



Cisco C880 M5 User Interface Guide

December 2017

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706 USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2017 Cisco Systems, Inc. All rights reserved.

Contents

1	Welcome	7
1.1	Purpose and target groups.....	7
1.2	Introduction of Cisco C880 M5.....	7
1.3	Documentation overview	8
1.4	Overview of the iRMC functions.....	9
1.4.1	Standard functions	9
1.5	Notational conventions	14
1.6	Required user permissions	15
1.7	Display requirements.....	20
2	Main Window.....	21
2.1	System menu.....	26
2.1.1	System Overview.....	28
2.1.1.1	System Information.....	28
2.1.1.2	Operating System Information.....	29
2.1.1.3	Systemboard Information.....	29
2.1.1.4	Power Status Summary.....	29
2.1.1.5	Running iRMC Firmware.....	29
2.1.1.6	Active Session Information	29
2.1.1.7	Installed License Keys.....	29
2.1.2	Systemboard	30
2.1.2.1	Processors.....	30
2.1.2.2	Memory Modules	30
2.1.2.3	Operating Voltages	30
2.1.2.4	PCI Slots.....	30
2.1.2.5	Trusted Platform Module (TPM)	30
2.1.2.6	Power On Self Test (POST).....	30
2.1.3	Power	31
2.1.3.1	Power Supplies	31
2.1.3.2	Power Supply Redundancy and Configuration	31
2.1.3.3	Power Consumption	31
2.1.4	Cooling.....	32
2.1.4.1	Cooling Devices	32
2.1.4.2	Temperature Sensors.....	32
2.1.5	Mass Storage	33
2.1.5.1	RAID Controllers.....	33
2.1.5.2	Directly Connected Devices.....	33
2.1.6	Software.....	34
2.1.6.1	Driver Monitor.....	34
2.1.6.2	System Management Software	34
2.1.7	Network.....	35
2.1.7.1	Ethernet Ports	35
2.1.8	AIS Connect	35
2.2	Logs menu.....	36

2.2.1	Logs Overview.....	36
2.2.1.1	System Event Log.....	37
2.2.1.2	Internal Event Log.....	37
2.2.2	System Event Log.....	38
2.2.2.1	Event Log Information	39
2.2.2.2	Event Log Content	40
2.2.3	Internal Event Log.....	41
2.2.3.1	Event Log Information	42
2.2.3.2	Event Log Content	43
2.2.3.3	Service Notice	43
2.3	Tools menu	44
2.3.1	Tools Overview.....	44
2.3.2	Update.....	45
2.3.2.1	iRMC Update.....	45
2.3.2.2	BIOS Update	47
2.3.2.3	Online Update	48
2.3.2.4	Offline Update	48
2.3.2.5	Updating the BIOS.....	49
2.3.3	Deployment.....	50
2.3.4	Custom image	50
2.3.5	Certificates.....	51
2.3.5.1	Current SSH/TLS Certificate.....	52
2.3.5.2	Current CA Certificate	52
2.3.5.3	Generate certificate dialog	53
2.3.5.4	Generating a self-signed RSA Certificate	54
2.3.5.5	Upload SSH/TLS certificate dialog	55
2.3.5.6	Loading the DSA/RSA public and private key from local files	56
2.3.5.7	Upload CA certificate dialog.....	57
2.3.5.8	Loading a CA certificate from a local file.....	58
2.3.5.9	Restoring the SSH/TLS certificate/CA certificate.....	58
2.3.6	Reports.....	59
2.3.6.1	System Report	60
2.3.6.2	System Event Log.....	61
2.3.6.3	PrimeCollect	61
2.3.7	Backup and Restore	62
2.3.7.1	Backup and Restore iRMC Configuration.....	63
2.3.7.2	Backup and Restore BIOS Configuration	64
2.4	Settings menu.....	66
2.4.1	Settings Overview	66
2.4.2	System	67
2.4.2.1	Asset Tag	67
2.4.2.2	Operating System Information.....	68
2.4.2.3	BIOS Update Settings	68
2.4.2.4	BIOS Backup Settings.....	68
2.4.2.5	Boot Options.....	69
2.4.3	Network Management.....	70
2.4.3.1	Network Interface.....	71
2.4.3.2	IPv4 Protocol.....	72
2.4.3.3	IPv6 Protocol.....	73
2.4.3.4	DNS.....	74
2.4.3.5	DNS Name Registration.....	75
2.4.3.6	Virtual LAN (VLAN).....	76


