Using the Y-cable

> **i** When engaging between the Y-cable connector and the server blade connector is strong, and the Y cable is detached as it is, the Y-cable connector might be damaged.
>
> Therefore, please remove the Y-cable as follows.

Procedure for detaching the Y-cable

While strongly pushing the hook of the Y-cable connector (server blade side : 2 points),

– push it toward the server blade strongly,

– and remove it straight
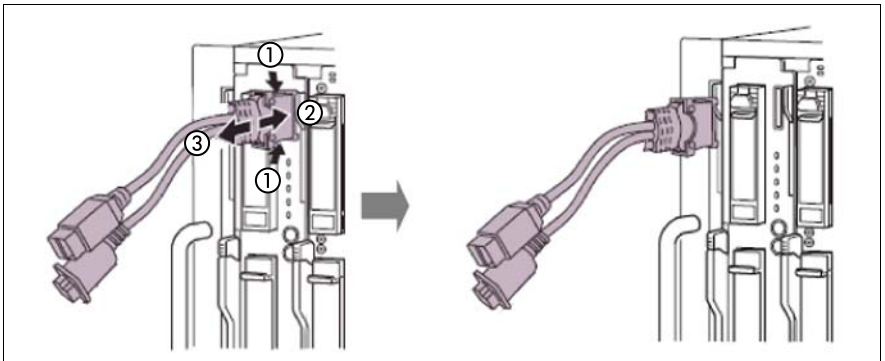
Figure 6: BX900 / BX400 system unit (rack version)
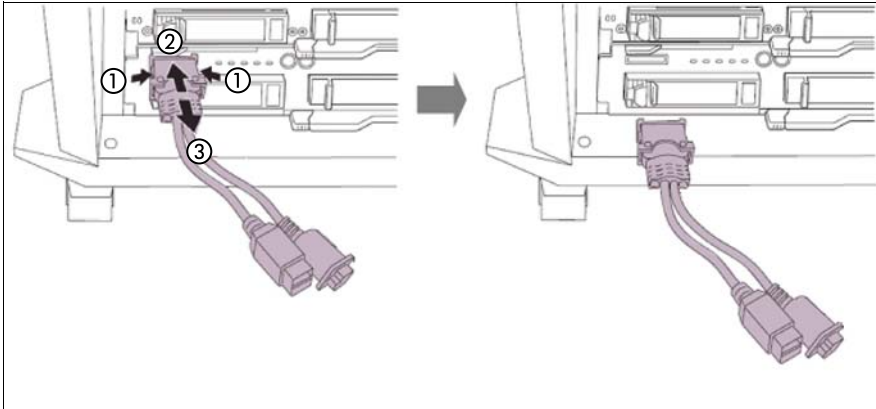
Figure 7: BX400 S1 system unit (floorstand version)

 Important

● You may find it difficult to remove the Y-cable because the load hangs in the join with the Y-cable connector.

  Therefore make sure it is straight when you remove it.

● Do not leave a Y-cable connected.

● Do not close the rack door while the Y-cable is connected, to avoid damaging the Y-cable.

6 Starting up and operation

⚠️ **CAUTION!**

Follow the safety instructions in the chapter "Important information" on page 27.

