

User Guide - English



FUJITSU Software ServerView Suite

iRMC S4

Configuration and Maintenance

Edition March 2017

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 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

Copyright 2017 FUJITSU LIMITED.

All rights reserved.

Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

Contents

1 Preface	5
1.1 Purpose and target groups	6
1.2 ServerView Suite link collection	6
1.3 Documentation for the ServerView Suite	8
1.4 Documents for the iRMC	8
1.5 What's new	8
1.6 Notational conventions	9
2 Overview	10
2.1 Overview of the iRMC functions	10
2.1.1 Standard functions	10
2.1.2 Extended functions	14
2.2 User interfaces of the iRMC S4	16
2.3 Communication protocols used by the iRMC	17
2.4 Embedded Lifecycle Management	18
2.5 Front panel LEDs controlled by the iRMC	19
3 First Steps	20
3.1 Configuration of the LAN interface	20
3.1.1 Prerequisites	20
3.1.2 Configuring the LAN interface using the UEFI setup utility	21
3.1.3 Testing the LAN interface	23
3.2 Logging in to the iRMC S4 for the first time	23
3.2.1 Requirements	23
3.2.2 iRMC factory defaults	24
3.2.3 Logging in	24
3.2.4 Logging out	25
4 User management	26
4.1 User management concept	26
4.2 User permissions	29
4.3 Local user management for the iRMC S4	30
4.3.1 Local user management using the iRMC web interface	30
4.3.2 Local user management using the Server Configuration Manager	31

4.3.3 Secure Authentication via SSHv2	31
4.3.3.1 Creating public and private SSHv2 keys	32
4.3.3.2 Uploading the public SSHv2 key	34
4.3.3.3 Using the public SSHv2 key	35
4.3.3.4 Example: Public SSHv2 key	39
5 Remote installation of the operating system	41
5.1 General procedure for installing the operating system	41
5.2 Connecting a storage medium as Virtual Media	43
5.3 Booting the managed Server	44
5.4 Installing Windows on the managed server	47
5.5 Installing Linux on the managed server	48
6 Firmware update	50
6.1 Firmware Selector	51
6.2 Firmware image downgrade	51
6.3 Firmware image update	52
6.3.1 Setting up the USB memory stick	53
6.3.2 Updating using the flash tools	55
6.3.3 Emergency flash	56
6.4 FlashDisk menu	57
6.4.1 Updating via the FlashDisk menu	58
6.5 Flash Tools	59

1 Preface

Modern server systems are becoming increasingly complex. The requirements with respect to the management of such systems are growing accordingly.

In response to this development, a number of vendors founded the "Intelligent Platform Management Interface" (IPMI) initiative with the objective of defining a standardized, abstract, message-based interface between the central system controller (Baseboard Management Controller - BMC) and intelligent hardware for platform management. For further information on IPMI, refer to the "iRMC S4 - Concepts and Interfaces" user guide.

The integrated Remote Management Controller iRMC represents a BMC with integrated LAN connection and extended functions. In this way, the iRMC offers comprehensive control over PRIMERGY servers, irrespective of the system status. In particular, the iRMC allows for out-of-band management (Lights Out Management, LOM) of PRIMERGY servers. Out-of-band management uses of a dedicated management channel that enables a system administrator to monitor and manage servers via remote control regardless of whether the server is powered on.

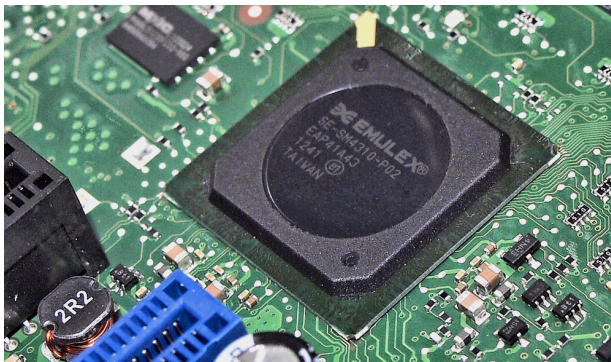


Figure 1: iRMC S4 on the system board of a PRIMERGY server

As an autonomous system on the system board of a modern PRIMERGY server, the iRMC has its own operating system, its own web server, separate user management and independent alert management. The iRMC remains powered up even when the server is in stand-by mode.

Beyond making it possible to manage a PRIMERGY server out-of-band, the enhanced functions of the newest version of the iRMC, which comes with an integrated SD card, allows for comprehensive lifecycle management of a PRIMERGY server. As lifecycle management is largely integrated ("embedded") in and entirely controlled by the iRMC, it is called "embedded Lifecycle Management (eLCM)".

Some eLCM functions require the iRMC to communicate and cooperate with the ServerView Agentless Service running on the managed server. Communicating with the ServerView Agentless Service also provides the iRMC with additional in-band information.

1.1 Purpose and target groups

This user guide is aimed at system administrators, network administrators, and service staff who have a sound knowledge of hardware and software. It provides basic information on the configuration of the iRMC and deals with the following aspects in detail:

- The Introduction provides the basic facts of the iRMC's functions.
- The First Steps provide information about the LAN connection and how to log on to the iRMC.
- iRMC Configuration gives an overview of the possibilities to configure the iRMC.
- User management comprises the iRMC related user management.
- Firmware Update describes the firmware update of the iRMC.
- Remote installation of the operating system via iRMC

1.2 ServerView Suite link collection

Via the ServerView Suite link collection, Fujitsu provides you with numerous downloads and further information on the ServerView Suite and PRIMERGY servers.

Under **ServerView Suite**, links are offered on the following topics:

- Forum
- Service Desk
- Manuals
- Product information
- Security information
- Software downloads
- Training

 **Software downloads** includes the following downloads:

- Current software statuses for the ServerView Suite as well as additional Readme files.
- Information files and update sets for system software components (BIOS, firmware, drivers, ServerView Agents and ServerView Update Agent) for updating the PRIMERGY servers via ServerView Update Manager or for locally updating individual servers via ServerView Update Manager Express.
- The current versions of all documentation on the ServerView Suite.

You can retrieve the downloads free of charge.


Under **PRIMERGY Server**, links are offered on the following topics:

- Service Desk
- Manuals
- Product information
- Spare parts catalogue

Access to the ServerView Suite link collection

You can reach the link collection of the ServerView Suite in various ways:

1. Via ServerView Operations Manager.
 - Select **Help – Links** on the start page or the menu bar.
2. Via the start page of the online documentation for the ServerView Suite on the Fujitsu manual server.

 You access the start page of the online documentation via the following link:

<http://manuals.ts.fujitsu.com>

- In the selection list on the left, select **x86 Servers**.
 - On the right, click **PRIMERGY ServerView Links** under **Selected documents**.
3. Via the ServerView Suite DVD 2.
 - In the start window of the ServerView Suite DVD 2, select the option **ServerView Software Products**.
 - On the menu bar select **Links**.

This opens the start page of the ServerView Suite link collection.

1.3 Documentation for the ServerView Suite

The documentation can be downloaded free of charge from the Internet. You will find the online documentation at <http://manuals.ts.fujitsu.com> under the link **x86 Servers**.

ServerView Sitemap

For an overview of the documentation to be found under **ServerView Suite** as well as the filing structure, refer to the [ServerView Suite Sitemap](#):

1. In the selection list on the left, select **x86 Servers** and then **Software**.
2. On the right, select **ServerView Suite**.
3. Click **ServerView Suite Sitemap** under **Selected documents**.

1.4 Documents for the iRMC

This manual is part of a documentation suite describing the iRMC S4 up to firmware version 8.8. The documentation suite of the iRMC S4 comprises the following manuals:



- iRMC S4 Web Interface
- iRMC S4 Configuration and Maintenance
- iRMC S4 Concepts and Interfaces

1.5 What's new

The manual has been optimized but no functional changes are made in regard of configuration and maintenance.

1.6 Notational conventions

The following notational conventions are used in this manual:

Notational conventions	Indicates
	Indicates various types of risks, namely health risks, risk of data loss and risk of damage to devices.
	Indicates additional relevant information and tips.
Bold	Indicates references to names of interface elements.
<code>monospace</code>	Indicates system output and system elements, for example file names and paths.
monospace semibold	Indicates statements that are to be entered using the keyboard.
blue continuous text	Indicates a link to a related topic.
purple continuous text	Indicates a link to a location you have already visited.
<abc>	Indicates variables which must be replaced with real values.
[abc]	Indicates options that can be specified (syntax).
[Key]	Indicates a key on your keyboard. If you need to explicitly enter text in uppercase, the Shift key is specified, for example [Shift] + [A] for A. If you need to press two keys at the same time, this is indicated by a plus sign between the two key symbols.

Screenshots

The screenshots are to some degree system-dependent and consequently will not necessarily match the output on your system in all the details. The menus and their commands can also contain system-dependent differences.

2 Overview

2.1 Overview of the iRMC functions

The iRMC supports a wide range of functions that are provided by default. With Advanced Video Redirection (AVR) and Virtual Media, the iRMC also provides two additional advanced features for the remote management of PRIMERGY servers.

To use AVR, Virtual Media and embedded Life cycle Management (eLCM), you require a valid license key, which can be purchased separately.

2.1.1 Standard functions

Browser access

The iRMC features its own web server which can be accessed by the management station from a standard web browser.

Security (SSL, SSH)

Secure access to the web server and secure graphical console redirection, including mouse and keyboard, can be provided via HTTPS/SSL. An encrypted connection protected by SSH mechanisms can be set up to access the iRMC using the Remote Manager. The Remote Manager is an alphanumeric user interface for the iRMC.

ServerView integration

The ServerView Agents detect the iRMC and automatically assign it to the relevant server. This means that it is possible to start the iRMC web interface and text console redirection using the ServerView Remote Management front end directly from ServerView Operations Manager.

Communication between the iRMC and the ServerView Agentless Service (as of ServerView Operations Manager 7.0) allows for enhanced out-of-band management of PRIMERGY servers.

Power management

Irrespective of the status of the system, you have the following options for powering the managed server on or off from the remote workstation:

- Using the iRMC web interface
- Using the Remote Manager and the command line interface (CLP)
- With a script

Power consumption control

The iRMC allows comprehensive control of power consumption on the managed server. You

can also specify the mode (minimum power consumption or maximum performance) that the iRMC uses to control power consumption on the managed server. You can switch between these modes as required.

Customer Self Service (CSS)

Summary tables for the server components, sensors and the power supply on the iRMC web interface provide information in a separate column as to whether the server component affected is a CSS component or not. In addition, the error list of the system event log (SEL) shows whether each event has been triggered by a CSS component.

Text console redirection

You can start a Telnet/SSH session to the iRMC from the ServerView Remote Management front end. This calls the Remote Manager, via which you can start a text console redirection session.

Basic functions of a BMC

The iRMC supports the basic functions of a BMC such as voltage monitoring, event logging and recovery control.

"Headless" system operation

The managed server does not require a mouse, monitor or keyboard to be connected. The benefits of this include lower costs, much simpler cabling in the rack and increased security.

Identification LED

To facilitate identification of the system, for instance if it is installed in a fully populated rack, you can activate the identification LED from the iRMC web interface.

Global error LED

A global error LED indicates the status of the managed system at all times and also shows the CSS status.

Power LED

The power LED tells you whether the server is currently switched on or off.

S5 LED

The S5 LED indicates the power status of the server.

CIM support

The iRMC supports CIM-XML, WS-Man and SMASH CLP (System Management Architecture for Server Hardware Command Line Protocol).

LAN

On some systems, the LAN interface of the fitted system NIC (Network Interface Card) on the server is reserved for the management LAN. On other systems, you have the option of configuring this LAN interface to:

- Reserve it for the management LAN
- Set it up for shared operation with the system
- Make it completely available to the system

The ports marked with a wrench symbol are assigned to the iRMC.

Network bonding

Network bonding for the iRMC is designed for redundancy in the event of Ethernet network adapter failures. Thus, iRMC network management traffic is protected from loss of service due to failure of a single physical link.

The iRMC supports the active-backup mode, i.e. one port is active until the link fails, then the other port takes over the MAC and becomes active.

SNMPv1/v2c/v3 support

You can configure an SNMP service on the iRMC which supports SNMPv1/v2c/v3 GET requests on SNMP SC2 MIB (Sc2.mib), SNMP MIB-2, SNMP OS.MIB and SNMP STATUS.MIB.

When the SNMP service is enabled, information on devices such as fans, temperature sensors etc. is available via the SNMP protocol and can be viewed on any system running an SNMP Manager.

Command line interface (CLP)

In addition to the Remote Manager, the iRMC also supports SMASH CLP as standardized by the DMTF (Distributed Management Task Force).

Simple configuration - interactive or script-based

The following tools are available for configuring the iRMC:

- iRMC web interface
- Server Configuration Manager
- UEFI BIOS Setup

It is also possible to perform configuration with the Server Configuration Manager or IPMIVIEW using scripts. This means you can configure the iRMC when the server is first configured via ServerView Installation Manager. You can also configure a large number of servers on the basis of scripts.

Support for the LocalView service panel

If PRIMERGY servers are equipped with a ServerView local service panel, this module allows you to determine which module is faulty and whether you can replace it yourself.

Local user management

The iRMC has its own user management function which allows up to 16 users to be created with passwords and to be assigned various rights depending on the user groups they belong to.

Global user management using a directory service

The global user IDs for the iRMC are stored centrally in the directory of the directory service. This allows the user identifications to be managed on a central server. They can therefore be used by all the iRMCs that are connected to this server in the network.

