

User Guide - English



**FUJITSU Software ServerView Suite**  
**iRMC S6**  
**Configuration and Maintenance 2.x**

Edition March 2023

## **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](mailto:manuals@ts.fujitsu.com).

## **Documentation creation according to ISO 9001 and ISO 27001**

To ensure high quality and information security standards while creating documentation, the quality management system and information security management system of cognitas are certified in compliance with ISO 9001 and ISO 27001.

cognitas. Gesellschaft für Technik-Dokumentation mbH

[www.cognitas.de/en/](http://www.cognitas.de/en/)

## **Copyright and trademarks**

Copyright 2023 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

<b>1 Preface</b>	<b>6</b>
1.1 Purpose and target groups	7
1.2 ServerView Suite link collection	7
1.3 Documentation for the ServerView Suite	8
1.4 Documents for the iRMC	9
1.5 What's new	9
1.6 Typographic conventions	10
<b>2 Overview of the iRMC functions</b>	<b>11</b>
2.1 Standard functions	11
2.2 Extended functions	17
2.3 Embedded Lifecycle Management	20
2.4 User interfaces	22
2.5 Application programming interfaces	23
2.6 Communication protocols used	24
2.7 Front panel LEDs and ID button controlled by the iRMC	26
<b>3 First steps</b>	<b>27</b>
3.1 Configuration of the LAN interface	27
3.1.1 Requirements	27
3.1.2 Configuring the LAN interface using UEFI	28
3.1.3 Testing the LAN interface	30
3.2 Logging on to the iRMC S6 for the first time	30
3.2.1 Requirements	30
3.2.2 iRMC factory defaults	31
3.2.3 Logging on for the first time	31
3.2.4 Logging out	35
<b>4 Certificates</b>	<b>36</b>
4.1 Server certificate	37
4.1.1 Importing the certificates for secure communication	37
4.1.2 Generating a certificate	38

4.2 CA certificate for the iRMC .....	38
4.3 CA certificate for the eLCM .....	39
4.4 S/MIME certificate for Email encryption .....	40
<b>5 User management .....</b>	<b>42</b>
5.1 User management concept .....	42
5.2 User permissions .....	45
5.3 Local user management .....	46
5.3.1 Two factor authentication (2FA) .....	47
5.3.2 Secure Authentication via SSHv2 .....	53
5.3.3 Configuring E-mail alerting to local iRMC users .....	62
5.4 Global user management .....	68
5.4.1 Concept of user management via an LDAP directory service .....	69
5.4.2 Steps to configure collaboration .....	75
5.4.3 SVS_LdapDeployer utility .....	76
5.4.4 iRMC user management via Microsoft Active Directory .....	80
5.4.5 iRMC user management via Novell eDirectory .....	90
5.4.6 iRMC user management via OpenLDAP .....	99
5.4.7 Configuring E-mail alerting to global iRMC users .....	102
5.4.8 Configuring the iRMC for LDAP authentication .....	107
5.4.9 User permission configuration .....	109
<b>6 Remote installation of the operating system .....</b>	<b>112</b>
6.1 General procedure for installing the operating system .....	112
6.2 Connecting a storage medium as Virtual Media .....	114
6.3 Booting the managed server .....	116
6.4 Installing Windows on the managed server .....	120
6.5 Installing Linux on the managed server .....	121
6.6 Installing ESXi on the managed server .....	123
<b>7 Firmware update .....</b>	<b>125</b>
7.1 Firmware selector .....	126
7.2 Golden image .....	126
7.3 Methods of firmware update .....	127
7.3.1 Firmware Update using the web interface .....	128
7.3.2 Firmware update using ServerView Update Manager Express .....	128

7.3.3 Firmware update using a USB stick .....	129
7.4 Firmware downgrade .....	133
7.5 Firmware alignment .....	133
7.6 Firmware backup .....	134
<b>8 RAID configuration .....</b>	<b>136</b>
8.1 Supported RAID levels .....	137
8.2 Integrity Checks .....	138
8.3 RAID controller .....	139
8.3.1 Physical disks .....	141
8.3.2 Logical drives .....	143
8.4 Creating a logical drive .....	145
8.5 Deleting a logical drive .....	145

---

# 1 Preface

Modern server systems are becoming increasingly complex, and the requirements for managing such systems are growing accordingly.

The integrated Remote Management Controller iRMC represents a BMC with integrated LAN connection and extended functions. The iRMC therefore 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 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 S6 on the system board of a PRIMERGY server

As an autonomous system on the system board of a PRIMERGY or PRIMEQUEST server, the iRMC has its own operating system, its own web server, separate user management and independent alert management. The iRMC remains powered on even when the server is powered off or in stand by mode. Communication occurs via a LAN connection, that can be shared with the Fujitsu PRIMERGY server or used exclusively for system management.

Beyond making it possible to manage a PRIMERGY server out-of-band, the enhanced functions of the iRMC, which comes with an integrated SD card, allow 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 (with optional ServerView PrimeUp) 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 **Overview** 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.
- **Certificates** describes why and how the iRMC uses certificates.
- **User management** explains the iRMC-related user management.
- **Remote installation** describes how to install the operating system via iRMC.
- **Firmware update** describes how to update the firmware of the 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.
- 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:

- Via the following link:  
[http://support.ts.fujitsu.com/prim\\_supportcd/SVSSoftware/start.html](http://support.ts.fujitsu.com/prim_supportcd/SVSSoftware/start.html)
- Via the ServerView Suite DVD 2.
  1. In the start window of the ServerView Suite DVD 2, select the option **ServerView Software Products**.
  2. 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 on the download area of the Fujitsu Technical Support pages.

To download the documentation, proceed as follows:

1. Open the web page  
<https://support.ts.fujitsu.com/IndexDownload.asp?PaOpenTab=manuals>.
2. Click **Browse For Product**. A list with product lines opens.
3. Select **Software - ServerView - Operation**. A list with products opens.
4. Select the appropriate product from the product list.

The corresponding page with the **Documents** tab opens.



Only for English and German Fujitsu Technical Support pages: If no tab is displayed, select **OS Independent (BIOS, Firmware, etc.)** under **Selected operating system** and then click **Documents** tab.

---

## 1.4 Documents for the iRMC

This user guide is part of a documentation suite describing the iRMC S6 firmware version 2.x. The documentation suite of the iRMC S6 comprises the following user guides:

- iRMC S6 Configuration and Maintenance
- iRMC S6 Concepts and Interfaces
- iRMC S6 Web Interface

The target systems for this iRMC version to be running on are the PRIMERGY M7 machines.

### Related readings

The "Specification iRMC Redfish API" describes in detail the commands and parameters of the Fujitsu Redfish API.

The iRMC "Redfish API" white paper describes the general handling of the iRMC Redfish API.

The "Specification iRMC RESTful API" describes in detail the commands and parameters of the iRMC RESTful API.

The iRMC "RESTful API" white paper describes the general handling of the iRMC RESTful API.

The "ServerView embedded Lifecycle Management (eLCM) 1.3 for iRMC S6" user guide describes in detail the update and image handling via the iRMC.

The "ServerView Installation Manager" user guide describes in detail the software installation within the ServerView environment.

## 1.5 What's new

In this edition of the iRMC several security functions have been implemented:

- Elaborated password policy
- Account locking after a number of failed attempts
- Two factor authentication
- Force to change a default password
- Customized log-on screen
- Power redundancy can be implemented and set.
- Automatic firmware alignment after a mainboard replacement

## 1.6 Typographic conventions

The following typographic conventions are used:

Convention	Explanation
!	Various types of risk, namely health risks, risk of data loss and risk of damage to devices.
	Additional relevant information and tips.
<b>bold</b>	References to names of interface elements.
monospace	System output and system elements, e.g., file names and paths inside text blocks.
monospace	Commands, system output, syntax and statements that are to be entered using the keyboard outside text blocks.
<b>monospace semibold</b>	Process example for statements that are to be entered using the keyboard.
<a href="#">blue continuous text</a>	A link to a related topic.
<a href="#">purple continuous text</a>	A link to a location you have already visited.
<abc>	Variables which must be replaced with real values.
[abc]	Options that can be specified (syntax).
[Key]	Key on your keyboard. If you need to enter text in uppercase, the Shift key is specified, e.g., [Shift] + [A] for an A. If you need to press two keys at the same time, this is indicated by a plus sign between the two key symbols.
Quotation marks	For names of chapters and manuals.

Table 1: Typographic conventions

### Screenshots

Some of the screenshots are system-dependent, so some of the details shown may differ from your system. There may also be system-specific differences in menu options and commands.

---

## 2 Overview of the iRMC functions

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

### 2.1 Standard functions

No special license key is needed for the standard functions.

#### **Account lock**

After a specified number of failed login attempts a user account can be locked for a specified time period or permanently.

#### **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 e-mail.

The iRMC also provides the ServerView Agentless Service with all the relevant information.

#### **Basic functions of a BMC**

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

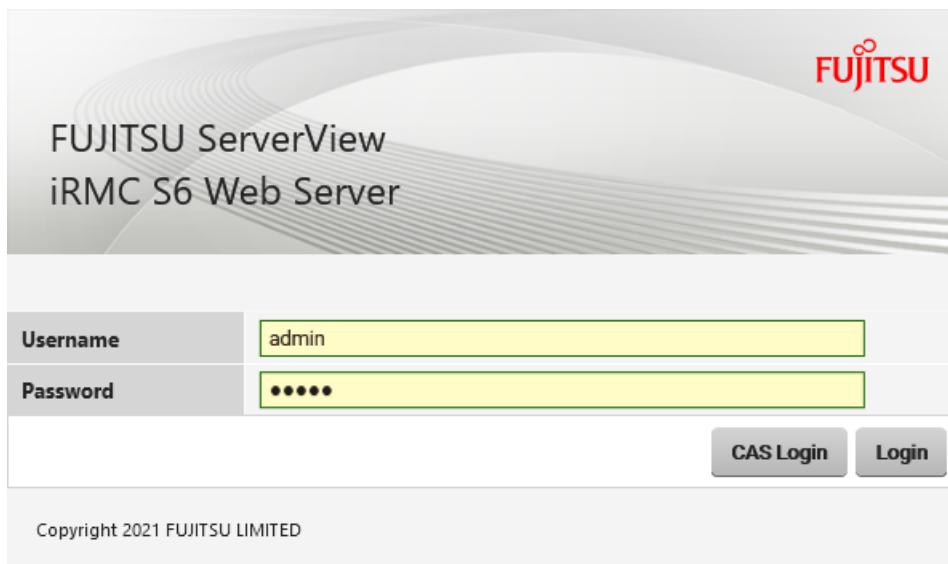
#### **Browser access**

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

#### **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 on 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.

### **Customer Self Service (CSS)**

You can replace several of the system's hardware components on your own. These components are marked in the iRMC S6 web interface.

In addition, the error list of the system event log (SEL) shows whether each event has been triggered by a CSS component.

### **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 three DNS servers are supported. If DNS/DHCP is not available, the iRMC also supports static IP addresses.

### **Global error LED**

A global error LED indicates the status of the managed server at all times.

### **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

### **"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 via the iRMC web interface.

### **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.

### **LAN over USB**

An interface called LAN over USB enables in-band communication between the managed server and the iRMC. This communication provides an additional interface from the managed server to the iRMC, e.g. to use the Redfish interface or access via SSH. It also avoids a shortcut between the management LAN and the productive LAN for e.g. Redfish access from managed server to iRMC. For more information, refer to the "iRMC S6 - Concepts and Interfaces" manual.

### **Local user management**

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

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

### **Password Policy**

For security reasons the password policy has been elaborated. A password needs to consist of at least 12 characters and a combination of alphanumeric and special characters.

### **Platform Firmware Resiliency (PFR)**

In the case the image file of the BIOS or iRMC firmware is broken or has been tampered with the iRMC recovers the tampered or broken image file with a Golden Image automatically.

### **Power consumption control**

The iRMC allows comprehensive control of power consumption on the managed server. You can also specify the mode the iRMC uses to control power consumption on the managed server. You can switch between these modes as required.

### **Power LED**

The power LED tells you whether the server is currently switched on or off and allows several power operations depending on the current power state if ServerView Agentless Service is installed and running.

### **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 **Power** menu of the AVR window
- Using the Remote Manager and the command line interface
- With a script

### **Power supply smart redundancy**

The new generation of modular power supply units (PSU Gen3) supports smart redundancy. That means the redundant PSUs of the managed server become active if the power load of the active PSU exceeds a defined limit.

## **RAID Configuration**

You can set up and maintain RAID configurations of the following levels:

- RAID-0
- RAID-1
- RAID-1E
- RAID-5
- RAID-6
- RAID-10
- RAID-50
- RAID-60

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

You can view, save and delete the contents of the SEL using a choice of interfaces:

- The iRMC web interface
- The Telnet/SSH-based interface (Remote Manager) of the iRMC
- With a script via Redfish API

## **Read, filter and save the internal event log (IEL)**

You can view, save and delete the contents of the IEL using a choice of interfaces:

- The iRMC web interface
- The Telnet/SSH-based interface (Remote Manager) of the iRMC
- With a script via Redfish API

## **Security (TLS, SSH)**

Secure access to the web server and secure graphical console redirection, including mouse and keyboard, is provided via HTTPS. An encrypted connection protected by SSH mechanisms can be set up to access the iRMC using the Remote Manager. The Remote Manager is a text-based user interface of the iRMC.

### **Simple configuration - interactive or script-based**

The following tools are available for configuring the iRMC:

- iRMC web interface
- Profile Management
- Redfish API
- Remote Manager
- RESTful API
- SCCI API
- UEFI BIOS Setup

It is also possible to perform configuration with 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 and profile management.

### **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, SNMP RAID.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.

Furthermore SNMP traps can be sent to the recipient specified in the destination configuration of the trap. For more information, refer to the "iRMC S6 - Concepts and Interfaces" manual.

### **Text console redirection**

You can establish a Telnet/SSH session to the iRMC using a Telnet/SSH client to access the text based Remote Manager. The Remote Manager offers a restricted menu-based access to the iRMC. Besides Telnet there is support for SOL (serial over LAN) and SSH (Secure Shell).

### **Two factor authentication**

Local iRMC user accounts can be configured to use two factor authentication via TOTP. TOTP stands for Time-based One-Time Passwords and is a common form of two factor authentication (2FA). Unique numeric passwords are generated with a standardized algorithm that uses the current time as an input. The time-based passwords are available offline and provide user friendly, increased account security when used as a second factor.

### **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.

## **2.2 Extended functions**

Alongside the standard functions, the iRMC also supports Advanced Video Redirection, Virtual Media and embedded Lifecycle Management (eLCM). These extended functions require a valid license key, which can be purchased separately.

### **Advanced Video Redirection (AVR)**

The iRMC supports Advanced Video Redirection via HTML5, Java or VNC.

AVR via Java or HTML5 offers the following benefits:

- Operation via a standard web browser. No additional software needs to be installed on the management station other than a 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 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 Network Computing (VNC)**

You can also use a VNC viewer for redirecting to the managed server. VNC is open source and platform-independent – there are clients and servers for many GUI-based operating systems and for Java. Two clients may connect to a VNC server at the same time. Only the first session can be used to redirect control. The other session works in a read only mode.

- The VNC server, implemented into the iRMC, is the program that shares some screen of the managed server and allows the client to share control of it.
- The VNC client (or viewer) is the program that displays the screen data originating from the server, receives updates from it, and presumably controls it by informing the server of collected local input.
- The VNC protocol (RFB protocol) is a simple one, based on transmitting one graphic primitive from server to client and event messages from client to server.

In order to use a VNC session a third party VNC client software is required on your machine such as: TightVNC or RealVNC. Some VNC clients, like the popular TightVNC, do not encrypt your connection beyond the initial sign-in stage. For a secure connection you can tunnel a VNC connection over a Secure Shell (SSH) tunnel.

If you want to tunnel VNC through SSH, it is recommended you use PuTTY to make the connection to the iRMC.

### **Embedded Lifecycle Management (eLCM)**

The embedded Lifecycle Management (eLCM) solution allows you to control lifecycle 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 (Online/Offline update)
- eLCM image management (Custom Image)
- eLCM deployment
- eLCM health management (PrimeCollect)
- eLCM simple update

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

### **VMware HCL support**

During update preparation of a managed server with VMware ESXi operating system, inventory data is compared with the HCL file, which is downloaded from the update repository. This list is based on the information about certified server configuration published by VMware. The comparison results in the following actions:

- There are no entries for the component: the newest version is added to the update list
- There are entries for a component: the most recent certified version is added to the update list

You can skip the VMware HCL verification in the Update settings. This setting only affects systems with ESXi and ServerView CIM providers installed.

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

### **Virtual Media**

The Virtual Media function makes a "virtual" drive available which is 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 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/DVD drive
- CD/DVD image
- HDD/USB physical and logical drive (supported web browsers need to be run as Administrator on Windows)
- HDD/USB image
- Shared folder used via the Virtual Media wizard

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

## 2.3 Embedded Lifecycle Management

ServerView embedded Lifecycle Management (eLCM) for Fujitsu PRIMERGY servers supports general routine management tasks. System administrators benefit from simplified, highly integrated and automated server management processes.

The eLCM enhances ServerView functions directly available (embedded) within the server without the need for external media like USB, CD or DVD. Users have access to the following embedded ServerView functions:

- The embedded Installation Management (eIM) is the eLCM equivalent of the ServerView Installation Manager. The eIM and the repository are stored on the iRMC S6 SD card, so no external ServerView media needs to be set up to install Fujitsu PRIMERGY systems.
- The embedded RAID Management (eRM) serves as the eLCM equivalent of the ServerView RAID Manager and supplements the eIM with respect to RAID management.
- The embedded Offline and Online Update (eUM) is the eLCM edition of the ServerView Update Manager modules. The online update allows you to update BIOS and controller firmware while the server operating system is running (with optional ServerView PrimeUp). The offline update allows you to update system components like network or storage controller firmware on the managed server.
- In contrast to highly automated offline and online updates, the eLCM Simple Update allows you to update an individual component to the necessary version. Depending on the component, the online or offline mode is available.
- The embedded custom image allows you to specify a URL from which you can download ISO images onto the iRMC SD card.
- eLCM PrimeCollect collects and stores detailed information about the hardware and software of Fujitsu PRIMERGY servers, including error information in the case of server malfunction. The collected information is stored in a ZIP file on the iRMC S6 SD card.

The eLCM update management and deployment use a repository server which provides the relevant packages for download.

Default update repository: <https://support.ts.fujitsu.com>

For an efficient access the content of the deployment repository is mirrored to the following regions:

- France: <https://webdownloads.ts.fujitsu.com>
- Austria: <https://webdownloads1.ts.fujitsu.com>
- Germany: <https://webdownloads2.ts.fujitsu.com>
- USA: <https://webdownloads3.ts.fujitsu.com>

For security reasons, iRMCs should not be directly connected to the Internet. But you can use the ServerView Update Repository software which mirrors the closest repository in the local data center or network.

eLCM bypasses the traditional server management, which requires the agent type and management software running on the server operating system. Shifting the management software to the iRMC improves the performance of the managed server.

The only software that eLCM in some cases needs to be running on the server's OS is the ServerView Agentless Service component. Exclusively communicating with the iRMC S6 over HTI (High-Speed Transfer Interface), the Agentless Service has only a very small footprint on the server operating system, with negligible impact on the system's overall performance.

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 internal eLCM SD card and is managed by eLCM.

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 [F5].
3. In the opened eLCM menu select the function to be used:
  - System configuration and installation
  - RAID configuration
4. Once 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 S6 - Concepts and Interfaces" user guide.
2. Start the iRMC web interface and open the **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 **Start Deployment**.

### **Unattended operation via the Redfish API**

1. Create a profile file specifying the intended system configuration and/or operating system installation. Profile handling is described in the "iRMC S6 - Concepts and Interfaces" user guide.
2. Apply the profile using the Redfish `/redfish/v1/Systems/0/Oem/ts_fujitsu/ProfileManagement/Actions/FTSProfileManagement.ApplyProfile` action. For more information see the "Specification iRMC Redfish API".

### Unattended process "SysRollOut Service" via RESTful API

For more information, refer to the RESTful API white paper.

## 2.4 User interfaces

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 Edge, Mozilla Firefox, Google Chrome).

Among other things, the web interface of the iRMC provides 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 using the web interface.

Secure access to the iRMC web server is provided with HTTPS. The web interface supports only HTTPS connections. HTTP links are redirected to HTTPS, ensuring secure access.

Operation of the iRMC using the web interface is described in the "iRMC S6 - Web Interface" user guide.

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

You can call the Remote Manager directly from a Telnet/SSH client.

The text-based user interface of the Remote Manager provides you with access to system and sensor information, power management functions and the error event log. You can also launch text console redirection. 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 S6 - Concepts and Interfaces" user guide.

## 2.5 Application programming interfaces

The iRMC S6 supports APIs (Application Programming Interface) for scripted configuration. With scripting, only one iRMC has to be configured according to the requirements of the environment. This configuration is then uploaded to all other PRIMERGY servers without the need to access them all one by one.

- Redfish

Redfish is a DMTF standard specification and schema that specifies a RESTful interface. Redfish utilizes a range of IT technologies that have been selected because of their widespread use. These technologies create a new foundation from which servers can be managed using common programming and scripting languages, such as Python, Java, PowerShell and C.

- RESTful

Representational state transfer is a way to provide interoperability between computer systems on the Internet. REST-compliant web services allow requesting systems to access and manipulate textual representations of web resources using a uniform and predefined set of stateless operations.

- SCCI

The Server Control Command Interface is a generic API defined by Fujitsu for different server management controller hardware as well as software. It can be easily extended to new commands or new configuration items.

For more information, refer to the "iRMC S6 Concepts and Interfaces" user guide.

## 2.6 Communication protocols used

The iRMC uses the following protocols and default ports for communication:

Remote side of the connection	Communication direction	iRMC side of the connection (port no. / protocol)	Configurable	Enabled by default
CAS / Single Sign-On	↔	3170/TCP	yes	yes
Email/SMTP	↔	25/TCP	yes	no
LDAP	↔	389/TCP/UDP	yes	no
HTTPS (web interface, Redfish API, RESTful API, etc.)	↔	443/TCP	yes	yes
RFB (AVR via VNC)	↔	5900/TCP	yes	no
RMCP	↔	623/UDP	no	yes
SNMP	↔	161/UDP	yes	no
SNMP trap	→	162/UDP	no	yes
SSH	↔	22/TCP	yes	yes
Telnet	↔	3172/TCP	yes	no
TFTP /repository	↔	69/UDP	no	no

Table 2: Communication protocols

The following table illustrates the connection between the iRMC and SMTP server(s) and whether it is established and secured depending on the configuration on both sides.

iRMC SNMP port number	iRMC SMTP SSL	Mail server SMTP Port Security	Connection
465	Yes	None	Not established
465	Yes	STARTTLS optional	Not established
465	Yes	STARTTLS required	Not established
465	Yes	SSL/TLS	Secured
465	No	None	Unsecured
465	No	STARTTLS optional	Unsecured
465	No	STARTTLS required	Not established
465	No	SSL/TLS	Not established
any other port number	Yes	None	Unsecured
any other port number	Yes	STARTTLS optional	Secured
any other port number	Yes	STARTTLS required	Secured
any other port number	Yes	SSL/TLS	Secured
any other port number	No	None	Unsecured
any other port number	No	STARTTLS optional	Unsecured
any other port number	No	STARTTLS required	Not established
any other port number	No	SSL/TLS	Not established

Table 3: Communication modes with SMTP servers

## 2.7 Front panel LEDs and ID button controlled by the iRMC

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

Status LEDs on the front panel (Nexperience design):

Status of the server	LED on the server	
	S6 LED (green)	Power LED (green)
AC-OFF	off	off
S6 (shutdown)	on	off
S0 (power-on)	off	on
S3 (sleep mode)	off	flashing with 1 Hz (BIOS-controlled)
iRMC not readyON	on	flashing 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
S6 (shutdown)	orange
S0 (power-on)	green
S3 (sleep mode)	flashing green with 1 Hz (BIOS-controlled)
iRMC not ready	flashing alternately in orange/green with 1 Hz (iRMC-controlled)
Power-on delay	yellow

The ID button on the front panel provides the following actions:

Situation	Action	Result
No special situation	Press ID button less than 5 seconds.	Toggles ID LED.
No special situation	Press ID button longer than 5 seconds.	Restarts iRMC firmware.

---

# 3 First steps

The first steps for working with the iRMC are as follows:

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

## 3.1 Configuration of the LAN interface

You configure the LAN interface for out-of-band communication with the UEFI setup utility. Before you configure the LAN interface, there are some requirements to be met.

After configuration you must test the LAN interface.



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

You can also configure in-band communication via LAN over USB. For more information, refer to the "iRMC S6 Concepts and Interfaces" user guide.

### 3.1.1 Requirements

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 on-board 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.

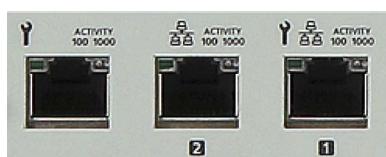


Figure 2: Ports for the iRMC (indicated by wrench symbol)

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)
	System LAN (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 UEFI

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

### 3.1 Configuration of the LAN interface

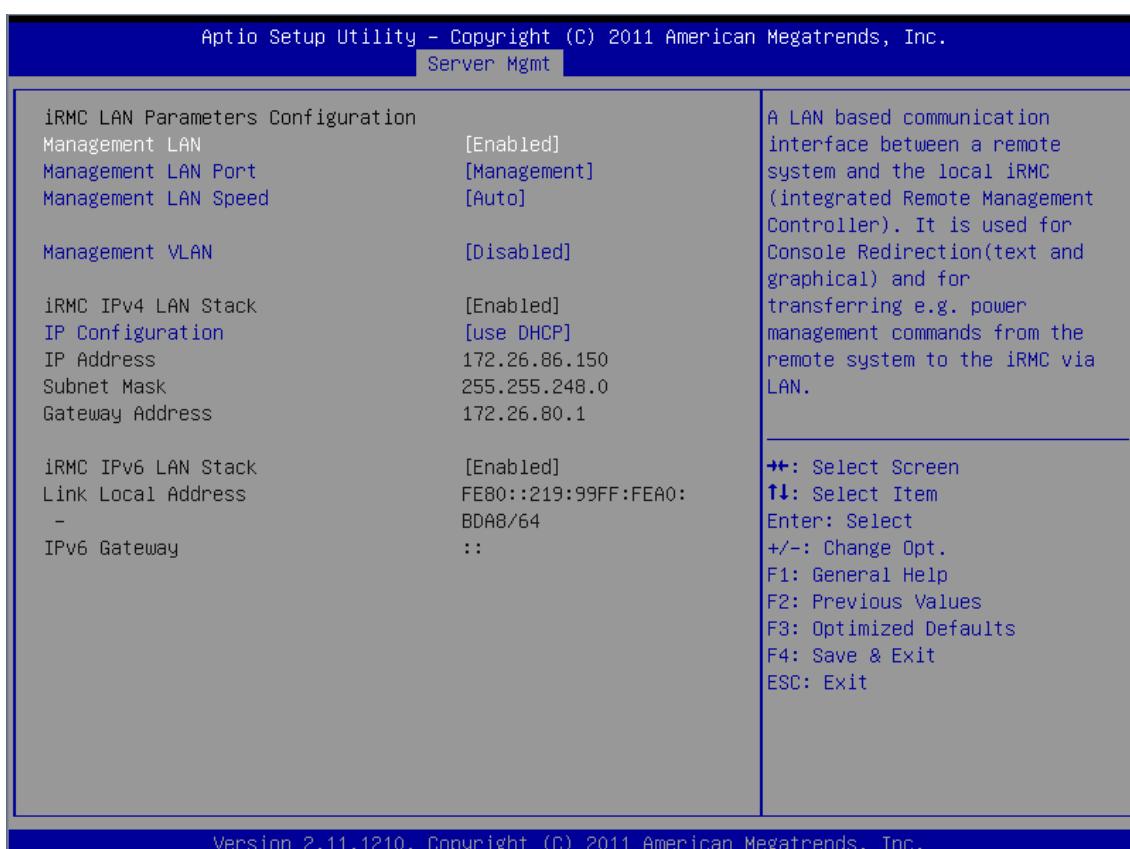


Figure 3: iRMC LAN Parameters Configuration Menu

3. In the **Management LAN** field, enter **Enabled**.
4. In the **Management LAN Port** field, enter **Management**.



For more information on configuring the remaining settings, refer to the "iRMC S6 - 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 S6" in the "iRMC S6 - 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 30](#)).

#### 3.1.3 Testing the LAN interface

You can test the LAN interface as follows:

1. Use a web browser to attempt to log on to 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 the ping command.

## 3.2 Logging on to the iRMC S6 for the first time

The factory default settings of the iRMC allow you to log on 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 you just need one of the following browsers to connect via the web interface:

- Microsoft Edge Browser
- Google Chrome as of version 50
- Mozilla Firefox as of version 50

If two factor authentication is enabled for your account, the following is required:

- The NTP service is configured and used with the iRMC.
- You use a TOTP-based authorization application to generate a one-time password , e.g.: MS authenticator or Fast 2FA.

For console redirection the prerequisite depends on the connection type used:

- Java: Java Runtime Environment
- HTML5: a web browser
- VNC: a VNC viewer of your choice

In your network:

- If you do not use static IP addresses there must be a DHCP server in your network.
- If you want to log on with a symbolic name rather than an IP address on 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.

#### 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      The password for your machine is provided on the System ID Card

---



For security reasons, you are forced to change the password of the admin user during the first logon.

A password must differ from the user name regardless of the character case and be at least 12 characters long. Blanks are not allowed. The password must contain three of the following character types:

- Lowercase letter
  - Uppercase letter
  - Special character (without "+" )
  - Digit (0-9)
- 

##### 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 read off 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 field in the **Network Interface** group of the **Network Management** page.

#### 3.2.3 Logging on for the first time

If you log on for the first time, you need to login as administrator using the administrator credentials to accept the End User License Agreement:

**Username:** admin

**Password:** The password for your machine is provided on the System ID Card.

Both the **Username** and the **Password** are case-sensitive.



For security reasons it is recommended that you create a new administrator account once you have logged in, and then delete the default one. At least change the password for the administrator account ("User management" on page 42).

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

A login dialog box opens.

The screenshot shows a login dialog box for the FUJITSU ServerView iRMC S6 Web Server. The title bar displays the FUJITSU logo and the text "FUJITSU ServerView iRMC S6 Web Server". The main area contains two input fields: "Username" with the value "admin" and "Password" with five asterisks. To the right of the password field is a "Login" button. At the bottom of the dialog box, there is a small text area that says "Copyright 2021 FUJITSU LIMITED".

Figure 4: Login dialog box

3. If no login dialog box opens, check the LAN connection.
4. Enter the data for the default administrator account.
5. Click **Login** to confirm your entries.
6. For security reasons, you are forced to change the password of the admin user during the first logon: Enter a new password and repeat it.



A password must differ from the user name regardless of the character case and be at least 12 characters long. Blanks are not allowed. The password must contain three of the following character types:

- Lowercase letter
- Uppercase letter
- Special character (without "+")
- Digit (0-9)

---

If two factor authentication is specified for your account the following dialog box opens:

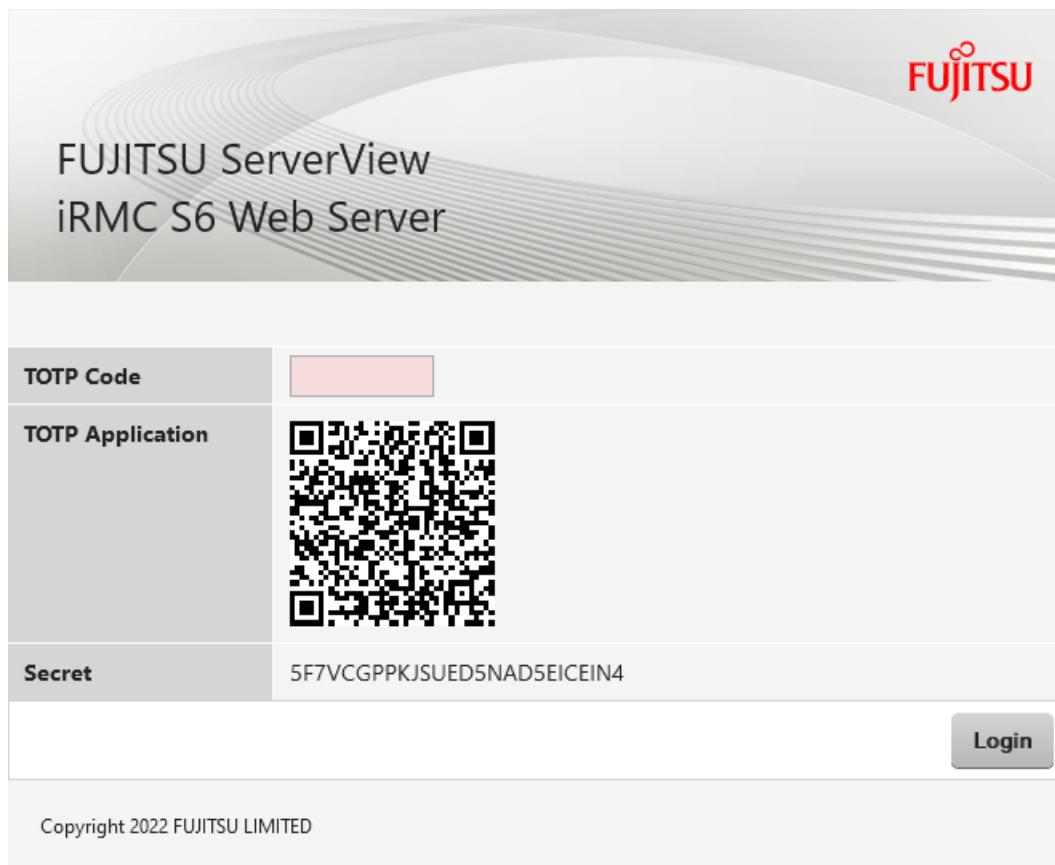


Figure 5: Login dialog box for 2FA

7. Use the QR code or the code displayed in the **Secret** field to generate a one-time password with your TOTP-based authorization application.
8. Enter the one-time password into the **TOTP Code** input field.
9. Click **Login**.