6.1 Control and display elements
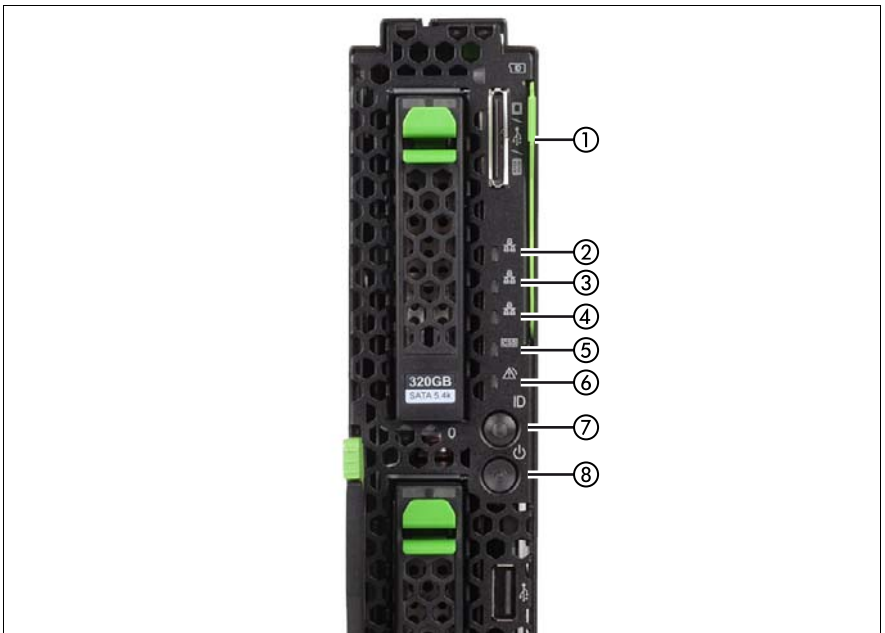
Figure 8: Control and display elements

1	ID card	5	CSS indicator
2	I/O indicator: fabric 3/4	6	Global Error indicator
3	I/O indicator: fabric 2	7	ID button with ID indicator
4	I/O indicator: fabric 1	8	On/Off button with power indicator

Control elements

On/Off button

When the server blade is switched off, it can be switched on again by pressing the On/Off button.

When the server blade is operating, pressing the On/Off button will switch off the server blade .

CAUTION!

Risk of loss of data!

The On/Off button does not disconnect the server blade from the mains voltage. To disconnect it from the mains completely, remove it from the system unit.

ID   ID button

Lights up (blue) on the front of the server blade when the ID button is pressed.

If the ID button is pressed for more than 5 seconds, released and pressed again within 1 second, an NMI is issued.

LEDs on the control panel

Power indicator (three-color)

Does not light up if no line voltage is present.

Lights orange when the server is switched off but line voltage is present.

Lights yellow to indicate a power supply error.

Lights up green when the server is switched on.

Flashes green when the server has been switched on and is in standby mode.

Global Error indicator (orange)

– **Lights up orange** if a prefailure event has been detected that requires (precautionary) service intervention.
– **Flashes orange** if an error was detected that requires service intervention.
– **Does not light up** if there is no critical event.

If the event is still acute after a power failure, the indicator is activated after the restart.

The indicator also lights up in standby mode.

You can find more details on the indicated errors in the System Event Log (SEL), in the Management Blade Web interface, on the ServerView Local Service Panel, on the ServerView Local Service Display, in the ServerView Operations Manager or via the iRMC S4's Web interface.

CSS CSS indicator (yellow)

– **Lights up yellow** if a prefailure event was detected for a CSS component that you can fix yourself (for reasons of precaution) with the CSS concept.
– **Flashes yellow** if an error was detected that you can fix yourself with the CSS concept.
– **Does not light up** when the system is OK.

If the event is still acute after a power cycle, the indicator is activated after the restart.

The indicator also lights up in standby mode.

For more information on the CSS concept, see "Customer Self Service (CSS)" on page 13.

ID ID indicator (blue)

Lights up blue when the system has been selected by pressing the ID button. To deactivate, press the button again.

The ID indicator can also be activated via the ServerView Operations Manager, the Management Blade web interface and the iRMC S4 web interface. Its status is reported to the ServerView Operations Manager and the iRMC S4.

I/O indicators* (green)

– **Lights up** to indicate a network connection.
– **Flashes** to indicate an active network connection.
– **Does not light up** if there is no network connection.

* The three I/O fabrics of the server blade are:

– Fabric 1: onboard CNA controller
– Fabric 2: mezzanine card 1
– Fabric 3/4: mezzanine card 2

ID card

You can pull out the ID card (see) as far as it will go and push it back in again.

The ID card contains various system information, such as the product name, serial number, order number, MAC addresses and DNS name.