The following directory services are currently supported for iRMC user management:

- Microsoft® Active Directory
- Novell® eDirectory

- OpenLDAP
- OpenDS, Open DJ, Apache DS

CAS-based single sign-on (SSO) authentication

The iRMC supports Centralized Authentication Service (CAS) configuration, which allows you to configure the iRMC web interface for CAS-based SSO authentication.

The first time a user logs in to an application (e.g. the iRMC web interface) within the SSO domain of the CAS service, they are prompted for their credentials by the CAS-specific login screen. Once they have been successfully authenticated by the CAS service, the user is granted access to the iRMC web interface as well as to any other service within the SSO domain without being prompted for login credentials again.

DNS / DHCP

The iRMC provides support for automatic network configuration. It has a default name and DHCP support is set by default so that the iRMC gets its IP address from the DHCP server. The iRMC name is registered by the Domain Name System (DNS). Up to five DNS servers are supported. If DNS/DHCP is not available, the iRMC also supports static IP addresses.

Power supply

The iRMC is powered by the standby supply of the system.

Alert management

The alert management facility of the iRMC provides the following options for forwarding alerts:

- Platform Event Traps (PET) are sent via SNMP.
- Direct alerting by email.

The iRMC also provides the ServerView Agents with all the relevant information.

Read, filter and save the system event log (SEL)

You can view, save and delete the contents of the SEL by using several interfaces:

- The iRMC web interface
- The Telnet/SSH-based interface (Remote Manager) of the iRMC

Read, filter and save the internal event log (iEL)

You can view, save and delete the contents of the iEL by using several interfaces:

- The iRMC web interface
- The Telnet/SSH-based interface (Remote Manager) of the iRMC

UEFI support

Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system. UEFI has a firmware validation process, called secure boot. Secure boot defines how platform firmware manages security certificates, validation of firmware, and a definition of the interface (protocol) between firmware and the operating system.

2.1.2 Extended functions

Alongside the standard functions, the iRMC also supports Advanced Video Redirection, Virtual Media and embedded Life cycle Management (eLCM).

Advanced Video Redirection (AVR)

The iRMC supports Advanced Video Redirection, which offers the following benefits:

- Operation via a standard web browser. No additional software needs to be installed on the management station other than the Java Runtime Environment if the Java applet is used. Otherwise the web browser must be able to interpret HTML5.
- System-independent graphical and text console redirection (including mouse and keyboard).
- Remote access for boot monitoring, BIOS administration and operation of the operating system.
- AVR supports up to two simultaneous “virtual connections” for working on a server from a different location. It also reduces the load on the network by using hardware and video compression.
- Local monitor-off support: It is possible to power down the local screen of the managed PRIMERGY server during an AVR session in order to prevent unauthorized persons from observing user input and actions carried out on the local server screen during the AVR session.
- Low bandwidth
If the data transfer rate is slow, you can configure a lower bandwidth (bits per pixel, bpp) in terms of color depth for your current AVR session.

Virtual Media

The Virtual Media function makes a “virtual” drive available which is physically located on a remote workstation or made available centrally on the network using the Remote Image Mount functionality.

The virtual drives available with Virtual Media are simply managed in much the same way as local drives and offer the following options:

- Read and write data
- Boot from Virtual Media
- Install drivers and small applications
- Update BIOS from remote workstation
- (BIOS update via USB)

Virtual Media supports the following device types to provide a virtual drive on the remote workstation:

- CD ROM
- DVD ROM
- Memory stick

- Floppy image
- CD ISO image
- DVD ISO image
- Physical hard disk drive
- HDD ISO image

The Remote Image Mount functionality provides ISO images centrally on a network share in the form of a virtual drive.

Embedded Lifecycle Management (eLCM)

The embedded Lifecycle Management (eLCM) solution allows you to control life cycle management of PRIMERGY servers with a few mouse clicks centrally from the iRMC web interface without the need to handle physical devices.

eLCM comprises the following functions:

- eLCM update management
- eLCM image management (Custom Image)
- eLCM deployment
- eLCM health management (PrimeCollect)

For further information refer to the "ServerView embedded Lifecycle Management (eLCM)" user guide.

Profile management

Using the profile management you can send and retrieve a full server configuration via the RESTful API.

Profile management supports the following functions:

- Create a profile (or sub-profile) inside the iRMC's profile store.
- Retrieve a profile (or sub-profile) from the iRMC's profile store.
- Apply a profile (or sub-profile) to the iRMC to be executed.
- Get session information that provides status and log information for creating and applying a profile.
- Control the version of a profile.

2.2 User interfaces of the iRMC S4

The iRMC provides the following user interfaces:

- **iRMC web interface (web interface)**

The connection to the iRMC web server is established via a standard web browser (e.g. Microsoft Internet Explorer, Mozilla Firefox).

Among other things, the web interface of the iRMC provides you with access to all system information and data from the sensors such as fan speeds, voltages, etc. You can also configure text-based console redirection and start graphical console redirection (Advanced Video Redirection, AVR). In addition, administrators can fully configure the iRMC over the web interface. Secure access to the iRMC web server can be provided with HTTPS/SSL.

Operation of the iRMC using the web interface is described in the "iRMC S4 - Web Interface" user guide

- **Remote Manager:** Text-based Telnet/SSH interface via LAN

You can call the Remote Manager:

- From the ServerView Remote Management Front end
- Directly from a Telnet/SSH client

The alphanumeric user interface of the Remote Manager provides you with access to system and sensor information, power management functions and the error event log. In addition, you can launch text console redirection or a SMASH CLP shell. If you call the Remote Manager over SSH (Secure Shell), the connection between the Remote Manager and the managed server is encrypted.

Operation of the iRMC using the Remote Manager is described in the "iRMC S4 - Concepts and Interfaces" user guide.

- **Remote Manager (Serial):** Text-based serial interface over Serial 1

The Remote Manager (serial) interface is identical to the Remote Manager interface.

2.3 Communication protocols used by the iRMC

The iRMC uses the following protocols and ports for communication:

Remote side of the connection	Communication direction	iRMC side of the connection (port no. / protocol)	Configurable	Enabled by default
RMCP	→	623/UDP	no	yes
	←	623/UDP		
HTTP port	→	80/TCP	yes	yes
	←	80/TCP		
HTTPS port	→	443/TCP	yes	yes
	←	443 TCP		
Telnet	→	3172/TCP	yes	no
	←	3172/TCP		
SSH	→	22/TCP	yes	yes
	←	22/TCP		
SNMP (general mess.)	→	161/UDP	yes	no
	←	162/UDP		
SNMP trap		162/UDP	no	yes
LDAP	→	389/TCP/UDP	yes	no
	←	389/TCP/UDP		
LDAP SSL	→	636/TCP/UDP	yes	no
	←	636/TCP/UDP		
Email/SMTP	→	25/TCP	yes	no
	←	25/TCP		
CIM	→	5988/CIM-XML	no	no
	←	5988/CIM-XML		
	→	80/WS-MAN	no	no
	←	80/WS-MAN		
REST	→	80/TCP	yes	yes
	←	80/TCP		

2.4 Embedded Lifecycle Management

As modern server systems are becoming increasingly complex, the requirements with respect to the management of these servers are growing accordingly. In response to this development, the out-of-band management (Lights Out Management, LOM) of servers is getting more and more into focus. Out-of-band management uses a dedicated management channel that enables a system administrator to monitor and manage servers via remote control regardless of whether the server is powered on.

Out-of-band management of a PRIMERGY server is provided by the integrated Remote Management Controller iRMC S4 which is part of most PRIMERGY servers. As an autonomous system on the system board of a PRIMERGY server, the iRMC S4 has its own operating system, its own web server, its own Linux file system, separate user management and independent alert management. The iRMC S4 remains powered on even when the server is in stand-by mode.

Beyond making it possible to manage a PRIMERGY server out-of-band, the enhanced functionality as of firmware version 7.6x of the iRMC S4, which comes with an integrated SD card, allows for comprehensive lifecycle management of a PRIMERGY server. As lifecycle management is largely integrated ("embedded") in and entirely controlled by the iRMC S4, it is called "embedded Lifecycle Management (eLCM)".

The ServerView Service Platform (SV SP) is used within embedded Lifecycle Management. It is an ISO image that is stored inside PRIMERGY servers on an optional eLCM SD card and is managed by eLCM.

The Service Platform provides the following functions:

- System configuration and installation: embedded Installation Manager (eIM)
- System diagnosis: embedded Diagnosis Manager (eDM)
- RAID management: embedded RAID Manager (eRM)

Different operation scenarios are supported for these functions:

Interactive operation via console (physical or redirected)

1. Power on the target system.
2. During POST (Power-On-Self-Test) press the [F5] key.
3. In the upcoming eLCM menu select the function to be used:
 - System configuration and installation
 - RAID configuration
 - System Diagnostics
4. After the platform has started follow the instructions displayed on the console.

Unattended operation via the iRMC web interface

1. Create a profile file specifying the intended system configuration and/or operating system installation. Profile handling is described in the "iRMC S4 - Concepts and Interfaces" user guide.
2. Start the iRMC web interface and open the **eLCM Deployment** page.
3. Set the intended boot mode either to Extensible Firmware Interface Boot (EFI) or PC compatible (legacy).
4. Upload the profile file.
5. Start the deployment process with **Activate**.

Unattended process "SysRollOut Service" via REST API

For further information refer to the REST API white paper.

2.5 Front panel LEDs controlled by the iRMC

The iRMC controls the status LEDs which are located on the front panel of the server. The LEDs and the layout of how they are arranged differ depending on the server type.

Status LEDs on the front panel (Nexperience design):

Status of the Server	LED on the Server	
	S5 LED (green)	Power LED (green)
AC-OFF	off	off
S5 (shutdown)	on	off
S0 (power on)	off	on
S3 (sleep mode)	off	blinking with 1 Hz (BIOS controlled)
iRMC not readyON	on	blinking with 0,5 Hz (iRMC controlled)
Power-on Delay	on	on

Status LEDs on the front panel (legacy design):

Status of the Server	Power LED on the Server
AC-OFF	off
S5 (shutdown)	orange
S0 (power on)	green
S3 (sleep mode)	blinking green with 1 Hz (BIOS controlled)
iRMC not ready	blinking alternately in orange/green with 1 Hz (iRMC controlled)
Power-on Delay	yellow

3 First Steps

The first steps in order to work with the iRMC are the following:

- Establish a LAN connection.
- Log in to the iRMC web interface.

3.1 Configuration of the LAN interface

You configure the LAN interface with the UEFI setup utility. Before you configure the LAN interface, there are some requirements to be met.

After configuration you test the LAN interface.

- **i** "Spanning Tree" tree for the connection of the iRMC must be deactivated (e.g. Port Fast=enabled; Fast Forwarding=enabled).

3.1.1 Prerequisites

Before you configure the LAN interface of the iRMC the following requirements must be met:

The LAN cable must be connected to the correct port.

The interface for a LAN connection is provided on an onboard LAN controller assigned to the iRMC.

Depending on the server type, the system board of a PRIMERGY server provides two or three LAN interfaces. The ports marked with a wrench symbol are assigned to the iRMC. Depending on the type of PRIMERGY server, different ports may be marked with the wrench symbol.

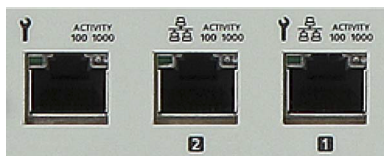





Figure 2: Ports for the iRMC (indicated by wrench symbol)

Icon	Meaning
	DedicatedService/Management LAN (port exclusively for the iRMC; with the iRMC a LAN speed up to 1000 MBit/s is available, depending on the server hardware)
	Management LAN (port exclusively for the system)
	Shared LAN (iRMC and system)

Two IP addresses are required

The LAN controller of the PRIMERGY server requires a separate IP address for the iRMC in order to ensure that data packets are reliably transferred to the iRMC (and not to the operating system).

The IP address of the iRMC must be different from that of the system (operating system).

A gateway is configured for access from a different subnet

If the remote workstation accesses the iRMC of the managed server from a different subnet and DHCP is not used, you must configure the gateway.