On successful login, the TOTP-based authorization application you use is accepted by the iRMC and a dialog box opens with emergency codes.

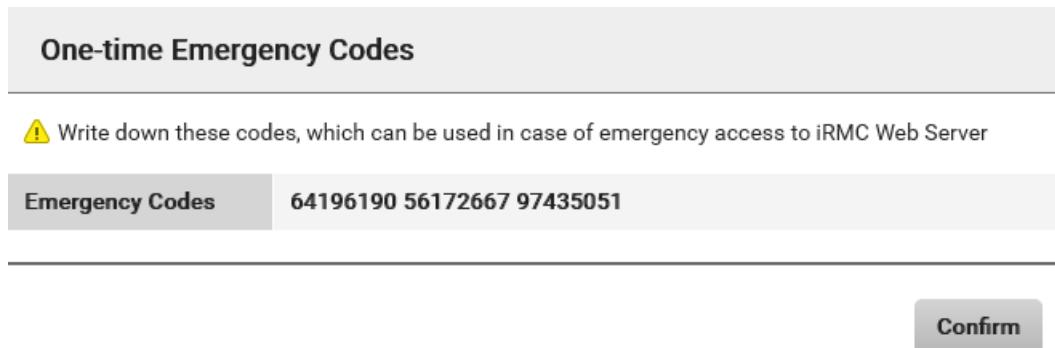


Figure 6: One-time Emergency Codes dialog box

These emergency codes are displayed only once. The codes can be used when you lose the ability to log in using two factor authentication, for instance when you lose the device with the TOTP-based authorization application or the device or application is damaged.

10. Save the emergency codes, e.g. with a screenshot.
11. Click **Confirm**.

The end user license agreement (EULA) opens.

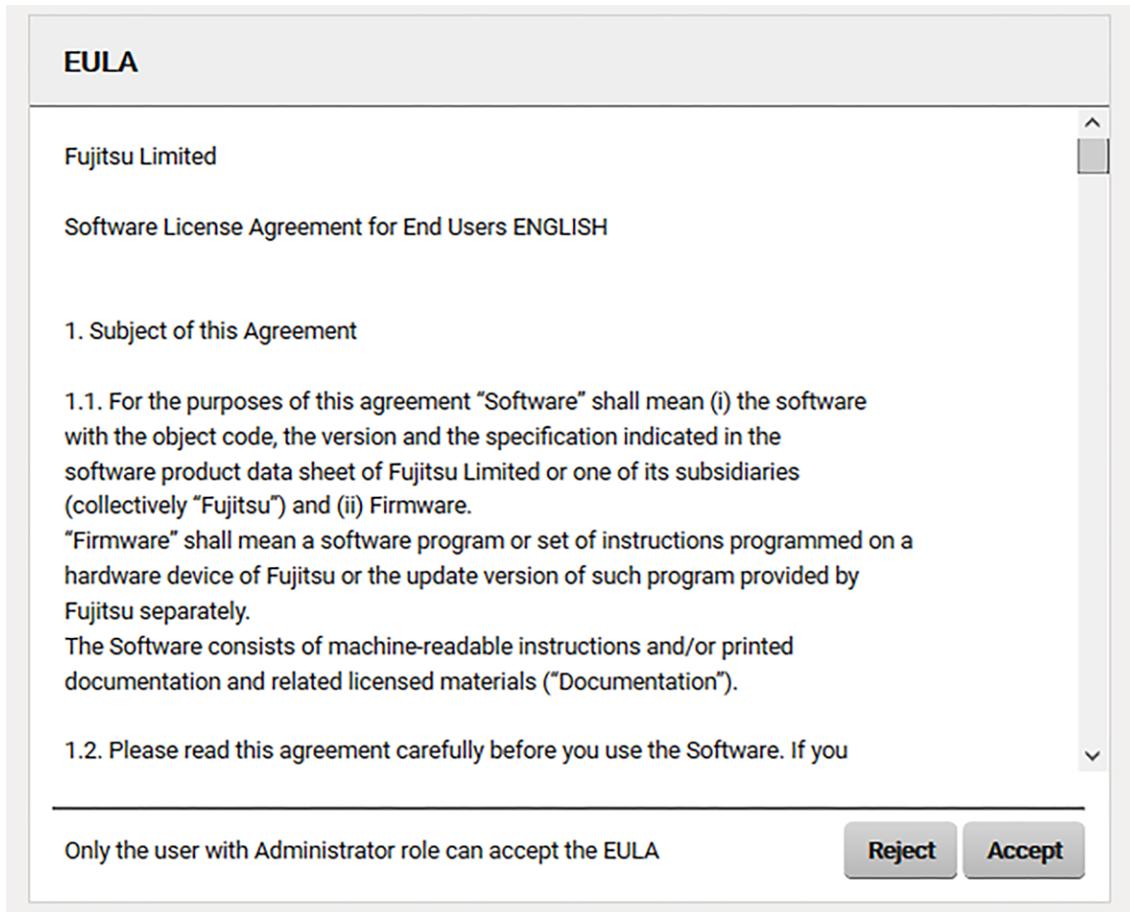


Figure 7: EULA dialog box

12. Read the agreement carefully and accept it with **Agree**.

The iRMC web interface opens with the **System Overview** page.

#### 3.2.4 Logging out

Logout allows you to terminate the iRMC session.

1. In the title bar open the <User> menu.
2. Click **Logout**.

The user is logged out and the login dialog box opens again. This allows you to log on again if required.

---

## 4 Certificates

Public key certificates are used for securing the communication. They are used to validate the authenticity and integrity of a message, software or digital document.

The most common format for public key certificates is defined by X.509.[2]. The iRMC accepts base64 (PEM) encoded X.509 certificates.

The iRMC uses certificates for the following purposes:

Certificate type	Purpose	Store	How to
Server certificate	Secure web based access to the iRMC (e.g. web interface / RESTful API / Redfish, etc.)	Key store	<a href="#">"Importing the certificates for secure communication" on page 37</a>
CA certificate	Secure communication between iRMC and CAS / SMTP servers	Trust store	<a href="#">"Importing the CA certificate for CAS/SMTP validation" on page 39</a>
CA certificate	Secure communication between iRMC and eLCM repositories	eLCM's trust store	<a href="#">"Importing the certificate for eLCM validation" on page 40</a>
S/MIME certificate	Email encryption	User store	<a href="#">"Uploading the S/MIME certificate" on page 41</a>

Table 4: Certificates used within the iRMC

The certificates available after the installation can be replaced by the following:

- A self-signed certificate
- A certificate signed by an internal CA
- A certificate signed by an external, usually commercial CA

It is highly recommended that you use SSL/TLS secured communication with the iRMC. Therefore replace the generated self-signed certificate with a valid one signed by a trusted CA, own or commercial, as soon as possible.

---

## 4.1 Server certificate

The iRMC is supplied with a unique self-signed server certificate (default certificate). This certificate is used to enable secure communication via HTTPS. The HTTP protocol does not provide a secure communication.

The self-signed certificate provides an initial - out of the box encrypted - but untrusted connection to the iRMC.

A browser warning regarding the self-signed certificate opens when you access the iRMC web interface via HTTPS.



For security reasons it's highly recommended to replace the generated self-signed certificate with a valid one signed by a trusted own or commercial CA as soon as possible.

---

To avoid browser security warnings when accessing the iRMC from a Web browser, the CA certificate must be imported to the trust store of all systems which are intended to access the server via HTTPS.

Firefox uses its own internal Certification Authorities store while Edge and Chrome use the Operating System's Trusted Certification Authorities store.

The certificates are exchanged via the web interface of the iRMC. Proceed as follows:

- Import the SSL certificate into the key store of the iRMC.
- Import the private key into the key store of the iRMC.

All server certificate-related actions on the iRMC can be initiated on the **Certificates** page of the iRMC web interface.

### 4.1.1 Importing the certificates for secure communication

The following steps are required to replace the initially created self-signed certificate with a certificate from a trusted CA into the key store of the iRMC.

1. Start the iRMC web interface and open the **Certificates** page in the **Tools** menu.
2. In the **Current SSL/TLS Certificate** group, click **Load from File**.  
The **Upload SSL/TLS Certificate** dialog box opens.
3. To import the SSL certificate and private key into the key store of the iRMC, specify the following:
  - `publickey.pem` in the **SSL/TLS public key** field
  - `privkey.pem` in the **SSL/TLS private key** field

To do this, click the associated **Select** button and navigate to the corresponding local files on the managed server. The size of the file containing a private or a public key must not be greater than 4 KB.



When you load the SSL certificate and private key from local files into the key store of the iRMC, the SSL certificate and the private key must be loaded at the same time.

4. Click **Upload** to load the SSL certificate and private key onto the iRMC.
5. Reboot the iRMC.

#### 4.1.2 Generating a certificate

Within the iRMC web interface you can create a self-signed certificate using the **Certificates** page of the **Tools** menu.

1. Open the **Certificates** page of the **Tools** menu.
2. In the **Current SSL/TLS Certificate** group, click **Generate**.  
The **Generate certificate** dialog box opens.
3. Enter the required details.
4. Click **Generate** to create the certificate.



When generating the new certificate, all the existing HTTPS connections are closed and the HTTPS server is automatically restarted. This can take up to two minutes depending on the length of the key.

No explicit reset of the iRMC is required.

## 4.2 CA certificate for the iRMC

The CA certificate is used for a SSL/TLS secured communication between the iRMC and

- CAS (Central Authentication Service for Single Sign On) servers
- SMTP (Email Alerting) servers

To enable a secure communication between the iRMC and CAS or SMTP servers the CA certificate that has been used to sign the CAS / SMTP servers' server certificate can be uploaded to the iRMC's trust store.

However both CAS and SMTP allow a SSL/TLS secured but untrusted communication if the corresponding **Verify SSL Certificate** option is deactivated. For security reasons it's highly recommended to replace the predefined CA certificate with the one that was used for

signing the CAS and SMTP servers' server certificate and to activate the **Verify SSL certificate** option.

## Importing the CA certificate for CAS/SMTP validation

The following steps are required on the iRMC, e.g. to replace the default CA certificate with the one that can be used to validate the server certificates of CAS and SMTP servers.

1. Start the iRMC web interface and open the **Certificates** page in the **Tools** menu.
2. Open the **Current CA Certificate for CAS and SMTP** group.
3. At the end of the group click **Load from File** to open the **Upload CA Certificate for CAS and SMTP** dialog box.
4. To import the CA certificate into the trust store of the iRMC, click **Select** and navigate to the CA certificate in the **Open file** dialog box.
5. Click **Upload** to load the CA certificate into the trust store of the iRMC.

## 4.3 CA certificate for the eLCM

The embedded Lifecycle Management function (eLCM) of the iRMC allows you to configure and perform Lifecycle Management of a PRIMERGY server centrally from the iRMC without the need to handle physical devices.

To use the eLCM functions, you need a valid eLCM license key, which is purchased together with the iRMC internal SD card.

The following eLCM functions require a connection to a web repository which provides the required packages for download, either via HTTP (insecure) or HTTPS (secure):

- Online Update
- Offline Update
- Deployment

The public Fujitsu default repositories for these functions use HTTPS. The CA certificates that have been used to sign their server certificates are included in the iRMC's eLCM trust store and thus allow a trusted secure connection.

However you might want to use a custom repository (e.g. an internal mirrored repository) instead of the public Fujitsu repositories.

To enable secure communication between the iRMC and custom repositories via HTTPS, the CA certificate(s) that have been used to sign the repositories' server certificate(s) can be uploaded to the iRMC's eLCM trust store.

## Importing the certificate for eLCM validation

The following steps are required on the iRMC to upload up to five CA certificates for validation of eLCM repositories into the trust store of the eLCM.

1. Start the iRMC web interface and open the **Certificates** page in the **Tools** menu.
2. To import the CA certificate into the trust store of the eLCM, in the **CA Certificate** group, click **Add**.  
The **Upload CA Certificate** dialog box opens.
3. Click **Select** and navigate to the CA certificate in the **Open file** dialog box.
4. Click **Upload** to load the CA certificate into the trust store of the eLCM.
5. Close the dialog box.

## 4.4 S/MIME certificate for Email encryption

The S/MIME certificate for Email encryption can be uploaded in the **S/MIME Certificate** sub tab of the **Certificates** tab in the **Edit Local User Account** dialog box.

Edit Local User Account	
User Information	Access Configuration
SNMPv3 Configuration	E-mail Configuration
Certificates	
SSHv2 public key	S/MIME certificate
Issuer	QA3 Root CA 5
Subject	admin@domain.com
Upload	<input type="button" value="Select..."/>
<input type="button" value="Upload"/> <input type="button" value="Delete"/>	
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

Figure 8: Uploading a S/MIME certificate

When the S/MIME certificate is uploaded, you can activate the **Enable Encryption** option in the **Email Configuration** group to send encrypted mails.

## Uploading the S/MIME certificate

To upload the S/MIME certificate onto the iRMC from a file, proceed as follows:

1. Log on to the iRMC web interface.
2. Open the **User Management** page in the **Settings** menu.
3. In the table of **iRMC Local User Accounts**, click **Edit** to edit the relevant user settings.
4. In the **Edit Local User Account** dialog box open the **Certificates** tab.
5. On the **Certificates** tab open the **S/MIME certificate** sub tab.
6. Click **Select** and navigate to the file containing the required certificate.
7. Click **Upload** to load the S/MIME certificate onto the iRMC.

After successful upload of the S/MIME certificate the **Enable Encryption** option in the **Email Configuration** tab of the user settings can be activated.

---

# 5 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 S6 user management:

- Microsoft® Active Directory
- Novell® eDirectory
- OpenLDAP
- Open directory services like OpenDJ, OpenDS or ApacheDS

For more information on global user management using the individual directory services, see the "User Management in ServerView" user guide.

## 5.1 User management concept

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

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

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

- If the user is authenticated successfully (user name and password and two factor authentication are valid) they can log on.
- Otherwise, the iRMC continues the verification with the next step.

**The iRMC authenticates itself to 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 ServerView Suite 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 so, 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.

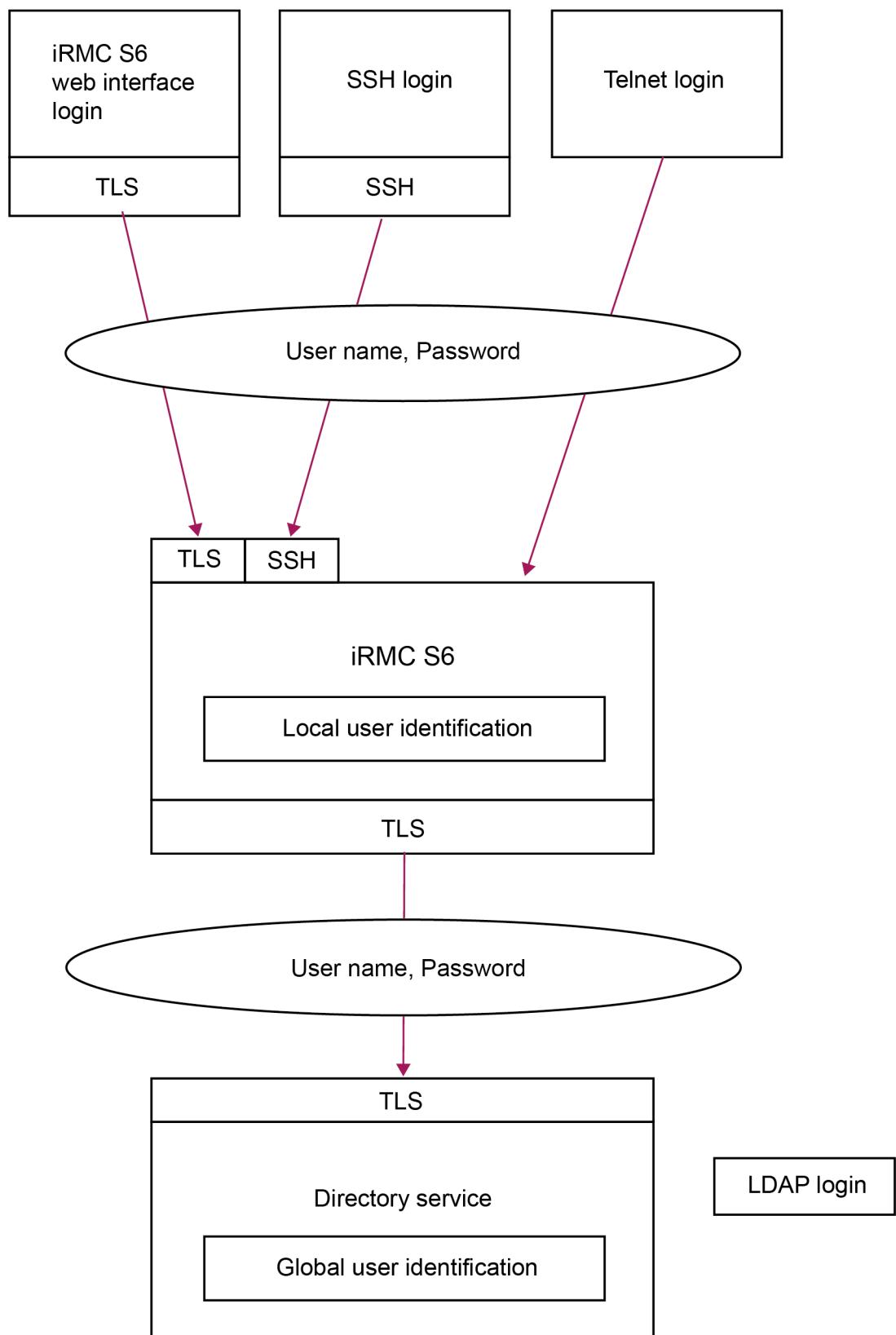


Figure 9: Login authentication via the iRMC S6



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

---

## 5.2 User permissions

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

- Channel privileges assigned to roles
- Explicitly assigned permissions

The channel privileges are bound to the protocol used for communication.

### Redfish channel specific privileges

The web interface and scripts via the Redfish API use Redfish defined privileges called roles. There are three roles defined:

- Administrator with no limitations
- Operator who can change the system related settings, but cannot manage users and iRMC settings
- ReadOnly operator who can only read information and change its own password.

### IPMI channel specific privileges

The IPMI privileges are used for the remaining iRMC interfaces like RESTful API, Profiles, Remote Management.

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

- User
- Operator
- Administrator
- OEM

Since the 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.

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.

As well as the group permissions, you can also individually assign users the following permissions:

Configure User Accounts - Permission to configure local user identifications

Configure iRMC Settings - Permission to configure the iRMC settings

#### IPMI permissions to use special iRMC functions

As well as the channel-specific permissions, you can also individually assign users the following permissions:

Permission	Meaning
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 S6 - Web Interface" user guide and the Redfish API specification.
- For the Remote Manager in the "iRMC S6 - Concepts and Interfaces" user guide

## 5.3 Local user management

The iRMC has its own local user management. Up to 16 users can be configured with passwords and 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 S6.

The iRMC also supports the following security features for local users:

- Two factor authentication using a TOTP-based authentication application
- SSHv2-based public key authentication using pairs of public and private keys (["Secure Authentication via SSHv2" on page 53](#)).

The web interface provides a list of configured iRMC users. You can also configure new users, change the configuration of existing ones 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 already configured users is displayed in the **iRMC Local User Accounts** group on the **User Management** page in the **Settings** menu.

In this list you can delete users and open a dialog box for configuring new ones.

### Configuring new users

You can configure a new user with the **Add** button below the list of configured users.

In the **Add Local User Account** dialog box you configure the basic settings for the new user.

### Modifying the configuration of a user

You can modify the settings of a user account with the **Edit** button next to the relevant user in the list of configured users.

In the **Edit Local User Account** dialog box you can change the settings for an existing user.

### Deleting users

You delete a user account with the **Delete** button next to the relevant user in the list of configured users.

For more information on the **User Management** page of the iRMC web interface, refer to the "iRMC S6 - Web Interface" user guide.

## 5.3.1 Two factor authentication (2FA)

Two-factor authentication (2FA) is an identity and access management security method that requires two steps of identification to access resources and data.

In general, the first factor to authenticate is by using a username and a password. The second factor is a code generated with a software-based authenticator. The additional generated one-time password (code) is required to use the iRMC web interface when 2FA is enabled.

The code can be generated by a TOTP-based authorization application. You can choose between smartphone apps (Google Play and App Store), desktop or web based application widely available on the internet. This TOTP-based authentication application is introduced during the setup procedure of the first logon.

It is strongly recommended to enable time synchronization via NTP server in the iRMC before enabling 2FA. The time settings of the iRMC must be the same as in the TOTP-based authorization application for proper operation.

If the time is not the same, 2FA in iRMC will not be possible. If the time is desynchronized over the time code generated in the TOTP-based authorization application, the entered code will not be accepted in iRMC.

To enable 2FA to a user account, the following steps are necessary:

- Administrator: "[Enabling 2FA for a user account](#)" on page 48
- iRMC user: "[Setting up 2FA](#)" on page 48

When 2FA is enabled and set up it is the regular logon operation for a user account. If no 2FA access is granted, access to iRMC web interface is blocked.

The access to the iRMC web interface is granted until:

- Access from new IP address has occurred ?for the same user account?
- The grace period has expired
- An iRMC reboot occurred

During the grace period you do not need to enter the one-time password again and can logon with the user credentials..

If the TOTP-based authenticator application is lost or damaged the following steps apply for a new setup:

- "[Using an emergency code](#)" on page 51
- "[Reconfiguring 2FA for a user account](#)" on page 53

### 5.3.1.1 Enabling 2FA for a user account

1. Log-on to the iRMC as an administrator.
2. Open the **User Management** page of the **Settings** menu.
3. Open the **iRMC Local User Accounts** group.
4. Create a new iRMC user or edit an existing one.
5. In the **Add Local User Account** or **Edit Local User Account** dialog box open the **Access Configuration** tab.
6. Open the **Two factor Authentication** tab.
7. Check the **Enable Two Factor Authentication** option.
8. Click **Ok**.

The two factor authentication is enabled for the user account.

The next time the user logs on to the iRMC the two factor authentication needs to be setup for the user account.

### 5.3.1.2 Setting up 2FA

For 2FA an iRMC user needs a TOTP-based authentication application that is used to generate the one-time password. This password is created based on a code provided by the iRMC at setup.

To setup 2FA proceed as follows:

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

A login dialog box opens.

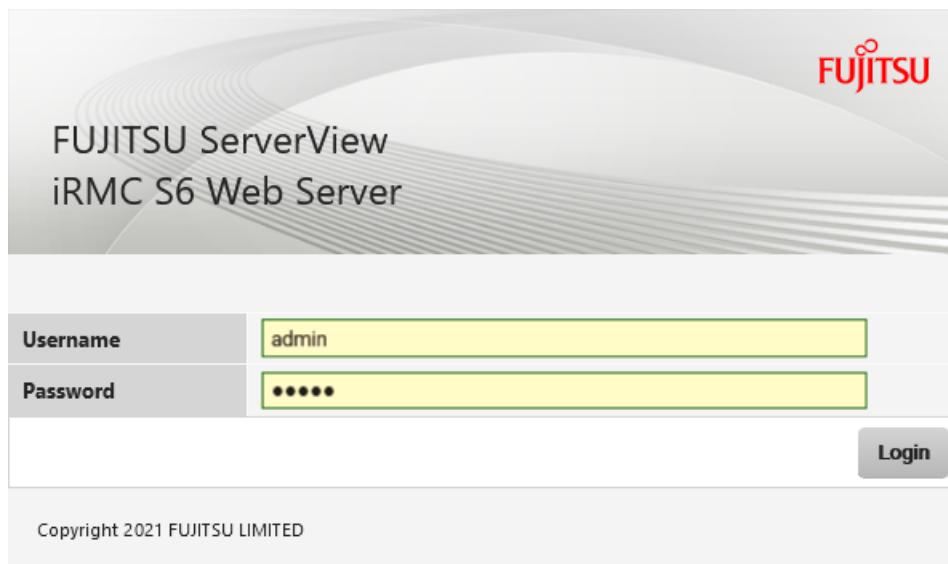


Figure 10: Login dialog box

3. Enter your credentials (username and password).
4. Click **Login** to confirm your entries.

The following dialog box opens:

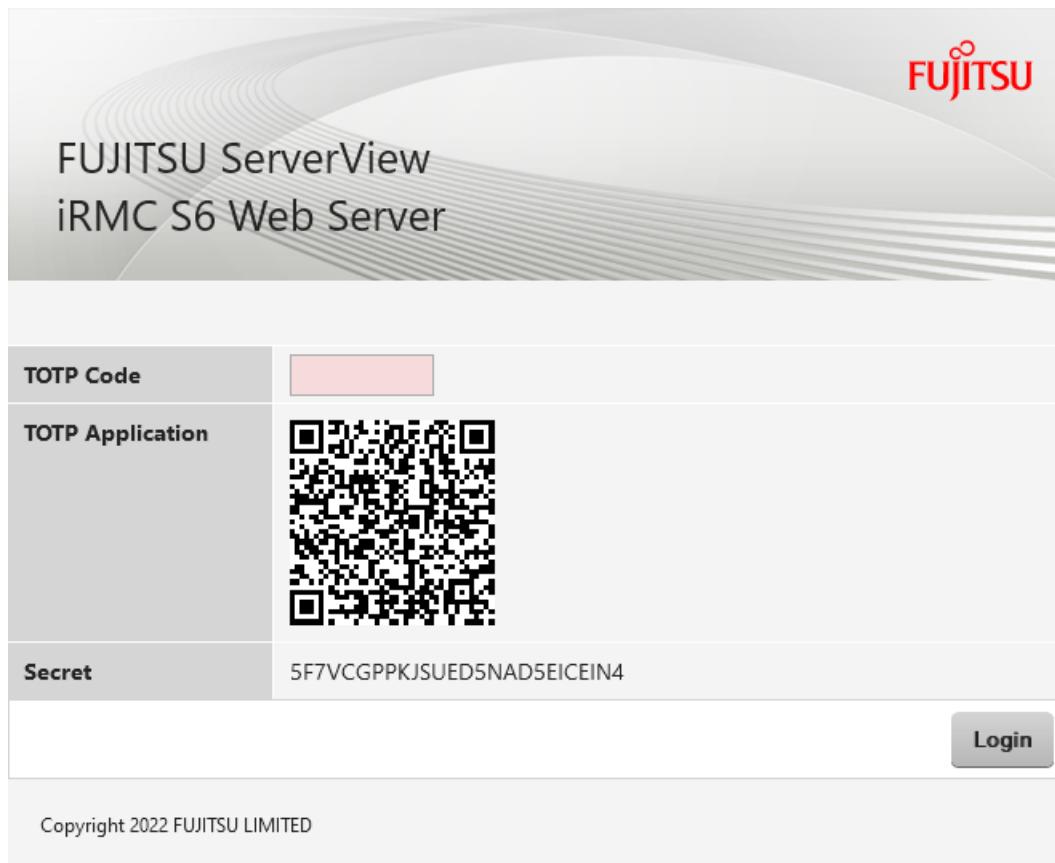


Figure 11: Login dialog box of 2FA

5. Use the QR code or the code displayed in the **Secret** field to generate a one-time password with the TOTP-based authorization application you want to use further on.
6. Enter the one-time password into the **TOTP Code** input field.
7. Click **Login**.

On successful login, the TOTP-based authorization application you use is accepted by the iRMC and a dialog box opens with emergency codes.

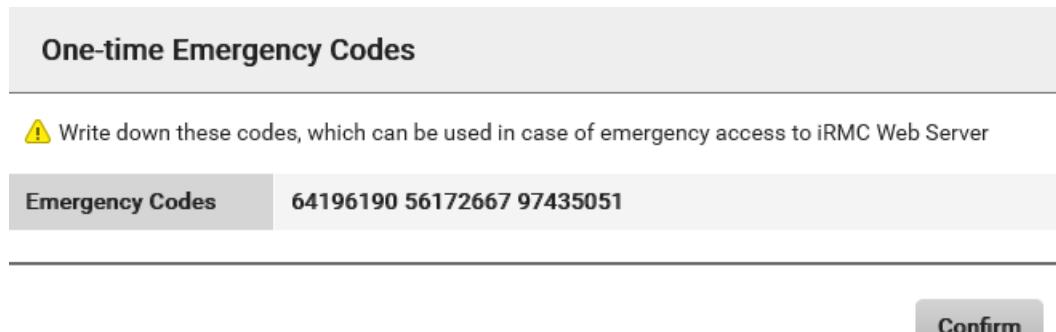


Figure 12: One-time Emergency Codes dialog box

These emergency codes are displayed only once. The codes can be used when you lose the ability to log in using two factor authentication, for instance when you lose the device with the TOTP-based authorization application or the device or application is damaged.

8. Save the emergency codes, e.g. with a screenshot.
9. Click **Confirm**.

The iRMC web interface opens with the **System Overview** page.

After the setup procedure your logon is bound to the TOTP-based authorization application you have used during the first logon. For all further logons the second authentication dialog box contains only the **TOTP Code** input field.

The status of the two factor authentication configuration of the user account changes to Enabled - Configured.

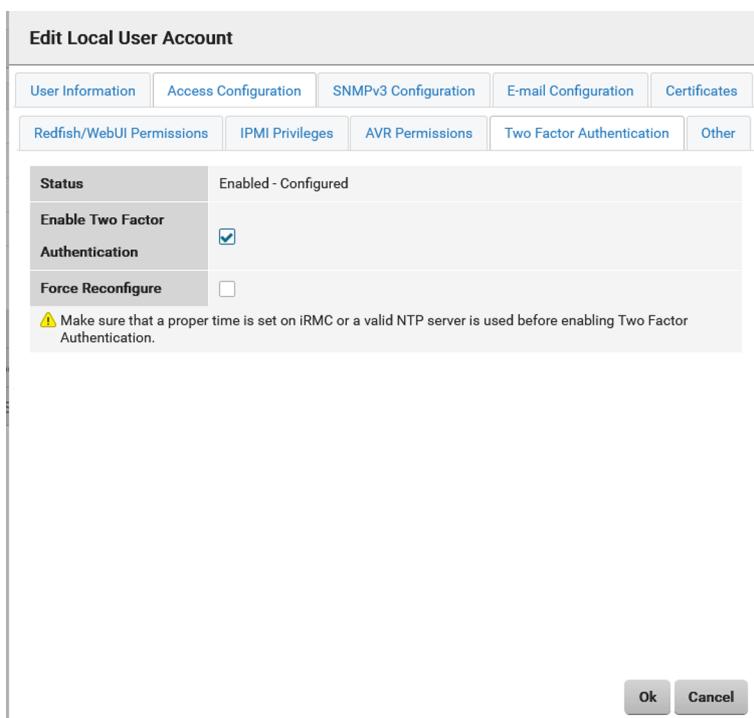


Figure 13: Edit User Account dialog box

If the authorization application is no longer available you can no longer logon to the iRMC web interface and 2FA needs to be reconfigured for your user account.

### 5.3.1.3 Using an emergency code

Each emergency code can be used once to get unconditional 2FA access to the iRMC web interface.

In the case the device with your TOTP-based authentication application used is lost or damaged proceed as follows to logon to the iRMC:

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

A login dialog box opens.