2.4.3.7	Proxy Server Configuration.....	76
2.4.3.8	Network bonding.....	77
2.4.4	Services.....	78
2.4.4.1	Web Access.....	78
2.4.4.2	Console Access.....	80
2.4.4.3	IPMI Access.....	81
2.4.4.4	Advanced Video Redirection (AVR).....	81
2.4.4.5	Update and Deployment.....	82
2.4.4.6	BIOS Console Redirection.....	83
2.4.4.7	Virtual Media.....	84
2.4.4.8	SNMP.....	86
2.4.4.9	Email Alerting.....	88
2.4.4.10	AIS Connect.....	92
2.4.4.11	Text console redirection.....	92
2.4.4.12	Starting AVR using Java.....	93
2.4.4.13	Starting AVR using HTML5.....	93
2.4.5	User Management.....	94
2.4.5.1	iRMC Local User Accounts.....	94
2.4.5.2	Lightweight Directory Access Protocol (LDAP).....	95
2.4.5.3	Central Authentication Service (CAS).....	100
2.4.5.4	iRMC user.....	103
2.4.5.5	LDAP user group.....	113
2.4.6	Server Management.....	118
2.4.6.1	Automatic System Recovery & Restart (ASR&R).....	118
2.4.6.2	Software Watchdog.....	119
2.4.6.3	Boot Watchdog.....	120
2.4.6.4	HP System Insight Manager (HP SIM) Integration.....	120
2.4.6.5	System UUID.....	121
2.4.6.6	Fan Test.....	121
2.4.6.7	Memory Operation Mode.....	121
2.4.7	Power Management.....	123
2.4.7.1	Power On/Off Scheduler.....	123
2.4.7.2	Power Consumption Control.....	123
2.4.7.3	Power Restore Policy.....	126
2.4.7.4	IPMI Fencing.....	126
2.4.8	Logging.....	127
2.4.8.1	System Event Log.....	127
2.4.8.2	Internal Event Log.....	128
2.4.8.3	Helpdesk.....	128
2.4.8.4	Syslog Server.....	128
2.4.9	Baseboard Management Controller.....	131
2.4.9.1	Time Synchronization.....	131
2.4.9.2	Firmware Update via TFTP.....	132
2.4.9.3	License Keys.....	133
2.4.9.4	User Interface.....	133
3	Advanced Video Redirection (AVR).....	134
3.1	Requirements for AVR.....	134
3.2	Parallel AVR sessions.....	136
3.3	Local Monitor Off Control function.....	138
3.4	Redirecting the keyboard.....	139
3.5	Starting AVR using Java.....	141

3.5.1	AVR window	141
3.5.2	Menus of the AVR window (Java)	142
3.5.2.1	Video menu	143
3.5.2.2	Keyboard menu	145
3.5.2.3	Mouse menu.....	149
3.5.2.4	Options menu.....	150
3.5.2.5	Media menu	150
3.5.2.6	Power menu	151
3.5.2.7	Active Users Menu	152
3.5.2.8	Help menu.....	152
3.5.3	AVR toolbar	153
3.6	Starting AVR using HTML5	155
3.6.1	HTML5 page	155
3.6.2	Menus of the AVR window (HTML5).....	157
3.6.2.1	Video menu	157
3.6.2.2	Mouse menu.....	158
3.6.2.3	Option menu.....	158
3.6.2.4	Keyboard menu	159
3.6.2.5	Send Keys menu	159
3.6.2.6	Hot Keys menu	160
3.6.2.7	Video Record menu	161
3.6.2.8	Power menu.....	162
3.6.2.9	Active Users Menu	163
3.6.2.10	Help menu.....	163
3.6.3	Status bar of the AVR window (HTML5).....	164
3.6.4	Supported Browsers	165
4	Virtual Media Wizard.....	166
4.1	Provision of virtual media on the remote workstation	166
4.2	Starting the Virtual Media wizard	167
4.3	Virtual Media dialog box.....	168
4.4	Providing storage media for virtual media	168
4.5	Clearing Virtual Media connections.....	169

1 Welcome

Welcome to the iRMC web interface. You can choose whether to show the menus and dialog boxes of the iRMC web interface in English, German, or Japanese.