3.1.2 Configuring the LAN interface using the UEFI setup utility

You can configure the iRMC's LAN interface using the UEFI setup utility:

1. Call the UEFI setup utility of the managed server. Do this by pressing [F2] while the server is booting.
2. Open the iRMC LAN parameter configuration menu:

```
Server Mgmt - iRMC LAN Parameters Configuration
```

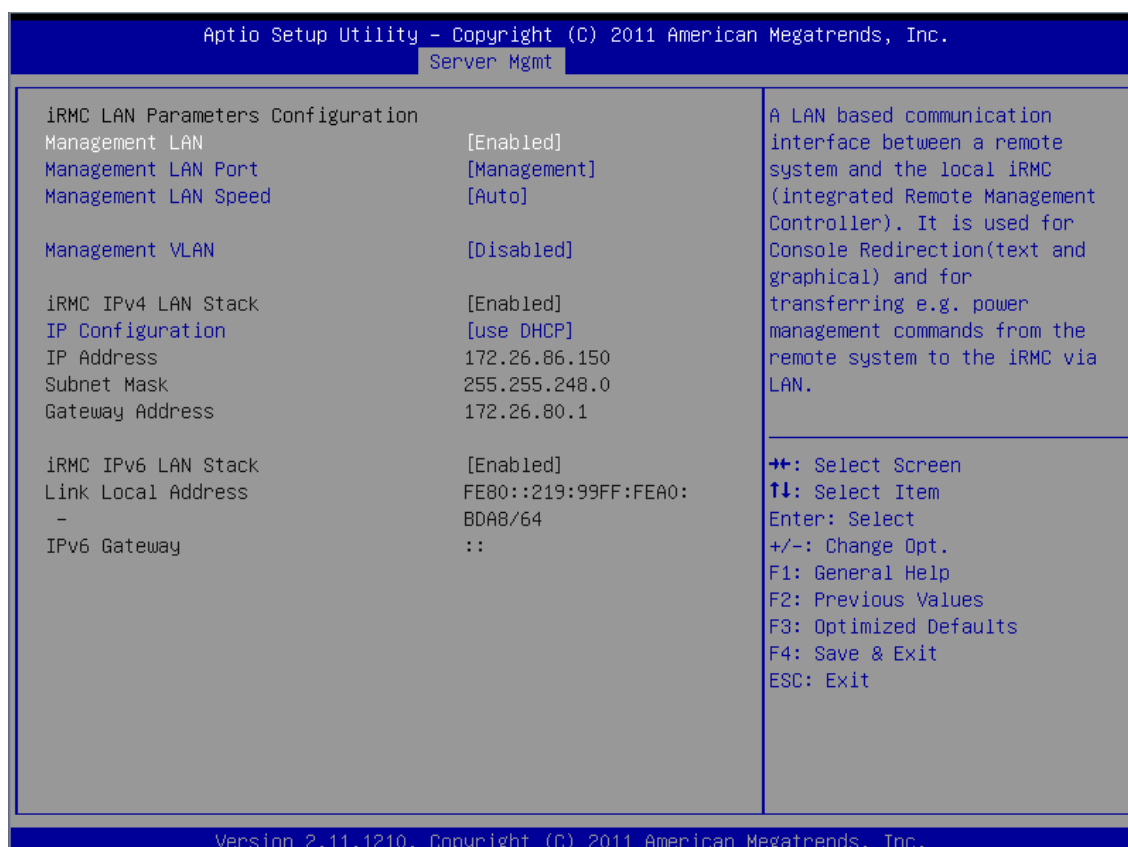


Figure 3: iRMC LAN Parameters Configuration Menu

3. In the **Management LAN** field, enter **Enabled**.
4. In the **Management LAN Port** field, enter **Management**.
 - i** For more information on configuring the remaining settings, refer to the "iRMC S4 - Web Interface" user guide and/or refer to the "BIOS (Aptio) Setup Utility" user guide corresponding to your server.
5. Save the settings.
6. If you want to use console redirection on the iRMC , continue with configuring text console redirection, refer to the section "Configuring text console redirection for the iRMC S4" in the "iRMC S4 - Concepts and Interfaces" user guide.
7. If you do not want to use text console redirection on the iRMC, exit the UEFI setup and continue with testing the LAN interface ("[Testing the LAN interface](#)" on page 23).

3.1.3 Testing the LAN interface

You can test the LAN interface as follows:

1. Use a web browser to attempt to log into the iRMC web interface. If no login prompt appears, it is probable that the LAN interface is not working.
2. Test the connection to the iRMC with a ping command.

3.2 Logging in to the iRMC S4 for the first time

The factory default settings of the iRMC allow you to log in to the iRMC for the first time without the need for any configuration activities.

3.2.1 Requirements

The following requirements must be met for a working connection:

On the remote workstation:

- Windows: Internet Explorer as of version 10.x.
- Linux: Mozilla Firefox as of version 3.x.
- For console redirection: Sun Java Virtual Machine Version 1.6 or higher.

In your network:

- There must be a DHCP server in your network.
- If you want to log in with a symbolic name rather than an IP address at the iRMC web interface, the DHCP server in your network must be configured for dynamic DNS.
- DNS must be configured. Otherwise you must ask for the IP address.

- **i** If you use the Internet Explorer 11 within an IPv6 network with HTTPS, it is recommended to provide the iRMC web interface with an IPv6 address in literal format instead of the standard format. E.g. use `2001-0db8-85a3-0000-0000-8a2e-0370-7334.ipv6-literal.net` instead of `http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]`.

3.2.2 iRMC factory defaults

The firmware of the iRMC provides a default administrator ID and a default DHCP name for the iRMC.

Default administrator ID

Both the administrator ID and the password are case-sensitive.

Administrator ID admin
Password admin

For reasons of security, it is recommended that you create a new administrator account once you have logged in, and then delete the default administrator account. At least change the password for the account ("[User management](#)" on page 26).

Default DHCP name of the iRMC

The default DHCP name of the iRMC uses the following pattern:

```
IRMC<SerialNumber>
```

The serial number corresponds to the last three bytes of the MAC address of the iRMC. You can take the MAC address of the iRMC from the label on your PRIMERGY server.

After you have logged in, the MAC address of the iRMC can be found as a read-only entry above the fields on the **Network Interface** page.

3.2.3 Logging in

1. Open a web browser on the remote workstation.
2. Enter the (configured) DNS name or IP address of the iRMC.

 You can take the DNS name of the iRMC from the label on your PRIMERGY server.

A login dialog box opens.

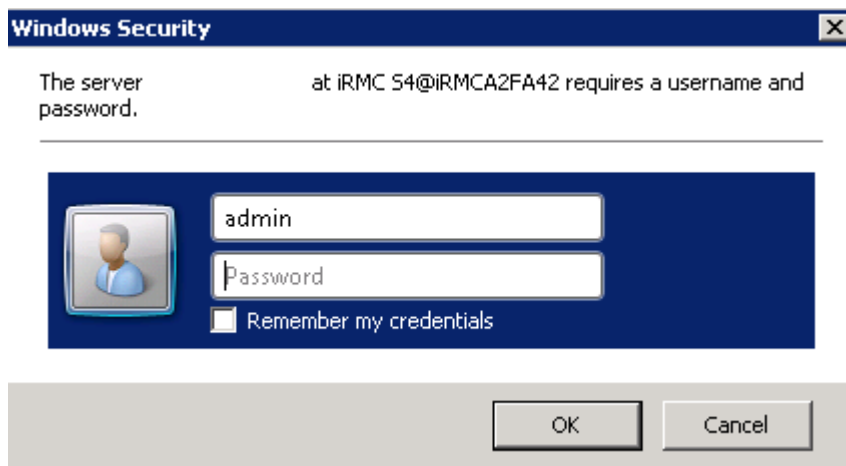


Figure 4: Login dialog box for the iRMC web interface

3. If no login dialog appears, check the LAN connection .
4. Enter the data for the default administrator account.
User name: **admin**

Password: **admin**

Both the User name and the Password are case-sensitive.

5. Click **OK** to confirm your entries.
The iRMC web interface opens with the **System Information** page.

For reasons of security, it is recommended that you create a new administrator account once you have logged in, and then delete the default administrator account. At least change the password for the account ("[User management](#)" on page 26).

3.2.4 Logging out

Logout allows you to terminate the iRMC session after you have confirmed this in a dialog box.

1. On the right hand side of the title bar click **logout**.
2. Confirm the logout action in the dialog box.
The login dialog box opens.
3. Click **Login** to open the login page of the web interface. This allows you to log in again if you want.

4 User management

User management for the iRMC uses two different types of user identifications:

- **Local** user identifications are stored locally in the iRMC's non-volatile storage and are managed via the iRMC user interfaces.
- **Global** user identifications are stored in the central data store of a directory service and are managed via this directory service's interfaces.

The following directory services are currently supported for global iRMC S4 user management:

- Microsoft® Active Directory
- Novell® eDirectory
- OpenLDAP
- OpenDJ

For detailed information on the global user management using the individual directory services, refer to the "User Management in ServerView" user guide.

4.1 User management concept

User management for the iRMC permits the parallel administration of local and global user identifications.

When validating the authentication data (user name, password) which users enter when logging in to one of the iRMC interfaces, iRMC proceeds as follows:

The iRMC compares the user name and password with the locally stored user identifications.

- If the user is authenticated successfully by iRMC (user name and password are valid) then the user can log in.
- Otherwise, the iRMC continues the verification with the next step.

The iRMC authenticates itself at the directory service via LDAP with a user name and password.

Depending on its LDAP configuration settings, the iRMC continues as follows:

- If ServerView-specific LDAP groups with authorization settings in the SVS structure on the LDAP server are used, the iRMC determines the user's permissions by using an LDAP query and checks whether the user is authorized to work on the iRMC.
Characteristics:

- Extension of the directory server structure required.
- Privileges/permissions are configured centrally on the directory server.
- If LDAP standard groups are used with authorization settings deposited locally on the iRMC, the iRMC proceeds as follows:
 1. The iRMC uses an LDAP query to determine which standard LDAP group on the directory server the user belongs to.
 2. The iRMC checks whether a user group with this name is also configured locally on the iRMC. If this applies, the iRMC determines the user's permissions by means of this local group.

Characteristics:

- No extension of the directory server structure required.
- Privileges/permissions are configured separately on each iRMC.

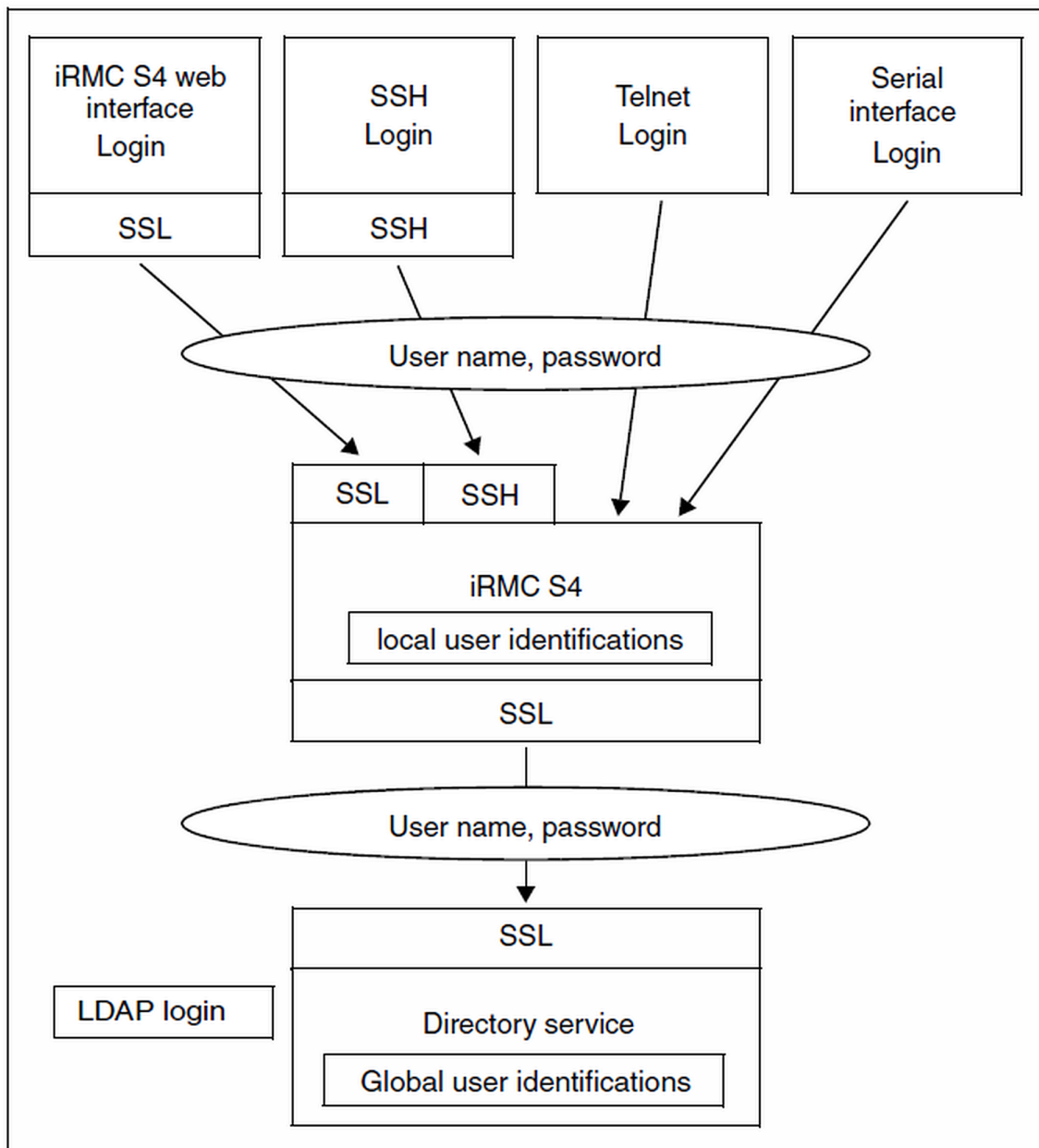


Figure 5: Login authentication via the iRMC S4

- i** Although optional, the use of SSL for the LDAP connection between the iRMC and directory service is recommended. An SSL-secured LDAP connection between iRMC and the directory service guarantees secure data exchange, and in particular the secure transfer of the user name and password data.

SSL login via the iRMC web interface is only required if LDAP is active.

4.2 User permissions

The iRMC distinguishes between two mutually complementary types of user permissions:

Channel-specific privileges (via assignment to channel-specific permission groups)

The iRMC assigns each user identification to one of the following four channel-specific permission groups:

- User
- Operator
- Administrator
- OEM

Since iRMC assigns these permissions on a channel-specific basis, users can have different permissions, depending on whether they access the iRMC over the LAN interface or the serial interface.

The scope of permissions granted increases from User (lowest permission level) through Operator and Administrator up to OEM (highest permission level).

The permission groups correspond to the IPMI privilege level. Certain permissions (e.g. for Power Management) are associated with these groups or privilege levels.