6.2 Switching the Server Blade on and off

⚠️ **CAUTION!**

If you switch the server blade on and flickering stripes appear on the connected monitor, switch the server blade off again immediately (see chapter "Troubleshooting and tips" on page 63).

The On/Off button does not disconnect the device from the mains. To fully disconnect the device from the mains, you must remove the server blade from the system unit or switch off the system unit and unplug the power plug(s).

Using the control panel to switch the Server Blade on and off

The system unit is switched on and the power-on indicator (item 8 in figure 8 on page 47) is flashing green.

The server blade can be switched on and off as follows:

– To switch the server blade on, press the On/Off button on the server blade (item 8 in figure 8 on page 47).

  To switch the server blade off, hold down the On/Off button on the server blade (item 8 in figure 8 on page 47) for 4 seconds.

  Defined switch-On/Off time

  The server blade is switched on and off at the times defined in the *ServerView Operation Manager*.

Other On/Off options

– **After power failure**

  Once a server blade has been switched on, it will switch itself on again automatically after a power failure (irrespective of the setting in the BIOS Setup).

ℹ️ You can also switch the server blade on and off via the system unit control panel or via the Web interface of the ServerView Management Blade. Detailed information is provided in the manuals "PRIMERGY BX900 Blade Server Systems ServerView Management Blade S1 User Interface Description" or "PRIMERGY BX400 Blade Server Systems ServerView Management Blade S1 User Interface Description".

6.3 Configuring the Server Blade

This section contains information about configuring the server blade and installing the operating system.

The operating system can be installed in various ways:

– Local installation with or without the ServerView Installation Manager

   You can find information on local installation in the following sections.

– Remote installation using console redirection via the user interface of the ServerView Management Blade. Please refer to the following manuals for more information on Advanced Video Redirection:

   – "PRIMERGY BX900 Blade Server Systems ServerView Management Blade S1 User Interface Description"
   – "PRIMERGY BX400 Blade Server Systems ServerView Management Blade S1 User Interface Description"
   – "iRMC S4 - integrated Remote Management Controller" user's guide (on the Fujitsu manuals server under *Industry Standard Servers - Software - ServerView Suite - Out-Of-Band Management*)

   Apart from this, the operating system installation is carried out in the same way as a local installation.

– Importing the clone images from an image repository to the desired server blades.

   For more information about this procedure, see the "ServerView Deployment Manager 5.0" manual (on the Fujitsu manuals server under *Industry Standard Servers - Software - ServerView Suite - Server Installation and Deployment*).

6.3.1 Preparing for local installation

Connect the monitor, mouse, keyboard and a DVD drive to the port on the server blade control panel with the aid of the special Y cable. See .

> **i** Make sure that the energy saving functions are disabled in the *Power* menu of the BIOS Setup during operation, and that the DVD drive has been activated as a boot medium.

6.3.2 Preparation for remote installation to use Advanced Video Redirection

Advanced Video Redirection (AVR) can be used with the iRMC Web user interface and the Management Blade Web user interface. This section describes how to prepare for using the Web user interface for management blades.

> **i** For using the iRMC Web user interface, please refer to the "iRMC S4 - integrated Remote Management Controller" User's Guide (*Industry Standard Servers - Software - ServerView Suite - Out-Of-Band Management* on the Fujitsu manuals server.

1. The remote management terminal is connected to the network.

   The remote control terminal (e.g. PC) is connected to a network that can connect to the management blade.

2. Network configuration

   Network settings for the remote management terminal, management blade and iRMC.

   a) **Remote management terminal**

      ► Setup a remote network management station, if necessary.

   b) **Management blade**

      ► Start your Web browser on the remote control terminal and log on to the Management Blade Web user interface.

      For details of the Management Blade Web user interface, please refer to the PRIMERGY BX400 Blade Server or PRIMERGY BX900 Blade Server manuals or the manual "ServerView Management Blade S1 User Interface Description", chapter 4 "Web User Interface".

      ► Network setting of the management blade (Management LAN)

      From the navigation frame of the Management Blade Web user interface, select each section: *Setting - System Unit - Network Interface - Management LAN*.