When you enter values in the iRMC S5 web interface, you will often receive assistance in the form of tool tips.

-  Third Party Licenses can be seen by clicking the **Help** menu in the title bar of the iRMC web interface.

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 deals with the following aspects in detail:

- iRMC web interface
- Logging on to the iRMC
- Configuring the iRMC
- Advanced Video Redirection via iRMC
- Virtual Media via iRMC

1.2 Introduction of Cisco C880 M5

The scalable Cisco C880 M5 is an Intel-based rack server for critical company scenarios, e.g. as database management system for medium or large-sized databases or as a consolidation basis to run an immensely large number of different applications using virtualization technologies.

Thanks to its highly developed hardware and software components, the server offers a high level of data security and availability. These include hot-plug HDD/SSD modules, hot-plug system fans, and also hot-plug power supply units, Prefailure Detection and Analysis (PDA) and Automatic Server Reconfiguration and Restart (ASR&R).

Security functions in the BIOS Setup and on the System Board protect the data on the server against manipulation. Additional security is provided by the lockable rack door.

The server occupies 5 height units (HU) in the rack.

1.3 Documentation overview

More information on your CISCO C880 M5 can be found in the following documents:

- Cisco C880 M5 Installation Manual
- Cisco C880 M5 Configuration Guide
- Cisco C880 M5 Administration Guide
- Cisco C880 M5 User Interface Guide
- Cisco C880 M5 BIOS Setup Guide

Further sources of information:

- Manual for the monitor
- Documentation for the boards and drives
- Operating system documentation
- Information files in your operating system

1.4 Overview of the iRMC functions

The iRMC supports a wide range of functions that are provided by default. With Advanced Video Redirection (AVR) and Virtual Media, the iRMC also provides two additional advanced features for the remote management of C880 M5 servers.

1.4.1 Standard functions

For the standard functions no special license key is necessary.

Alert management

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

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

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

Customer Self Service (CSS)

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

DNS / DHCP

The iRMC provides support for automatic network configuration. It has a default name and DHCP support is set by default so that the iRMC gets its IP address from the DHCP server.

The iRMC name is registered by the Domain Name System (DNS). Up to five DNS servers are supported. If DNS/DHCP is not available, the iRMC also supports static IP addresses.

Global error LED

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

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 from 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.

Local user management

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

Network bonding

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

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

Power consumption control

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

Power LED

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

Power management

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

- Using the iRMC web interface
- Using the Remote Manager
- With a script

Power supply

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

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

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

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

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

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

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

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 an alphanumeric user interface for the iRMC.

Simple configuration - interactive or script-based

The following tools are available for configuring the iRMC:

- iRMC web interface
- UEFI BIOS Setup

It is also possible to perform configuration with IPMIVIEW using scripts. You can also configure a large number of servers on the basis of scripts.

SNMPv1/v2c/v3 support

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

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

Text console redirection

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

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.

Advanced Video Redirection (AVR)

The iRMC supports Advanced Video Redirection via HTML5 or Java. AVR offers the following benefits:

- Operation via a standard web browser. No additional software needs to be installed on the management station other than the Java Runtime Environment if the Java applet is used. Otherwise the web browser must be able to interpret HTML5.
- System-independent graphical and text console redirection (including mouse and keyboard).
- Remote access for boot monitoring, BIOS administration and operation of the operating system.
- AVR supports up to two simultaneous “virtual connections” for working on a server from a different location. It also reduces the load on the network by using hardware video compression.
- Local monitor-off support: It is possible to power down the local screen of the managed C880 M5 server during an AVR session in order to prevent unauthorized persons from observing user input and actions carried out on the local server screen during the AVR session.
- Low bandwidth
If the data transfer rate is slow, you can configure a lower bandwidth (bits per pixel, bpp) in terms of color depth for your current AVR session.