Adding the iRMC to the ServerView Operations Manager server list requires LAN channel privilege Administrator or OEM (for more information, refer to the "ServerView Operations Manager" user guide).

Permissions to use special iRMC functions

In addition to the channel-specific permissions, you can also individually assign users the following permissions:

Permission	Meaning
Configure User Accounts	Permission to configure local user identifications
Configure iRMC Settings	Permission to configure the iRMC settings
Video Redirection Enabled	Permission to use Advanced Video Redirection (AVR) in "View Only" and "Full Control" mode
Remote Storage Enabled	Permission to use the Virtual Media function

The privileges and permissions required for the use of the individual iRMC functions are described:

- For the iRMC web interface in the "iRMC S4 - Web Interface" user guide
- For the Remote Manager in the "iRMC S4 - Concepts and Interfaces" user guide

4.3 Local user management for the iRMC S4

The iRMC possesses its own local user management. Up to 16 users can be configured with passwords and be assigned various rights depending on the user groups they belong to. The user identifications are stored in the local, non-volatile storage of the iRMC S4.

The following options are available for user management on the iRMC:

- User management via the web interface ("[Local user management using the iRMC web interface](#)" on page 30)
- User management via the Server Configuration Manager ("[Local user management using the Server Configuration Manager](#)" on page 31)

Additionally the iRMC also supports SSHv2-based public key authentication using pairs of public and private keys for local users ("[Secure Authentication via SSHv2](#)" on page 31).

4.3.1 Local user management using the iRMC web interface

On the web interface you can view a list of configured users. You can also configure new users, change the configuration of existing users and remove users from the list.

User management on the iRMC requires Configure User Accounts permission.

Showing the list of configured users

A list of configured users can be opened via the **iRMC S4 User** page of the **User Management** menu.

In this list you can delete users and call the page for configuring new users.

Configuring new users

You can configure a new user with the **New User** button in the list of configured users.

On the **New User Configuration** page you configure the basic settings for the new user.

Modifying the configuration of a user

You can modify the settings of a user account by clicking the name of the relevant user in the list of configured users.

On the **User "<name>" Configuration** page you can change the configuration parameters for the new user. 3.

Deleting users

You delete a user account with a click on the **Delete** button in the same line as the user in the list of configured users.

For more information on the **User Management** pages of the iRMC web interface, refer to the "iRMC S4 - Web Interface" user guide.

4.3.2 Local user management using the Server Configuration Manager

User management via the Server Configuration Manager largely conforms to user management using the iRMC web interface.

User management on the iRMC requires Configure User Accounts permission.

Prerequisite: The current ServerView agents must be installed on the managed server.

Refer to the "iRMC S4 - Web Interface" user guide for a description of how to start the Server Configuration Manager.

For further information on the individual Configuration Manager dialogs, refer to the online help of the Server Configuration Manager.

4.3.3 Secure Authentication via SSHv2

In addition to authentication by means of a user name and password, the iRMC also supports SSHv2-based public key authentication using pairs of public and private keys for local users. To implement SSHv2 public key authentication, the SSHv2 key of an iRMC user is uploaded to the iRMC. The iRMC user uses his private key with the program PuTTY or the OpenSSH client program ssh, for example.

The iRMC supports the following types of public keys:

- SSH DSS (minimum requirement)
- SSH RSA (recommended)

The public SSHv2 keys that you upload to the iRMC can be available either in RFC4716 format or in OpenSSH format ("[Example: Public SSHv2 key](#)" on page 39).

Public key authentication

In outline, public key authentication of a user on the iRMC happens as follows:

The user who wishes to log into the iRMC creates the key pair:

- The private key is read-protected and remains on the user's computer.
- The user (or administrator) uploads the public key to the iRMC.

If the configuration allows this, the user can now securely log into the iRMC and without the need to enter a password. The user is only responsible for keeping their private key secret.

The following steps are necessary to set up private key authentication. They are described in the subsequent sections:

1. Create the public and private SSHv2 keys with the program PuTTYgen or ssh-keygen and save them in separate files ("[Creating public and private SSHv2 keys](#)" on page 32).
2. Upload the public SSHv2 key onto the iRMC from a file ("[Uploading the public SSHv2 key](#)" on page 34).

3. Configure the program PuTTY or ssh for SSHv2 access to the iRMC ("Using the public SSHv2 key" on page 35).

4.3.3.1 Creating public and private SSHv2 keys

You can create public and private SSHv2 keys.

Using the PuTTYgen program

1. Start PuTTYgen on your Windows computer.
The main window of PuTTYgen opens.



Figure 6: PuTTYgen: Creating new private and public SSHv2 keys

2. In the **Parameters** group, select the key type **SSH-2RSA**.
3. Click **Generate** to start generation of the keys.
The progress of the generation is symbolized by a progress bar.
4. Move the mouse pointer over the progress bar to increase the randomness of the generated keys.
When the keys have been generated, PuTTYgen displays the key and the fingerprint of the public SSHv2 key.

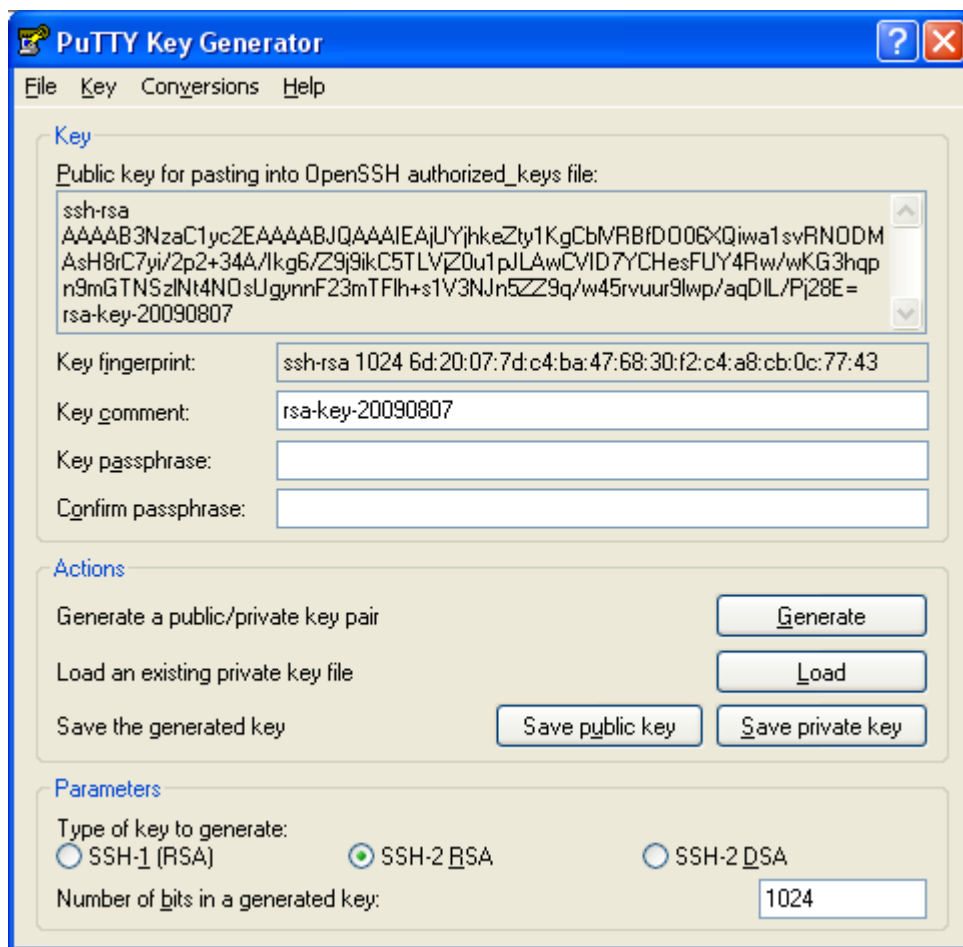


Figure 7: PuTTYgen: Generated private SSHv2 key

5. Click **Save public key** to save the public SSHv2 key to a file. You can upload the public key to the iRMC from this file ("[Uploading the public SSHv2 key](#)" on page 34).
6. Click **Save private key** to save the private SSHv2 key to a file for use with PuTTY.

Using the OpenSSH client program ssh-keygen

If it is not already pre-installed in the Linux distribution you are using, you can obtain OpenSSH from <http://www.openssh.org>.

You will find a detailed description of the operands on the OpenSSH manual pages at <http://www.openssh.org/manual.html>.

Proceed as follows:

1. Open a command window.
2. Call ssh-keygen to generate an RSA key pair:

```
ssh-keygen -t rsa
```

ssh-keygen logs the progress of the key generation operation. ssh-keygen queries the user for the file name under which the private key is to be stored and for the passphrase for the private key. ssh-keygen stores the resulting private and public SSHv2 keys in separate files and displays the fingerprint of the public key.

Example: Generating an RSA key pair with ssh-keygen

```

$HOME/benutzer1 ssh-keygen -t rsa

Generating public/private rsa key pair.
Enter file in which to save the key
($HOME/benutzer1/.ssh/id_rsa): _____ ①
Enter passphrase (empty for no passphrase): _____ ②
Enter same passphrase again: _____
Your identification has been saved in
$HOME/benutzer1/.ssh/id_rsa. _____ ③
Your public key has been saved in
$HOME/benutzer1/.ssh/id_rsa.pub. _____ ④
The key fingerprint is:
ee:99:d7:ac:8f:8e:c7:2f:2c:9b:81:80:3f:84:28:7d _____ ⑤
benutzer1@mycomp

```

Explanation:

1. ssh-keygen requests the file name in which the SSHv2 key is to be saved. If you press [Enter] to confirm without entering a file name, ssh-keygen uses the default file name id_rsa.
2. ssh-keygen requests you to enter a passphrase (and to confirm it) that is used to encrypt the private key. If you press [Enter] to confirm without entering a passphrase, ssh-keygen does not use a passphrase.
3. ssh-keygen informs the user that the newly generated private SSHv2 key has been saved in the file /.ssh/id_rsa.
4. ssh-keygen informs the user that the newly generated public SSHv2 key has been saved in the file /.ssh/id_rsa.pub.
5. ssh-keygen displays the fingerprint of the public SSHv2 key and the local login to which the public key belongs.

4.3.3.2 Uploading the public SSHv2 key

To upload the public SSHv2 key onto the iRMC from a file proceed as follows:

1. Login to the iRMC web interface.
2. Open the **iRMC S4 User** page in the **User Management** menu.
3. In the list of configured users click the relevant user.
4. On the **User "<name>" Configuration** page click **Browse** in the **User SSHv2 public key upload from file** group and navigate to the file containing the required public key.
5. Click **Upload** to load the public key onto the iRMC.
After the key has been successfully uploaded, the iRMC displays the key fingerprint in the **User SSHv2 public key upload from file** group.

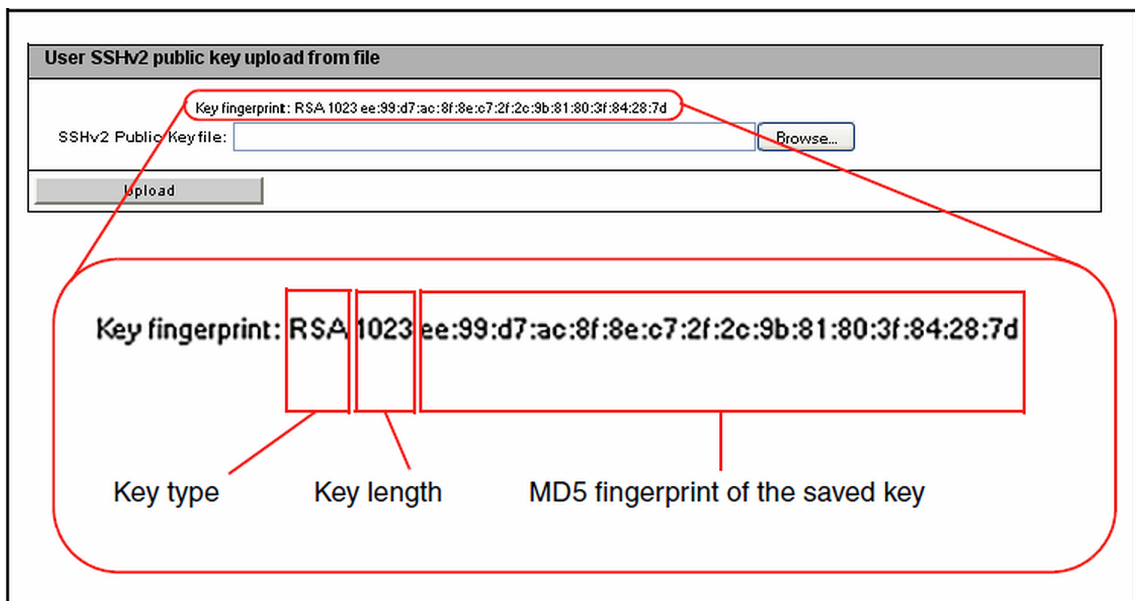


Figure 8: Display of the key fingerprint

6. For reasons of security, ensure that the fingerprint shown here matches that shown in PuTTYgen ("[Creating public and private SSHv2 keys](#)" on page 32) in the **Key fingerprint** field.

4.3.3.3 Using the public SSHv2 key

To use the public SSHv2 key you need to configure an appropriate tool:

Configuring PuTTY for using the public SSHv2 key

The PuTTY program allows you to set up a public-key-authenticated connection to the iRMC and log in either with your user name or using the auto-login mechanism. PuTTY handles the authentication protocol automatically on the basis of the public/private SSHv2 key pair previously generated.