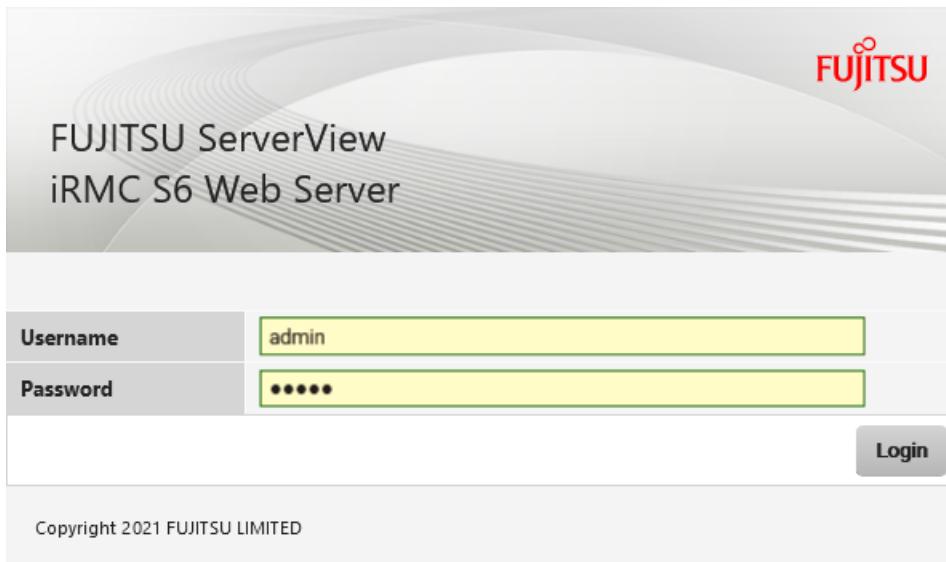


Figure 14: Login dialog box

3. Enter your credentials (username and password).
4. Click **Login** to confirm your entries.

The following dialog box opens:

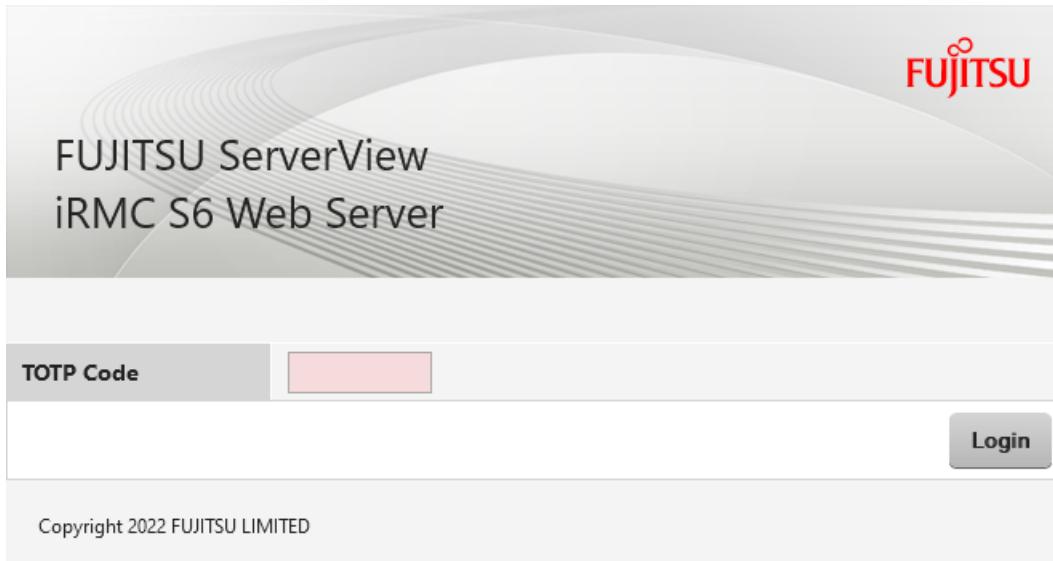


Figure 15: Login dialog box of 2FA

5. Enter one of the emergency codes into the **TOTP Code** input field.
6. Click **Login**.

The iRMC web interface opens with the **System Overview** page.

#### 5.3.1.4 Reconfiguring 2FA for a user account

In the case all emergency codes are used up and the used TOTP-based authentication application is no longer available, the two factor authentication needs to be setup with another application. In this case the administrator has to clear up the old configuration and allow a new one.

1. Log-on to the iRMC web interface as an administrator.
2. Open the **User Management** page of the **Settings** menu.
3. Open the **iRMC Local User Accounts** group.
4. Click **Edit** for an existing iRMC user.
5. In the **Edit Local User Account** dialog box open the **Access Configuration** tab.
6. Open the **Two factor Authentication** tab.
7. Check the **Force Reconfiguration** option.
8. Click **Ok**.

The two factor authentication configuration of the user account is cleared. The user has to introduce another TOTP-based authentication application to the iRMC.

#### 5.3.2 Secure Authentication via SSHv2

As well as 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 their private key with the program PuTTY or the OpenSSH client program ssh, for example.

The iRMC supports the SSH RSA public key. 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 62](#)).

##### Public key authentication

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

The user who wishes to log on to 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 on to the iRMC without needing 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 54](#)).
2. Upload the public SSHv2 key onto the iRMC from a file (["Uploading the public SSHv2 key" on page 57](#)).
3. Configure the program PuTTY or ssh for SSHv2 access to the iRMC (["Using the public SSHv2 key" on page 58](#)).

### 5.3.2.1 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 PuTTYgen main window of opens.

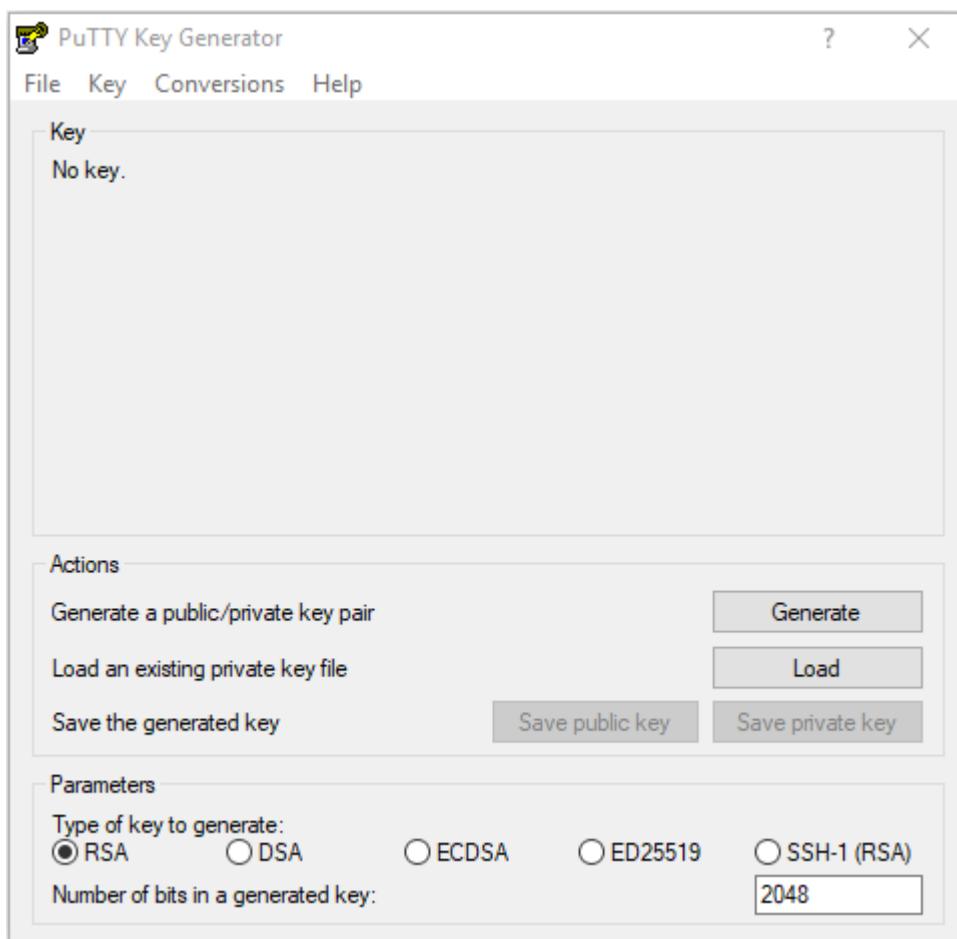


Figure 16: PuTTYgen: Creating new private and public SSHv2 keys

2. In the **Parameters** group, select the **RSA** key type.
  3. Click **Generate** to start generation of the keys.  
A progress bar indicates the progress of the generation.
  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.

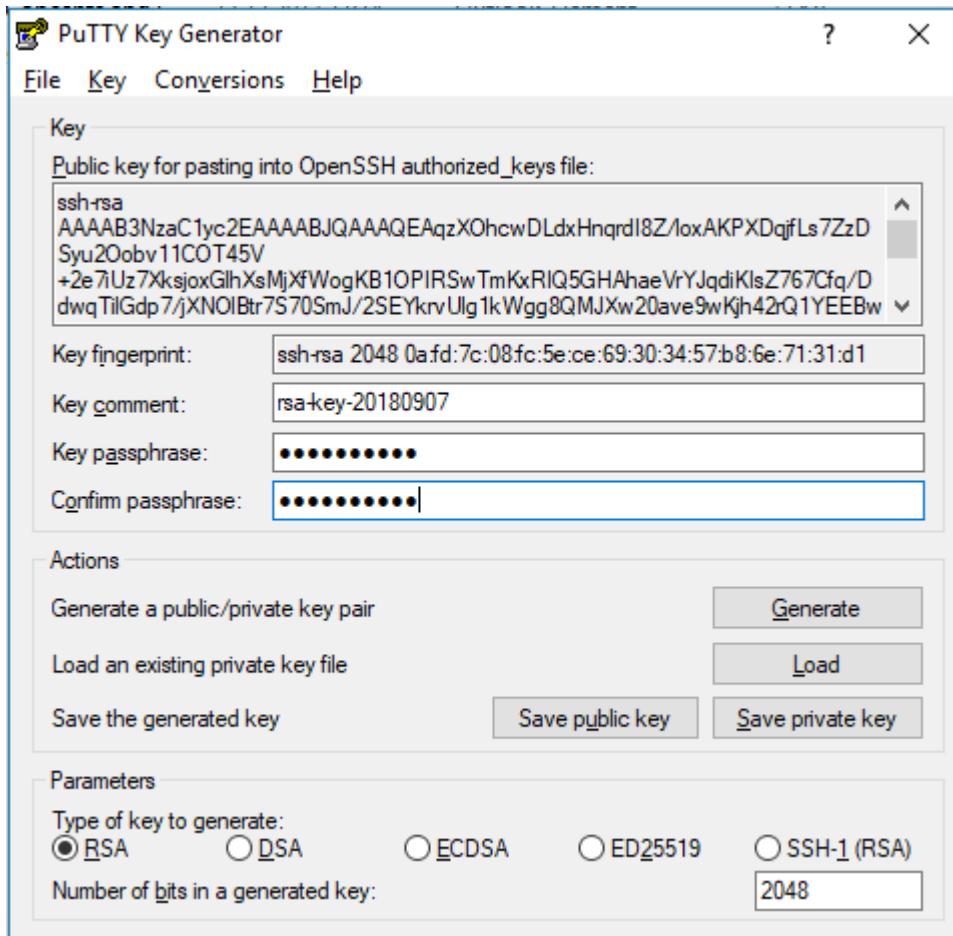


Figure 17: PuTTYgen: Generated private SSHv2 key

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 57](#)).
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 parameters 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 prompts the user for the file name under which the private key is to be stored and 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: _____ 2
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 prompts you to enter a passphrase (and 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 one.
3. ssh-keygen informs you that the newly generated private SSHv2 key has been saved in the file `/.ssh/id_rsa`.
4. ssh-keygen informs you 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.

### 5.3.2.2 Uploading the public SSHv2 key

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

1. Log on to the iRMC web interface.
2. Open the **User Management** page in the **Settings** menu.
3. In the list of configured users, click **Edit** next to the relevant user.
4. In the **Edit Local User Account** dialog box, open the **Certificates** tab.
5. Open the **SSHv2public Key** subtab.
6. Click **Select** in the **Upload** group and navigate to the file containing the required public key.
7. 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 **Fingerprint** field.

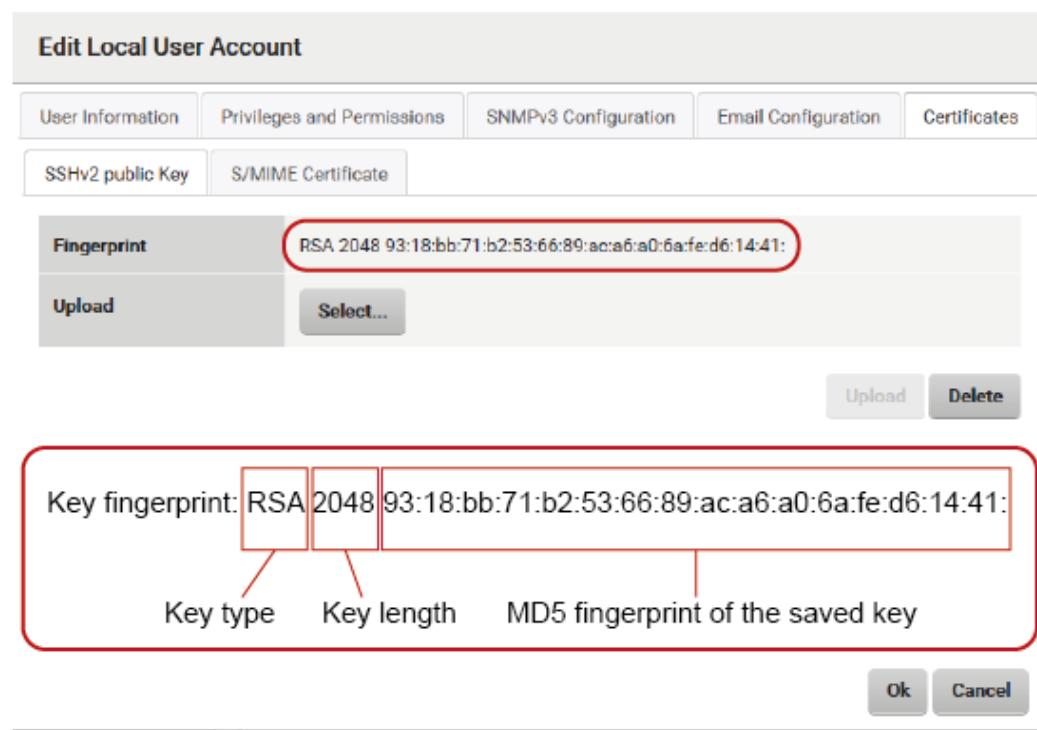


Figure 18: Display of the key fingerprint

8. For security reasons, make sure that the fingerprint shown here matches that shown in PuTTYgen ("Creating public and private SSHv2 keys" on page 54) in the **Key fingerprint** field.

### 5.3.2.3 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 on 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 PuTTY main window opens.

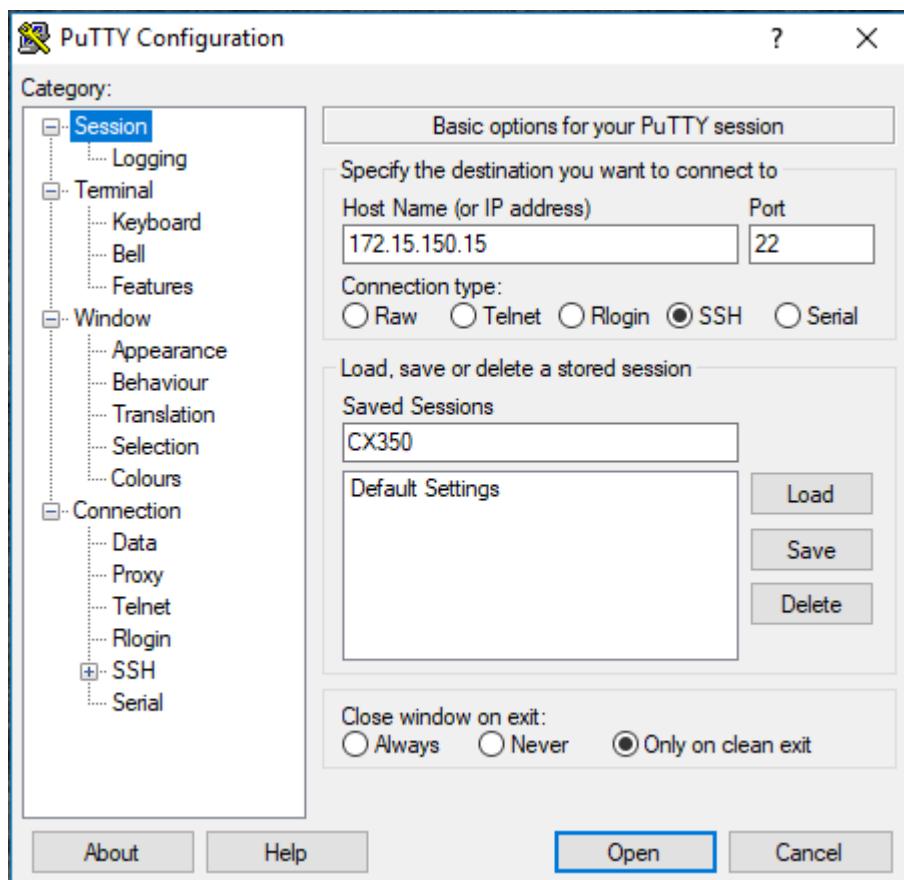


Figure 19: Selecting and loading an SSH session

2. In the **Saved Sessions** list, select an SSH session with the iRMC S6 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.

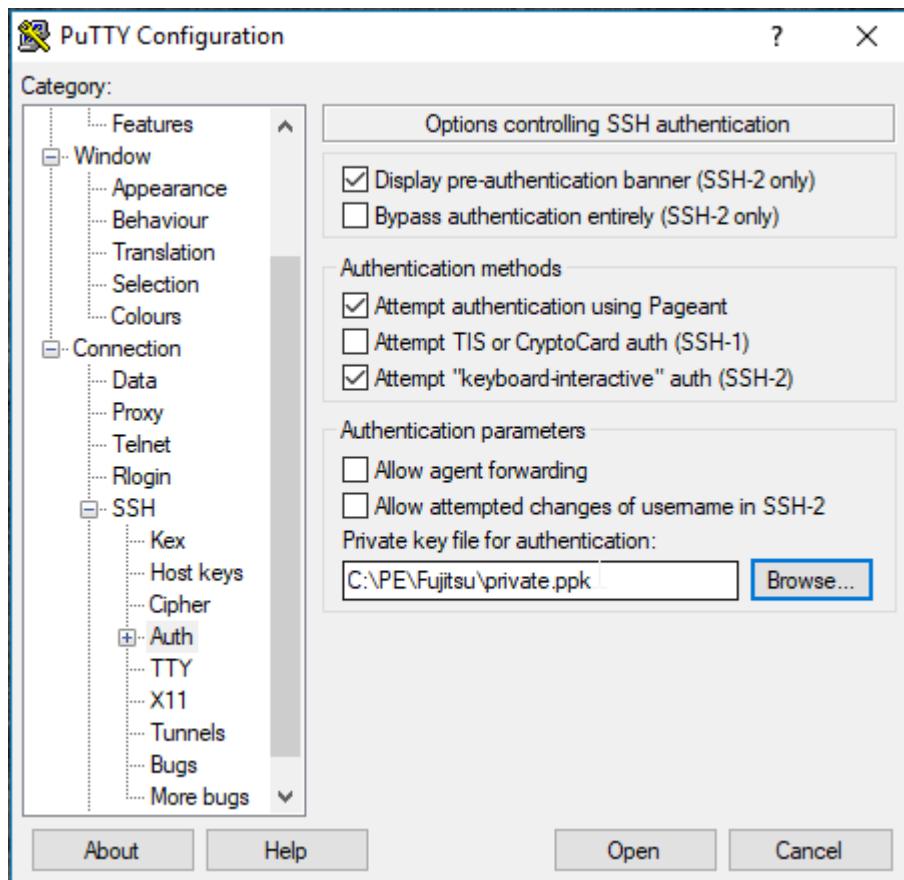


Figure 20: Configuring the SSH authentication options

5. Select the file containing the private key that you want to use with the iRMC S6.



At this point, you require the private key (["Creating public and private SSHv2 keys" on page 54](#)) 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 on the iRMC.

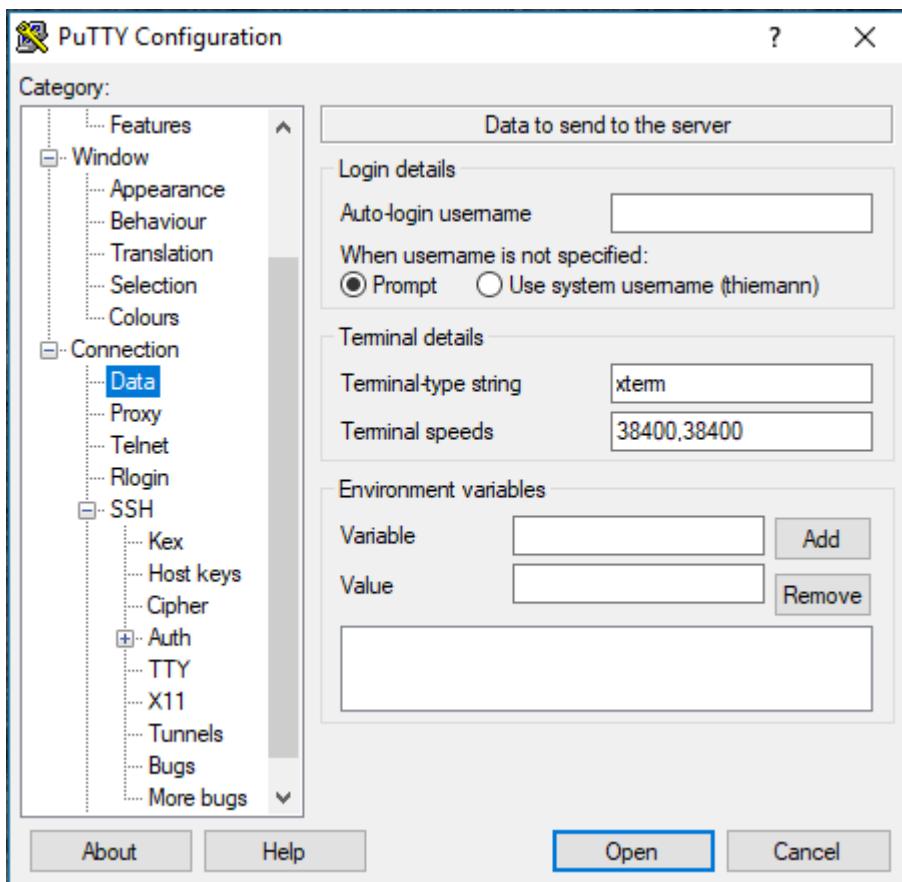


Figure 21: PuTTY: Specifying the user name for automatically logging on to the iRMC

### 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 on under either your current local login or 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 onto the iRMC S6.

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`)



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.



You will find detailed information on the configuration of SSH and its parameters on the manual pages for OpenSSH at:

<http://www.openssh.org/manual.html>

---

Proceed as follows:

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

`ssh -l [<user>] <iRMC_S6>`

or

`ssh [<user>@]<iRMC_S6>`

**<user>**

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

**<iRMC\_S6>**

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

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 54](#)) 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 57](#)).

You can then log on 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`

### 5.3.2.4 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"
AAAAB3NzaC1yc2EAAAABJQAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUi19US6/9Ar
Jxj1hXUz1PPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsf+F
pGJ2iw==
---- END SSH2 PUBLIC KEY ----
```

#### OpenSSH format

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+\n
AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUi19US6/9ArJxj
1hXUz1PPVzuBtPaRB7+\n
bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGwsfc+FpGJ2iw== rsa-key-
20090401
```

### 5.3.3 Configuring E-mail alerting to local iRMC users

E-mail alerting to local iRMC users is integrated in the iRMC user management system. This means that e-mail alerting can be configured and handled for the managed server. You can use a local iRMC user for instance to configure a Primergy Autocall to the Fujitsu Support Service Center.

The Autocall setup enables the managed server to generate and forward messages (Autocalls) to the Fujitsu Support Service Center when unusual component conditions or component failures are identified. The actual Support is then provided based on the contracted Service Level.

To setup the Autocall feature the following steps are necessary:

- ["Activating e-mail alerts for local users" on page 63](#)
- ["Configure the Autocall using e-mail alerts" on page 64](#)
- ["Registering contact data" on page 66](#)

### Prerequisite

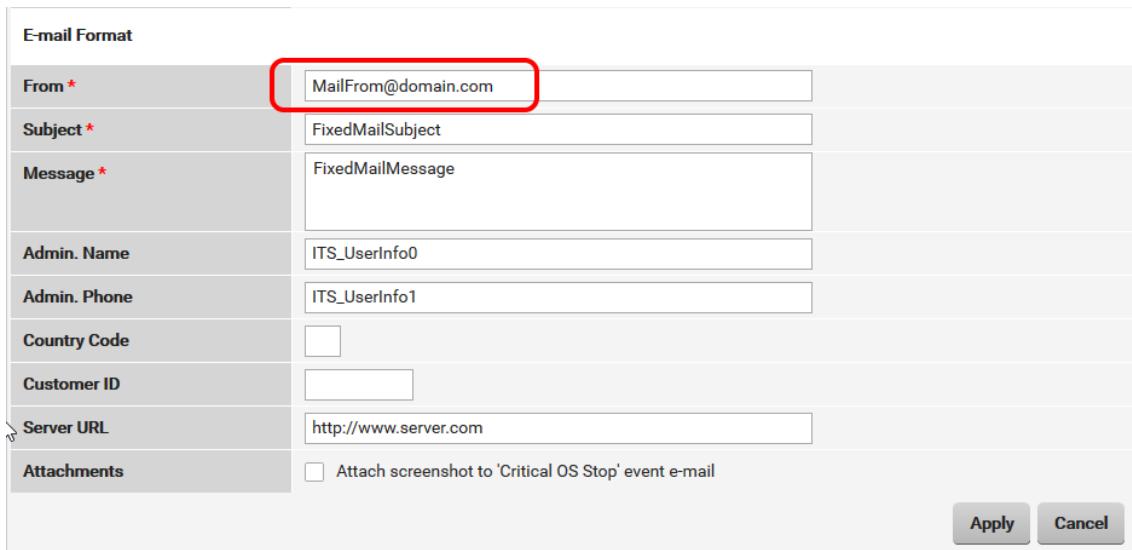
PRIMERGY systems are allowed and enabled to send out SMTP mails via Internet to the Fujitsu Support Center. A system is allowed to do this if a valid service contract is registered at Fujitsu. The enabling process is described below.

#### 5.3.3.1 Activating e-mail alerts for local users

This procedure describes, how to activate the e-mail alerting feature for all users.

1. Start the iRMC web interface of the managed server you want to configure the Autocall to the Fujitsu Support Service Center.
2. Log on to the iRMC web interface as an administrator.  
The System Overview opens.
3. Open the **Settings** menu.
4. Open the **Service** page.
5. In the **E-mail alerting** group check the **Enable E-mail Alerting** option.
6. Configure the SMTP settings at least of the **Primary SMTP Server**.
7. In the **E-mail Format** group enter a valid email address in the **From** field.

An Auto reply will be sent automatically to this address with the relevant Call ID for the reported issue.



E-mail Format	
<b>From *</b>	MailFrom@domain.com
<b>Subject *</b>	FixedMailSubject
<b>Message *</b>	FixedMailMessage
<b>Admin. Name</b>	ITS_UserInfo0
<b>Admin. Phone</b>	ITS_UserInfo1
<b>Country Code</b>	
<b>Customer ID</b>	
<b>Server URL</b>	http://www.server.com
<b>Attachments</b>	<input type="checkbox"/> Attach screenshot to 'Critical OS Stop' event e-mail
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

8. Edit the other input fields of the group as necessary.
9. Click **Apply** to accept your changes.

### 5.3.3.2 Configure the Autocall using e-mail alerts

To configure the Autocall feature you need to create a new local iRMC user and configure their e-mail alerting function with the Fujitsu specific values.

**Prerequisite:** E-mail alerting for local users is activated.

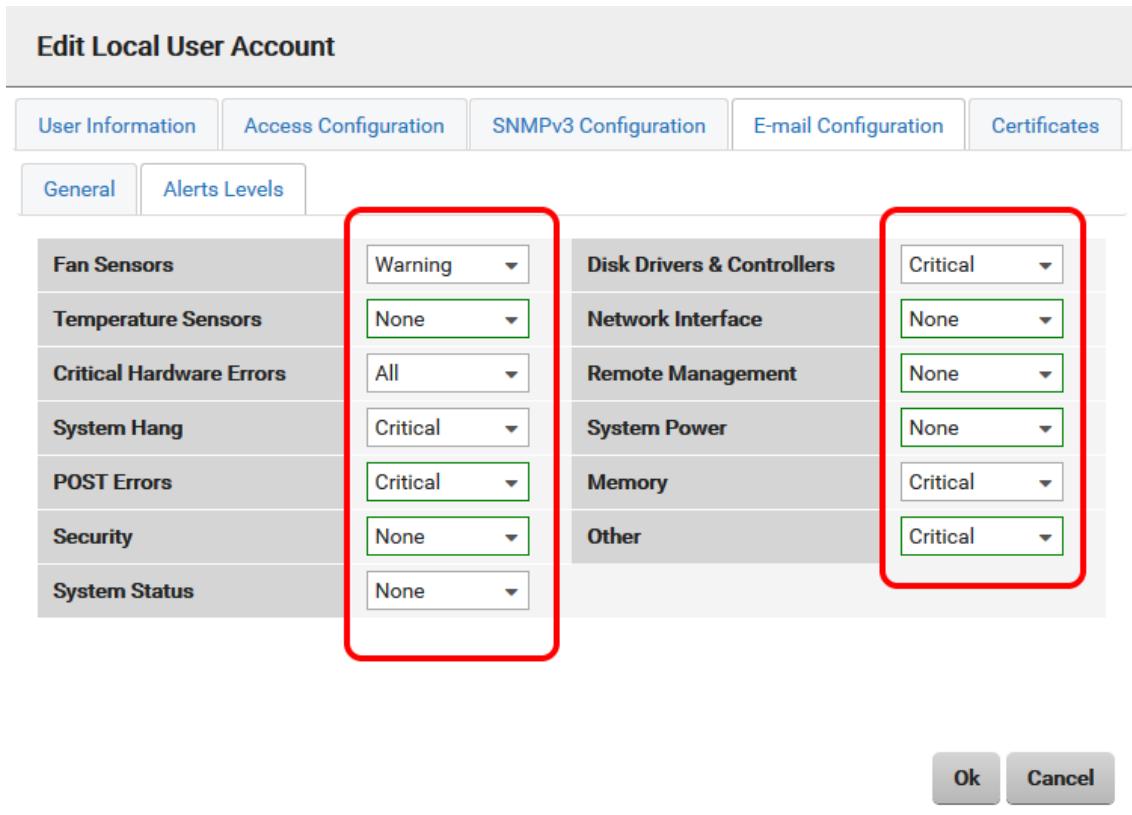
1. In the web interface of the iRMC open the **Settings** menu.
2. Open the **User Management** page.
3. In the **iRMC Local User Accounts** group click **Add** to create a new local iRMC user.

The **Add Local User Account** dialog box opens.

User Information		Access Configuration	SNMPv3 Configuration	E-mail Configuration	Certificates
<b>Enable User</b> <input checked="" type="checkbox"/> <b>Name *</b> <input type="text" value="FJService"/> <span style="border: 2px solid red; padding: 2px;"> </span> <b>Password</b> <input type="password" value="*****"/> <b>Confirm Password</b> <input type="password" value="*****"/> <b>Description</b> <input type="text"/>					
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>					

4. On the **User information** tab check the **Enable User** option.
5. Enter FJService in the **Name** field.
6. Enter a suitable **Password** and Confirm this Password for security reasons.
7. In the dialog box open the **E-mail Configuration** tab.
8. On the **General** tab check the **Enable E-mail Alerts** option.
9. In the **E-mail Address** field enter autocall.primergy@fujitsu.com to configure the Autocall e-mails to the Fujitsu Service Center for PRIMERGY.
10. Check the **Enable Attach System Report** option.
11. Open the **Alert Levels** tab.

12. Edit the alert levels as displayed:



13. Click **OK** to accept your settings.

The dialog box closes and the local iRMC user is created. An entry for the new user is visible in the **iRMC Local User Accounts** table.

14. Click  of the new user's entry to display all settings.

The screenshot shows the iRMC S6 Web Server interface with the 'User Management' tab selected. The left sidebar lists various management categories. The main content area is titled 'User Management' and shows a table of local user accounts. One account, 'admin', is selected and shown in detail. Below the table are several configuration sections: 'User Information', 'Access Configuration', 'SNMP Configuration', and 'E-mail Configuration'. The 'E-mail Configuration' section includes a 'Send Test E-mail' button, which is highlighted with a red circle.

- Click **Send Test E-mail** to check if all the settings are correct.

For test e-mails, an Autocall test ticket will be generated.

### 5.3.3.3 Registering contact data

In a final step you have to enter the contact data of the system administrator, his reachability per weekday and, if applicable, another contact person on the Fujitsu Product support page.

- Open a web browser.
- Enter the following URL in the address field of the browser: <http://ts.fujitsu.com/autocall>  
The **Support** page opens.
- In the **AIS Connect** tab click **Entry of the contact details of the System administrator of your system**.  
The input fields are expanded.