      Then set the network of the management blade on the "Ethernet" tab.

> **i** For the PRIMERGY BX400 system unit, log onto the blade server and then switch to the Web user interface (Advanced) via the "Experience" drop-down list in the top right.

c) **iRMC**

1. Start your Web browser on the remote control terminal and log on to Management Blade Web user interface.

2. Setting the iRMC network

   ► From the navigation frame of the Management Blade Web user interface, select each section: *Components - Server Blades - Server Blade*-x.

   ► Then set the network of the iRMC in the "iRMC Address Configuration" box.

   For how to set the network, please refer to the "iRMC S4 - integrated Remote Management Controller" User's Guide (chapter 3, "Configuring the iRMC S4" under *Industry Standard Servers - Software - ServerView Suite - Out-Of-Band Management* on the Fujitsu manuals server.

   ► If you want to use AVR from the remote control terminal connected to the management LAN port of the management blade, the LAN port of the iRMC must be set to "Management LAN".

   ► In addition, the iRMC and management LAN port of the management blade must also be set to the same network address.

3. Start the video redirection

   ► The Video Redirection button will appear on the status frame when you select each section: *Components - Server Blades - Server Blade-x*.
   Click this button to open the console screen of the server blade.

   For details of the Management Blade Web user interface, please refer to the "ServerView Management Blade S1 User Interface Description" for the PRIMERGY BX400 Blade Server and the PRIMERGY BX900 Blade Server.

   > **i** For more on AVR and Virtual Media, please refer to the "iRMC S4 - integrated Remote Management Controller" User's Guide ("Advanced Video Redirection (AVR)" in chapter 5 and "Virtual

Media Wizard" in chapter 6 under *Industry Standard Servers - Software - ServerView Suite - Out-Of-Band Management* on the Fujitsu manuals server.

6.3.3 Configuring the onboard SAS/SATA controller

A SAS/SATA controller is integrated on the system board. You can configure the onboard controller either before or during installation with the ServerView Installation Manager. Using the ServerView Installation Manager is recommended.

i A separate utility is available to the controller for MegaRAID configuration. For further information, refer to the "SAS Software User's Guide" (on the Fujitsu manuals server under *Industry Standard Servers - Expansion Cards - Storage Adapters - LSI Configuration Software)*

Further information on modular RAID controllers is provided in the "Modular RAID Controller Installation Guide" (on the Fujitsu manuals server under *Industry Standard Servers - Expansion Cards - Storage Adapters - LSI SAS / SCSI RAID Controllers*).

i The SAS functionality needs to be enabled separately by using an onboard SAS enabling key.

i Descriptions of operating systems not covered in the controller manual are provided in the corresponding readme under:

http://www.fujitsu.com/global/services/computing/server/ia/driver/index.html (for the EMEA market).
http://jp.fujitsu.com/platform/server/primergy/downloads/ (for the Japanese market).

i In the system BIOS the onboard SAS/SATA controller can be configured as "RAID" (default) or "non-RAID".

6.3.4 Configuring the SAS/SATA RAID controller

The server blade has a SAS/SATA RAID controller with "MegaRAID functionality". You can configure the SAS/SATA RAID controller either before or during installation with the ServerView Installation Manager. Using the ServerView Installation Manager is recommended.

i	A separate utility is available to the controller for MegaRAID configuration. For further information, refer to the "SAS Software User's Guide" (on the Fujitsu manuals server under *Industry Standard Servers - Expansion Cards - Storage Adapters - LSI Configuration Software*).

Further information on modular RAID controllers is provided in the "Modular RAID Controller Installation Guide" (on the Fujitsu manuals server under *Industry Standard Servers - Expansion Cards - Storage Adapters - LSI SAS / SCSI RAID Controllers*).

i	Descriptions of operating systems not covered in the controller manual are provided in the corresponding readme under:

http://www.fujitsu.com/global/services/computing/server/ia/driver/index.html (for the EMEA market).

http://jp.fujitsu.com/platform/server/primergy/downloads/ (for the Japanese market).