Proceed as follows:

1. Start PuTTY on your Windows computer.
The main window of PuTTY opens.

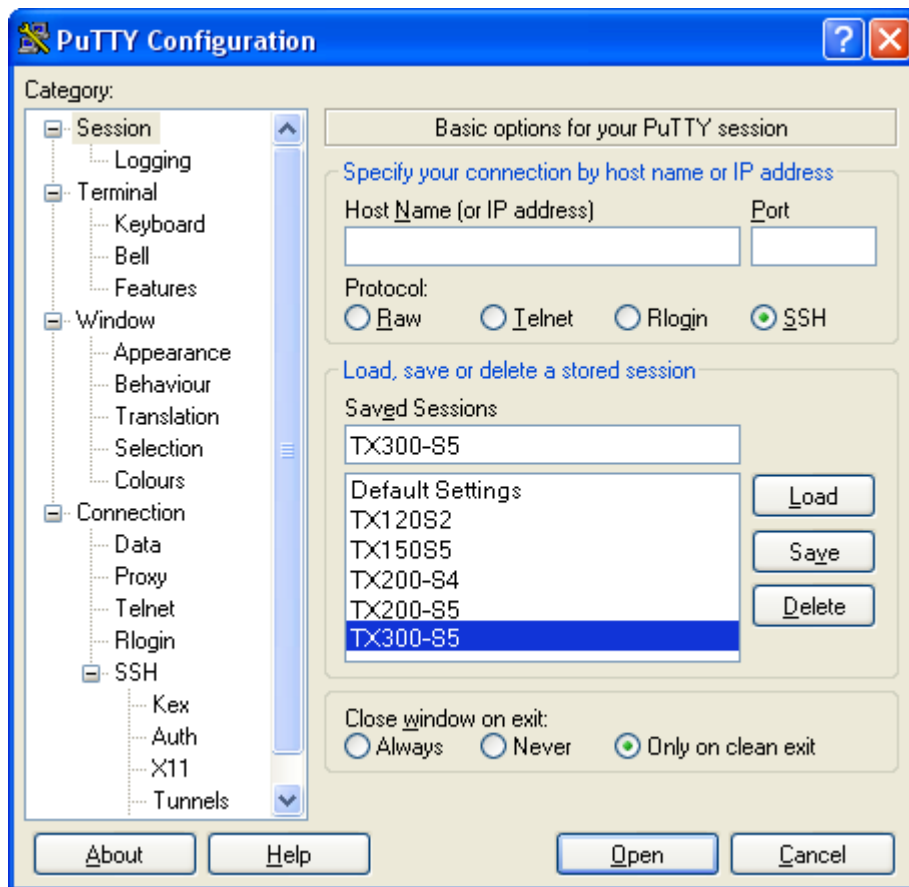


Figure 9: Selecting and loading an SSH session

2. In the **Saved Sessions** list select an SSH session with the iRMC S4 for which you want to use the SSHv2 key. You can also create a new session.
3. Click **Load** to load the parameters of the selected SSH session.
4. In the **Category** tree select **SSH/Auth** to configure the SSH authentication options. The **Authentication** parameters are displayed.

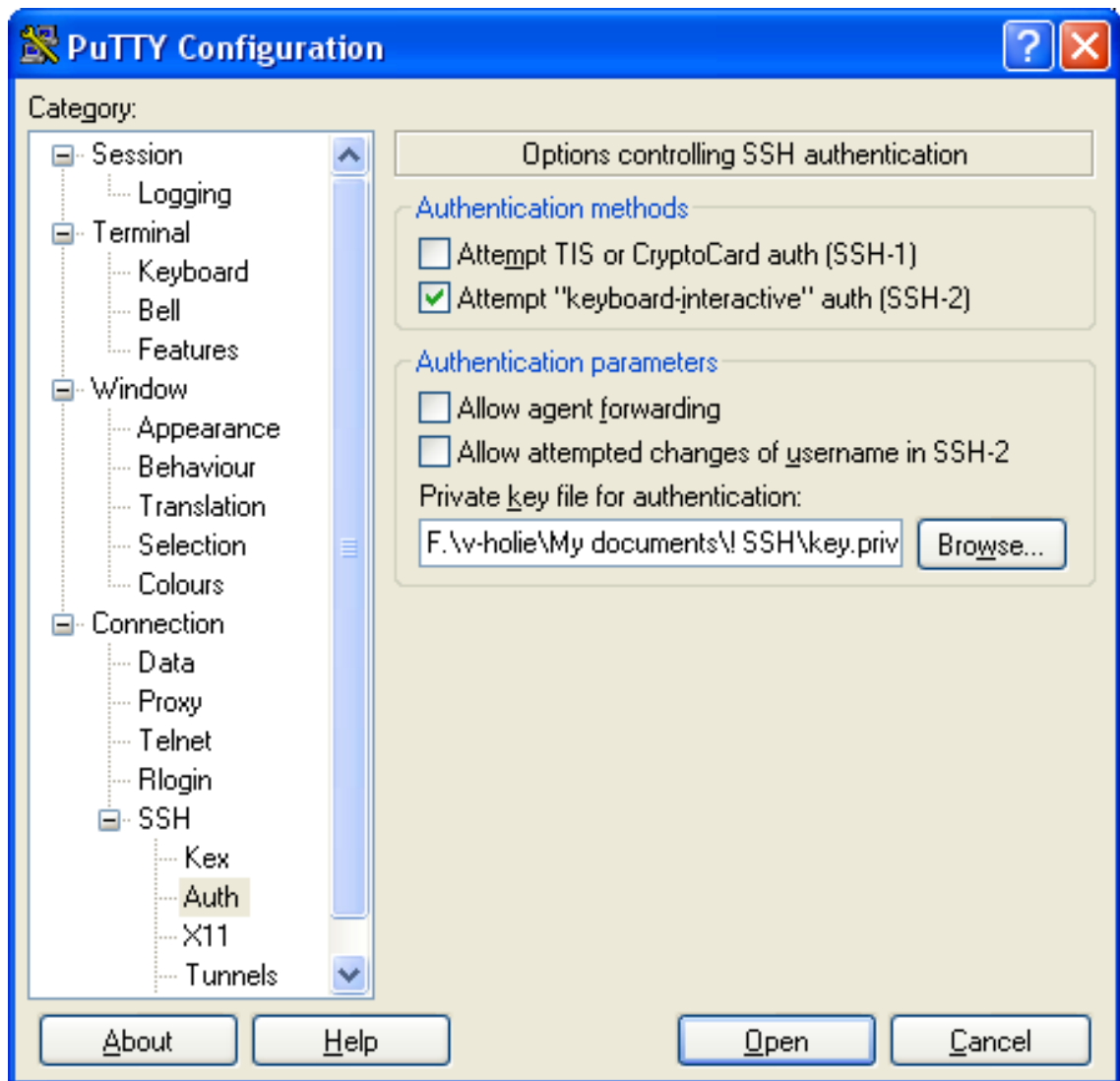


Figure 10: Configuring the SSH authentication options

5. Select the file containing the private key that you want to use with the iRMC S4.
 - i** At this point, you require the private key ("[Creating public and private SSHv2 keys](#)" on page 32) and not the public key that you uploaded onto the iRMC.
6. In the **Category** tree select **Connection/Data** to additionally specify a user name for automatic login onto the iRMC.

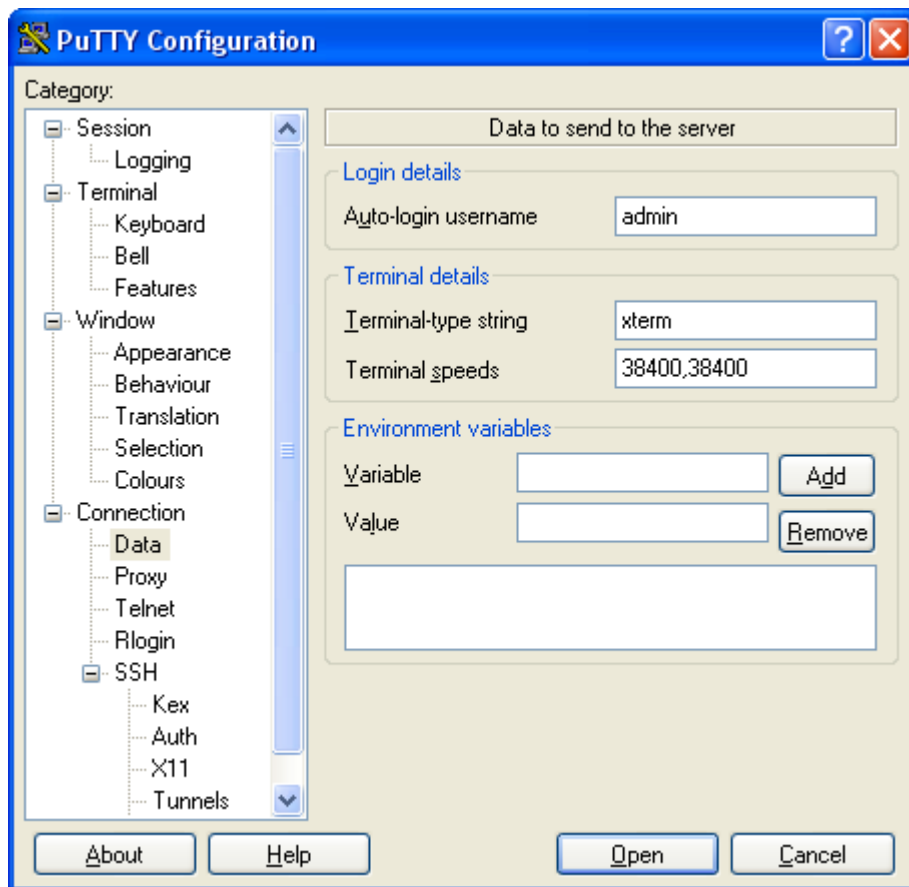


Figure 11: PuTTY: Specifying the user name for automatically logging into the iRMC

Configuring the OpenSSH client program ssh for using the public SSHv2 key

You establish an SSHv2-protected connection to the iRMC using the OpenSSH client program `ssh`. You can log in either under your current local login or under a different login.

The login must have been configured as a local login on the iRMC and the associated SSHv2 key must have been loaded on the iRMC S4.

`ssh` reads its configuration options from the sources in the following order:

- Command line arguments that you specify when calling `ssh`.
- User-specific configuration file (`$HOME/.ssh/config`)
 - **i** Although this file contains no security-critical information, read/write permission should only be granted to the owner. Access should be denied to all other users.
- System-wide configuration file (`/etc/ssh/ssh_config`)

This file contains default values for configuration parameters:

 - If there is no user-specific configuration file
 - If the relevant parameters are not specified in the user-specific configuration file

The value found first applies for each option.

- i** You will find detailed information on the configuration of ssh and on its operands on the manual pages for OpenSSH under:

`http://www.openssh.org/manual.html`

Proceed as follows:

1. Open a command window.
2. Start ssh, to log in to the iRMC under SSHv2-authentication:

```
ssh -l [<user>] <iRMC_S4>
```

or

```
ssh [<user>@]<iRMC_S4>
```

<user>

User name under which you want to log into the iRMC. If you do not specify <user>, ssh uses the user name under which you are logged into your local computer to log you in to iRMC.

<iRMC_S4>

iRMC name or IP address of the iRMC you want to log into.

Example: SSHv2-authenticated login on the iRMC

For the following ssh- call, it is assumed that ssh-keygen has been used to generate a public/private RSA key pair ("[Creating public and private SSHv2 keys](#)" on page 32) and that the public key `User1/.ssh/id_rsa.pub` has been loaded onto the iRMC for an iRMC user `user4` ("[Uploading the public SSHv2 key](#)" on page 34).

You can then log in from your local computer under `$HOME/User1` as follows on the iRMC "RX300_S82-iRMC" using the user name `user4`:

```
ssh user4@RX300_S82-iRMC
```

4.3.3.4 Example: Public SSHv2 key

The following shows the same public SSHv2 key in different formats:

RFC4716 format

```
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "rsa-key-20090401"
```

```
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4  
hx
```

```
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9  
Ar
```

```
Jxj1hXUz1PPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsfc+F  
pGJ2iw==
```

```
---- END SSH2 PUBLIC KEY ----
```

OpenSSH format

ssh-rsa

AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4
hxv6+\

AUFRF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9ArJ
xj1hXUzlPPVzuBtPaRB7+\

bISTJVMUorNwrcN48b6AAoYBhKC4AotOP1OGwsfc+FpGJ2iw== rsa-key-
20090401

5 Remote installation of the operating system

You can use the ServerView Installation Manager (abbreviated to Installation Manager below) and the iRMC features "Advanced Video Redirection (AVR)" and "Virtual Media" to install the operating system on the managed server from the remote workstation.

The chapter discusses the following specific topics:

- General procedure for the remote installation of an operating system using storage media which are provided via the "Virtual Media" feature. In the following, storage media provided via the "Virtual Media" feature are referred to as virtual storage media for short.
- Booting the managed server from the remote workstation using the ServerView Suite DVD 1 (Windows and Linux).
- Installing Windows from the remote workstation after configuration on the managed server.
- Installing Linux from the remote workstation after configuration on the managed server.
- The description focuses primarily on the handling of the virtual storage media. It is assumed that readers are familiar with the Installation Manager functionality (for more information, refer to the "ServerView Installation Manager" user guide).