**– Entry of the contact details of the System administrator for your system**

After your system has sent an Autocall to the Fujitsu Service Center, you will be contacted at this address. Therefore, please provide here the details where and how your System administrator can be reached, also at out-of-office times.

Serial number*:	<input type="text"/>	If entering more than one system, please separate the Identification Numbers by ";" (semicolon, no blanks). (e.g. YXXX123456 or YXXX123456;YXXX654321)
Company*:	<input type="text"/>	
Street address*:	<input type="text"/>	
Zip-/postcode*:	<input type="text"/>	
City*:	<input type="text"/>	
Country*:	<input type="text"/> Great Britain and Northern Irele	<input type="button" value="▼"/>
Title:	<input type="text"/> Please select	<input type="button" value="▼"/>
Surname*:	<input type="text"/>	
First Name*:	<input type="text"/>	
E-mail address*:	<input type="text"/>	
Telephone number*:	<input type="text"/>	
<b>+ Reachability</b>		
Comment:	<input type="text"/>	
<b>+ Add another contact for your system</b>		

\* = Required fields

**Privacy protection statement:**  
Fujitsu requires the following personal data from you in order to fulfill your support request and to verify whether Fujitsu has a contractual and/or legal support obligation to you: Your name, address, telephone number, e-mail address and other personal data/information voluntarily provided by you. Fujitsu collects, stores, processes and discloses this information to third parties involved in the support process when Fujitsu is required to provide support. The transfer may be to companies of the Fujitsu Group, their partners or other contractually commissioned third parties (hereinafter referred to as "third parties"), always for the purpose of processing your support request. Please note: These third parties may also be located outside the European Economic Area. This data will not be passed on to third parties who are not involved in the support process. Fujitsu will store your personal data for a specific purpose and delete it if it is not used or if it becomes obsolete.

[Continue >](#)

#### 4. Enter all relevant data.



Keep in mind that Fujitsu can only work on an Autocall if the required information is available in the mandatory fields.

##### 5.3.3.4 Deactivating Autocall function

In the case a service contract for a PRIMERGY system with activated email notification has expired and will not be renewed anymore, the sending of emails to the Fujitsu Support Center must be disabled.

1. In the web interface of the iRMC open the **Settings** menu.
2. Open the **User Management** page.
3. In the **iRMC Local User Accounts** table mark the **FJService** user with a click.

4. Click **Delete**.

The user **FJService** is deleted from the table and from the system.

## 5.4 Global user management

The global user IDs for the iRMC are stored centrally for all platforms in the directory service's directory. This makes it possible to manage the user identifications on a central server. They can therefore be used by all the iRMCs that are connected to this server in the network.

Furthermore, using a directory service for the iRMC makes it possible to use the same user identifications for logins at the iRMC as are used for the operating system of the managed servers.

-  Global user management is currently not supported for the following iRMC functions:
- Login via IPMI-over-LAN
  - Console redirection via SOL

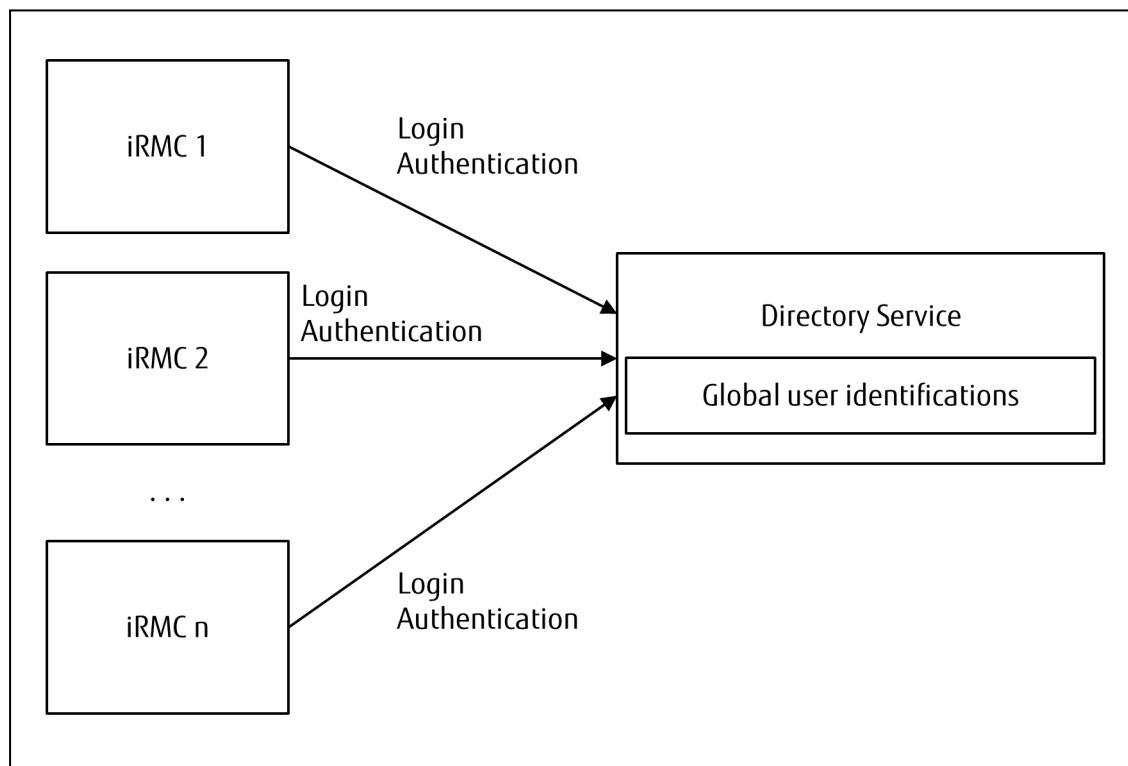


Figure 22: Shared use of the global user identifications by multiple iRMCs

Communication between the individual iRMCs and the central directory service is performed via the TCP/IP protocol **LDAP** (**L**ightweight **D**irectory **A**ccess **P**rotocol). LDAP makes it possible

to access the directory services which are most frequently used and most suitable for user management. Optionally, communication via LDAP can be secured by SSL.



Configuring the settings for global iRMC user management requires detailed knowledge about the Directory Service used. Only a person who has adequate knowledge of the Directory Service should perform the operation.

---

### 5.4.1 Concept of user management via an LDAP directory service

The concept of directory service-based, global user management applies equally to the following directory services:

- Microsoft Active Directory
- Novell eDirectory
- Open directory services such as OpenLDAP, OpenDJ, OpenDS or ApacheDS

The figures are based on the example of the **Active Directory Users and Computers** console in the Microsoft Active Directory user interface.



The following characters are reserved as meta characters for search strings in LDAP: \*, \, &, (, ), |, !, =, <, >, ~, :

You must therefore not use these characters as components of Relative Distinguished Names (RDN).

---

#### 5.4.1.1 User roles

Global iRMC user management via an LDAP directory server requires no extension to the standard directory server schema. Instead, all information relevant for the iRMC, including the user permissions (privileges), is provided via additional LDAP groups and organizational units (OUs) which are combined in separate OUs in a domain of the LDAP directory server (see figure "[Organizational unit \(OU\) SVS](#)" on page 70).

iRMC users obtain their privileges by being assigned a role (user role) declared in the organizational unit (OU) **SVS**.

#### Assigning permissions with user roles (abbreviated to: roles)

Global user management on the iRMC controls the assignment of permissions by means of user roles. In this case, each role defines a specific, task-oriented permission profile for activities on the iRMC.

Several roles can be assigned to each user with the result that the permissions for this user are defined by the sum of the permissions of all the assigned roles.

The figure illustrates the concept of role-based assignment of user permissions with the roles **Administrator**, **Maintenance**, **Observer** and **UserKVM**.

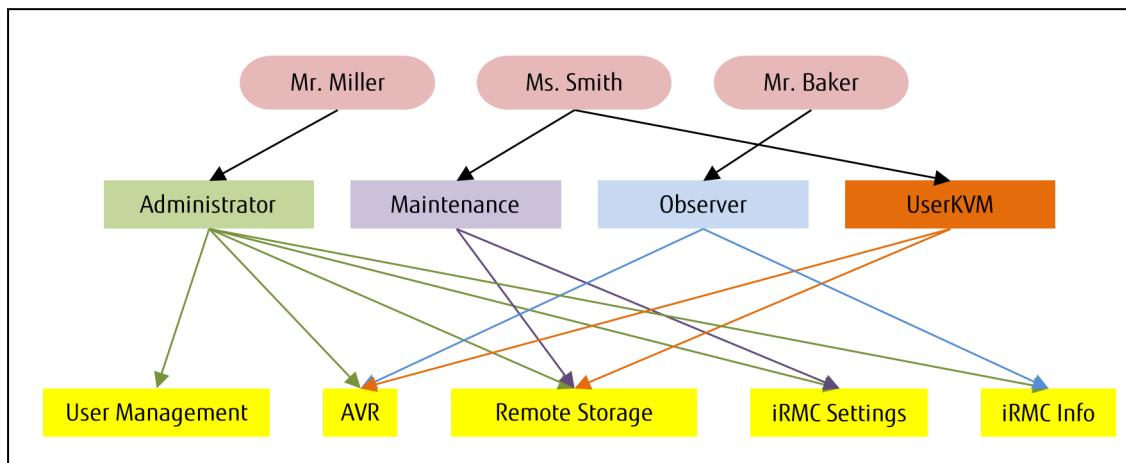


Figure 23: Role-based assignment of user permissions

The concept of user roles offers important advantages, including:

- The individual permissions do not need to be assigned to each user or user group individually. Instead, they are assigned to the user role.
- It is only necessary to adapt the permissions of the user role in the event that the permission structure changes.

### 5.4.1.2 Organizational unit (OU) SVS

The iRMC firmware supports LDAP v2 structures that are stored in the OU **SVS**. LDAP v2 structures are all set for future functional extensions.

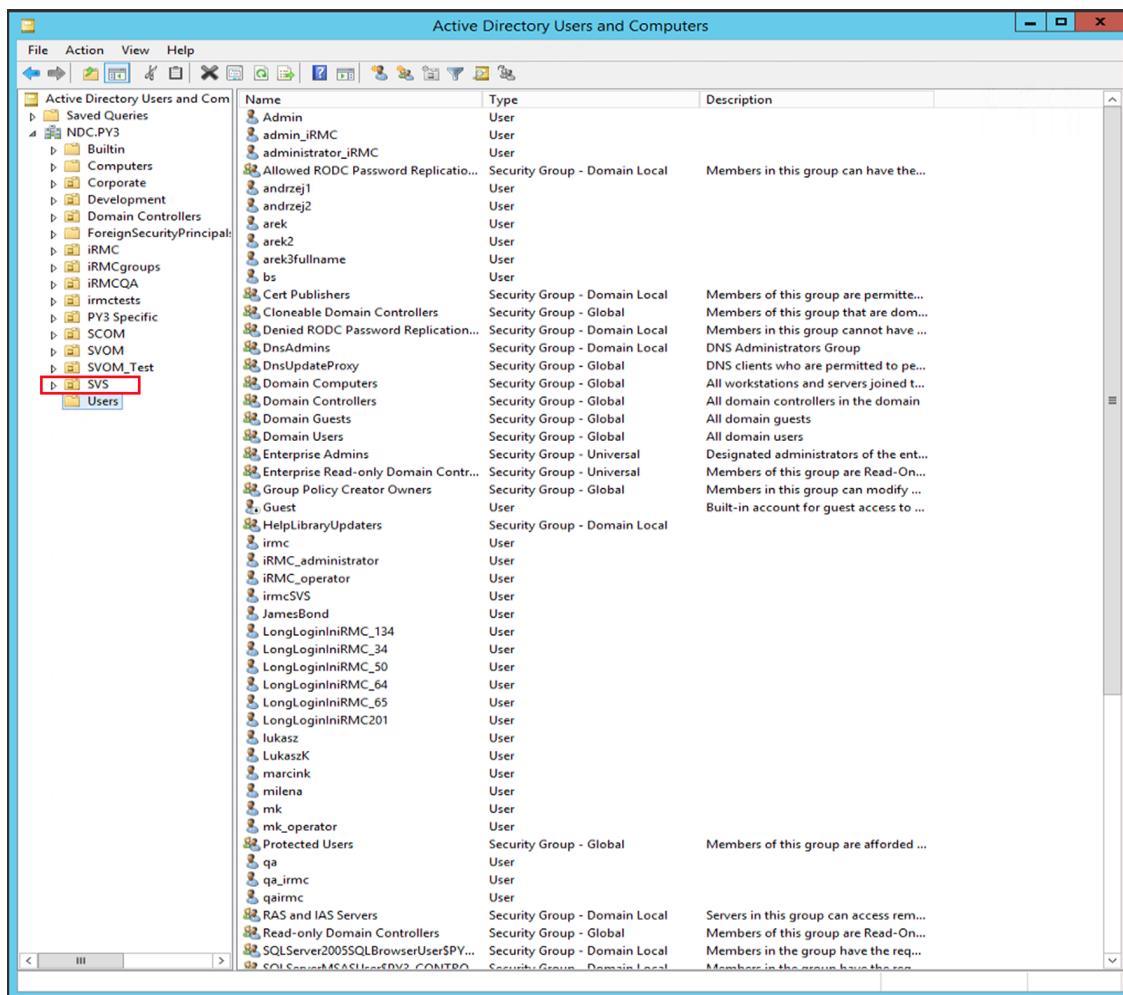


Figure 24: The OU **SVS** in the NDC.PY3 domain

### SVS contains the OUs **Declarations**, **Departments** and **User Settings**:

- **Declarations** contains a list of the defined roles and the list of predefined iRMC user permissions.
- **Departments** contains the groups for the user privileges.
- **User Settings** contains details specific to users or user groups such as the mail format (for email alerting) and the groups for the user shells.

The user entries for the iRMC can be located at any points below the base domain. Permission groups can also be located at any point within the base domain.

In the case of Microsoft Active Directory, for example, the entries for the iRMC users are located in the standard OU **Users**. Unlike the standard users, however, iRMC users are also members of one or more groups of the OU **SVS**.



Operating both ServerView user management and iRMC global user management within the same Organizational Unit (OU) **SVS** requires that the iRMC is configured to belong to the **DEFAULT** department.

#### 5.4.1.3 Cross-server, global user permissions

In large enterprises, the servers which are managed via iRMC are usually assigned to different departments. Furthermore, the administrator permissions for the managed servers are also often assigned on a department-specific basis.

The OU **Departments** combines the servers which are managed by iRMC to form a number of groups. These groups correspond to the departments in which the same user IDs and permissions apply. In the figure, for example, these are the departments **CMS**, **DEFAULT**, **irmctests**, **Others** and **PY3irmc**.

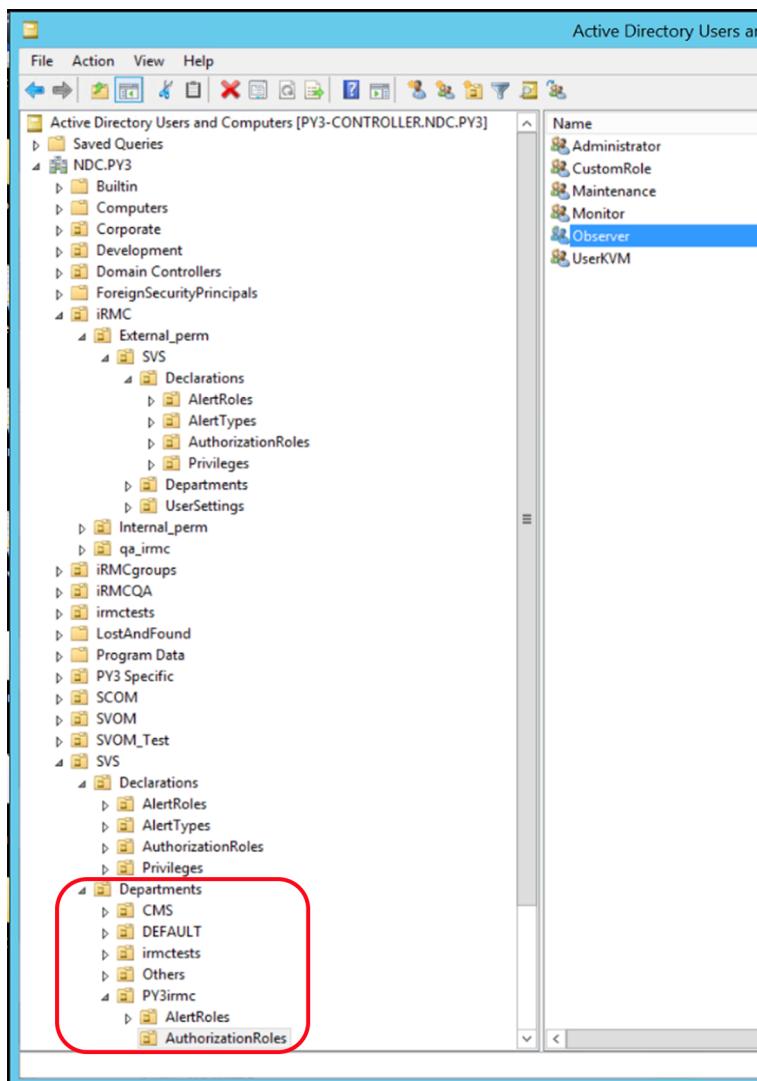


Figure 25: Organizational structure of the **NDC.PY3** domain

The entry **Others** is optional, but recommended. **Others** is a predefined department name subsuming all those servers which do not belong to another department. There are no restrictions concerning the number of departments (OUs) listed under **Departments**.

- 
-  When configuring the directory service using the iRMC web interface you specify the name of the department to which the managed server with the relevant iRMC belongs. If there is no department of this name in the LDAP directory, then the permissions present in the **Others** department are used.
- 

### 5.4.1.4 SVS: Permission profiles are defined via roles

The associated user roles (authorization roles) that are required are listed directly below each department. All the roles listed here must be defined in the OU **Declarations**. Otherwise, there are no restrictions concerning the number of roles. The names of the roles can be chosen as required subject to certain syntactic requirements imposed by the employed directory service. Each authorization role defines a specific, task-oriented permission profile for activities on the iRMC.

- 
-  The alert roles are listed as well as the authorization roles. Each alert role defines a specific alerting profile for email alerting (see section "[Configuring E-mail alerting to global iRMC users](#)" on page 102).
- 

#### Displaying user roles

If you select a department (e.g. **PY3irmc**) under **SVS** in the structure tree for **Active Directory Users and Computers** and mark the associated node **PY3irmc – Authorization Roles**, the user roles defined for this department (here: **PY3irmc**) are displayed in the right area.

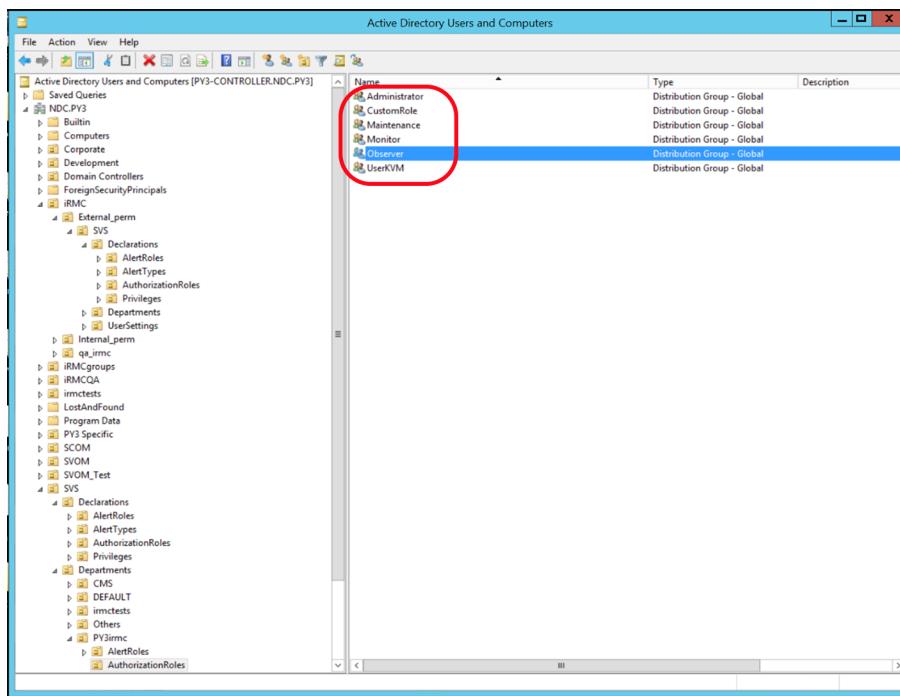
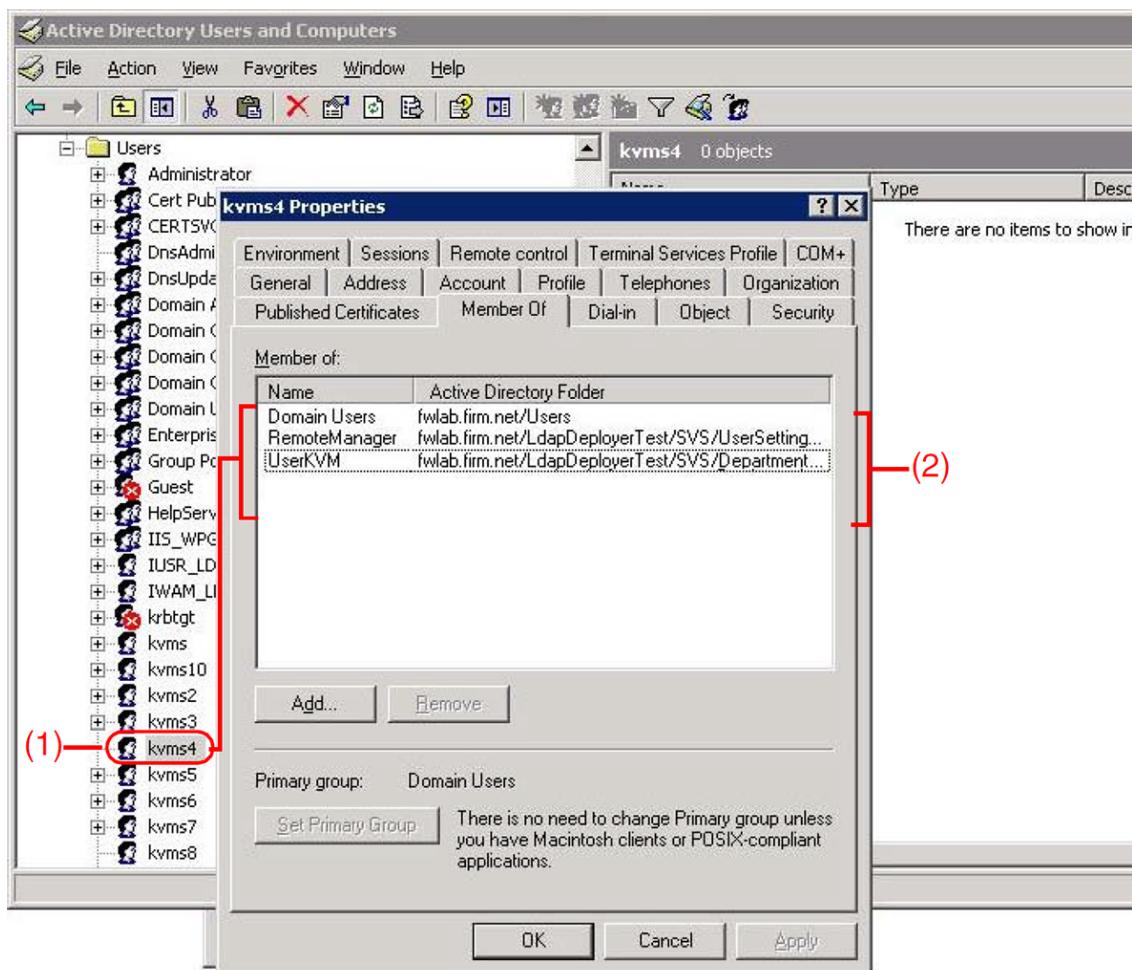


Figure 26: Display of the user roles in the **Users and Computers** snap-in

### Displaying the Active Directory folders to which a user is member of

If you select a user (e.g. **kvms4**) under **Users** in the structure tree for **Active Directory Users and Computers** (1) and open the **Properties** dialog box for this user by choosing **Properties – Members** from the context menu, the permission groups to which the user belongs (here: **kvms4**) are displayed in the **Members** tab (2).

Figure 27: **Properties** dialog box for the user kvms4

### 5.4.2 Steps to configure collaboration

As the iRMC can work with various types of LDAP directory services there are some steps necessary to configure this collaboration with a running directory service to ensure global user authentication.

1. Create the necessary SVS OU using the SVS\_LdapDeployer utility.
2. Optional: prepare a secure connection between iRMC and LDAP server using a CA certificate.
3. Integrate iRMC user management into the directory service.
4. In the directory service assign user roles to iRMC users.
5. Optional: in the directory service configure Email alerting.
6. Configure the iRMC for LDAP authentication.

### 5.4.3 SVS\_LdapDeployer utility

To allow global iRMC user management via a directory service, the (OU) **SVS** structures must be present in the LDAP directory service. The **SVS\_LdapDeployer** utility helps you to generate and modify the necessary **SVS** structures.

**SVS\_LdapDeployer** generates the LDAP structures on the basis of an **XML** configuration file. This input file contains the structure information for the **SVS** structure in **XML** syntax.

 Valid data for the connection to the directory server must be entered in the **<Settings>** area in the configuration file. You can enter the authentication data for accessing the server either in the configuration file or on the command line of the **SVS\_LdapDeployer**.

If you do not specify the authentication data when calling the **SVS\_LdapDeployer**, the **SVS\_LdapDeployer** prompts you to enter the authentication data at runtime.

The **SVS\_LdapDeployer** is a Java archive (**SVS\_LdapDeployer.jar**) provided in the [download area](#) of the FUJITSU support pages. The **SVS\_LdapDeployer** comes together with a set of samples configuration files for different purposes and directory services grouped in the **sampleFiles** folder.

#### 5.4.3.1 Syntax of **SVS\_LdapDeployer**

In the following, the terms "LDAPv1 structure" and "LDAPv2 structure" are used to denote ServerView-specific configuration layouts of the authorization data and do not refer to version 1 and 2 of the LDAP protocol.

 User management for the iRMC S6 always requires an LDAP v2 structure.

##### Syntax

```
java -jar SVS_LdapDeployer.jar <command> <file>[<option>...]
```

##### <command>

Specifies the action to be performed.

The following commands are available:

-deploy

Creates an LDAP structure for global iRMC user management on the directory server.

-delete

Deletes an LDAP structure used for global iRMC user management from the directory server.

The following commands are described for compatibility reasons only. They are not used regarding the iRMC S6:

**-import**  
Creates an equivalent LDAP v2 structure from an existing LDAP v1 structure. Both structures will be located in the same sub-tree, specified in <Settings>\<root> .

**-synchronize**  
Makes corresponding changes in an existing LDAP v1 structure to reflect any changes that you make in an LDAP v2 structure.

#### <file>

The configuration file (.xml) used as an input file by SVS\_LdapDeploy. This configuration file contains the structure information for the **SVS** structure in XML syntax.



The syntax of the configuration file is illustrated in the sample configuration files that are supplied together with the jar archive.

#### <option>

Options that control the execution of the specified command. All options are optional.

**-structure v1 | -structure v2 | -structure both**  
iRMC S3 only: Creates an LDAP v1 structure or an LDAP v2 structure or an LDAP v1 and an LDAP v2 structure.

**-username <user>**  
User name for logging in to the directory server.

**-password <password>**  
Password for the <user>.

**-store\_pwd**  
Encrypts the password <password> using a randomly generated key and saves the encrypted password in the configuration file after <command> has been executed successfully. By default, the randomly generated key is stored in the folder in which the SVS\_LdapDeployer is executed.



Save the randomly generated key in a safe place. If the predefined target folder is not adequate for your security needs, or if the folder in which the key is saved can also be accessed by other users, use the options **-kloc** and **-kpwd** to save the key securely.

**-kloc <path>**  
Saves the randomly generated key under <path>.

If you do not specify this option, the key is saved in the folder in which SVS\_LdapDeployer is executed.

**-kpwd [<password>]**  
Specifies a password to protect the randomly generated key.  
If you do not specify <password>, the password is automatically generated on the basis of a snapshot of the current runtime environment. In order to decrypt again the user

password stored in the deployment file, you need to run the application in the same context as the one you used for encryption.

### 5.4.3.2 Starting SVS\_LdapDeployer

#### Prerequisite:

- An LDAP directory service is installed and running on the corresponding server.
- The Administrator role is assigned to the user account that you use for the following steps.

Proceed as follows to start the SVS\_LdapDeployer:

1. Open the [FUJITSU download area](#) and download the SVS\_LdapDeployer utility.
2. Decompress the downloaded zip-file.
3. Edit or create an appropriate configuration file with all relevant data.
4. Login to the LDAP directory server.
5. Save the Java archive (`.jar` archive) `SVS_LdapDeployer.jar` and the configuration file in a folder on the directory server.
6. Open the command interface of the directory server.
7. Switch to the folder in which the `.jar` archive `SVS_LdapDeployer.jar` resides.
8. Call the SVS\_LdapDeployer utility, see the examples below.

SVS\_LdapDeployer generates all required subtrees including all groups, but not the relations between users and groups.

You are informed about the various steps that are being performed while the SVS\_LdapDeployer is running. You will find detailed information in the file `log.txt`, which is created in the execution folder every time that SVS\_LdapDeployer is run.



After generating the OU **SVS** in the directory service you need to create and assign user entries to groups by means of the corresponding tools in the directory service used.

---

### 5.4.3.3 Examples

The following examples comprise the three typical scenarios for using SVS\_LdapDeployer:

#### Performing an initial configuration of an LDAP v2 structure

To set up global user management for an iRMC for the first time you require an LDAP v2 structure.

Recommended method:

Generate the **Department** definition for LDAP v2 structures (**SVS**):

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml  
-structure v2
```

#### Re-generating or expanding an LDAP v2 structure

To re-generate an LDAP v2 structure or expand an existing LDAP v2 structure.

Recommended method:

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml  
-structure -structure v2
```

or

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
```

#### Re-generating an LDAP v2 structure and prompting for and saving authentication data

You wish to re-generate an LDAP v2 structure. The authentication data is to be provided and saved using the command line.

Recommended method:

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml  
-store_pwd -username admin -password admin
```

After the login data has been saved, you can connect to the directory server using SVS\_LdapDeployer without specifying a user name and password. The SVS\_LdapDeployer then uses the values stored in the XML configuration file if available.

SVS\_LdapDeployer can only use a saved password if it can decrypt it. This requires you to execute SVS\_LdapDeployer in the same runtime environment that applied for the previous call with `-store_pwd`. In this context, "the same runtime environment" means "the same user on the same computer" or "a user with permission to access the folder under which they key is stored (`-kloc` option)".

You can also use user accounts that have already been saved when you call SVS\_LdapDeployer in the future. Furthermore, other authentication data can also be used temporarily by explicitly specifying the data in the command line or when requested to do so by SVS\_LdapDeployer.

## 5.4.4 iRMC user management via Microsoft Active Directory

This section describes how you integrate iRMC user management into Microsoft Active Directory.

**Prerequisite:** An LDAP v2 structure has already been created in the Active Directory service (see section "[SVS\\_LdapDeployer utility](#)" on page 76).

To integrate iRMC user management in Microsoft Active Directory perform the following steps:

1. Configure iRMC LDAP/SSL access at the Active Directory server.
2. Assign iRMC users to iRMC user groups in Active Directory.

### 5.4.4.1 Configuring iRMC LDAP/SSL access at the Active Directory server

 The iRMC -LDAP integration uses the SSL implementation developed by Eric Young on the basis of the OpenSSL Project.

An RSA certificate is required before the iRMC can use LDAP via SSL.

The following steps are involved in configuring LDAP access:

1. Install an Enterprise CA.
2. Create an RSA certificate for the domain controller.
3. Install the RSA certificate on the server.

#### Installing the Enterprise CA

An Enterprise CA (certification authority for enterprises) can be installed on the domain controller itself or on another server.

Installation directly on the directory server is simpler since fewer steps are required than when installing on another server.

Below is a description of how to install the Enterprise CA on a server other than the domain controller.

 To install and configure Enterprise CA successfully, you require an Active Directory environment and an installed IIS (Internet Information Services).

Proceed as follows to install an Enterprise CA:

1. Open the control panel and there select:

### **Software - Add/Remove Windows Components**

2. In the wizard for Windows components, select **Certificate Services** under **Components**.
3. Double-click on **Certificate Services** and make sure that the **Certificate Services Web Enrollment Support** and **Certificate Services CA** options are selected.
4. Select **Enterprise root CA**.
5. Select the option **Use custom settings to generate the key pair and CA certificate**.
6. Select **Microsoft Base DSS Cryptographic Provider** to create DSA certificates of length 1024 bytes.
7. Export the public certification authority certificate (CA certificate).