Virtual Media

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

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

- Read and write data
- Boot from Virtual Media
- Install drivers and small applications



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

- CD ROM
- DVD ROM
- Memory stick
- Floppy image
- CD ISO image
- DVD ISO image
- Physical hard disk drive
- HDD ISO image

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

1.5 Notational conventions

The following notational conventions are used in this manual:

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

Screenshots

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

1.6 Required user permissions

The following table provides an overview of the permissions required to use the individual functions available on the iRMC web interface.

Functions in the iRMC web interface	Required Redfish privilege level			Required iRMC-specific permission			
	Administrator	Operator	ReadOnly	Configure User Accounts	Configure iRMC Settings	Video Redirection Enabled	Remote Storage Enabled
Switch identification LED on/off.	X	X	X				
System menu							
Open Overview page.	X	X	X				
Open Systemboard page.	X	X	X				
Open Power page.	X	X	X				
Open Cooling page.	X	X	X				
Start fan test.	X						
Open Mass Storage page.	X	X	X				
Open Software page.	X	X	X				
Reset driver status.	X	X					
Open Network page.	X	X	X				
Open AIS Connect page.	X	X	X				
Logs menu							
Open Overview page.	X	X	X				
Open System Event Log page.	X	X	X				
Clear the system event log (SEL).	X						
Open Internal Event Log page.	X	X	X				
Clear the internal event log (iEL).	X						
Add Service Notice	X						
Tools menu							

Functions in the iRMC web interface	Required Redfish privilege level			Required iRMC-specific permission			
	Administrator	Operator	ReadOnly	Configure User Accounts	Configure iRMC Settings	Video Redirection Enabled	Remote Storage Enabled
Open Overview page.	X	X	X				
Open Update	X	X	X				
Start iRMC Update .	X						
Reboot iRMC	X						
Start BIOS Update .	X						
Start Check for Online Updates. ¹⁾	X	X					
Start online update. ¹⁾	X	X					
Start Prepare for Offline Updates. ¹⁾	X	X					
Start offline update. ¹⁾	X	X					
Open Deployment page. ¹⁾	X	X	X				
Update List of operating system types. ¹⁾	X						
Download Service Platform . ¹⁾	X						
Remove SVS platform image. ¹⁾	X						
Start Deployment . ¹⁾	X						
Open Custom Image	X						
Edit Custom Image settings. ¹⁾	X						
Open Certificates page.	X	X	X				
Reset to the default SSH/SSL certificate.	X						
Generate a self-signed RSA certificate.	X						
Load SSH/SSL license key onto the iRMC.	X						
Reset to the default CA certificate.	X						
Load CA license key onto the iRMC.	X						
Open Report page.	X	X	X				
Download System Report.	X	X					

1.6 Required user permissions

Functions in the iRMC web interface	Required Redfish privilege level			Required iRMC-specific permission			
	Administrator	Operator	ReadOnly	Configure User Accounts	Configure iRMC Settings	Video Redirection Enabled	Remote Storage Enabled
Download System Event Log.	X	X					
Edit PrimeCollect settings. ¹⁾	X						
Open Backup and Restore page.	X	X	X				
Backup and Restore iRMC Configuration.	X						
Backup and Restore BIOS Configuration.	X						
Settings menu							
Open Overview page.	X	X	X				
Open System page.	X	X	X				
Set Asset Tag.	X						
Set Operating System Information.	X						
Edit BIOS Update Settings .	X						
Edit BIOS Backup Settings.	X						
Edit Boot Options.	X						
Open Network Management page.	X	X	X				
Edit Network Interface.	X						
Edit IPv4/Ipv6 Protocol	X						
Edit DNS Configuration.	X						
Edit Proxy Server Configuration.	X						
Open Services page.	X	X	X				
Edit Web Access.	X						
Modify Console Access.	X						
Edit the Advanced Video Redirection settings.	X						
Edit Update and Deployment settings. ¹⁾	X						
Edit Virtual Media settings.	X						
Edit SNMP Configuration.	X						