Prerequisites for the remote installation of the operating system via iRMC S4:

- The iRMC's LAN interface must be configured (["Configuring the LAN interface using the UEFI setup utility" on page 21](#)).
- The license key for the use of the iRMC functions "Advanced Video Redirection (AVR)" and "Virtual Media" must be installed.

5.1 General procedure for installing the operating system

The Installation Manager regards the remote installation of the operating system via iRMC as a local installation and configuration on the managed server. You perform installation from the remote workstation via the AVR window using virtual media.

The following steps are required in order to install and configure via the Installation Manager:

1. Connect the virtual storage medium (DVD or Installation Manager boot image) from which you want to boot as virtual storage medium.
2. Boot and configure the managed server via DVD or the Installation Manager boot image.

3. Use the Installation Manager at the remote workstation to install the operating system on the managed server.

Nevertheless you can install and configure the operating system without the Installation Manager using the CD/DVDs for:

Windows

You can perform a remote installation of Windows via Virtual Media either using the Installation Manager or exclusively using the Windows installation CD/DVDs. The two procedures correspond in terms of the handling of the virtual storage media.

However, you are advised to install Windows via the Installation Manager for the following reasons:

- The Installation Manager itself identifies the required drivers and copies these to the system.
- All the Installation Manager functions are available to you during installation. This means that you can, for example, configure the entire system including the server management settings.
- Installation using the Installation Manager does not take significantly longer than installation using the operating system CD/DVDs.

Installations without the Installation Manager have to be controlled via the keyboard since the mouse cursor cannot be synchronized during the installation process. In contrast, if you install using the Installation Manager then all configuration and installation steps can be performed using the mouse.

Linux

If you know which drivers are required by the system then you can start the Linux installation by booting from the Linux installation CD/DVD.

If the installation requires you to integrate drivers from the floppy disk then, before starting the installation, you must set up a virtual media connection:

- To the storage medium (CD-ROM/DVD-ROM or ISO image) from which you want to boot
- If necessary to storage medium for driver installation

5.2 Connecting a storage medium as Virtual Media

The Virtual Media function makes a "virtual" drive available which is located elsewhere in the network.

The source for the virtual drive can be:

- Physical drive or image file at the remote workstation. The image file may also be on a network drive (with drive letter, e.g. "D:" for drive D).
- Image file provided centrally in the network via Remote Image Mount.

For more information on the "virtual Media" feature, refer to the "iRMC S4 - Web Interface" user guide.

Proceed as follows at the remote workstation to establish the virtual media connection:

1. Log into the iRMC web interface with Remote Storage Enabled permission.
2. Open the **Advanced Video Redirection (AVR)** page and start the AVR.
3. Start Virtual Media in the AVR window.
The **Virtual Media** dialog box opens.
4. In the appropriate panel of the **Virtual Media** dialog box, click **Browse**.
The **Open** file browser dialog box opens.
5. In the **Open** dialog box, navigate to the directory of the storage medium that you want to make available as virtual medium from your remote workstation.
 - Installation with Installation Manager:
ServerView Suite DVD 1 or an Installation Manager boot image and optionally a formatted USB memory stick as a status backup medium.
 - Installation from the vendor's installation CD/DVD: Windows or Linux installation CD/DVD and optional drivers.
It is recommended that the ServerView Suite DVD 1 and the operating system installation CD/DVD are stored in a folder as an image file (ISO image) and that they are connected from there as virtual storage media or provided via Remote Image Mount.
6. Select the required device type in the **Files of Type** field.
7. Specify the storage medium you want to connect as a virtual medium in the **File Name** field:
 1. In the case of an ISO image (ISO/NRG image), enter the file name. Alternatively, click on the file name in the Explorer.
 2. In the case of a drive, enter the name of the drive, e.g.
D for drive D (Windows)
/dev/ . . . (Linux)

8. Click **Open** to confirm your selection.
The selected storage medium is made available as a virtual medium and displayed in the corresponding panel of the **Virtual Media** dialog box.
9. Click **Connect** to connect the DVD ROM drive (DVD) or the Installation Manager boot image as virtual storage media.

5.3 Booting the managed Server

To boot the managed server from ServerView Suite DVD 1 and configure it with the Installation Manager, proceed as follows:

1. Use the options in **the Power Control** group on the **Power On/Off** page of the iRMC web interface to start up or reboot the managed server. You can follow the progress of the boot process in the AVR window.
During the managed server's BIOS POST phase, virtual storage media are displayed as USB 2.0 devices. Virtual storage media are represented by the following entries in the BIOS boot sequence:

- A (physical) floppy disk is represented by a separate entry "Fujitsu RemoteStorage FD-(USB 2.0)".
- All other virtual storage device types are represented by the shared entry "CD-ROM DRIVE".

If a local CD-ROM/DVD-ROM drive and a CD-ROM/DVD-ROM drive connected as virtual media are both present at the managed server then the managed server boots from the CD-ROM/DVD-ROM drive provided via Virtual Image.

2. Press [F2] while the server is booting.
3. In the UEFI set-up, open the **Boot** menu in which you can define the boot sequence.
4. Specify **Boot Priority=1** (highest priority) for the ServerView Suite DVD 1 which is connected as virtual storage medium.
5. Save your settings and exit the UEFI setup.
The managed server then boots from ServerView Suite DVD 1 which is connected as virtual storage.

If the system does not boot from the virtual storage medium (ServerView Suite DVD 1 or Installation Manager boot image):

1. Check whether the storage medium is displayed during the BIOS POST phase and connect the storage medium as a virtual medium if necessary.
2. Make sure that the correct boot sequence is specified.
It takes about 5 minutes to boot from ServerView Suite DVD 1 via a virtual storage medium. The boot progress is indicated during the boot process. Once the boot process has completed, the Installation Manager startup displays a dialog box in

which you are asked to select a medium for the status backup area (status backup medium).

3. Select **Standard mode** as the **Installation Manager** mode.
4. Specify where the configuration data is to be stored:
Status backup medium
Stores the configuration data on a local replaceable data medium.

Prerequisites

- The backup medium must not be write-protected.
- A USB stick must already be connected to the USB port when the system is booted. If you fail to do this and wish to save the configuration file: Connect the USB stick now and reboot from ServerView Suite DVD 1.


1. Select the option **on local drive (floppy / USB stick)**.
2. Select the corresponding drive from the list to the right of this option.

For further information on creating Installation Manager status disks, refer to the "ServerView Installation Manager" user guide.

Connecting the status medium and/or the installation media via the network

Stores the configuration data on a network medium.

1. Set up the required shares for this purpose.

-  If you provide a medium with a prepared configuration file and/or an installation medium via the network, you have to select this option. Depending on your infrastructure, you can either obtain a temporary IP address via DHCP or manually configure an IPv4 or IPv6 address for the current Installation Manager session.

If you do not select any status backup option all the configuration data is lost when you reboot.

5. Start the Installation Manager by clicking **Continue**.
The **Welcome** page of the Installation Manager opens.

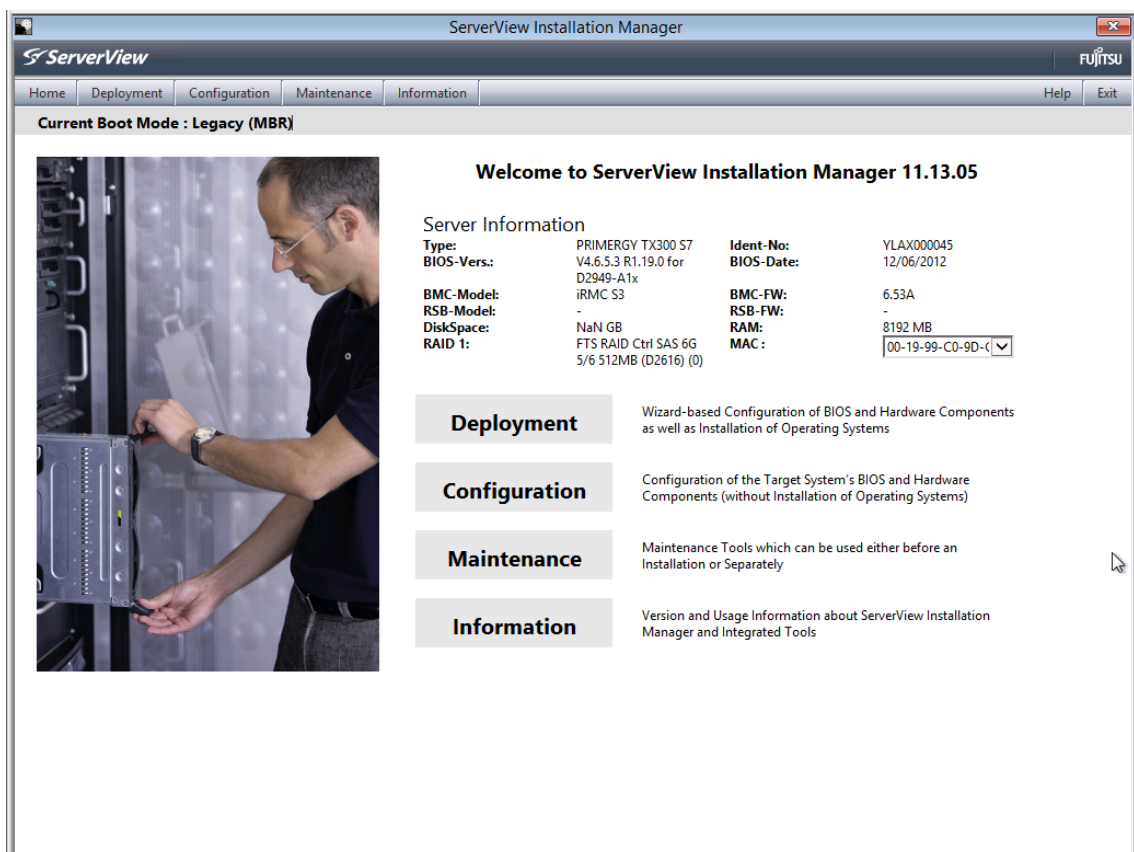


Figure 12: Installation Manager - Welcome page

6. Click **Deployment** to start preparation of the local installation (deployment).

To prepare the installation, the Installation Manager wizards take you through a sequence of configuration steps that gather specifications for configuring the system and for subsequent unattended installation of the operating system.

7. Configure the local CD ROM/DVD ROM drive of the managed server as the installation source. You can then also make the Windows installation CD/DVD available from the CD ROM/DVD ROM drive of the remote workstation if you connect it to the managed server as a virtual storage medium ("[Installing Windows on the managed server](#)" on [page 47](#)).

Once you have completed configuration with the Installation Manager, the **Installation Info** page for the Windows installation ("[Installing Windows on the managed server](#)" on [page 47](#)) or for the Linux installation ("[Installing Linux on the managed server](#)" on [page 48](#)) is displayed. This allows you to start the installation process.

5.4 Installing Windows on the managed server

After configuration has been completed, the Installation Manager displays the **Installation Info** page.

The screenshot shows the ServerView interface with the following configuration details:

MS Windows Server 2008 R2 Installation Info			
Bootdisk			
Controller:	raid controller	PartitionSize:	32000 MB
OperatingSystem			
Type:	Windows Server 2008 Enterprise x64 R2	R2 Components:	
ProductKey:		Organisation:	
Timezone:	-	Admin Passwd:	not set
UserName:			
ComputerName:			
DHCP	true		
SNMP			
Privileges:	4	Community:	public
Trap Destination:	127.0.0.1		


Save the Configuration to File: serstartbatch.xml

Note that this file on the server is used as a workfile and will be overwritten. It should not be used for permanent storage.

Buttons: Back, Save, Start Installation, Cancel

Figure 13: Installation Manager - Installation Info page

If you have configured the local CD ROM/DVD ROM drive of the managed server as the installation source, proceed as follows at the remote workstation:

1. In the menu bar of the AVR window, select **Media/Virtual Media Wizard** to open the **Virtual Media** dialog box.
2. **Safely remove** the storage device, i.e. ensure that no more applications/programs are accessing the storage media.
3. To clear a virtual media connection, click the corresponding **Disconnect** button.
4. Clear all virtual media connections.
5. Remove ServerView Suite DVD 1 from the DVD ROM drive at the remote workstation.
6. Insert the Windows installation CD/DVD in this DVD ROM drive.
 -  Close the application if autostart is active.
7. Connect the CD ROM/DVD ROM drive containing the Windows installation CD/DVD as virtual storage medium.

8. In the **Installation Info** page of the Installation Manager, click **Start installation**. All the installation files are copied to the managed server.
The Installation Manager opens a confirmation dialog page when the copy operation is complete and prompts you to remove all the storage media from the removable media drives before the managed server is rebooted.
9. Clear again all current virtual media connections.
10. On the confirmation dialog page, click **OK** to reboot the managed server. Once the managed server has rebooted, you can monitor the entire installation by means of the AVR.

5.5 Installing Linux on the managed server

During the installation you can use the mouse but cannot synchronize it.

Whenever you change a virtual storage medium, you must remove the virtual media connection for the currently connected medium and then connect the new medium as a virtual storage medium.

After configuration has been completed, the Installation Manager displays the **Installation Info** page.