To do this, proceed as follows:

- a. Enter **mmc** in the Windows prompt window to start the Management Console.
  - b. Add the snap-in for local computer certificates.
  - c. Navigate to **Certificates (Local Computer) - Trusted Root Certification Authorities - Certificates** and double-click.
  - d. Double-click the certificate from the newly created certification authority.
  - e. Open the **Details** tab in the certificate window.
  - f. Click **Copy to File**.
  - g. Choose a file name for the certification authority certificate and click **Finish**.
8. Load the public certification authority certificate to the certificate directory **Trusted Root Certification Authorities** on the domain controller.

To do this, proceed as follows:

- a. Transfer the file containing the CA certificate to the domain controller.
- b. In Windows Explorer, open the certificate from the newly created CA.
- c. Click **Install Certificate**.
- d. Under **Place all certificates in the following store** click **Browse** and choose **Trusted Root Certification Authorities**.
- e. Enter **mmc** in the Windows prompt window to start the Management Console.
- f. Add the snap-in for local computer certificates.
- g. Add the snap-in for the current user's certificates.
- h. Copy the CA certificate from the current user's **Trusted Root Certification Authorities** directory to the local computer's **Trusted Root Certification Authorities**.

### Creating a domain controller certificate

Proceed as follows to create an RSA certificate for the domain controller:

1. Create a file named `request.inf` with the following content:

```
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=<full path of domain controller host>"
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic
Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1; this is for Server Authentication
```

2. In the file `request.inf`, adapt the specification under `Subject=` to the name of the employed domain controller, e.g.  
`Subject = "CN=domino.fwlab.firm.net".`
3. Enter the following command in the Windows prompt window:  
`certreq -new request.inf request.req`
4. Enter the following URL in the certification authority browser: <http://localhost/certsrv>
5. Click **Request a Certificate**.
6. Click **advanced certificate request**.
7. Click **Submit a certificate request**.
8. Copy the content of the file `request.req` to the **Saved Request** window.
9. Select the **Web Server** certificate template.
10. Download the certificate and save it (e.g. in the file `request.cer`).
11. Enter the following command in the Windows prompt window:  
`certreq -accept request.cer`

12. Export the certificate with the private key.

To do this, proceed as follows:

- a. Enter **mmc** in the Windows prompt window to start the Management Console.
- b. Add the snap-in for local computer certificates.
- c. Navigate to  
**Certificates (Local Computer) - Personal Certificates - Certificates**.
- d. Double-click the new server certification authentication certificate.
- e. Open the **Details** tab in the certificate window.
- f. Click **Copy to File**.
- g. Select **Yes, export the private key**.
- h. Assign a password.
- i. Choose a file name for the certificate and click **Finish**.

### Installing the domain controller certificate on the server

Proceed as follows to install the domain controller certificate on the server:

1. Copy the domain controller certificate file that has just been created to the domain controller.
2. Double-click the domain controller certificate.
3. Click **Install Certificate**.
4. Use the password which you assigned when exporting the certificate.
5. Under **Place all certificates in the following store** click **Browse** and choose **Personal Certificates**.
6. Enter **mmc** in the Windows prompt window to start the Management Console.
7. Add the snap-in for local computer certificates.
8. Add the snap-in for the current user's certificates.
9. Copy the domain controller certificate from the current user's **Personal Certificates** directory to the local computer's **Personal Certificates** directory.

#### 5.4.4.2 Assigning user roles to iRMC users

You can assign user roles (authorization roles) to iRMC users via one of the following entries:

- User
- Role / group

In Active Directory you assign the users to the groups individually.

Proceed as follows to assign a user role based on the role entry in the OU **SVS**:

1. Open the snap-in **Active Directory Users and Computers**.

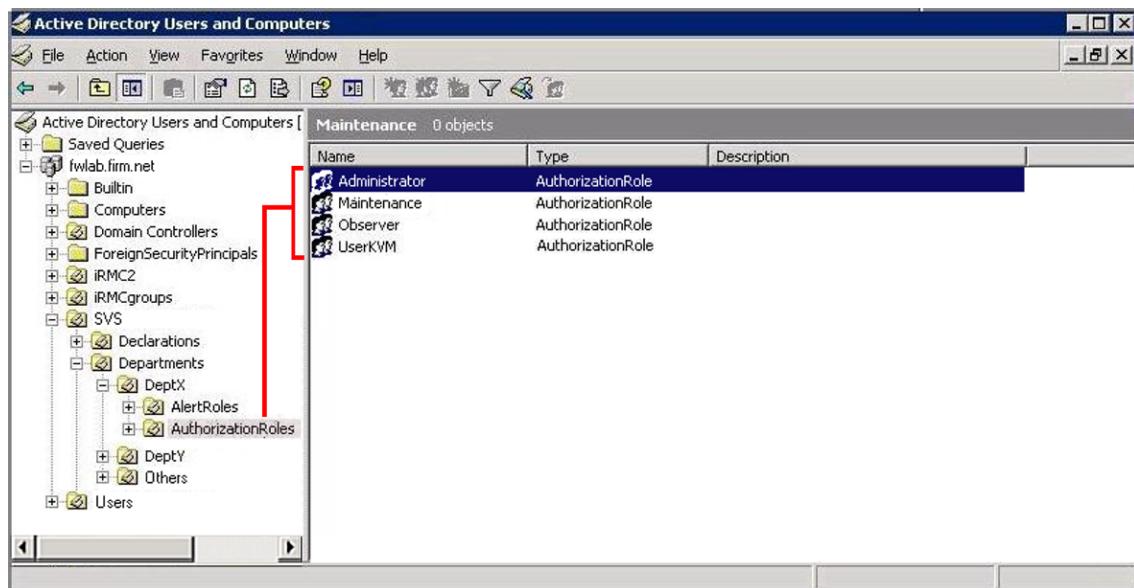


Figure 28: **Active Directory Users and Computers** snap-in

2. Double-click the authorization role (here: **Administrator**).

The **Administrator Properties** dialog box opens.

3. Open the **Members** tab.

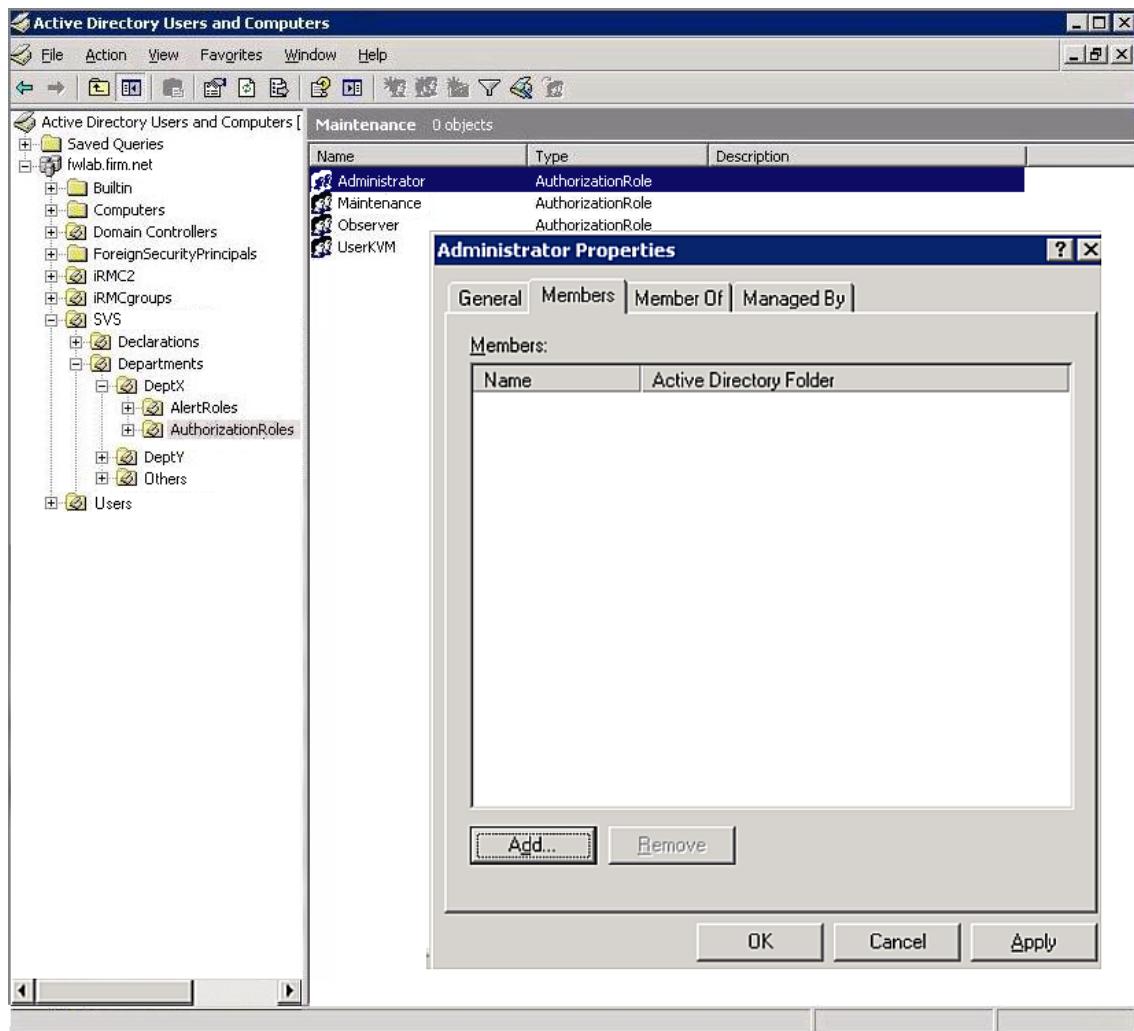


Figure 29: **Administrator Properties** dialog box

4. Click **Add**.

The **Select Users, Contacts, or Computers** dialog box opens.

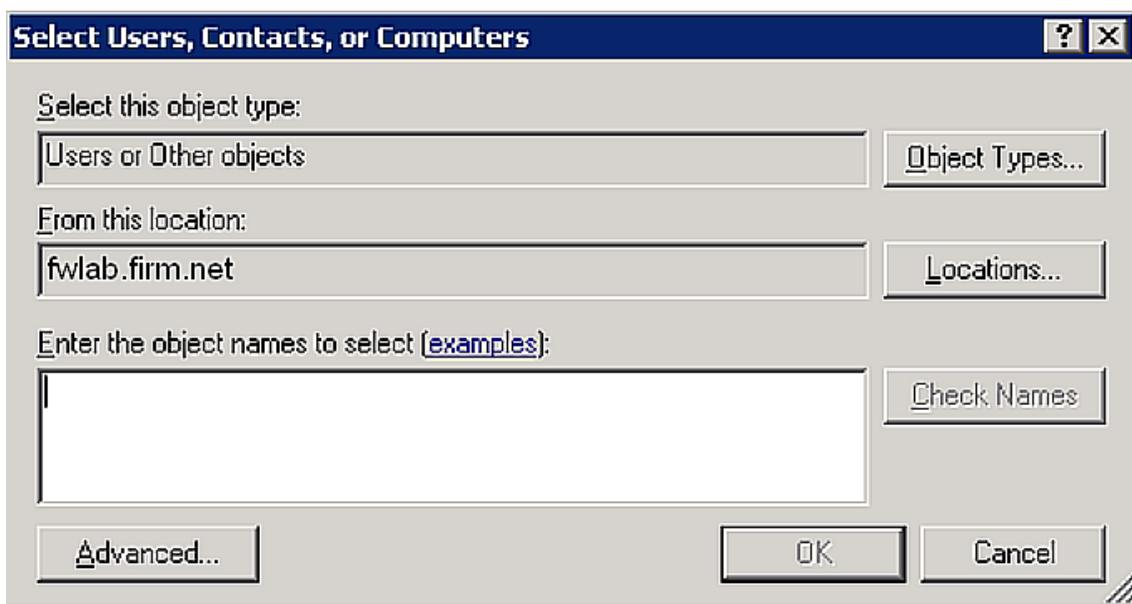


Figure 30: **Select Users, Contacts, or Computers** dialog box

5. Click **Locations**.

The **Locations** dialog box opens.

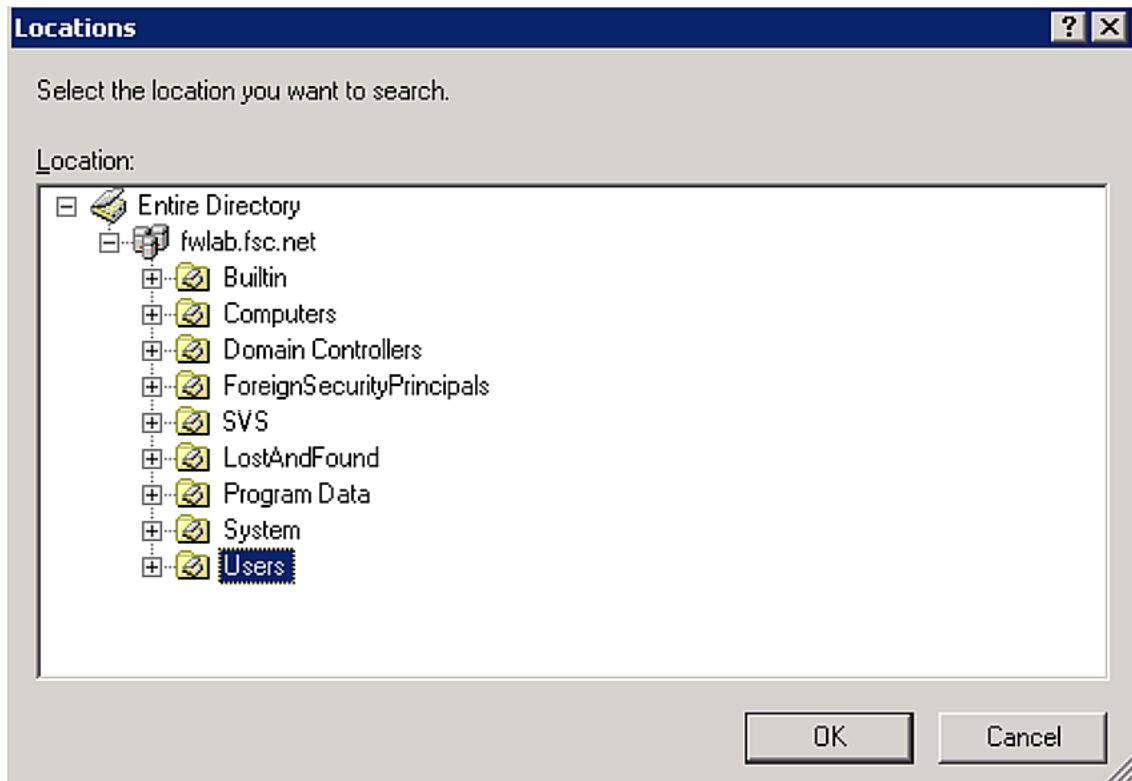


Figure 31: **Locations** dialog box

6. Select the container (OU) containing your users. (By default, this is the OU **Users**). Users may also be entered at a different location in the directory.
7. Click **OK** to confirm.

The **Select Users, Contacts, or Computers** dialog box opens.

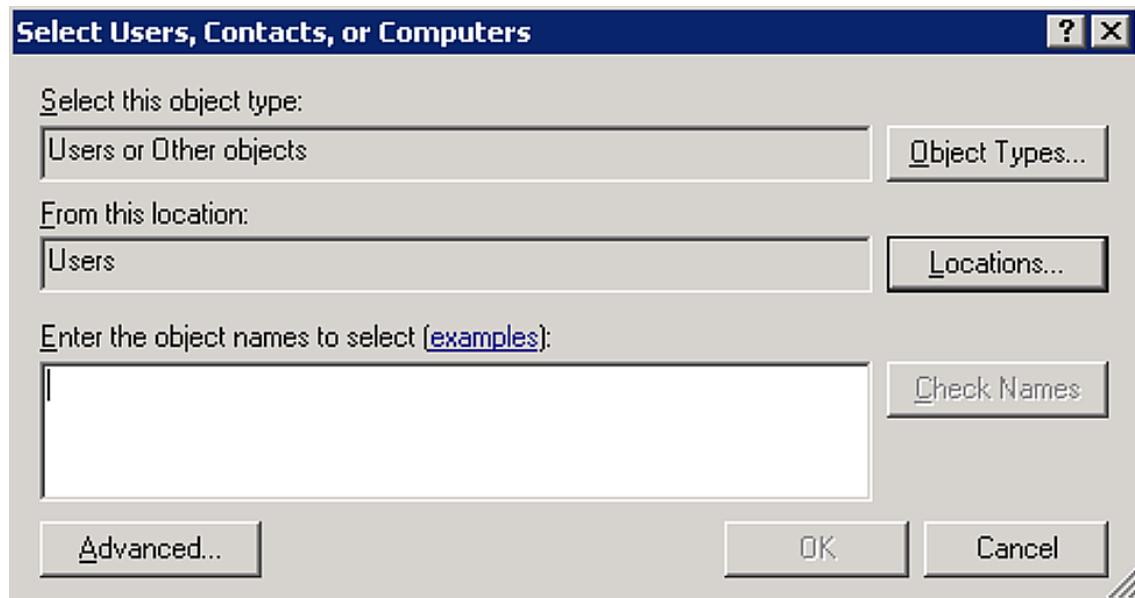


Figure 32: **Select Users, Contacts, or Computers** dialog box

8. Click **Advanced**.

The **Select Users, Contacts, or Computers** extended dialog box opens.

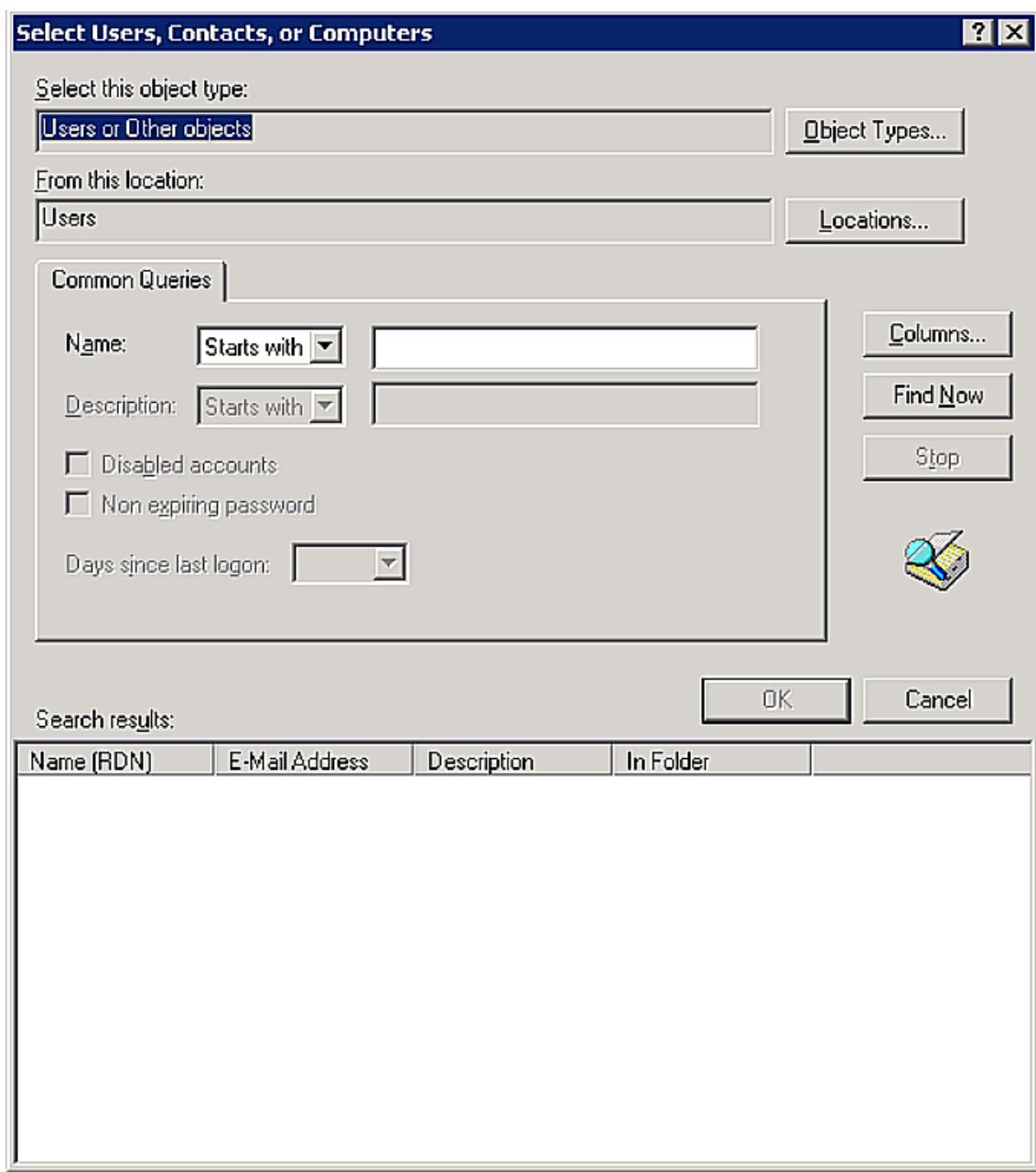


Figure 33: **Select Users, Contacts, or Computers** dialog box - searching

9. Click **Find Now** to display all the users in your domain.

In the **Search results** area all found users are displayed.

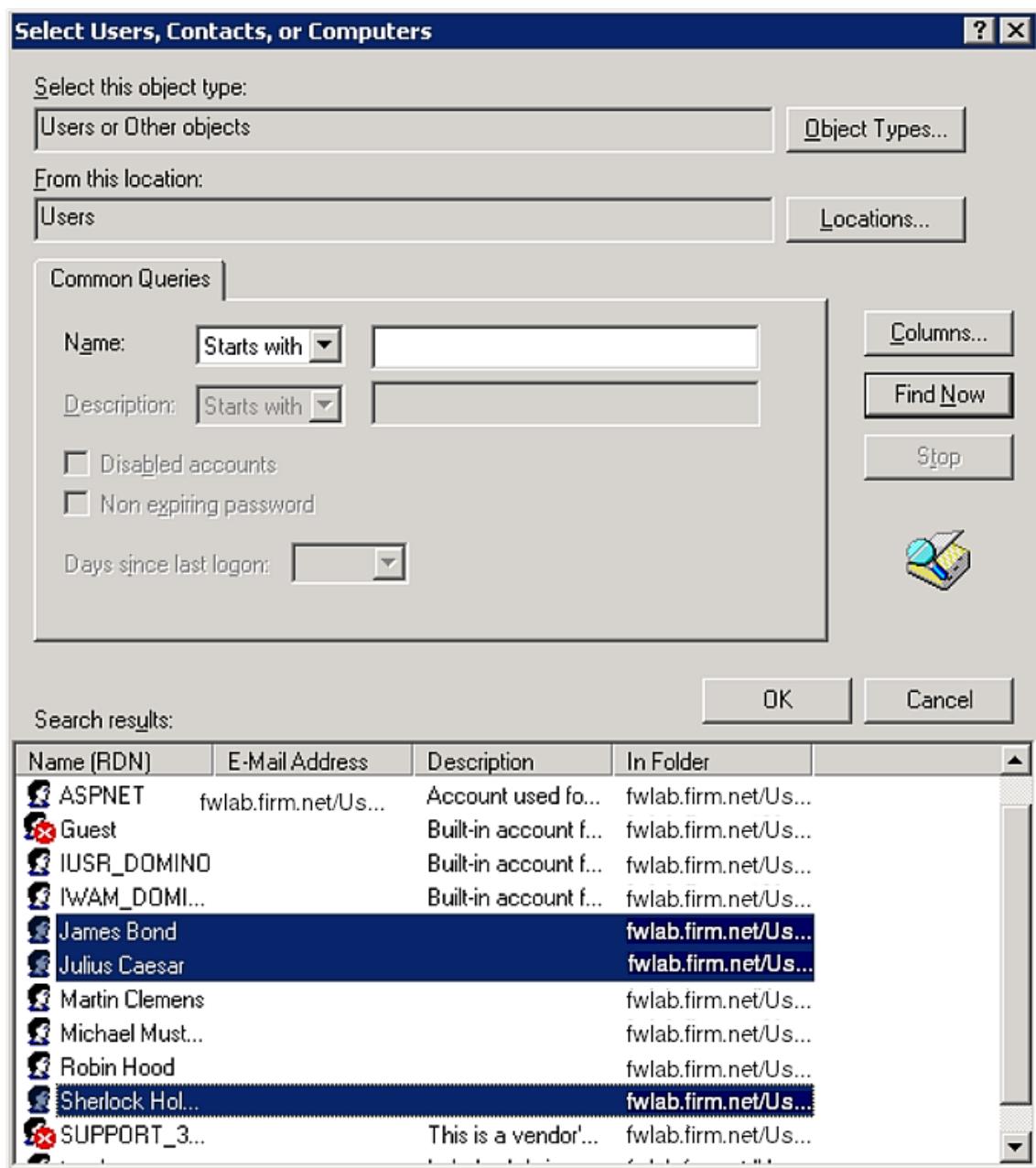


Figure 34: Select Users, Contacts, or Computers dialog box - displaying the search results

10. Select the users to be added to the group and click **OK** to confirm.

The selected users are now displayed.

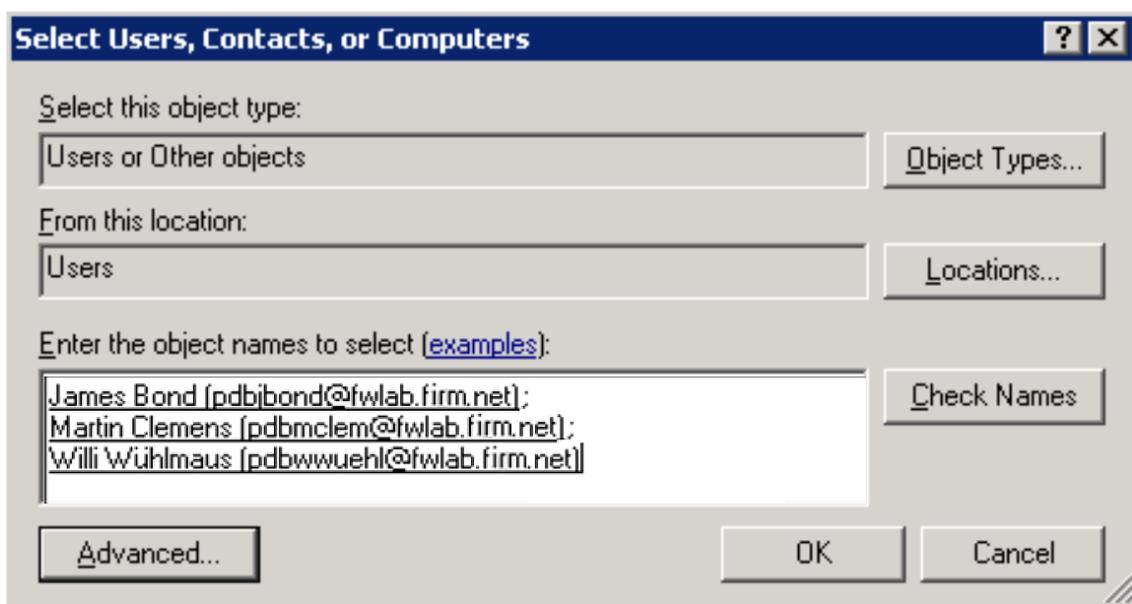


Figure 35: **Select Users, Contacts, or Computers** dialog box - confirming the search results

11. Confirm with **OK**.

## 5.4.5 iRMC user management via Novell eDirectory

This section describes how you integrate iRMC user management into Novell eDirectory.

**Prerequisite:** An LDAP v2 structure has already been created in the Novell eDirectory service (see section "[SVS\\_LdapDeployer utility](#)" on page 76).

To integrate iRMC user management into Novell eDirectory perform the following steps:

1. Integrating iRMC user management into Novell eDirectory
2. Assign an iRMC user to a permission group

### 5.4.5.1 Integrating iRMC user management into Novell eDirectory

You perform the following steps in order to integrate iRMC user management in Novell eDirectory:

- Create the principal iRMC user.
- Declare the iRMC groups and user permissions in eDirectory.
- Assign users to the permission groups.

### LDAP authentication process for iRMC users in eDirectory

The authentication of a global iRMC user on login at the iRMC is performed in accordance with a predefined process (see "[User management concept](#)" on page 42). The figure illustrates this process for global iRMC user management with Novell eDirectory.

The establishment of a connection and login with the corresponding login information is referred to as a BIND operation.

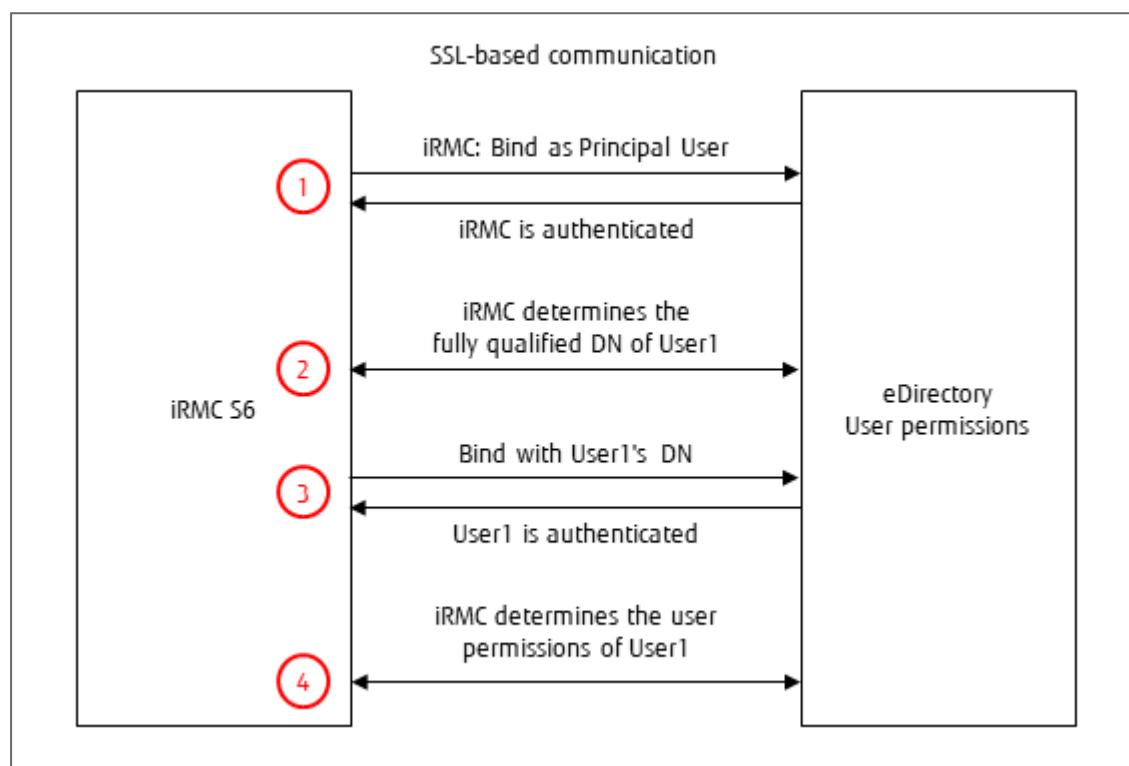


Figure 36: Authentication diagram for global iRMC permissions

1. The iRMC logs in at the eDirectory server with the predefined, known permission data (iRMC setting) as "Principal User" and waits for the successful bind.
2. The iRMC asks the eDirectory server to provide the fully qualified Distinguished Name (FQDN) of the user with "cn=User1". eDirectory determines the DN from the preconfigured subtree (iRMC setting).
3. The iRMC logs in at the eDirectory server with the FQDN of User1 and waits for the successful bind.
4. The iRMC asks the eDirectory server to provide the user permissions of User1.



You configure the Principal User's permission data and the subtree which contains the DNs on the **User Management** page of the iRMC web interface. A user's CN must be unique within the searched subtree.

## Creating the Principal User for the iRMC

Proceed as follows to create the Principal User for the iRMC:

1. Log in at iManager with valid authentication data.
2. Select **Roles and Tasks**.
3. Select **Users - Create User**.
4. Enter the necessary specifications in the displayed template.
  - The Principal User's Distinguished Name (DN) and password must match the corresponding specifications for the iRMC configuration.
  - The user's **Context**: may be located at any position in the tree.
5. Assign the Principal User search permissions for the following subtrees:
  - Subtree (OU) **SVS**.
  - Subtree (OU) that contains the users (e.g. **people**).

## Assigning user permissions to the iRMC groups and users

By default, an object in eDirectory possesses only very limited query and search permissions in an LDAP tree. If an object is to be able to query all the attributes in one or more subtrees, you must assign this object the corresponding permissions.

You may assign permissions either to an individual object (i.e. a specific user) or to a group of objects which are collated in the same organizational unit (OU) such as **SVS** or **people**. In this case, the permissions assigned to an OU and identified as "inherited" are automatically passed on to the objects in this group.