Functions in the iRMC web interface	Required Redfish privilege level			Required iRMC-specific permission			
	Administrator	Operator	ReadOnly	Configure User Accounts	Configure iRMC Settings	Video Redirection Enabled	Remote Storage Enabled
Edit Email Alerting .	X						
Edit AIS Connect settings.	X						
Open User Management page.	X	X	X				
Edit iRMC Local User Accounts .	X						
Edit Lightweight Directory Access Protocol (LDAP) settings.	X						
Edit Central Authentication Service (CAS) .	X						
Open Server Management page.	X	X	X				
Edit Automatic System Recovery and restart (ASR&R) settings.	X						
Edit Software Watchdog settings.	X						
Edit Boot Watchdog settings.	X						
Set Fan Check Time (Fan Test group).	X						
Set Memory Operation Mode	X						
Open Power management page	X	X	X				
Edit Power On/Off Scheduler .	X						
Edit Power Consumption Control Settings.	X						
Edit Power Restore Policy .	X						
Open Logging page	X	X	X				
Change SEL mode.	X						
Change IEL mode.	X						
Change Helpdesk Information.	X						
Edit Syslog Server settings.	X						
Open Baseboard Management Controller page.	X	X	X				
Edit iRMC Time Synchronization .	X						

1.6 Required user permissions


Functions in the iRMC web interface	Required Redfish privilege level			Required iRMC-specific permission			
	Administrator	Operator	ReadOnly	Configure User Accounts	Configure iRMC Settings	Video Redirection Enabled	Remote Storage Enabled
Set User interface .	X						
1) Feature is not available.							

1.7 Display requirements

An up-to-date browser is necessary to use all functions of the web interface of the iRMC S5. The following versions and settings are supported:

- Microsoft Internet Explorer version 11 and higher
- Microsoft Edge Browser
- Google Chrome version 50 and higher versions
- Mozilla Firefox version 46 and higher
- For AVR(Java): Sun Java Virtual Machine Version 1.8 or higher.

The iRMC web interface has been optimized for the default settings of the desktop and for the browsers supported. If you have configured Internet Explorer with a large font, the display can be impaired.

-  You can use the browser's favorite function to directly address individual pages of the web interface.

2 Main Window

The main window of the web interface contains the following sections, from top to bottom:

- The title bar with the language and user menus
- The menu bar with the function menus and the global icons
- The functions area where the functions of the selected menu are displayed as links
- The working area, that displays the page of the selected function