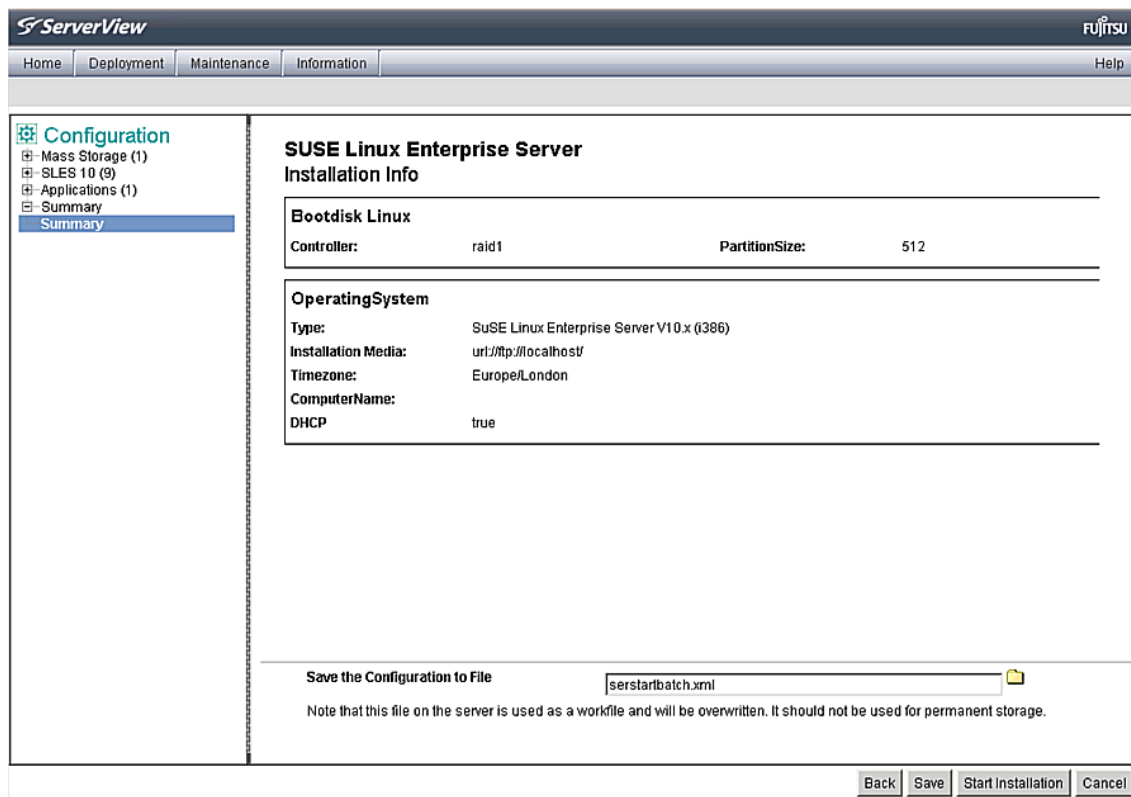



Figure 14: Installation Manager - Installation Info page

If you have configured the local CD ROM/DVD ROM drive of the managed server as the installation source, proceed as follows at the remote workstation:

1. In the menu bar of the AVR window, select **Media/Virtual Media Wizard** to open the **Virtual Media** dialog.
2. "Safely remove" the storage device, i.e. ensure that no more applications/programs are accessing the storage media.
3. To clear a Virtual Media connection, click the corresponding **Disconnect** button.
4. Clear all virtual media connections.
5. Remove ServerView Suite DVD 1 from the DVD ROM drive at the remote workstation.
6. Insert the Linux installation CD/DVD in this DVD ROM drive.

 Close the application if autostart is active.

7. Connect the CD ROM/DVD ROM drive containing the Windows installation CD/DVD as virtual storage medium.
8. In the **Installation Info** page of the Installation Manager, click **Start installation**. All the installation files are copied to the managed server.

The Installation Manager opens a confirmation dialog page when the copy operation is complete and prompts you to remove all the storage media from the removable media drives before the managed server is rebooted.

9. Clear again all current virtual media connections.
10. On the confirmation dialog page, click **OK** to reboot the managed server. Once the managed server has rebooted, you can monitor the entire installation by means of the AVR.

6 Firmware update

The iRMC uses two different firmware images. The two firmware images each are stored on a 32-MB EEPROM (Electrically Erasable Programmable Read-Only Memory):

- Firmware image 1 (low FW image)
- Firmware image 2 (high FW image)

One of the two firmware images is active (running) at any given time, while the other is inactive. The firmware image that is active depends on the so-called firmware selector ("[Firmware Selector](#)" on page 51).

The firmware of the iRMC is not executed in the EEPROM, but is instead loaded into SRAM memory on startup and executed there. This means that it is possible to update both active and inactive firmware images online, i.e. with the server operating system (Windows or Linux) running.

If an error occurs while loading the firmware from one of the images, the firmware is automatically loaded from the other image.

- ❗ When updating/downgrading the firmware, note that the problem-free operation of the firmware can only be guaranteed if the runtime firmware and the SDR (Sensor Data Record) both belong to the same firmware release.

Besides the possibility of performing a firmware update, you can also downgrade the firmware to the previous version.

The current firmware versions are present on the ServerView Suite DVD 2 or can be downloaded manually from the Download section of the Fujitsu web server.

You can obtain the up-to-date version of the ServerView Suite DVD 2 at two-monthly intervals.

Before updating or downgrading the firmware, read the supplementary documentation supplied with the new firmware carefully (in particular the Readme files).

Information on the iRMC firmware and EEPROM can be found:

- In the iRMC web interface, page **iRMC S4 Information**
- Using the flash tool ("[Flash Tools](#)" on page 59)

6.1 Firmware Selector

The firmware selector specifies the iRMC S4 firmware to be executed. Every time the iRMC is reset and restarted, the firmware selector is evaluated and processing branches to the corresponding firmware.

The firmware selector can have the following values:

- 0 Firmware image containing the most recent firmware version
- 1 firmware image 1
- 2 firmware image 2
- 3 Firmware image containing the oldest firmware version
- 4 Firmware image most recently updated
- 5 Firmware image that has been updated least recently

Depending on the update variant used, the firmware selector is set differently after the update.

You can query and explicitly set the firmware selector:

- On the **iRMC S4 Information** page of the iRMC web interface (for more information, refer to the "iRMC S4 - Web Interface" user guide)
- Using the flash tool ("[Flash Tools](#)" on page 59)

6.2 Firmware image downgrade

Besides the possibility of performing a firmware update, you can also downgrade the firmware to the previous version.

The simplest way to downgrade the firmware is to store the previous-version firmware image as the inactive firmware image in the EEPROM of the iRMC. In this case, you only have to set the firmware selector to this previous-version image ("[Firmware Selector](#)" on page 51) and subsequently restart the iRMC to activate the firmware.

- i** You can also downgrade the firmware by applying the methods described in the following sections. In these cases, you perform a firmware update based on the firmware of the previous version. Special requirements to perform the downgrade are pointed out separately in the following sections.

When downgrading the firmware, please note:

- Downgrade via Update Manager Express:
The firmware downgrade is only feasible in the Expert mode. In addition, the Downgrade option must be activated.
- Downgrade via ASP:

Windows You can perform the downgrade if you start the ASP by double-clicking the corresponding *.exe file. When starting the ASP via the CLI, you must explicitly specify the Force=yes option.

Linux You must explicitly specify option -f or option --force.

6.3 Firmware image update

Since the iRMC firmware executes in the SRAM memory of the iRMC, it is possible to update both active and inactive firmware images online, i.e. with the server operating system running.

The following methods are available for updating the firmware images:

With the iRMC web interface

The **iRMC S4 Firmware Update** page allows you to update the firmware of the iRMC by providing the firmware image either:

- Locally on the remote workstation
- On a network share
- On a TFTP server (for more information, refer to the "iRMC S4 - Web Interface" user guide)

Using the ServerView Update Manager

Using the ServerView Update Manager, you can start the update of the iRMC firmware via a graphical user interface or via a command line interface (Windows and Linux). The ServerView Update Manager accesses the update data via its Update Repository on the ServerView Suite DVD 2 or on the management server.

You update the update repository on the management server by means of the Download Manager or by performing a manual download from the **Download** section of the Fujitsu web server.

For more information on firmware updates with the ServerView Update Manager, refer to the "ServerView Update Manager" user guide.

Using ServerView Update Manager Express or ASP

On Windows and Linux operating systems, you can update the iRMC firmware either using the graphical user interface of ServerView Update Manager Express or by using the ASP (Autonomous Support Package) command interface.

Under Windows, you can also start an ASP in the Windows Explorer by double-clicking the corresponding ASP-* .exe file.

For detailed information on firmware updates with Update Manager Express and ASP, refer to the "Local System Update for PRIMERGY Servers" user guide.

Using the operating system flash tools

An online update using the operating system flash tools is performed as a recovery flash, i.e. no version check is performed.

Prerequisite: The flash tools and the files for the firmware update must be present in the file system of the managed server.

You call the appropriate flash tool in the Windows command line or at the Linux CLI.

For the syntax and operands for the flash tools ["Flash Tools" on page 59](#).

If a new version of the bootloader is available, both firmware images will be automatically flashed within the same update process.

6.3.1 Setting up the USB memory stick

You do not need the USB memory stick if you update the firmware of the iRMC in one of the following ways:

- Using the ServerView Update Manager
- Using ServerView Update Manager Express or ASP
- Using the iRMC web interface and TFTP server

In all other cases proceed as follows:

1. Download the firmware **iRMC Firmware Update for USB Stick** from the Download section of the Fujitsu web server to a directory on your computer.
The ZIP archive `Fujitsu_<spec>.zip` can be found in your download directory.
(The `<spec>` part of the name provides information on the system type, system board, firmware/SDRR version etc.)

The ZIP archive includes the following files:

- `USBImage.exe`
 - `iRMC_<Firmware-Version>.exe`
 - `iRMC_<Firmware-Version>.IMA`
2. Connect the USB memory stick to your computer.
 3. Start the file `iRMC_<Firmware-Version>.exe` or the file `USBImage.exe`.
The **USB image** dialog box opens.

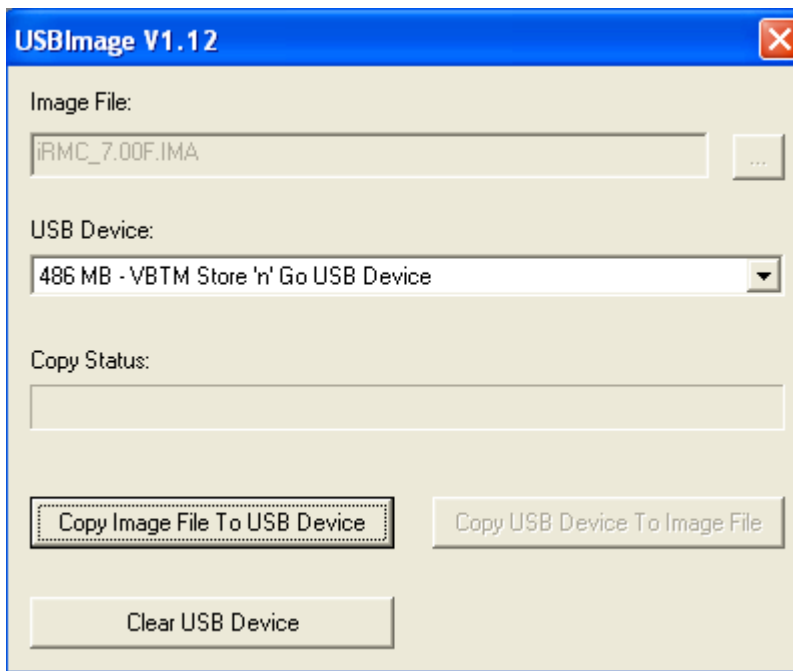


Figure 15: Copying the image file to the USB memory stick (with iRMC_<Firmware version>.exe)

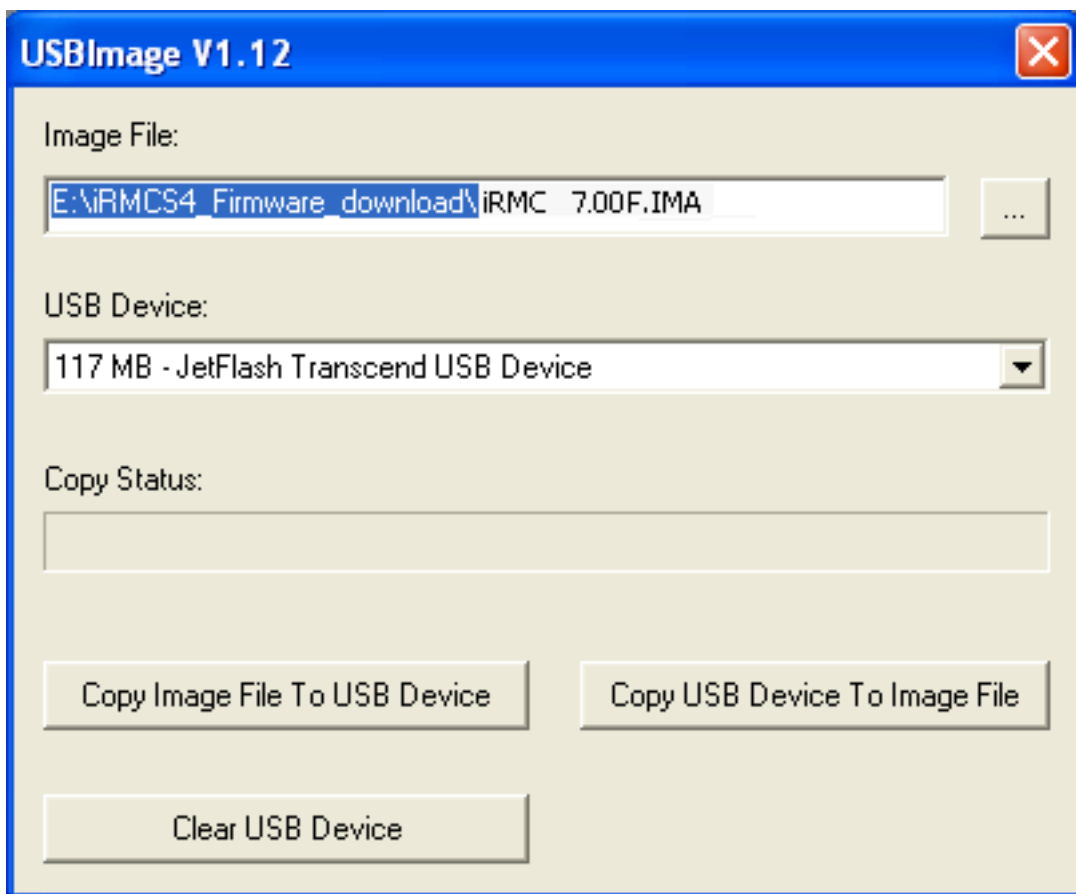



Figure 16: Copying the image file to the USB memory stick (with USBImage.exe)

4. If you have called `USBImag.exe`, you must explicitly specify the `iRMC_<Firmware-Version>.IMA` file in the **Image File** field.
5. Click **Clear USB Device** to delete the data from the USB memory stick.
6. Click **Copy Image File to USB Device** to copy the file `BMC_<Firmware-Version>.IMA` to the USB memory stick and extract it.