To integrate iRMC user management in Novell eDirectory, it is necessary to assign search permissions to the following objects (trustees):

- **Principal User**
- Subtree which contains the iRMC users

Proceed as follows to assign an object search permissions for all attributes:

1. Start iManager via the web browser.
2. Log in at iManager with valid authentication data.
3. In iManager, click the **Roles and Tasks** button.
4. In the menu tree structure, select **Rights - Rights to Other Objects**.

The page **Rights to Other Objects** is displayed.

5. Under **Trustee Name**, specify the name of the object (in the figure below: **SVS.sldr4**) to which the permission is to be granted.
6. Under **Context to Search From**, specify the eDirectory subtree (**SVS**) which iManager is to search through for all the objects for which the trustee **Users** currently has read permission.

7. Click **OK**.

A progress display indicates the status of the search. Once the search operation has been completed, the page **Rights to Other Objects** is displayed with the results of the search.

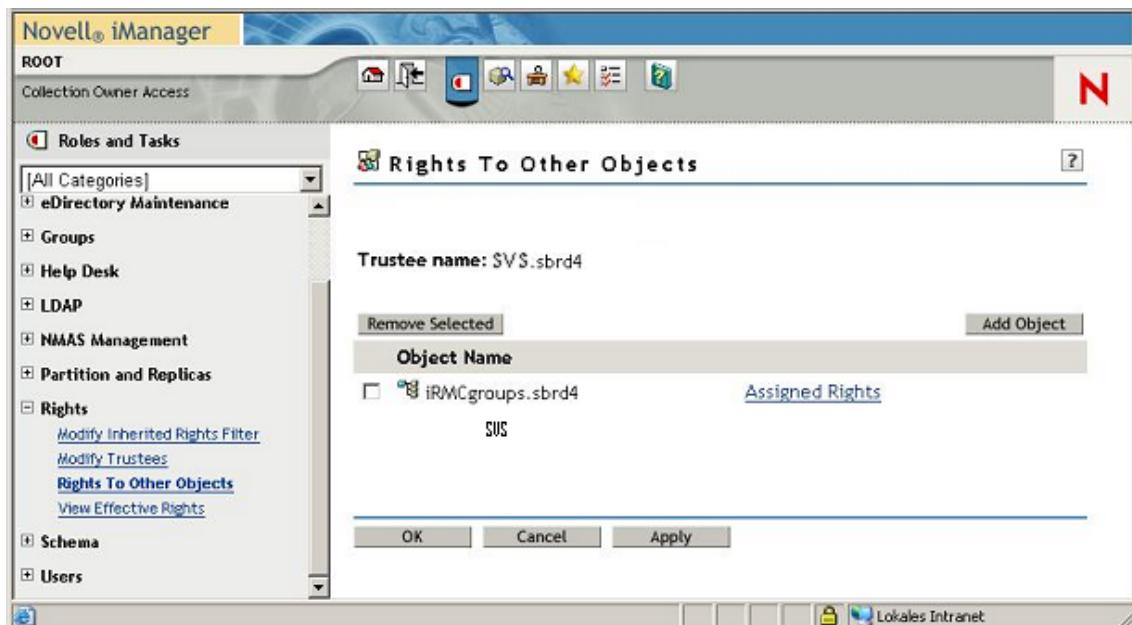


Figure 37: iManager - Roles and Tasks - Rights To Other Objects

If no object is displayed below **Object Name**, then the trustee currently has no permissions within the specified context.

8. Assign the trustee additional permissions if necessary:

a. Click **Add Object**.

b. Click the object selector button to select the object for which you want to assign the trustee a permission.

c. Click **Assigned Rights**.

If the property **[All Attributes Rights]** is not displayed:

i. Click **Add Property**.

The **Add Property** dialog box opens.

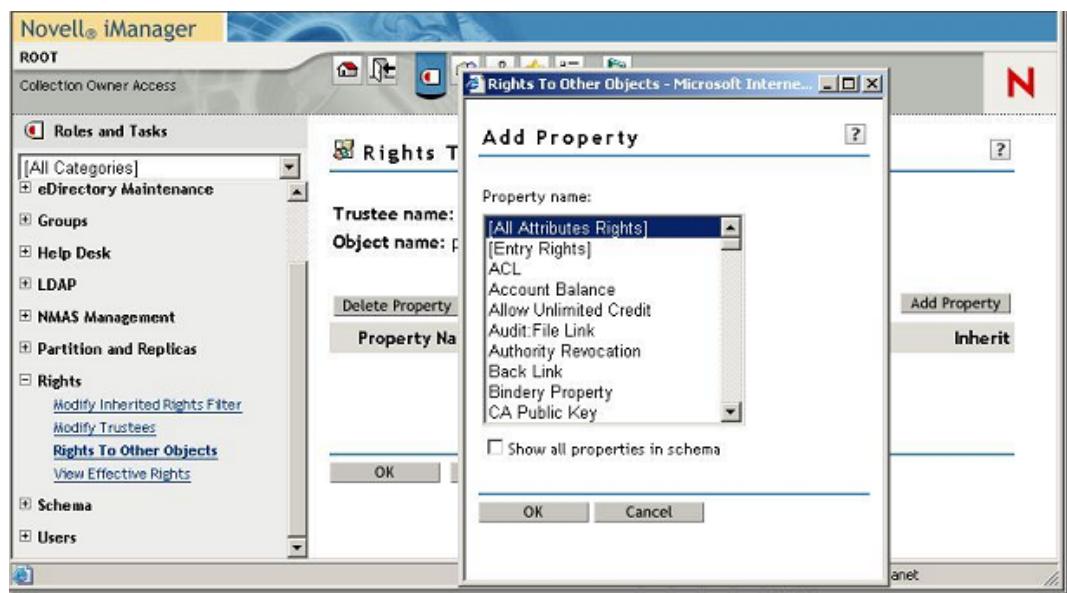


Figure 38: iManager - Roles and Tasks - Rights To Other Objects - **Add Property** dialog box

- ii. Highlight the property **[All Attributes Rights]** and click **OK** to add it.
- d. For the property **[All Attributes Rights]**, enable the options **Compare**, **Read** and **Inherit** and click **OK** to confirm.  
This authorizes the user/user group to query all the attributes in the selected object's subtree.
- e. Click **Apply** to activate your settings.

#### 5.4.5.2 Assigning an iRMC user to a permission group

You can assign iRMC users (for instance from the OU **people**) to the iRMC permission groups starting from one of the following entries:

- User (preferable if there only a few user entries)
- Role / group (preferable if there are a lot of user entries)

The following example shows the assignment of iRMC users from an OU **people** to a permission group. The assignment starting from the group entry / role entry is explained. The assignment procedure on the basis of the user entry is very similar.

In eDirectory you assign the users to the groups individually.

Proceed as follows:

1. Start iManager via the web browser.
2. Log in at iManager with valid authentication data.
3. Select **Roles and Tasks**.
4. Select **Groups - Modify Group**.

The **Modify Group** page opens.

5. Perform the following steps for all the permission groups to which you want to assign iRMC users:

- a. Use the object selector button  to select the permission group to which you want to add iRMC users. In the example of the LDAP v2 structure (see the figure below) this is: **Administrator.AuthorizationRoles.DeptX.Departments.SVS.sbrd4**.
- b. Open the **Members** tab.

The **Members** tab of the **Modify Group** page opens.

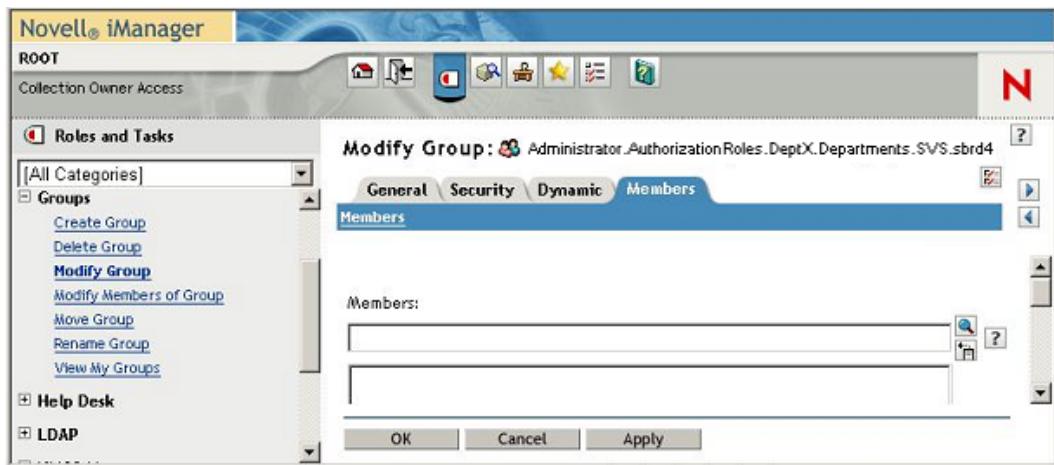


Figure 39: iManager - Roles and Tasks - Modify Group - **Members** tab (LDAP v2)

- c. Perform the following steps for all the users of the OU **people** which you want to assign to the iRMC group:

- i. Click the object selector button .

The **Object Selector (Browser)** dialog box opens.

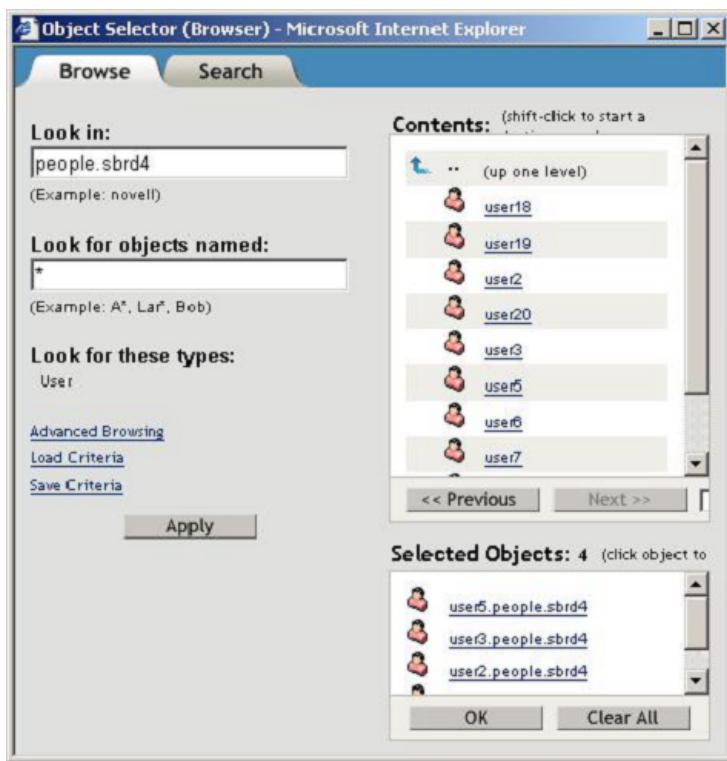


Figure 40: Assigning users to the iRMC group - selecting users

- ii. In the **Object Selector (Browser)** dialog box, select the required user(s) in the OU **people** and click **OK** to confirm.

The selected users are now listed in the display area in the **Members** tab of the **Modify Group** page.

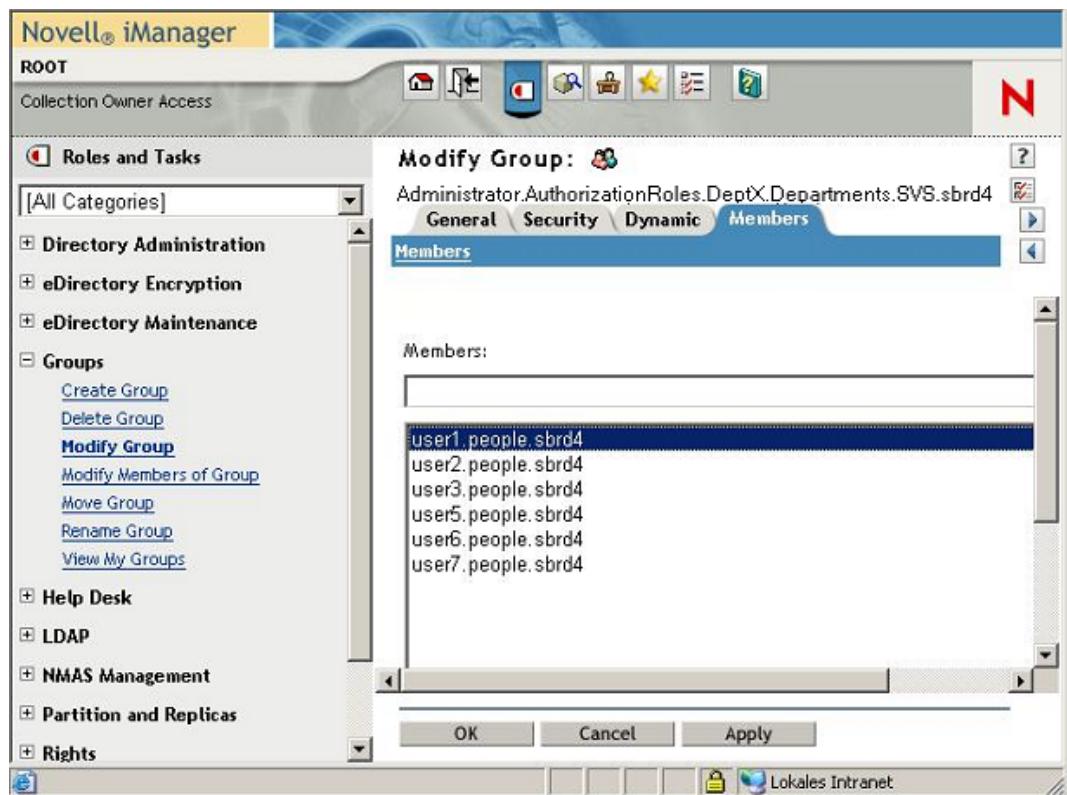


Figure 41: Display of the selected iRMC users in the **Members LDAP v2** tab

- iii. Confirm with **Apply** or **OK** in order to add the selected users to the iRMC group (here: ... .SVS.sbrd4).

### 5.4.5.3 Tips on administering Novell eDirectory

#### Restarting the NDS daemon

Proceed as follows to restart the NDS daemon:

1. Open the command box.
2. Log in with root permission.
3. Execute the following command:

```
rcndsd restart
```

If, for any unidentifiable reason, the nldap daemon fails to start:

1. Start the lndap daemon "manually":

```
/etc/init.d/nldap restart
```

If iManager does not respond:

1. Restart iManager:

```
/etc/init.d/novell-tomcat4 restart
```

## Reloading the configuration of the NLDAP server

Proceed as follows:

1. Start ConsoleOne and log in to eDirectory.



If you start ConsoleOne for the first time, no tree is configured.

Proceed as follows to configure a tree:

- a. Under **My World**, select the node **NDS**.
- b. In the menu bar, select: **File - Authenticate**
- c. Enter the following authentication data for login:
  - Login-Name: root
  - Password: <password>
  - Tree: MY\_TREE
  - Context: mycompany

2. In the left-hand part of the window, click the **Base DN** object (**Mycompany**).

The **LDAP Server** object is then displayed in the right-hand side of the window.

3. Right-click on the **LDAP Server** object and select **Properties...** in the context menu.
4. In the **General** tab, click **Refresh NLDAP Server Now**.

## Configuring the NDS message trace

The `nds` daemon generates debug and log messages which you can trace using the `ndstrace` tool. The purpose of the configuration described below is to redirect the output from `ndstrace` to a file and display the content of this file at another terminal. For this latter task, you use the `screen` tool.

The following procedure is recommended:

1. Open the command box (e.g. **bash**).

## Configure ndtrace

1. Go to the eDirectory directory **/home/eDirectory**:

```
cd /home/eDirectory
```

2. Start **screen** by means of the command `screen`.

3. Start **ndstrace** with the command `ndstrace`.

4. Select the modules that you want to activate.

For example, if you want to display the times at which events occurred, enter `dstrace TIME`.



You are very strongly recommended to activate the modules **LDAP** and **TIME** by making the following entry:

```
dstrace LDAP TIME
```

## 5. Terminate **ndstrace** by entering **quit**.

This terminates the configuration of **ndstrace**.

### Outputting messages at a second terminal

#### 1. Start **ndstrace** and redirect message output:

```
ndstrace -l >ndstrace.log
```

#### 2. Use the following key combination to open a second terminal:

[Ctrl] + [a], [Ctrl] + [c]

#### 3. Activate log recording:

```
tail -f ./ndstrace.log
```

#### 4. To switch between the virtual terminals, use the key combination [Ctrl] + [a], [Ctrl] + [0].

(The terminals are numbered from 0 to 9)

## 5.4.6 iRMC user management via OpenLDAP

This section describes how you integrate iRMC user management into Open LDAP.

**Prerequisite:** An LDAP v2 structure has already been created in the Open LDAP service (see section "[SVS\\_LdapDeployer utility](#)" on page 76).

To integrate iRMC user management into Open LDAP perform the following steps:

- Generating the principal iRMC user.
- Creating the new iRMC user and assigning this user to the permission group.

### 5.4.6.1 Creating the new iRMC user

Proceed as follows:

1. Start the LDAP Browser.
2. Log in at the OpenLDAP directory service with valid authentication data.
3. Create a new user.

To do this, proceed as follows:

- a. Select the subtree (subgroup) in which the new user is to be created. The new user can be created anywhere in the tree.

- b. Open the **Edit** menu.
  - c. Select **Add Entry**.
  - d. Select **Person**.
  - e. Edit the Distinguished Name **DN**.
  - f. Click **Set** and enter the password.
  - g. Enter a Surname **SN**.
  - h. Click **Apply**.
4. Assign the new user to the permission group.
- To do this, proceed as follows:
- a. Select the **SVS** subtree (subgroup) to which the user is to belong, i.e.  
**cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS,  
dc=myorganisation,dc=mycompany**
  - b. Open the **Edit** menu.
  - c. Select **Add Attribute**.
  - d. Specify "Member" as the attribute name. As the value, specify the fully-qualified DN of the user you have just created, i.e.  
**cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS,  
dc=myorganisation,dc=mycompany**

#### 5.4.6.2 Generating the Principal User

To generate the Principal User you need an LDAP browser, for example the LDAP browser/editor published by Jarek Gawor. This LDAP browser/editor is easy to use via a graphical user interface. The browser is available for download in the internet.

Proceed as follows to install the LDAP browser/editor:

1. Unpack the Zip archive `Browser282.zip` to an installation directory of your choice.
2. Set the environment variable `JAVA_HOME` to the installation directory for the JAVA runtime environment, e.g.:

```
JAVA_HOME=C:\Program Files\Java\jre7
```

To generate the Principal User (ObjectClass: **Person**) proceed as follows:

1. Start the LDAP Browser.
2. Log in at the OpenLDAP directory service with valid authentication data.
3. Select the subtree (subgroup) in which the Principal User is to be created. The Principal User can be created anywhere in the tree.
4. Open the **Edit** menu.
5. Select **Add Entry**.
6. Select **Person**.

7. Edit the Distinguished Name **DN**.



The Principal User's Distinguished Name (DN) and password must match the corresponding specifications for the iRMC configuration.

8. Click **Set** and enter a password.
9. Enter a Surname **SN**.
10. Click **Apply**.

#### 5.4.6.3 Tips on OpenLDAP administration

##### Restarting the LDAP service

Proceed as follows to restart the LDAP service:

1. Open the command box.
2. Log in with root permission.
3. Enter the following command:

```
rcldap restart
```

##### Message logging

The LDAP daemon uses the Syslog protocol for message logging.

The logged messages are only displayed if a log level other than 0 is set in the file /etc/openldap/slapd.conf.

For an explanation of the various levels, see:

<http://www.zytrax.com/books/ldap/ch6/#loglevel>

The following table provides an overview of the log levels and their meanings.

Log level	Meaning
-1	Comprehensive debugging
0	No debugging
1	Log function calls
2	Test packet handling
4	Heavy trace debugging
8	Connection management
16	Show sent/received packets
32	Search filter processing
64	Configuration file processing
128	Processing of access control lists

Log level	Meaning
256	Status logging for connections/operations/events
512	Status logging for sent entries
1024	Output communication with shell back-ends.
2048	Output results of entry parsing.

Table 5: OpenLDAP - log levels

## 5.4.7 Configuring E-mail alerting to global iRMC users

E-mail alerting to global iRMC users is integrated in the global iRMC user management system. This means that e-mail alerting can be configured and handled centrally for all platforms using a directory server. Appropriately configured global user IDs can receive e-mail alerts from all iRMCS that are connected to a directory server in the network.

**Prerequisites** The following requirements must be met for e-mail alerting:

- A principal user is configured in the iRMC web interface who has been granted permission to search the LDAP tree.
- When configuring the LDAP settings on the **User Management** page, e-mail alerting must have been enabled in the **LDAP** group.

### 5.4.7.1 Global E-mail alerting

Alert roles are required for global e-mail alerting via the directory server. These are defined in addition to the authorization roles in the configuration file of the SVS\_LdapDeployer utility ([see page 76](#)).

#### Displaying alerting groups (alert roles)

An alert role groups together a selection of alert types (e.g. temperature threshold exceeded), each with an assigned severity (e.g. "critical"). Assigning a user to a particular alert group specifies what alert types and severities the user will be alerted of by e-mail.

The syntax of the alert roles is illustrated in the sample configuration files that are supplied together with the jar archive `svs_LdapDeployer.jar` via download from the FUJITSU support pages.

## Displaying alert types

The following alert types are supported:

Alert type	Cause
FanSens	Fan sensors
Temperat	Temperature sensors
HWError	Critical hardware error
Security	Security
SysHang	System hung
POSTErr	POST error
SysStat	System status
DDCtrl	Disk drives and controllers
NetInterf	Network interface
RemMgmt	Remote Management
SysPwr	Power management
Memory	Memory
Others	Miscellaneous

Table 6: Alert types

Each alert type can be assigned one of the following severity levels: **Warning**, **Critical**, **All**, (**none**).

## Preferred mail server.

For global e-mail alerting, the setting **Automatic** is used on the preferred mail server: If the e-mail cannot be successfully sent immediately, for instance if the first mail server is not available, the e-mail is sent to the second mail server.

## Supported mail formats

The following e-mail formats are supported:

- Standard
- Fixed Subject
- ITS-Format
- Fujitsu REMCS Format



If a mail format other than **Standard** is used, you must add the users to the corresponding mail format group.

## LDAP E-mail table

If e-mail alerting is configured (see page 104) and the **LDAP E-mail Alert Enable** option is selected, the iRMC sends e-mails to the following users when an alert is issued:

- All appropriately configured local iRMC users.
- All global iRMC users registered in the LDAP e-mail table for this alert.

The LDAP e-mail table is initially created by the iRMC firmware the first time the iRMC is started and then updated at regular intervals. The size of the LDAP e-mail table is limited to a maximum of 64 LDAP alert roles and a maximum of 64 global iRMC users for whom e-mail alerting is configured.



It is recommended that you use e-mail distribution lists for global e-mail alerting.

The LDAP directory server gets the following information from the e-mail table for the purposes of e-mail alerting:

- List of the global iRMC users for whom e-mail alerting is configured.
- For each global iRMC user:
  - List of the configured alerts for each alert type (type and severity).
  - Required mail format.

The LDAP e-mail table is updated in the following circumstances:

- The iRMC is started for the first time or restarted.
- The LDAP configuration is changed.
- At regular intervals (optional). You specify the update interval as part of the LDAP configuration in the iRMC web interface (with the **LDAP Alert Table Refresh** option).

## Configuring global e-mail alerting on the directory server

This section describes how to configure e-mail alerting on the directory server. Settings must also be made for the iRMC dialog. You configure these in the iRMC web interface.

Proceed as follows:

1. In the directory service, enter the e-mail addresses of the users to whom e-mails are to be sent.



The method used to configure the e-mail addresses differs depending on the directory service used (Active Directory, eDirectory or OpenLDAP).

2. Create a configuration file in which the alert roles are defined.
3. Start the **SVS\_LdapDeployer** using this configuration file in order to generate a corresponding LDAP v2 structure (**SVS**) on the directory server (see sections "Starting **SVS\_LdapDeployer**" on page 78).

### 5.4.7.2 Displaying alert roles

After the LDAP structure has been generated, the newly created OU **SVS** is displayed in Active Directory, for instance, together with the components **Alert Roles** and **Alert Types** under **Declarations** and together with the component **Alert Roles** under **DeptX**:

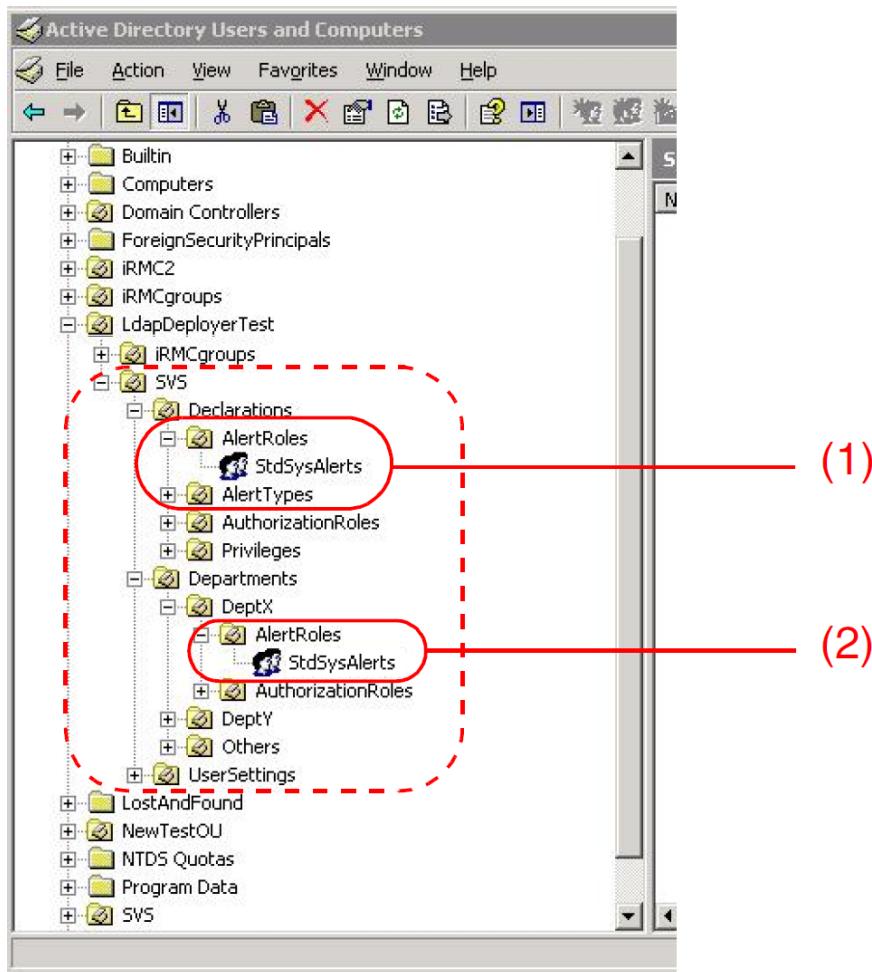


Figure 42: OU **SVS** with alert roles

1. Under **Declarations, Alert Roles** displays all the defined alert roles and all the alert types are displayed under **Alert Types** (1).
2. Under **DeptX, Alert Roles** displays all the alert roles that are valid in the OU **DeptX** (2).

 To ensure that e-mails are sent to the users in the individual alert roles, the relevant department must be configured in iRMC (in the figure above: **DeptX**).

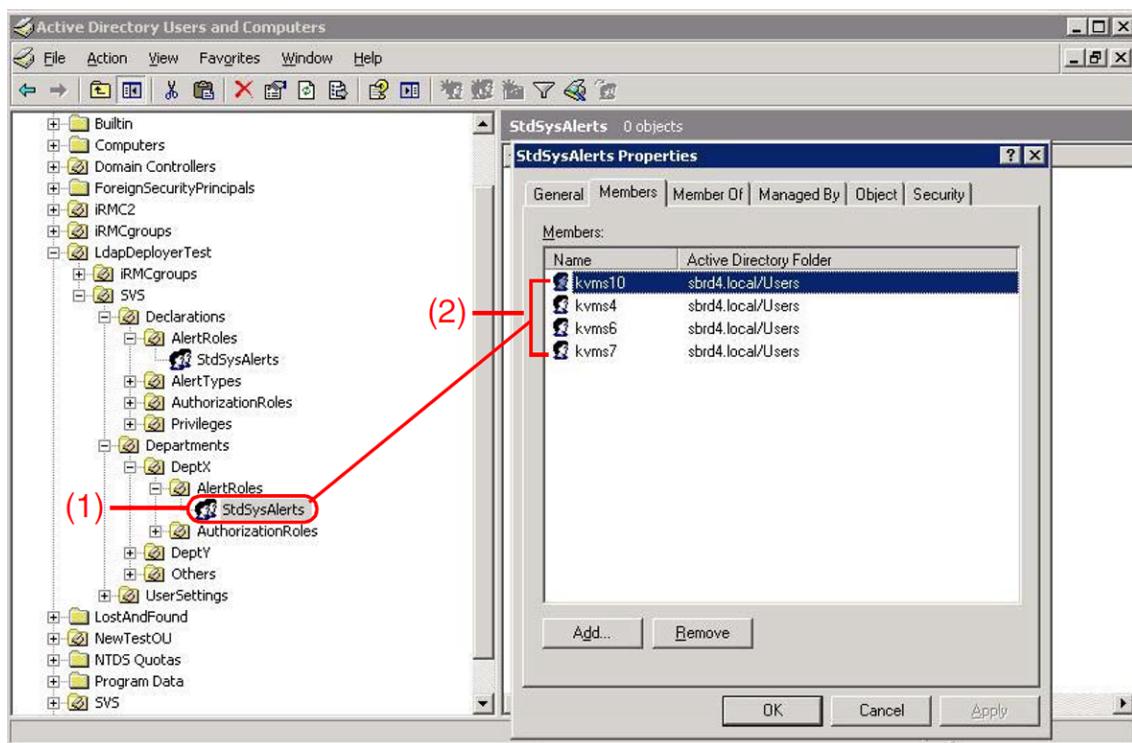


Figure 43: Users assigned to the alert role "StdSysAlert"

If you select an alert role (e.g. **StdSysAlerts**) under **SVS – Departments – DeptX – Alert Roles** in the structure tree for **Active Directory Users and Computers** (1) and open the **Properties** dialog box for this alert role by choosing **Properties – Members** from the context menu, all the users that belong to the alert role (here: **StdSysAlerts**) are displayed in the **Members** tab (2).

#### 5.4.7.3 Assign iRMC users to an alert role

You can assign iRMC users to alert roles either on the basis of the user entry or on the basis of the role entry.

In the various different directory services (Microsoft Active Directory, Novell eDirectory and OpenLDAP), iRMC users are assigned to iRMC alert roles in the same way in which iRMC users are assigned to iRMC authorization roles and using the same tools.

In Active Directory, for instance, you make an assignment by clicking **Add...** in the **Properties** dialog box of the **Active Directory Users and -Computers** snap-in ([see page 106](#)).

## 5.4.8 Configuring the iRMC for LDAP authentication

As a last step, after the **SVS** structure in the directory service of the LDAP server has been created and elaborated, the iRMC itself needs to be configured to connect to the LDAP server for user authentication.

The configuration steps depend on the type of the connection:

- Insecure without SSL/TLS: in this case the **DNS** function must be enabled. In the **DNS Server 1** field of the **DNS** group on the **Network Management** page enter the IP address of the target Directory Service server.
- Secure via SSL/TLS: in this case the DNS information is not relevant.

### Configuring DNS (insecure connection only)

1. Open the web interface of the iRMC.
2. Open the **Network Management** page in the **Settings** menu.
3. In the **DNS** group check the **Enable DNS** option.
4. In the **DNS Server 1** field enter the IP address or host name of the LDAP server to be used.