6.3.5 Configuring the onboard CNA controller

A CNA controller is integrated on the system board. You can configure the onboard CNA controller either before or during installation with the ServerView Installation Manager. Using the ServerView Installation Manager is recommended.

i	The onboard CNA controller has its own configuration utility. Please refer the onboard CNA controller manuals as follows:

http://cmw3wbq1.emulex.com/downloads/fujitsu-technology-solutions.html (for the EMEA market).
http://jp.fujitsu.com/platform/server/primergy/manual/ (for the Japanese market).

6.3.6 Configuring the server and installing the operating system with the ServerView Installation Manager

Using the ServerView Installation Manager on the ServerView Suite DVD provided, you can conveniently configure the server and install the operating system. This includes configuring the server-specific settings using the ServerView Configuration Manager and configuring the RAID controller using the **ServerView RAID Manager**.

Advantages of the ServerView Installation Manager

– Wizard assisted configuration of your server hardware and disk arrays

– Wizard assisted installation of all leading server operating systems

– Wizard-assisted creation of configuration files for unattended installation of several PRIMERGY servers with identical hardware configurations.

– Installation of drivers and additional software.

> **i** The software that can be installed depends on your server's hardware configuration. This configuration is detected automatically.

> **i** Descriptions of operating systems not covered in the RAID controller manual are provided in the corresponding readme files under:

http://www.fujitsu.com/global/services/computing/server/ia/driver/index.html
(for the EMEA market).

http://jp.fujitsu.com/platform/server/primergy/downloads/
(for the Japanese market).

To find out how to operate the ServerView Installation Manager and for further information, refer to the associated manual.

If you are using the ServerView Installation Manager, you can skip the following section on how to configure the server and install the operating system. Continue from section .

6.3.7   Configuring the server and installing the operating system without ServerView Installation Manager

Configuring the onboard SAS/SATA controller

Configure the controller as described in section "Configuring the onboard SAS/SATA controller" on page 55.

Configuring the SAS/SATA RAID controller with "MegaRAID functionality"

Configure the controller as described in section "Configuring the SAS/SATA RAID controller" on page 55.

Configuring the onboard CNA controller

Configure the controller as described in section "Configuring the onboard CNA controller" on page 57.

Installing the operating system

► Insert the DVD for the operating system you want to install.

► Reboot the server blade.

► Follow the instructions on screen and in the manual for the operating system.

6.4   Cleaning the Server Blade

⚠ **CAUTION!**

Switch off the server blade and remove it from the system unit (see page 40).

Do not clean any interior parts of the server blade yourself; leave this job to a service technician.

Do not use abrasive powder or detergents which dissolve plastic to clean the housing exterior.

Make sure that no liquid gets inside the device and that the ventilation slits on the Server Blade remain open.

Wipe the server blade housing with a dry cloth to clean. If it is very dirty you can use a damp cloth that has been dipped in water with a mild detergent and well wrung out.

7 Property and data protection

The lockable rack door protects the server against unauthorized access.

To protect the system and data internally against unauthorized access, you can activate the security functions of the *BIOS Setup*.

7.1 BIOS Setup security functions

The *Security* menu in the *BIOS Setup* provides you with various options for protecting your data from unauthorized access. By combining these options, you can also achieve optimum protection for your system.

> **i** A detailed description of the *Security* menu and how to assign passwords can be found in the *BIOS Setup* documentation on the Fujitsu manuals server.

Preventing unauthorized BIOS Setup calls

You can activate this protection by entering a setup password in the *Security* menu. You can also suppress the `Press F2 for Setup` message in this menu. This message is then no longer displayed while the server's startup routine is in progress.

Preventing unauthorized system access

You can activate this protection by entering a system password in the *Security* menu.

Preventing unauthorized access to the boards with their own BIOS

You can activate this protection by selecting the *Extended* item for *Setup Password Lock* field in the *Security* menu.

Protecting BIOS from being overwritten

To activate this protection, select the value *Disabled* for the *Flash Write* field in the *Security* menu.