 This action overwrites the content of the USB memory stick.

When the copy operation is complete, the flash tools and image files are present on the USB memory stick.

Name	Size	Type	Date Modified
FDOS		Dateiordner	26.09.2012 10:26
MENU		Dateiordner	26.09.2012 10:26
700F_317.bin	30.720 KB	BIN-Datei	29.07.2013 11:43
Autoexec.bat	1 KB	Stapelverarbeitung...	09.11.2007 15:02
CHECK.EXE	15 KB	Anwendung	19.05.2009 10:44
clibmc.bat	1 KB	Stapelverarbeitung...	08.03.2006 10:46
command.com	65 KB	Anwendung für MS-...	16.02.2007 13:29
config.sys	1 KB	Systemdatei	16.02.2007 14:40
CVT100.EXE	20 KB	Anwendung	06.08.1988 20:17
CVT100.SET	1 KB	SET-Datei	05.12.2002 15:06
DosYafuf.exe	183 KB	Anwendung	22.07.2013 08:01
flashm.bat	6 KB	Stapelverarbeitung...	29.07.2013 11:42
FLIRMCS4.EXE	42 KB	Anwendung	17.07.2013 09:08
IPMIVIEW.EXE	148 KB	Anwendung	03.05.2013 10:59
IPMIVIEW.INI	14 KB	Konfigurationseinst...	03.08.2010 14:20
KERNEL.SYS	45 KB	Systemdatei	16.02.2007 15:11
readme.txt	9 KB	Textdokument	26.07.2013 08:03
SLEEP.EXE	9 KB	Anwendung	25.02.1998 20:17
WBAT.INI	3 KB	Konfigurationseinst...	08.06.2004 14:12

Figure 17: Image files and flash tool on the USB memory stick

6.3.2 Updating using the flash tools

To update the iRMC's firmware using the operating system flash tools proceed as follows:

1. Connect the USB memory stick to the managed server.
2. In the Windows command line or the Linux CLI switch to the drive corresponding to the USB memory stick.
3. Set the firmware selector to the value 4 by calling the flash tool with the parameter `/s 4`.

E.g., in the Windows command line you enter:

```
w32flirmcs4 /b 4 or w64flirmcs4 /b 4
```

4. Start the update of the firmware and the SDR data by calling the flash tool with the corresponding update files.

E.g., in the Windows command line you enter:

```
w32flirmcs4 *.bin /i or w64flirmcs4 *.bin /i
```

This flashes the new version into the inactive EEPROM.

Firmware and SDR are flashed from the same *.bin file.

If you call the flash tool with the parameter `/wr`, the updated firmware will automatically be activated once the flash has completed. In this case, it will not be necessary to reboot the iRMC.

During the firmware update, the console informs you about the progress of the update operation. If an error occurs, the update operation is aborted and a corresponding return code is reported ("[Flash Tools](#)" on page 59).

5. Restart the managed server. This automatically activates the firmware image with the updated firmware.

6.3.3 Emergency flash

If the iRMC firmware can no longer be executed, e.g. because the SDRs are not compatible with the system, then you can use the emergency mode to start the firmware running again. In emergency mode, the system automatically branches to the bootloader and is ready for the firmware update.

Emergency mode is indicated by the error LED (global error LED) (red) and the identification LED (blue) flashing alternately.

To switch the managed server to emergency mode and then update the iRMC's firmware, proceed as follows:

1. Disconnect the power supply connector.
2. Insert the connector in the socket again with the **Identify** key held down.
The managed server is now in emergency mode.
3. Boot the server to DOS and use the recovery flash procedure to update the iRMC's firmware.

If the firmware is not active then the boot operation may take up to two minutes to start. You can ignore the error message "iRMC S4 Controller Error" which the BIOS outputs during this period.

6.4 FlashDisk menu

The **FlashDisk** menu opens after a boot process with booting from the USB memory stick.

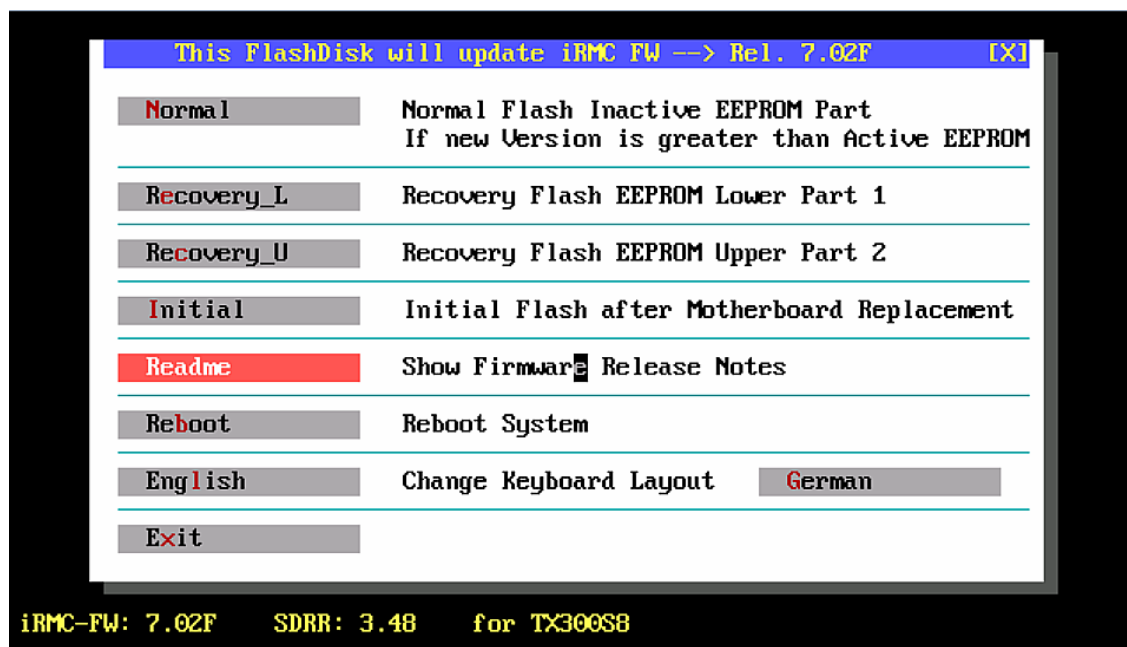


Figure 18: FlashDisk menu

The **FlashDisk** menu offers commands to update the firmware of the iRMC in various ways.

Normal

Performs a normal flash.

During a normal flash operation, those areas of the EEPROM that contain the active firmware are checked to see whether they are up to date. If one of these areas is not up to date then the corresponding area for the inactive firmware is updated if it is not already up to date.

Recovery_L

Performs a recovery flash for firmware image 1 (Low Firmware Image).

In the case of a recovery flash, the flash is performed for all three areas of firmware image 1 without any version check.

Recovery_U

Performs a recovery flash for firmware image 2 (High Firmware Image).

In the case of a recovery flash, the flash is performed for all three areas of firmware image 2 without any version check.

Initial

Flashes both active and inactive firmware.

Readme

The Readme file is opened.

Reboot

Performs an iRMC warm start.

English / German

Specify keyboard layout. German is set by default.

6.4.1 Updating via the FlashDisk menu

For an update via the **FlashDisk** menu, you require a bootable USB memory stick (for more information, refer to ["Setting up the USB memory stick" on page 53](#)).

1. Connect the USB memory stick to the managed server (directly or via remote storage).
2. Boot from the USB memory stick.
After completion of the boot operation, the data in the USB memory stick is automatically copied to a RAM disk. The `autoexec.bat` file is then started automatically.

The **FlashDisk** menu opens.

3. Start the required update variant by clicking on the corresponding button.
During the firmware update, the console informs you about the progress of the update operation. If an error occurs, the update operation is aborted. A corresponding return code is reported (for more information, refer to ["Flash Tools" on page 59](#)).
4. Once the update operation has been completed, click on **Exit**, to close the **FlashDisk** menu.
5. Remove the USB memory stick from the managed server.
6. Restart the managed server (e.g. with [Ctrl]+[Alt]+[Del]).

6.5 Flash Tools

Depending on the operating system you are running, you use one of the following flash tools:

Operating system	Flash tool
DOS	flirmcs4
Windows	winflirmcs4 Prerequisite: The ServerView agents for the used Windows operation system (32/64 bit) must be running on the managed server.
Windows (32 bit)	w32flirmcs4 (No agents required.)
Windows (64 bit)	w64flirmcs4 (No agents required.)
Linux	linflirmcs4

You call the appropriate flash tool in the Windows command line or at the Linux CLI.

The flash tools differ only in respect of the name and the environment in which they are called. This means that the description below applies to each of these tools.

Syntax

```
w32flirmcs4 <filename> [<Option>]...
```

Options

Option	Meaning
<filename>	Without options: update firmware (same as /u).
/1	Flash 1st EEPROM with version check.
/2	Flash 2nd EEPROM with version check.
99	No flash because EEPROM firmware is up to date.
?	Shows this Help Info.

Option	Meaning
/b [0-5]	Shows/sets FW Boot Selector. 0 Auto select higher firmware version 1 Image 1, Low Firmware Image 2 Image 2, High Firmware Image 3 Auto select lower firmware version 4 Auto select most recently programmed firmware 5 Auto select least recently programmed firmware
/d [0-99] [0-99]	Additional debug output [verbose level] <ul style="list-style-type: none"> Without verbose level: print whole debug output One verbose level: print debug output <= verbose level Two verbose level: print debug output between 1st and 2nd verbose level
/e	Emulation test mode (no access to iRMC, for test only)
/f1	Flash forced 1st EEPROM without version check.
/f2	Flash forced 2nd EEPROM without version check.
/fi	Flash forced inactive EEPROM without version check.
/h	Shows this Help Info.
/i	Flash inactive EEPROM with version check.
/ignore	Flash the selected EEPROM without any checks (FW version, SDR ID).
/logError[file]	Writes errors to logfile, default: w32flirmcs4.logError.
/logOutput [file]	Writes each terminal output to logfile, default: w32flirmcs4.logOutput.
/logDebug[file]	Writes each internal debug output to logfile, default: w32flirmcs4.logDebug.
/n	No console output, no user entry necessary
/noUserEntry	No user entry necessary, but with console output
/noExitOnError	No exit and continue program after error (for test only)
/o	Show the actual revisions of the firmware.
/s [0-2]	Shows/sets FW Upload Selector. 0 Auto inactive image 1 Image 1, Low Firmware Image 2 Image 2, High Firmware Image

Option	Meaning
/u	Flash inactive EEPROM if new version is greater than active EEPROM
/v	Shows the actual program version of w32flirmcs.
./vNoDriverload	Shows the actual program version of w32flirmcs.
/wr	Initiate a warm reset of the firmware.

Return codes

Code	Meaning
00	No error, program successfully terminated
01	Arguments are missing or not correct.
02	Firmware upload selector value is out of range (0-2).
03	Firmware boot selector value is out of range (0-5).
04	Firmware image file is missing.
05	Firmware image file could not be opened.
06	Communication with BMC is not possible.
07	Incorrect completion code of the IPMI command
08	The system has no iRMC.
09	SDR ID of the system and the flash image file are not the same.
10	Cannot allocate memory buffer.
11	File transfer failed.
12	IPMI call failed (response data size is 0).
13	HTI interface is not available.
14	HTI interface detection failed (other detection error).
15	HTI interface detection failed (ScSBB2.sys driver not available).
16	Connecting to HTI failed.
17	Flash process failed.
18	Error completion code of [F5 0B Start TFTP Flash]: 0xCB]. Data not present (TFTP Server could not provide the requested image file).
19	Error completion code of [F5 0B Start TFTP Flash]: 0xD3]. Destination unavailable (TFTP Server is not reachable).
20	Unknown completion code of [F5 0B Start TFTP Flash].
21	Wrong file size of the firmware image file

Code	Meaning
22	Seek error with the firmware image file.
23	GetFullPathName failed.
24	Cannot load image because flash status is 0x04 (image download in progress).
25	Cannot load image because flash status is 0x08 (flash in progress).
26	Unexpected flash status of the iRMC before loading file.
27	Firmware image file does not exist.
28	Unexpected IPMI command response data size.
29	Unexpected return value from HTI function.
30	The operating system cannot run this application program.