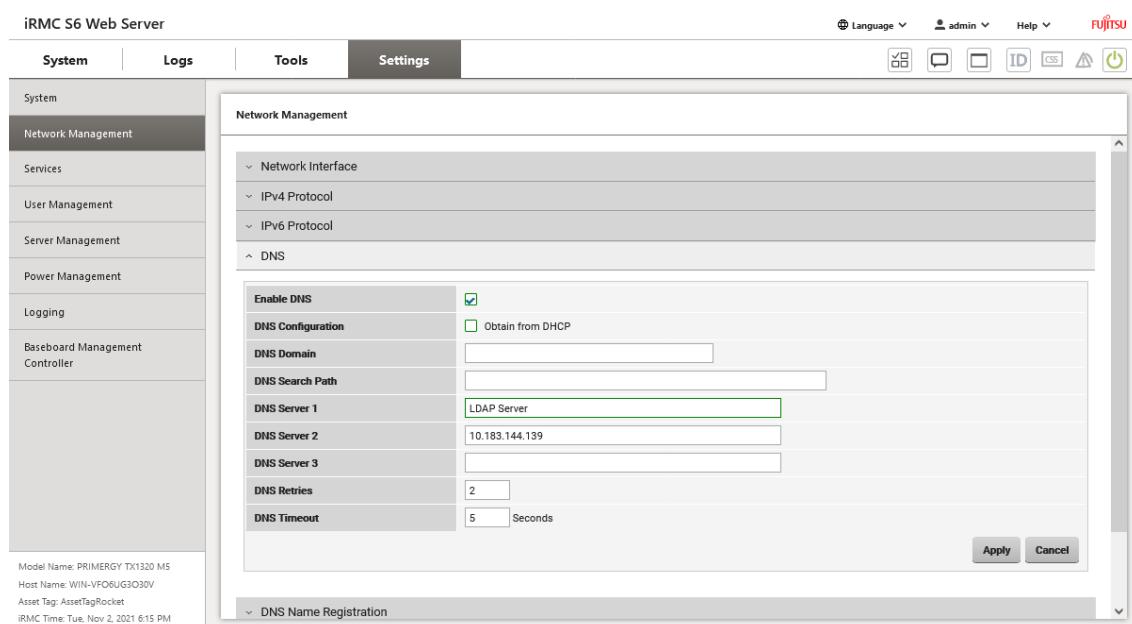


Figure 44: Configure DNS settings

5. Click **Apply** to confirm your settings.

The settings are checked and applied.



For your changes to become effective you need to reboot the iRMC via the **Reboot** button on the **Update** page of the **Tools** menu.

## Configuring LDAP

1. Open the **User Management** page on the **Settings** menu.
2. In the **Lightweight Directory Access Protocol (LDAP)** group select the **Enable LDAP** option.
3. Select the **Enable LDAP SSL/TLS** option for a secure connection or deselect it for an insecure one.
4. Select the **Directory Service Type** running on the LDAP server from the list.
5. In the **Primary LDAP Server** group enter the IP address or host name in the **Server** field.
6. Select the corresponding **Network Port**.
7. In the **Directory Configuration** group select the **Authorization Type**.
8. According to the settings in the directory service enter the values into the **Department Name** and **Domain Name** fields. The values must be equal in both systems.

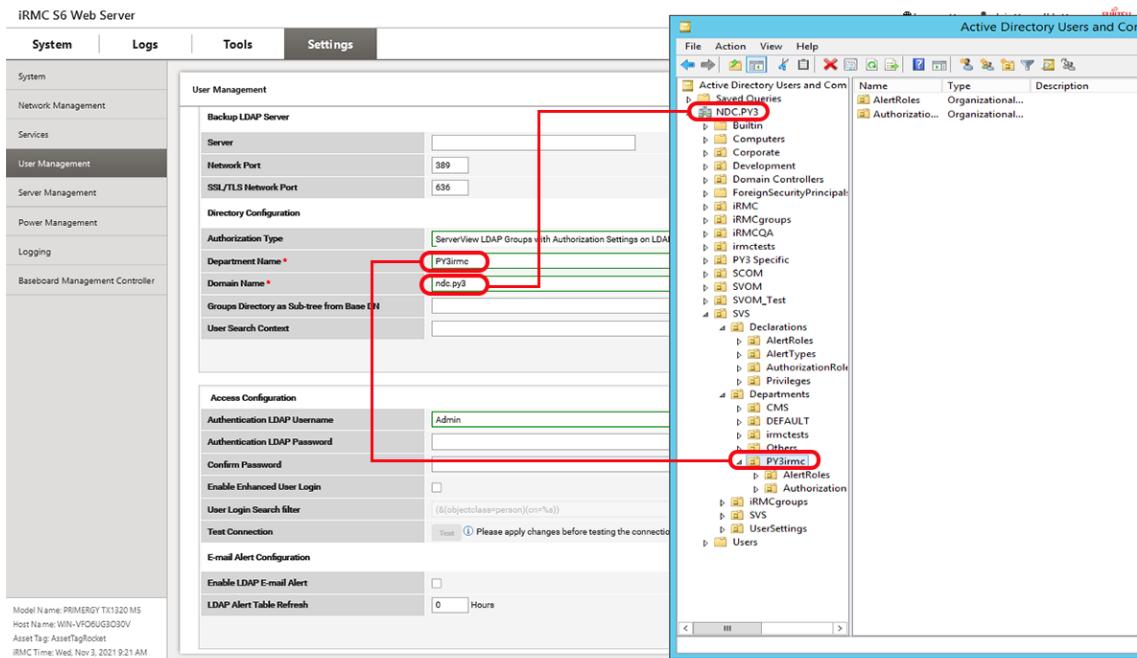


Figure 45: Configure LDAP connection

9. Click **Apply** to confirm your settings.

## Establishing a connection to the LDAP server

1. In the **Access Configuration** group within the **Lightweight Directory Access Protocol (LDAP)** group enter your LDAP user name in the **Authentication LDAP Username** field.
2. Enter your password in the **Authentication LDAP Password** field.

3. Enter your password again in the **Confirm Password** field.
4. Click **Test** to test if the connection data are correct.

The settings are checked and if a connection can be established a positive feedback is displayed near the **Test** icon.

### Configuring E-mail Alerting

1. In the **E-mail Alert Configuration** group within the **Lightweight Directory Access Protocol (LDAP)** group select the **Enable LDAP E-mail Alert** option.
2. In the **LDAP Alert Table Refresh** enter an integer for the time interval the alert table is to be stored internally.
3. Click **Apply** to confirm your settings.

A permanent connection to the LDAP server is established and all the settings are applied.

## 5.4.9 User permission configuration

In the **Directory Configuration** group of the **User Management** page the iRMC administrator can configure the user permissions in two different ways.

### Permissions managed by LDAP server

If you select **ServerView LDAP Groups with Authorization Settings on LDAP Server** from the **Authorization Type** list users and groups are created on LDAP side.

Directory Configuration	
<b>Authorization Type</b>	ServerView LDAP Groups with Authorization Settings on LDAP Server
<b>Department Name *</b>	PY3irmc
<b>Domain Name *</b>	ndc.py3
<b>Groups Directory as Sub-tree from Base DN</b>	

Figure 46: ServerView LDAP Groups with Authorization Settings on LDAP Server

iRMC permissions are granted by assigning a user to an appropriate LDAP group.

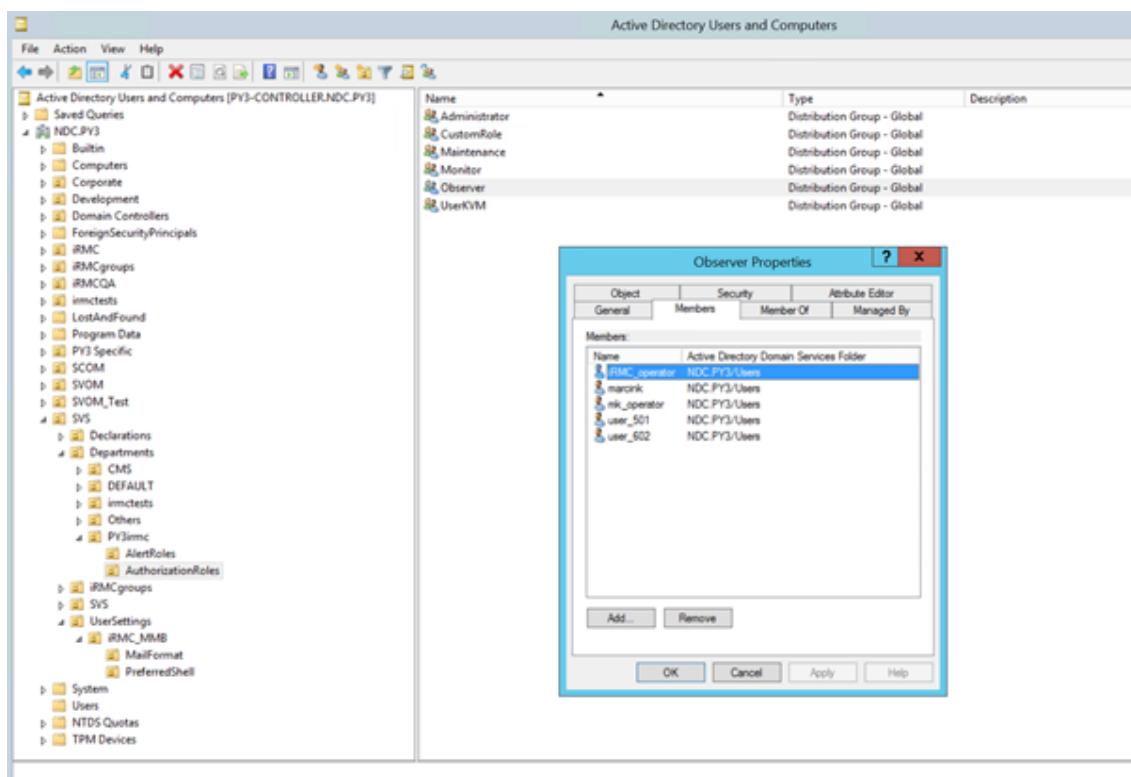


Figure 47: Members of the Observer group

### Permissions managed by iRMC

If you select **ServerView LDAP Groups with Authorization Settings on iRMC** from the **Authorization Type** list, users and groups are created on LDAP side and the users are assigned to groups as well.

This screenshot shows the configuration interface for 'ServerView LDAP Groups with Authorization Settings on iRMC'. It consists of two main sections: 'Directory Configuration' and 'User Group Information'.

**Directory Configuration:**

- Authorization Type:** Standard LDAP Groups with Authorization Settings on iRMC
- Department Name:** PY3/Domain
- Domain Name:** ndc.py3
- Groups Directory as Sub-tree from Base DN:** (empty input field)

**User Group Information:**

	Name	Action
Administrator		Edit   Delete
Observer		Edit   Delete
Operator		Edit   Delete

Figure 48: ServerView LDAP Groups with Authorization Settings on iRMC

But by creating a corresponding LDAP group in iRMC, you can set the appropriate permissions for this group.

Access Configuration	
User Shell (Text Access)	Remote Manager
LAN Channel Privilege	Administrator
Serial Channel Privilege	✓
Configure User Accounts	✓
Configure iRMC Settings	✓
Video Redirection	✓
Remote Storage Enabled	✓
Redfish Role	Administrator
E-mail Configuration	
E-mail Enabled	—
E-mail Format	UserDefined
Preferred Mail Server	Auto

Figure 49: Corresponding LDAP group on iRMC

Thus the Observer group can be provided with administrator permissions, the group defined on the LDAP server does initially not provide.

---

## 6 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.

This 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, such storage media 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 function (for more information, refer to the "ServerView Installation Manager" user guide).

Requirements for the remote installation of the operating system via iRMC S6:

- The iRMC's LAN interface must be configured (["Configuring the LAN interface using UEFI" on page 28](#)).
- The license key for use of the iRMC functions "Advanced Video Redirection (AVR)" and "Virtual Media" must be installed.

### 6.1 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 a virtual storage medium.
2. Boot and configure the managed server via DVD or the Installation Manager boot image.

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

You can still 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 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 must be controlled via the keyboard, as 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, you can start the Linux installation by booting from the Linux installation CD/DVD.

If the installation requires you to integrate drivers from the external device 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 the storage medium for driver installation

## 6.2 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 on 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 S6 - Web Interface" user guide.

To establish the virtual media connection, proceed as follows on the remote workstation:

### Java applet

1. Log on to the iRMC web interface with Remote Storage Enabled permission.
2. In the **Settings** menu, open the **Services** page.
3. In the **Advanced Video Redirection (AVR)** group, select the **JViewer (Java)** option from the **KVM Redirection Type** list.
4. Click **Apply** to submit your changes.  
5. In the menu bar, click  to open the context menu.
6. Select **Start Video Redirection** to start a AVR session.

The Java applet for Advanced Video Redirection starts. If there is another redirection session running, both sessions are shown in the **AVR Active Session Table**.

7. Click **Media/Virtual Media Wizard...**  
or  
8. Click one of the three Virtual Media icons on the toolbar.  
The **Virtual Media** dialog box opens.
9. In the appropriate panel of the **Virtual Media** dialog box, click **Select**.  
The **Open** file browser dialog box opens.
10. In the **Open** dialog box, navigate to the directory of the storage medium that you want to make available as a 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 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.

11. Select the required device type in the **Files of Type** field.
12. 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)
13. 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.
14. Click **Connect** to connect the DVD-ROM drive (DVD) or the Installation Manager boot image as virtual storage media.

### HTML5

1. Log on to the iRMC web interface with Remote Storage Enabled permission.
2. In the **Settings** menu, open the **Services** page.
3. In the **Advanced Video Redirection (AVR)** group, select the **HTML5 Viewer** option from the **KVM Redirection Type** list.
4. Click **Apply** to submit your changes.
5. In the menu bar click  to start Advanced Video Redirection.  
This opens the AVR window.
6. In the status bar click **Select**. An **Upload file** dialog box opens in which you can select an ISO image that is then displayed in the **CD image** field.
7. Click **Start Media**.  
The CD image is mounted.

## 6.3 Booting the managed server

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

1. In the title bar of the iRMC web interface click  to power off and  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 shared entry "CD-ROM DRIVE" in the BIOS boot sequence:

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

2. Press [F2] on the keyboard 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 a virtual storage medium.
5. Save your settings and exit the UEFI setup.

The managed server then boots from the 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 five minutes to boot from the ServerView Suite DVD 1 via a virtual storage medium. The boot progress is indicated during the 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.

### Requirements

- 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 the ServerView Suite DVD 1.
1. Select the option **Removable media (USB memory stick)**.
  2. Select the corresponding drive from the list to the right of this option.

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

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

Store 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 must 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 will be lost when you reboot.

5. Start the Installation Manager by clicking **Continue**.

The Installation Manager **Welcome** page opens.

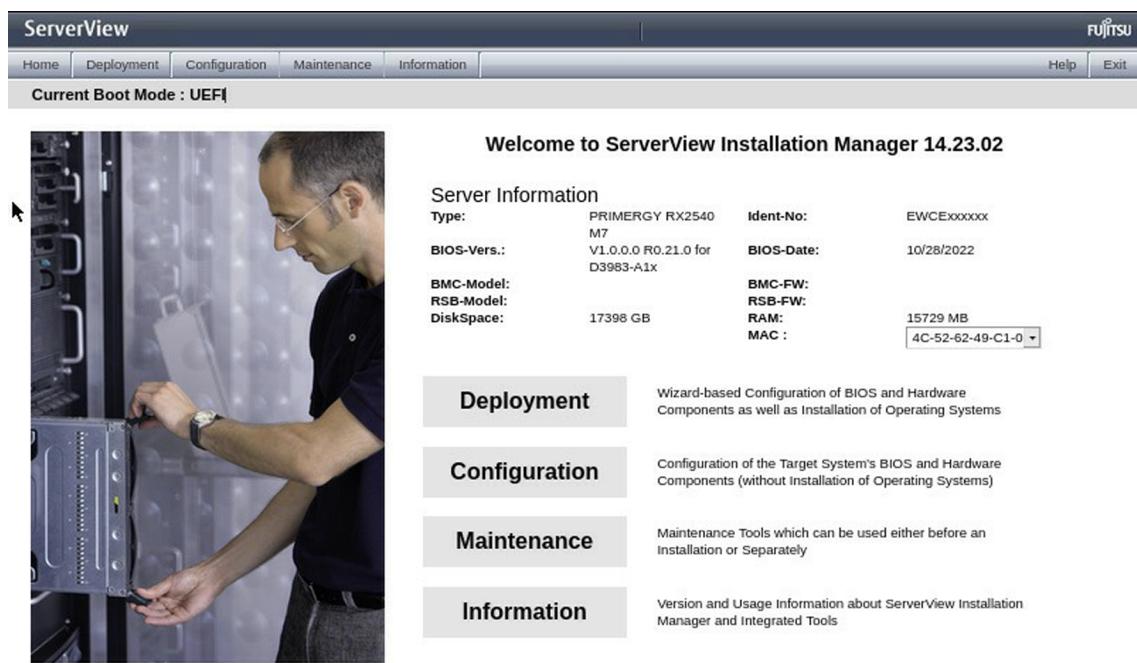


Figure 50: Installation Manager - Welcome page

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

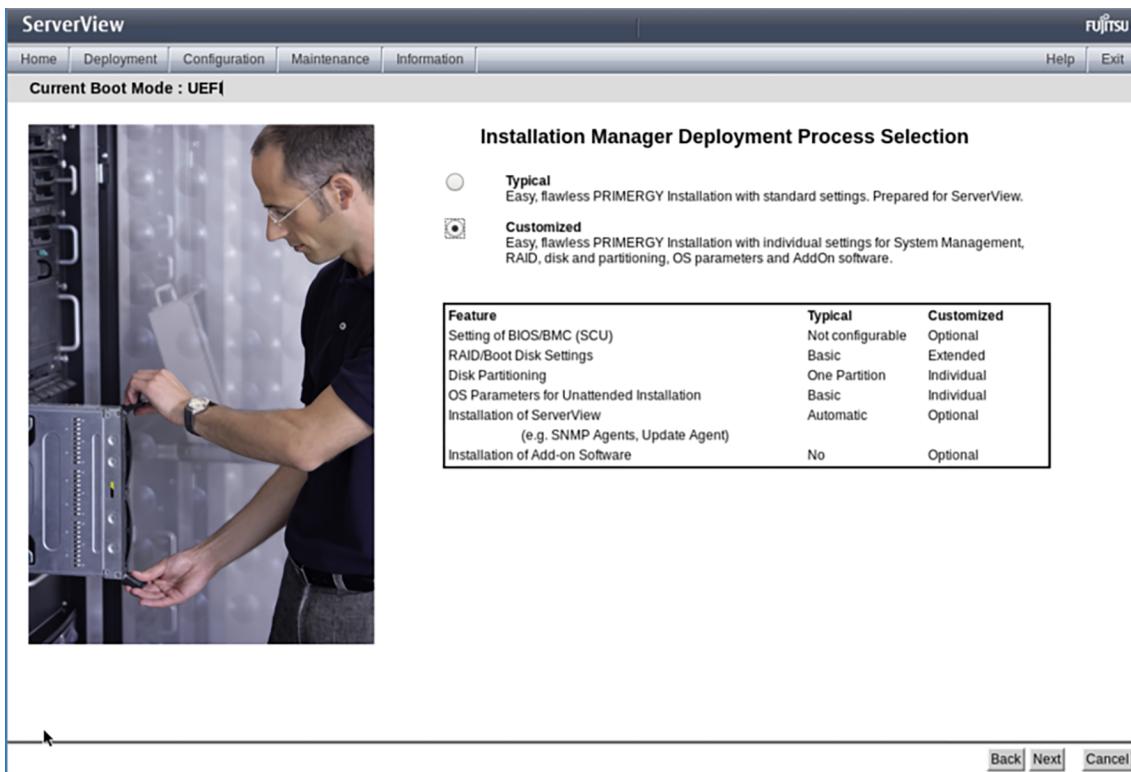


Figure 51: Installation manager: Select between typical and customized installation

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.

- 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 120](#)).

Once you have completed the configuration with the Installation Manager, the **Installation Info** page for the Windows installation (["Installing Windows on the managed server" on page 120](#)), for the Linux installation (["Installing Linux on the managed server" on page 121](#)) or the ESXi installation is displayed (["Installing ESXi on the managed server" on page 123](#)). This allows you to start the installation process.

## 6.4 Installing Windows on the managed server

Once configuration is complete, the Installation Manager displays the **Installation Info** page.

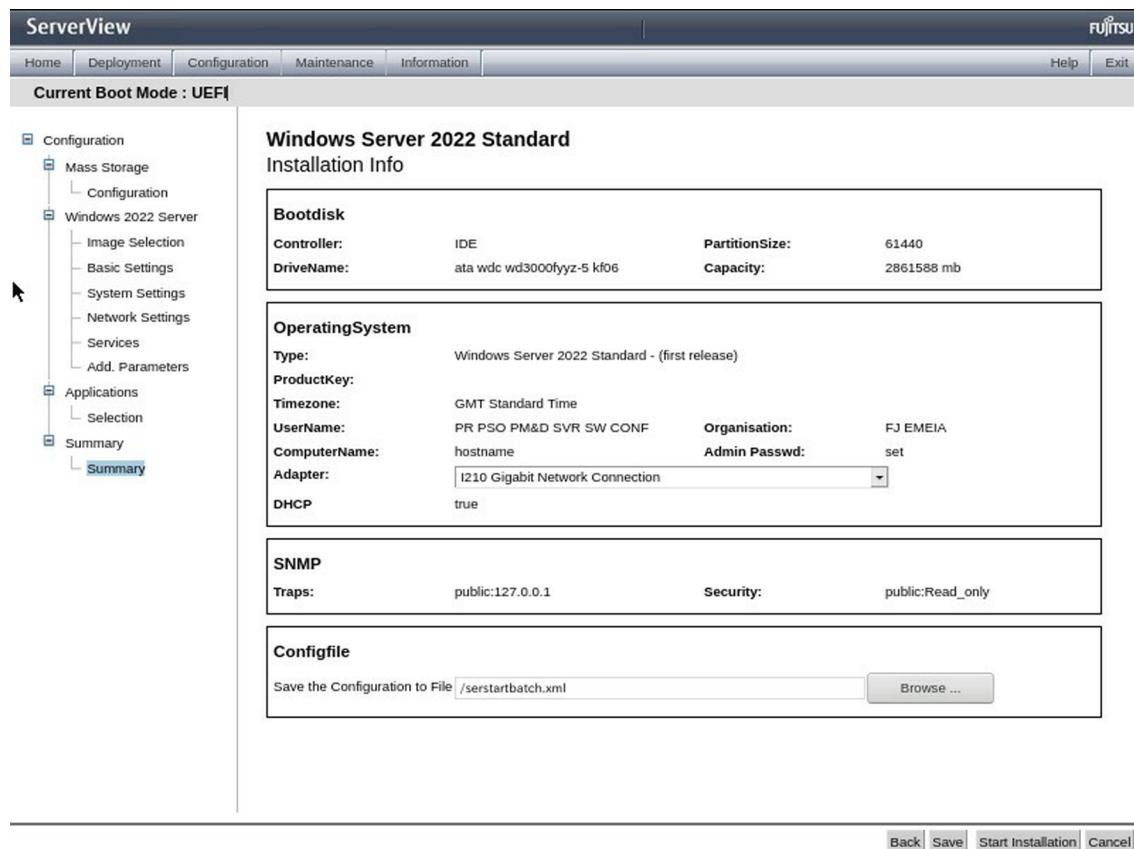


Figure 52: Installation Manager - Installation Info page

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 the ServerView Suite DVD 1 from the DVD-ROM drive at the remote workstation.
6. Insert the Windows installation CD/DVD into this drive.



Close the application if autostart is active.

7. Connect the CD-ROM/DVD-ROM drive containing the Windows installation CD/DVD as a 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.  
When the copy operation is complete, the Installation Manager opens a confirmation dialog box and prompts you to remove all the storage media from the removable media drives before the managed server is rebooted.
9. Clear all current virtual media connections again.
10. In the confirmation dialog box, click **OK** to reboot the managed server.  
Once the managed server has rebooted, you can monitor the entire installation by means of the AVR.

## 6.5 Installing Linux on the managed server

Before installing Linux on the managed server, keep in mind that you can use the mouse during the installation but you 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.

Once configuration is complete, the Installation Manager displays the **Installation Info** page.

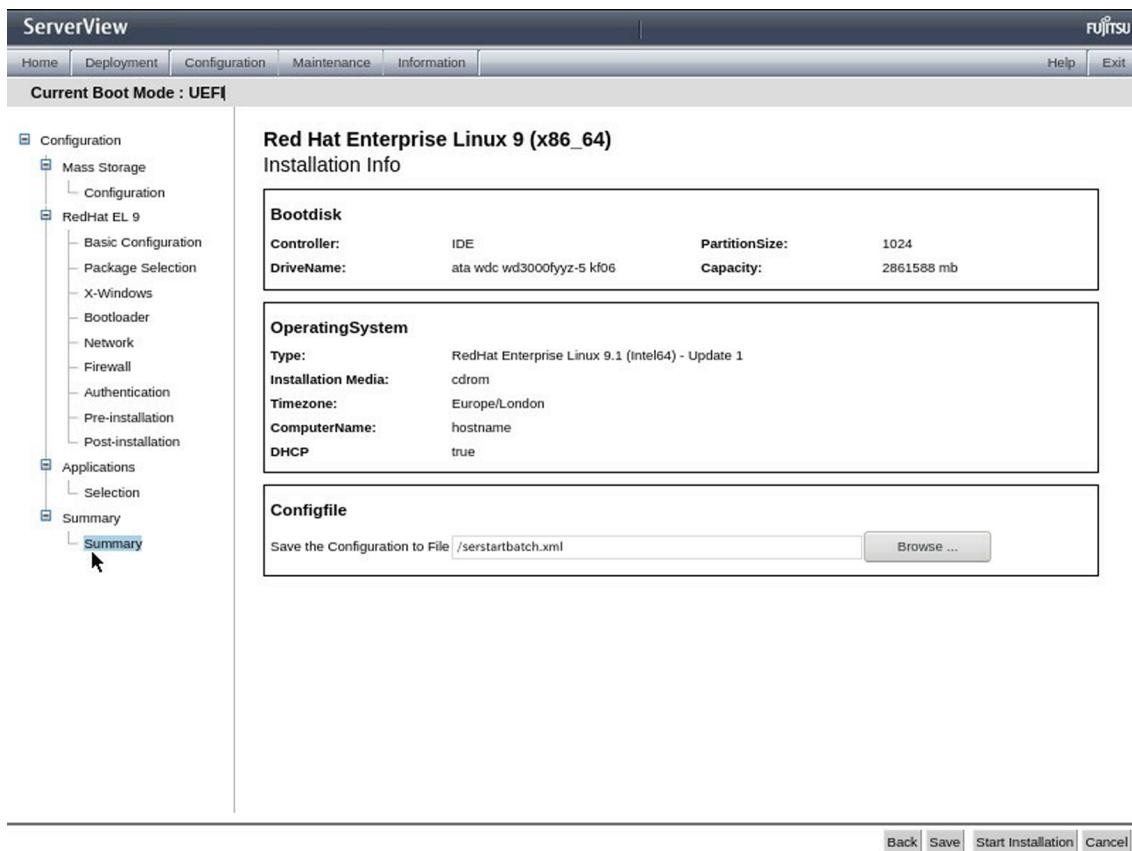


Figure 53: Installation Manager - Installation Info page

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 the ServerView Suite DVD 1 from the DVD-ROM drive at the remote workstation.
6. Insert the Linux installation CD/DVD into this drive.



Close the application if autostart is active.

7. Connect the CD-ROM/DVD-ROM drive containing the Windows installation CD/DVD as a 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.

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

9. Clear all current virtual media connections again.
10. In the confirmation dialog box, click **OK** to reboot the managed server.

Once the managed server has rebooted, you can monitor the entire installation by means of the AVR.

## 6.6 Installing ESXi on the managed server

Before installing ESXi on the managed server, keep in mind that you can use the mouse during the installation but you 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.

Once configuration is complete, the Installation Manager displays the **Installation Info** page.

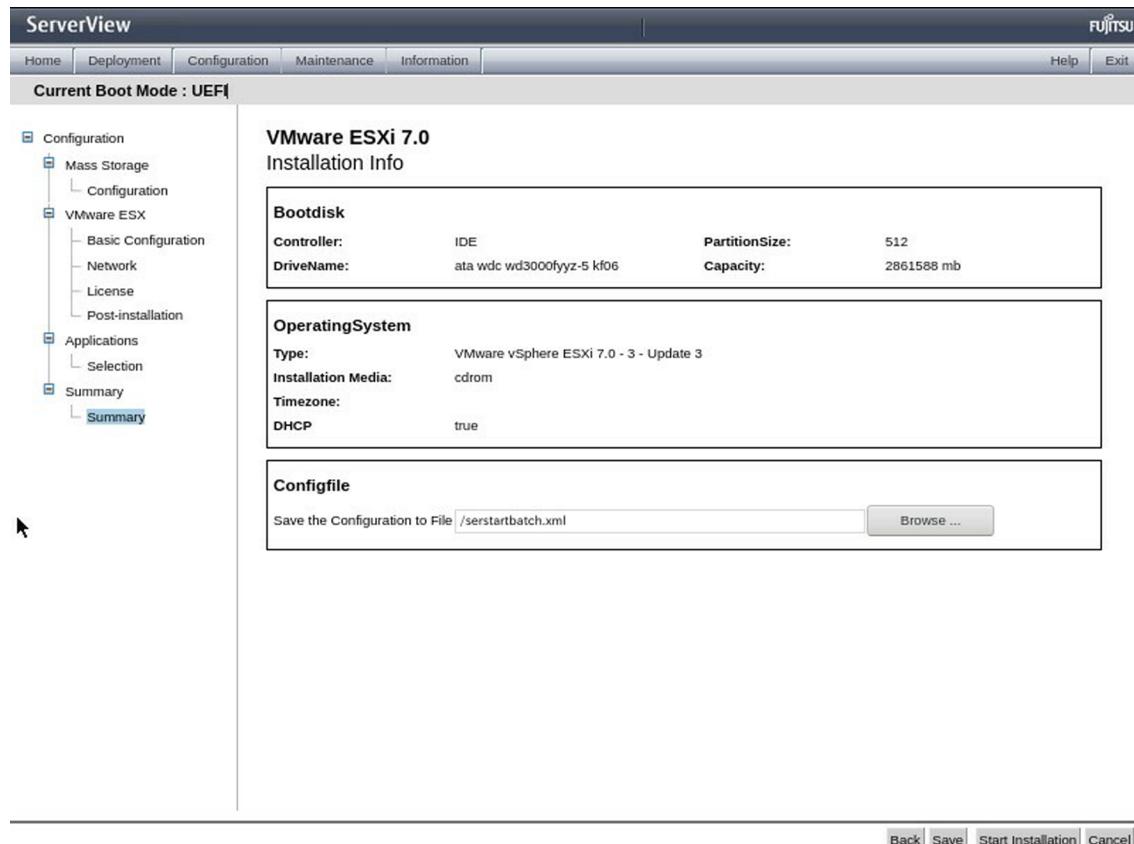


Figure 54: Installation Manager - Installation Info page

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 the ServerView Suite DVD 1 from the DVD-ROM drive at the remote workstation.
6. Insert the Linux installation CD/DVD into this drive.



Close the application if autostart is active.

- 
7. Connect the CD-ROM/DVD-ROM drive containing the Windows installation CD/DVD as a 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.  
When the copy operation is complete, the Installation Manager opens a confirmation dialog box and prompts you to remove all the storage media from the removable media drives before the managed server is rebooted.
  9. Clear all current virtual media connections again.
  10. In the confirmation dialog box, click **OK** to reboot the managed server.

Once the managed server has rebooted, you can monitor the entire installation by means of the AVR.

---

## 7 Firmware update

The iRMC S6 uses two separate banks in flash memory. Each bank has a capacity of 46 MB and can contain a firmware image. The firmware images in the banks can differ. The iRMC SPI ROM has three regions: a Low region, a High region, and a Recovery region.

The images stored in these regions are called Low Image, High Image, and Golden 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 see (["Firmware selector" on page 126](#)).

The firmware of the iRMC is not executed in the EEPROM, but is loaded into SRAM memory on startup instead 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.

When the iRMC is started, the region where the iRMC reads the image is called an active region, and the region where the iRMC F/W does not read the image is called the inactive region.

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

Besides the possibility of performing a firmware update, you can also downgrade the firmware to the previous version. This feature is not supported in the Japanese 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).

---

## 7.1 Firmware selector

The firmware selector specifies the iRMC S6 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 in the first bank of the flash memory
- 2 Firmware image in the second bank of the flash memory
- 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 set the firmware selector explicitly:

- Query via the **System Overview** page of the iRMC web interface in the **Running iRMC Firmware** group (for more information, refer to the "iRMC S6 - Web Interface" user guide)
- Set via the **iRMC Update** group on the **Update** page of the **Tools** menu.

## 7.2 Golden image

Prior to the firmware update the image file to be used is checked:

- The image file is verified to prevent an unauthorized image from being used.
- It is checked if the image file has been tampered with.

If the result of the check shows that the image file is not the original one any longer or is damaged during flashing it is automatically recovered by using a golden image. This golden image overwrites the tampered or broken firmware image.

During the recovery process of the iRMC firmware image do not power-off/on the iRMC. The power-on LED blinks white during firmware recovery. The detection of a tampered firmware image and its recovery are logged to the system event log (SEL). The iRMC settings of the firmware remain.

You can configure and update a golden image using the web interface or the Redfish API of the iRMC.