8 Troubleshooting and tips

⚠️ **CAUTION!**

Follow the safety instructions in the "Safety notes and regulations" manual or " 安全上のご注意 " and in chapter "Important information" on page 27.

If a fault occurs, attempt to resolve it using the measures described:

– in this chapter,
– in the documentation for the connected devices,
– in the help systems of the software used.

If you fail to correct the problem, proceed as follows:

► Make a list of the steps performed and the circumstances that led to the fault. Also make a list of any error messages that were displayed.

► Switch off the server.

► Contact our customer service team.

8.1 Server switches itself off

Server Management has detected an error

► Check the Event Log of the management blade or – if ServerView Operations Manager is installed – its error list or the ErrorLog file, and attempt to eliminate the error.

8.2 Screen remains blank[1]

Monitor is switched off

► Switch on your monitor.

Screen has gone blank

► Press any key on the keyboard.

---

[1] In the case of a monitor connected locally via the Y cable, see "Connecting devices" on page 42.

or

► Deactivate screen saver. Enter the appropriate password.

Brightness control is set to dark

► Set the brightness control on the monitor to light. For detailed information, refer to the operating manual supplied with your monitor.

Power cable or monitor cable not connected

► Switch off the monitor and the server.

► Check whether the power cable is properly connected to the monitor and to the grounded socket.

► Check whether the monitor cable is properly connected to the server and monitor (if it is plugged in with a connector).

► Switch on the monitor and the server.

8.3 Flickering stripes on monitor screen[1]

⚠ **CAUTION!**

Switch off the server immediately. Risk of damaging the server.

Monitor does not support the set horizontal frequency

► Find out which horizontal frequency your monitor screen supports. You will find the horizontal frequency (also known as line frequency or horizontal deflection frequency) in the documentation for your monitor.

► Refer to the documentation for your operating system or the software for the screen controller for details of how to set the correct horizontal frequency for your monitor, and follow the procedure accordingly.

---

[1] In the case of a monitor connected locally via the Y cable, see .

8.4   No screen display or display drifts[1]

The wrong horizontal frequency or resolution has been selected for the monitor or for the application program.

► Find out which horizontal frequency your monitor screen supports. You will find the horizontal frequency (also known as line frequency or horizontal deflection frequency) in the documentation for your monitor.

► Refer to the documentation for your operating system or the software for the screen controller for details of how to set the correct horizontal frequency for your monitor, and follow the procedure accordingly.

8.5   Incorrect date and time

► Set the date and time in the operating system or in the BIOS Setup under the Main menu, using System Date and System Time respectively.

> **i** Note that the operating system may affect the system time. For example, the operating system time may deviate from the system time under Linux, and would overwrite the system time in the default setting on shutdown.

If the date and time are still wrong after the server has been switched off and back on again, replace the lithium battery (for a description refer to the PRIMERGY BX920 S4 Server Blade Upgrade and Maintenance Manual) or contact our customer service team.

8.6   System will not boot

The system will not boot after installing a new hard disk drive.

SAS configuration incorrect

► Check the settings for the hard disk drives (SAS Device Configuration) and the additional settings in the SAS configuration menu.

---

[1] In the case of a monitor connected locally via the Y cable, see .

Power budget limit value exceeded

► Check whether the power budget limit value set in the management blade has been exceeded. You may need to install an additional power supply unit.

8.7 Hard disk drive error messages at system boot

Various hard disk drive error messages may appear when the system is rebooted. These error messages are caused by modifications in the selected RAID configuration.

RAID controller configuration incorrect

► Check and correct the settings for the drives using the RAID controller configuration program.

Further information can be found in the operating manual for the RAID controller.

8.8 Added drive reported as defective

RAID controller is not configured for this drive

The drive was probably installed when the system was switched off.

► Reconfigure the RAID controller for the drive using the corresponding utility. Information is provided in the documentation for the RAID controller.

8.9 Error message on screen

The meaning of the error message is explained in the documentation for the relevant components and programs on the Fujitsu manuals server.