The screenshot shows the 'iRMC Update' interface. At the top, there's a table listing two firmware images:

Firmware Image	Status	Firmware Version	Booter Version	SDRR Version	SDRR ID	Firmware Date	Description
Low firmware image	Active	1.00P	1.19	3.83	0516	2020-08-18 11:58:15	PRODUCTION RELEASE
High firmware image	Inactive	1.00i	1.19	3.83	0516	2020-06-09 11:24:19	PRODUCTION RELEASE

Below the table, there are several configuration fields:

- Update Source:** A dropdown menu set to "Image file".
- Image to Flash:** A dropdown menu set to "Low firmware image".
- Boot From:** A dropdown menu set to "Low firmware image".
- Image File:** A "Select..." button.
- (i) Don't leave this page until file is uploaded
- (i) Allowed file extensions: bin, bin\_enc, ima, ima\_enc
- Golden Image Update:** A "Perform" button.

At the bottom right are two buttons: "Start Update" and "Reboot iRMC".

Figure 55: Golden image for firmware image recovery within the web interface

The Golden Image is adjusted to the same firmware version as the Active Image.

You should update the golden image along with the active image when there are security fixes of the firmware, such as iRMC fixes for iRMC vulnerabilities.

## 7.3 Methods of firmware update

Several methods are available for updating the iRMC firmware.

The following methods can be performed while the server's (host) operating system is running. These are the so-called online firmware updates. The firmware update will not harm the operation system:

- Update using iRMC web interface
- Update using ServerView Update Manager Express or ASP

The following methods can also be run without a running server's operating system. These are the so-called offline firmware updates:

- Update using iRMC web interface
- Update using ServerView Update Manager Express or ASP
- Update using an USB stick

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

### 7.3.1 Firmware Update using the web interface

This update can be executed in online or offline mode of the server operating system (OS).

The **Update** page of the **Tools** menu 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 S6 - Web Interface" user guide)

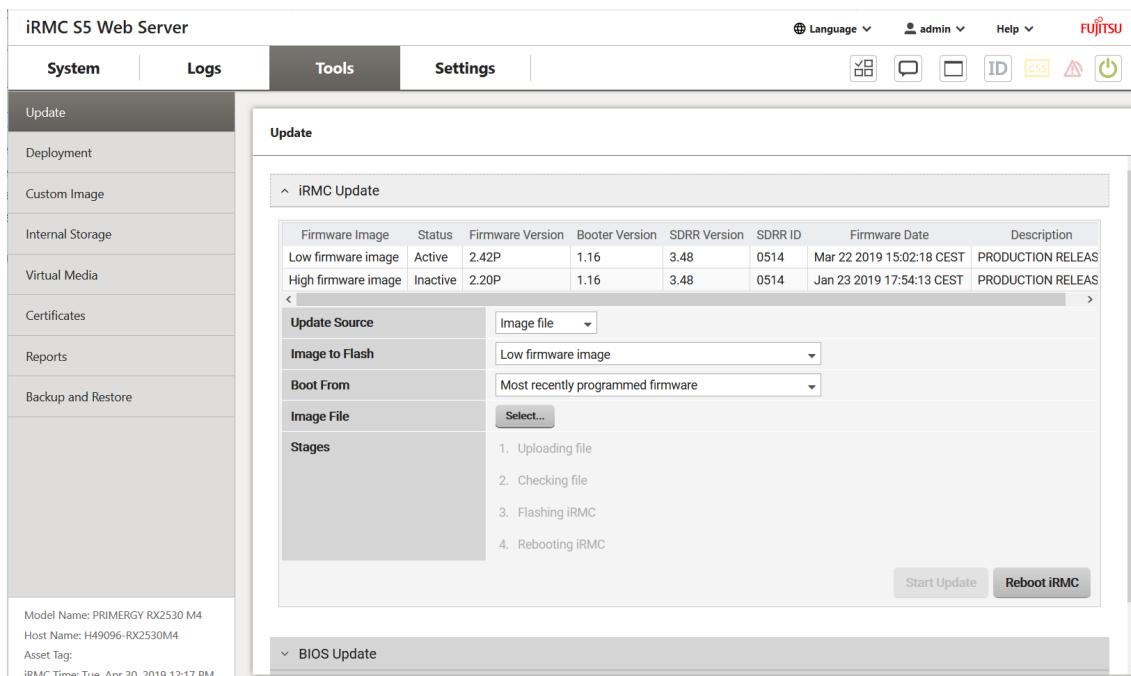


Figure 56: **Update** page

### 7.3.2 Firmware update using ServerView Update Manager Express

This update can be executed in online or offline mode of the server OS.

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

### 7.3.3 Firmware update using a USB stick

This update can be run only when the server OS is down. This update requires the preparation of a USB stick.

#### 7.3.3.1 Preparing the USB stick

You can prepare the USB stick at any time. You need a Windows<sup>©</sup> system that allows decrypted writing to USB sticks.

1. Download the firmware **Firmware Update for USB Stick** from the [Download section of the Fujitsu web server](#) to a directory on your computer.

You can search for the serial number (see identification plate) or for the name of your PRIMERGY system. The search will provide the needed <system> iRMC (Kronos6) Firmware Update for USB Stick product in the Driver – Flash - Firmware section . For example: RX1330 M4 / D3675 iRMC (Kronos6) Firmware Update for USB Stick.

Title	Version (Build/Date)	Size	Language
RX1330 M4 / D3675 iRMC (Kronos5) Firmware Update for TFTP Flash	RX1330M4_02.42P_sdr03.17 (26/03/2019)	46 MB	English
RX1330 M4 / D3675 iRMC (Kronos5) Firmware Update for USB Stick	RX1330M4_02.42P_sdr03.17 (26/03/2019)	747.1 MB	English

After accepting the license, the related ZIP archive is copied to your download directory.

The ZIP archive contains everything necessary to prepare a USB stick.

### 2. Extract the ZIP archive.

After you have extracted the downloaded ZIP archive, will find a Windows<sup>©</sup> executable named `iRMC_<system>_<firmware release>_<SDR release>.exe` (Example: `iRMC_RX1330M4_02.42P_sdr03.17.exe`). This file is a self-extracting archive that allows the writing of both the firmware and the Flashtools to an USB stick.

The created USB stick will be bootable, so that it can be used to boot your PRIMERGY system and to update the iRMC Firmware.

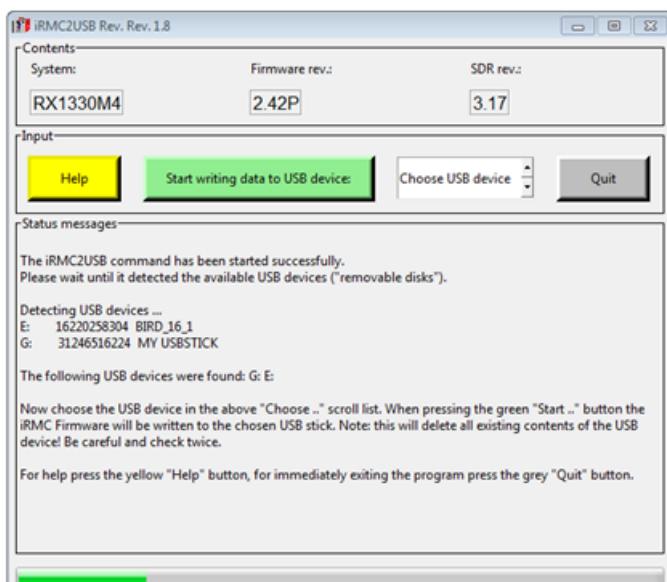
### 3. Connect a USB stick to your computer.



Some of the USB sticks available on the market may not work as boot media. Fujitsu suggests to use certified Fujitsu USB devices in order to support the full functionality.

### 4. Double-click the `iRMC_<system>_<firmware release>_<SDR release>.exe` file.

The contents of the file are extracted and the iRMC2USB program opens.



### 5. Select your USB stick from the list.

### 6. Click **Start writing data to USB device**.

The program writes the iRMC firmware and the flash tools to the USB stick. The Status messages area displays all relevant messages about the progress.

### 7. When the USB stick has been written without errors, click **Quit** to end the program.

### 8. Safely remove the USB stick from your system.

You can now use this USB stick to boot the managed server in UEFI and legacy environments.

 Do not change the name of the just created USB stick.

### 7.3.3.2 Flashtools menu

The **Flashtools** menu opens when the server is booted successfully via the prepared USB stick.

To select a command, enter the related number or navigate with the arrow keys of your keyboard and press [Enter].

Below the menu, the version of firmware intended for the iRMC update is displayed.

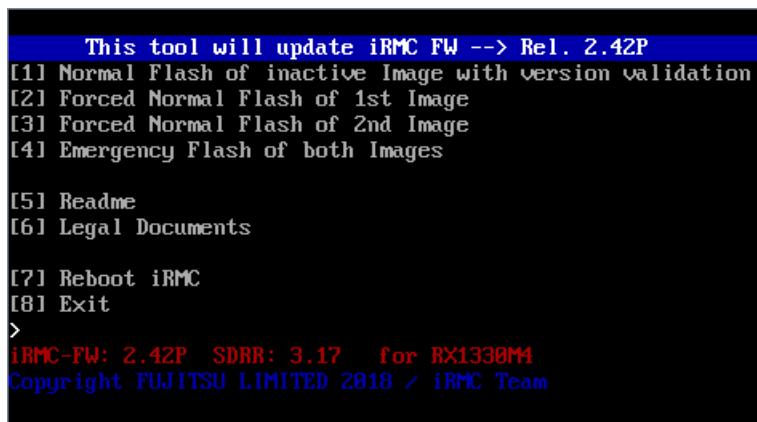


Figure 57: Flashtools menu

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

#### Normal Flash of inactive Image with version validation

Performs a normal flash of the inactive memory image.

The flash operation uses the high speed data transfer interface when the iRMC is in normal mode. The flash operation is only performed if the provided firmware version is higher than the one that is already stored in the iRMC inactive image.

#### Forced Normal Flash of 1st Image

Performs a normal flash for firmware image 1 (firmware image in the first bank of the flash memory).

The flash operation uses the high speed data transfer interface when the iRMC is in normal mode. The flash is performed for all three areas of firmware image 1 without any version check.

#### Forced Normal Flash of 2nd Image

Performs a normal flash for firmware image 2 (firmware image in the second bank of the flash memory).

The flash operation uses the high speed data transfer interface when the iRMC is in normal mode. The flash is performed for all three areas of firmware image 2 without any version check.

### **Emergency Flash of both Images**

Flashes both the first and the second image if the iRMC is in emergency mode.

The flash operation uses the low speed data transfer interface when the iRMC is in emergency mode. The emergency flash can also be used in normal mode but due to low speed type of interface it is recommended for emergency mode only. In iRMC normal mode only the inactive memory image will be upgraded with provided firmware.

### **Readme**

Displays the Readme file with the important information about firmware image and additional information about the Flashtools. Details about the Flashtools are available in the `FlashtoolsManual.txt` file in file system of the dedicated Linux system.

### **Legal Documents**

Displays a sub menu with links to following legal documents:

- General usage of the software
- Flashtools with relevant dependencies and resources (ThirdPartyLicenses)
- Host operation system with dependencies

### **Reboot iRMC**

Reboots iRMC if it is not restarted automatically once flashing is completed. The automatic iRMC restart can be suspended when the host operation system is running.

If AVR is active the iRMC reboot will cause the AVR screen to be closed and be available again only when the reboot cycle is completed.

### **Exit**

Closes the Flashtools menu and displays the command line interface of the Linux system.

### **7.3.3.3 Restarting the Flashtools menu**

You can restart the Flashtools menu with the `systemd unit flashtool-if`, included in the dedicated Linux system on the USB stick. The unit starts the Flashtools menu only on terminal TTY2.

### **Usage**

```
systemctl status flashtool-if  
systemctl start flashtool-if  
systemctl restart flashtool-if
```

For more information on the `systemctl` command, refer to the associated man page on the Linux system.

## 7.4 Firmware downgrade

Besides the possibility of performing a firmware update, you can also downgrade the firmware to the previous version. This feature is not supported in the Japanese version.

The easiest 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 126) and restart the iRMC thereafter to activate the firmware.



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, note:

- Downgrade via Update Manager Express:

The firmware downgrade is only feasible in 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 either option `-f` or option `--force`.

## 7.5 Firmware alignment

The firmware version alignment is necessary in the case of the replacement of the mainboard. The alignment automatically restores the firmware of the iRMC or the BIOS to the operating version before the replacement. For the automatic alignment a SD card mounted on the mainboard is necessary.

The image of the running BIOS and iRMC is stored (backup) on the SD card mounted on the mainboard. After the mainboard exchange, the image is read out from the SD card and written back (restore) to the SPI ROM of the BIOS/iRMC.

The iRMC detects the replacement of the mainboard by comparing the serial numbers stored in the following locations:

- FRU ROM on the mainboard
- ROM of the Operator Panel (OPL) at power-on

Different serial numbers indicate that the mainboard has been replaced. In this case the serial number stored in the OPL is updated to the number of the new mainboard and then the firmware version alignment is started automatically.

If the power is switched off after the mainboard is replaced and before the automatic firmware version alignment is completed, the firmware version alignment fails. The firmware version alignment will not be performed again automatically even if the power is switched on again. At the second power-on, the serial numbers are equal thus indicating, that the mainboard has not been replaced.

### Manual alignment

You can start the firmware version alignment manually using the iRMC web interface or the Redfish API to restore the information stored on the SD card to the SPI ROM.

Log on as an administrator to the iRMC web interface and proceed as follows:

1. Open the **Update** page of the **Tools** menu.
2. Open the **iRMC Update** group.
3. Select **Memory Card** from the **Update Source** list.
4. Click **Start Update**.

The iRMC firmware update from the SD card is started.

Both low and high side of iRMC are updated to the state before the mainboard replacement.

5. Open the **BIOS Update** group.
6. Select **Memory Card** from the **Update Source** list.
7. Click **Perform Active Image Recovery**.

During a restore, the following functions are suppressed:

- Manual automatic version matching in both the iRMC web interface and Redfish API
- System power-on

The manual version matching can be performed even if the system is powered-on.

## 7.6 Firmware backup

A firmware backup on the SD card becomes necessary in the case the SD card was exchanged or formatted. This causes the firmware image stored on the SD card to be lost.

Therefore, when these operations are performed, the BIOS/iRMC firmware image is automatically backed up to the SD card.

The effects of combined SD card replacement/format, BIOS Update, and a mainboard replacement are summarized in the following table.

If the SD card is replaced/formatted after a BIOS update and before the new BIOS image is stored in the iRMC, the BIOS image backup data will be completely lost.

If you replace/format the SD card and then replace the mainboard before the BIOS image is updated to the SD card, the BIOS firmware version count will fail.

Combined operation			Result	Problem	Measure
1st operation	Timing of 2nd operation	2nd operation			
BIOS update	Before transfer to iRMC is completed	SD card exchange or format	No SEL message indicating "Both the SD card and OS storage lost the BIOS image" when the server is switched on after SD card replacement.	Firmware restore failed after mainboard exchange	BIOS backup
SD card exchange	Before transfer to SD card completed	BIOS update	The new BIOS firmware version is on the SD card after the BIOS update. The new BIOS is stored on the iRMC at power-on.	No	
BIOS update	During transfer to iRMC	Shutdown	Transfer of BIOS image to iRMC at next boot.	No	
SD card exchange	During transfer to SD card	Shutdown	Transfer of BIOS image to SD card at next boot.	No	
BIOS update	Before transfer to SD card is completed	Mainboard exchange	After mainboard replacement the BIOS is updated to the version before the replacement. The updated BIOS image is stored in the iRMC at the next power-on.	No	
SD card exchange	Before transfer to iRMC is completed	Mainboard exchange	An error message is output to SEL indicating that there is no image on the SD card after the replacement of the mainboard.	Yes	BIOS update

---

## 8 RAID configuration

RAID (Redundant Array of Independent Disks) is a data storage virtualization technology that combines multiple physical disks into one or more logical drives for the purposes of data redundancy, performance improvement, or both. Data is distributed across the drives in one of several ways, referred to as RAID levels, depending on the required level of redundancy and performance.

There are different RAID schemes to spread or replicate data across different member disks. Each of the configurations provides a unique balance between capacity, performance, and resilience. Generally, the three main concepts are striping, mirroring, and parity. Each of these concepts has its merits and limitations, but can be combined for better performance.

Striping spreads the data evenly across multiple physical disks, mirroring replicates data on two or more disks, while parity uses raw data to calculate and store parity information for error correction. By writing or accessing information simultaneously in striping, the RAID improves performance while mirroring allows the data to be accessed from remaining good drives in case of a disk failure.

The iRMC supports creation and maintenance of various types of RAID arrays bound to controllers installed at the managed server. Maintenance in this context means:

- Configuring the integrity checks for a RAID controller
- Maintaining physical disks related to this RAID controller
- Creating and maintaining logical drives running on these physical disks

## 8.1 Supported RAID levels

The RAID level describes how data is distributed over the various disks of a logical drive. For simplicity's sake the different RAID types all use complete disk drives of the same size. In fact the usable capacity of each drive is limited by the disk drive with the lowest capacity if drives with different capacities are used.

RAID level	Technique	Minimum disks	Data security	Rebuild after disk failure	Rebuild after two disk failure
RAID 0	Striping	2	None	No	No
RAID 1	Mirroring	2	Disk failure	Copy mirrored disk	No
RAID 1E	Striping and mirroring	3	Disk failure	Calculation of the original content using XOR	No
RAID 5	Block-level striping with distributed parity	3	Disk failure	Calculation of the original content using XOR	NO
RAID 6	Block-level striping with double distributed parity	4	Two Disk failure	Calculation of the original content of the disk	Calculation of the original content of the disk
RAID 10	Stripe of mirrors	4	Disk failure per sub-array	Copy mirrored disk	Only if two disks of different mirrors are affected: then copy mirrored disk
RAID 50	Stripe of dedicated parity	6	Disk failure	Calculation of the original content using XOR	Only if two disks of different mirrors are affected: then copy mirrored disk
RAID 60	Stripe of distributed double parity	8	Disk failure	Calculation of the original content of the disk	Only if two disks of different mirrors are affected: then copy mirrored disk

## 8.2 Integrity Checks

Integrity checks and actions can be performed on the RAID controller, its related physical disks and the logical drives.

### Background initialization (BGI)

Background initialization is a consistency check that is forced when you create a logical drive. This is an automatic operation that starts within a specified time after you create the logical drive.

Background initialization is a check for media errors on the disks. The initialization ensures that striped data segments are the same on all disks in a disk group. The default and recommended background initialization rate is 30 percent. Before you change the rebuild rate, you must stop the background initialization or the rate change will not affect the background initialization rate.

### Consistency check (MDC)

The consistency check operation verifies correctness of the data in logical drives that use RAID levels 1, 5, 6, 10, 50, and 60. (RAID-0 does not provide data redundancy). For example, in a system with parity, checking consistency means computing the data on one disk and comparing the results to the contents of the parity disk.

Make data consistent (MDC) does not only verify the correctness of data but also attempts to correct inconsistent data automatically.

### Copyback

Copyback allows you to copy data from a source disk of a logical drive to a destination disk that is not a part of the logical drive. Copyback is often used to create or restore a specific physical configuration for an array (for example, a specific arrangement of array members on the device I/O buses). Copyback can be run automatically or manually.

Typically, when a disk fails or is expected to fail, the data is rebuilt on a hot spare. The failed disk is replaced with a new disk. Then the data is copied from the hot spare to the new disk, and the hot spare reverts from a rebuild disk to its original hot spare status. The copyback operation runs as a background activity, and the logical drive is still available online to the host.

Copyback is also initiated when the first Self-Monitoring Analysis and Reporting Technology (SMART) error occurs on a disk that is part of a logical drive. The destination disk is a hot spare that qualifies as a rebuild disk. The disk with the SMART error is marked as failed only after the successful completion of the copyback. This avoids putting the array in degraded status.

.

### Patrol Read

Patrol read involves the review of your system for possible disk errors that could lead to disk failure and then action to correct errors. The goal is to protect data integrity by detecting disk failure before the failure can damage data. The corrective actions depend on the array configuration and the type of errors.

Patrol read starts only when the controller is idle for a defined period of time and no other background tasks are active, though it can continue to run during heavy I/O processes.

Some of the checks need more time to be executed and can therefore be scheduled to a time period not so busy.

## 8.3 RAID controller

The installed RAID controllers of the managed server, also called storage controllers, are displayed in the **Mass Storage** page of the web interface.

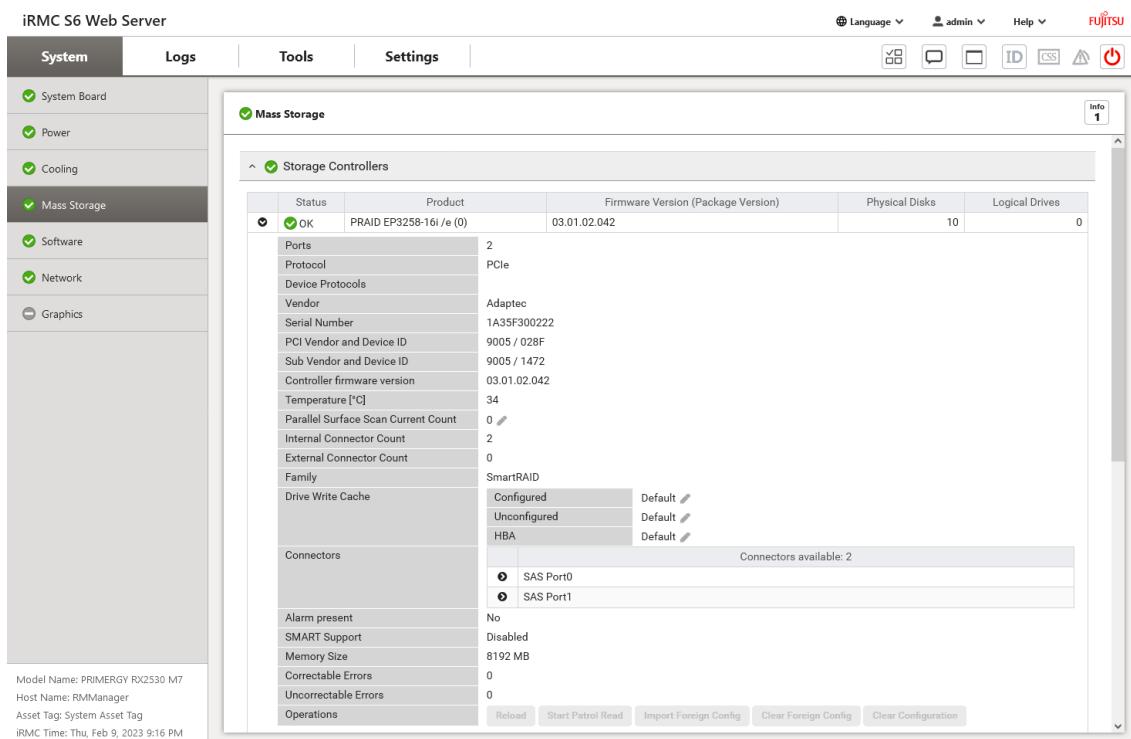
Status	Product	Firmware Version (Package Version)	Physical Disks	Logical Drives
<span>OK</span>	PRAID EP400i (1)	4.680.00-8417 (24.21.0-0076)	16	4
<span>OK</span>	Windows Advanced Host Controller Interface (0)		1	0
<span>OK</span>	PSAS CP400e (2)	16.00.00.00	0	0

Figure 58: **Mass Storage** page

A RAID controller is a physical device that is either integrated on the mainboard, or available as an add-on PCI or PCIe extension card. The controller runs everything and has its own CPU and memory. Controllers are designed to support specific hard disk interfaces and RAID levels.

When you click  close to the controller entry in the **Storage Controller** group, a drop-down displays all items related to this controller:

- Properties
- Related tasks
- Physical disks
- Enclosures
- Logical drives



Status	Product	Firmware Version (Package Version)	Physical Disks	Logical Drives
OK	PRAID EP3258-16i/e(0)	03.01.02.042	10	0
Ports	2			
Protocol	PCIe			
Device Protocol				
Vendor	Adaptec			
Serial Number	1A35F300222			
PCI Vendor and Device ID	9005 / 028F			
Sub Vendor and Device ID	9005 / 1472			
Controller firmware version	03.01.02.042			
Temperature [C]	34			
Parallel Surface Scan Current Count	0			
Internal Connector Count	2			
External Connector Count	0			
Family	SmartRAID			
Drive Write Cache	Configured  Default			
	Unconfigured  Default			
	HBA  Default			
Connectors	Connectors available: 2			
	SAS Port0			
	SAS Port1			
Alarm present	No			
SMART Support	Disabled			
Memory Size	8192 MB			
Correctable Errors	0			
Uncorrectable Errors	0			
Operations	<input type="button" value="Reload"/> <input type="button" value="Start Patrol Read"/> <input type="button" value="Import Foreign Config"/> <input type="button" value="Clear Foreign Config"/> <input type="button" value="Clear Configuration"/>			

Model Name: PRIMERGY RX2530 M7  
Host Name: RMManager  
Asset Tag: System Asset Tag  
iRMC Time: Thu, Feb 9, 2023 9:16 PM

Figure 59: Storage controller drop-down

All properties marked with  can be edited. When you click the  a little dialog box opens presenting the relevant parameters and their values.

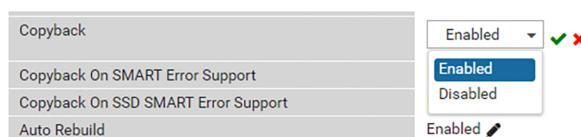


Figure 60: Edit dialog box

Some hardware controllers have an additional cache to avoid data loss in case of a power outage as well as increase the read and write operations.

### 8.3.1 Physical disks

Below the properties of a storage controller the physical disks the RAID controller manages are displayed in a table in the **Physical Disks** group.

Physical Disks									
	Status	Enclosure Number	Slot	Device Number	Interface Type	Type	Product	Physical Size [GB]	ID LED
●	Operational		0	1	SATA	HDD	ST1000NX0423	931.51	ID
●	Operational		1	3	SATA	SSD	5100 MTFDDAK240TCB	223.57	ID
●	Operational		2	2	SATA	SSD	5100 MTFDDAK240TCB	223.57	ID
●	Operational		3	0	SATA	SSD	5100 MTFDDAK240TCB	223.57	ID
●	Operational		4	7	SATA	HDD	ST1000NX0423	931.51	ID
●	Operational		5	6	SATA	SSD	5100 MTFDDAK240TCB	223.57	ID
●	Available		6	5	SATA	SSD	5100 MTFDDAK240TCB	223.57	ID
●	Operational		7	4	SATA	SSD	5100 MTFDDAK240TCB	223.57	ID

Figure 61: **Physical Disks** group

The columns of the table summarize the main properties of a physical disk. The **Status** column displays the current status of the disk:

Status	Meaning
Available	The disk is not part of a logical drive but ready.
Operational	The disk is part of a logical drive and working.
Global Hotspare	The disk is configured as a global hot spare to prevent general data loss.
Dedicated Hotspare	The disk is configured as a dedicated hot spare to prevent data loss of an individual logical drive.
Failed	The disk is broken.

When you click  close to the disk entry in the **Physical Disks** group, a drop-down displays all properties and tasks related to this disk:

**Physical Disks**

	Status	Enclosure	Port	Slot	Device Number	Interface Type	Type	Product	Physical Size [GB]	ID
①	Operational		8	0	2	SATA	SSD	5100 MTFDDAV240TCB	223.57	ID
Foreign Configuration: No Max Device Speed: 6 Gb/s Serial Number: 17431BF379C7 Firmware Version: DOMU037 Temperature [°C]: 25 Miscellaneous errors: 0 S.M.A.R.T. Errors: 0 Media Errors: 0 Predicted Life Left: 100% Estimated Life Time: 2025-01-21 SAS Address: 300605B00E78AEA9 Power Status: Activated Transfer Width: 1 bits Configurable Size: 239511535616 B VROC Usage: Not supported Operations: <b>Make Offline</b> , Start Rebuild, Start Copyback, Create Hot Spare, Replace Missing Disk, Clear										
②	Operational		9	1	3	SATA	SSD	5100 MTFDDAV240TCB	223.57	ID
③	Operational		12	4	1	SATA	HDD	HUS722T1TALA604	931.51	ID
④	Available		13	5	0	SATA	HDD	HUS722T1TALA604	931.51	ID
⑤	Operational		10	6	5	SAS	HDD	ST300MM0048	279.46	ID

Figure 62: **Physical Disks** drop-down

The tasks related to a physical disk revolve around resilience (Copyback and Rebuild) and preventing data loss.

When the controller detects that the RAID configuration is inconsistent or not synchronized with the rest of the array, it is marked as Foreign. This could happen when the drive was moved to another machine, but it also could happen when the drive went offline. The drive could go offline when a failure occurs, when a failure is happening right now, or when an unexpected situation occurs in the firmware.

The Self-Monitoring and Reporting Technology (SMART) feature monitors certain physical aspects of all motors, heads, and physical disk electronics to help detect predictable physical disk failures. Data on SMART compliant physical disks can be monitored to identify changes in values and determine whether the values are within threshold limits.

A hot spare is a physical disk which is available in a redundant logical drive as a replacement for a failed disk. If a drive fails the hot spare replaces it and the logical drive is recreated. The data is then reconstructed on this new disk during ongoing operation. Until reconstruction has been completed the access to the data takes a little longer but is possible at any time.

You can configure a global hot spare, that can be used by all logical drives or a dedicated hot spare, which is assigned to only one logical drive.

### 8.3.2 Logical drives

Below the properties of a storage controller and its related physical disks the logical drives are displayed in the **Logical Drives** group.

Logical Drives						
	Status	Drive	Name	Logical Size [GB]	RAID Type	ID LED
0	Operational	0	LogicalDrive_0	931	RAID-1	ID
1	Operational	1	LogicalDrive_1	223.06	RAID-1	ID
2	Operational	2	LogicalDrive_2	223.06	RAID-0	ID
3	Operational	3	drive3	446.13	RAID-0	ID

Figure 63: **Logical Drives** group

The columns of the table summarize the main properties of a logical drive. The **Status** column displays the current status of the drive:

Status	Meaning
Operational	The logical drive is working.
Degraded	The physical disk has failed.
Failed	The logical drive is broken and cannot be accessed.

When you click  close to the disk entry in the **Logical Drives** group, a drop-down displays all properties and tasks related to this disk:

**Logical Drives**

	Status	Drive	Name	Logical Size [GB]	RAID Type	ID LED
LogicalDrive_0	Operational	0	LogicalDrive_0	223.06	RAID-0	ID
Stripe Size	64 KB					
Access Mode	Read write					
Emulation Type	Default					
Read Mode	No read-ahead					
Write Mode	Write-through					
Disk Cache Mode	Unchanged					
Preserved Cache	No					
Initialized	Yes					
Operations						

**Schedules**

	Schedule Type	Action
No records found		

**Create Schedule**

**Physical Disks**

Status	Slot	Interface Type	Type	Vendor	Product	Physical Size [GB]	ID LED
Operational	1	SATA	SSD	MICRON	5100 MTFDDAV240TCB	223.57	ID
LogicalDrive_1	1	LogicalDrive_1				223.06	RAID-0

Figure 64: **Logical Drives** drop-down

The tasks related to a logical drive revolve around consistency checks (BGI and MDC) and resilience. In the case of critical logical drives of the type RAID-1, RAID-5 or RAID-10 you can start rebuilding the logical drive. Generally the failed disk is automatically replaced by a hot spare and a rebuild is subsequently started automatically provided this is set on the controller. The action runs in the background, and as long as no further disk fails it is still possible to work with the logical drive.

With the iRMC web interface you can create a logical drive, even bundle the necessary disks to a disk group. If necessary you can migrate a logical drive to another RAID level and edit the volume of physical disks for this purpose.

You can migrate an existing and running logical drive to another RAID level and expand its capacity online if there is free storage space on all disks of an array. Afterwards existing file systems can be adapted to the new capacity with operating system tools.

## 8.4 Creating a logical drive

Before creating a logical drive, you must decide which RAID level to use, what parameters the chosen RAID level requires and what (physical and/or logical) drives this logical drive should consist of. It is assumed here that you are familiar with the concepts of RAID and the various RAID levels.

1. In the web interface of the iRMC open the **Mass Storage** page in the **System** menu.
2. In the **Storage Controllers** group expand the details drop-down of the operational controller that should manage the logical drive.

All information of the controller is displayed.
3. Below the **Physical Disks** table click **Create Logical Drive**.

The **Create Logical Drive** dialog box opens.
4. On the **Settings** tab fill-in the relevant parameters.

In this tab you set the RAID level and access modes.
5. Open the **Layout** tab.

On this tab you select the physical drives to be used as a logical drive. If no disk group exists you have to create one.
6. If all necessary options are set click **OK** to confirm your settings.

Your options are checked and if everything is plausible the logical drive is created.
7. You can edit all the settings at any time.

## 8.5 Deleting a logical drive

1. In the web interface of the iRMC open the **Mass Storage** page in the **System** menu.
2. In the **Storage Controllers** group expand the details drop-down of the operational controller that should manage the logical drive.

All information of the controller is displayed.
3. In the **Logical Drives** table expand the logical drive to be deleted.
4. Click **Delete Logical Drive** below the table.

The logical drive is deleted.