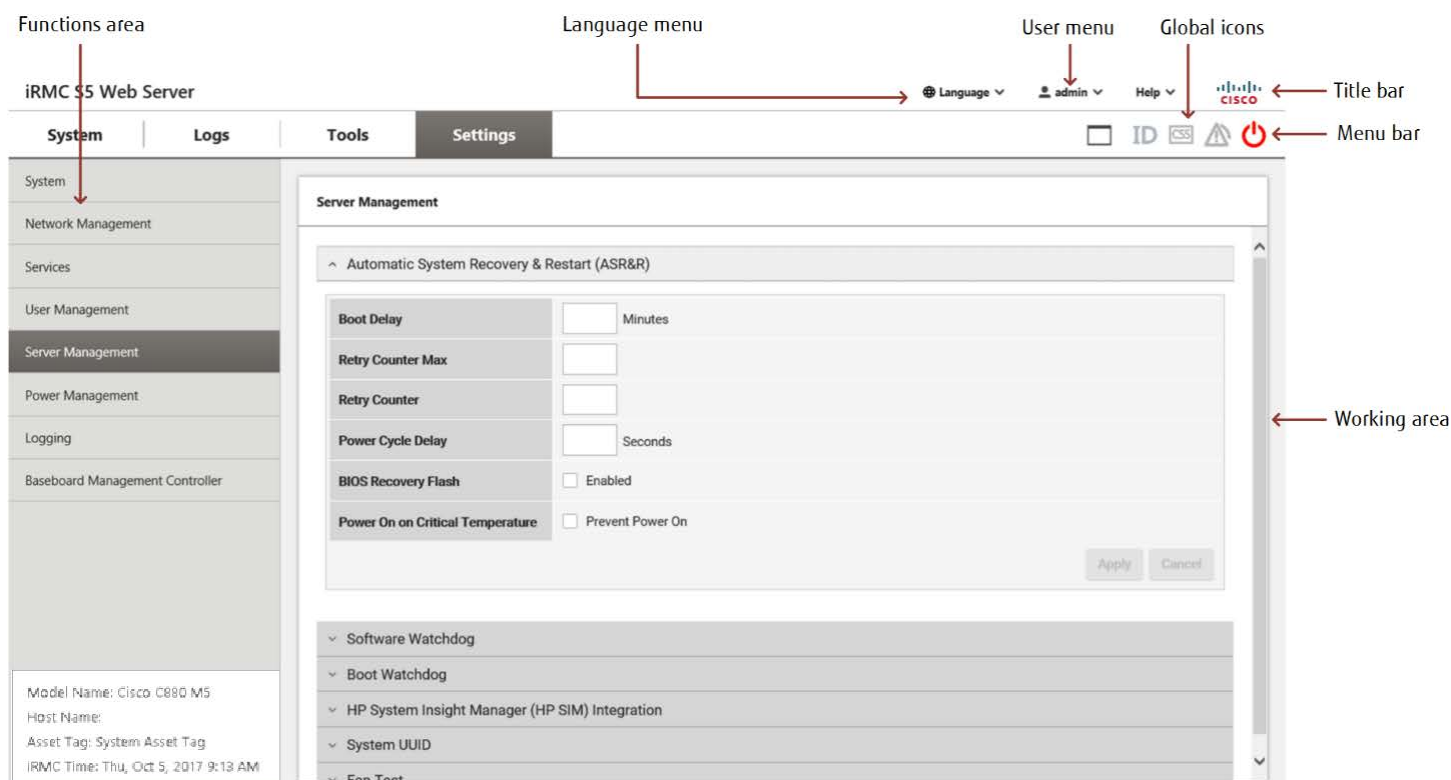


Figure 1: Structure of the main window of the iRMC web interface

Title bar






The title bar resides at the top of the main window and contains the following menus:

- **Language** menu to select the user interface language
Currently the web interface of the iRMC can be displayed in the following languages:
 - English
 - German
 - Japanese
- **<User>** menu to access user specific settings
- **Help** menu to show license and version information

Menu bar

The menu bar resides below the title bar and contains the function menus and the global icons. The selected function menu is highlighted and the functions contained are displayed in the functions area.

The global icons on the right of the menu bar have the following meaning:

Icon	Meaning
	Video Redirection: launches the Advanced Video Redirection (AVR) via the selected protocol, Java or HTML5.
	ID LED: Indicates the status of the server identifier. Switches the systems ID LED on/off. The icon is color coded, thus displaying the status of the LED: <ul style="list-style-type: none"> ▫ Gray: The LED is off. ▫ Blue: The LED is on.
	Indicates the status of the server's CSS LED: <ul style="list-style-type: none"> ▫ Off: The server is operational (no light) ▫ On: Prefailure event for a CSS component (light yellow) ▫ Alarm: Defective CSS component (blinking yellow)
	Indicates the status of the server's Global Error LED: <ul style="list-style-type: none"> ▫ Off: No critical event (no light) ▫ On: Prefailure event for a non CSS component (light red) ▫ Alarm: Critical event (blinking red)
	Power Control: Switches the managed server on and off. The icon is color coded, thus displaying the status of the server: <ul style="list-style-type: none"> ▫ Red: The server is powered off. ▫ Green: The server is powered on.

Function area

The function area resides on the left of the main window. It displays the links to the functions of the selected menu.

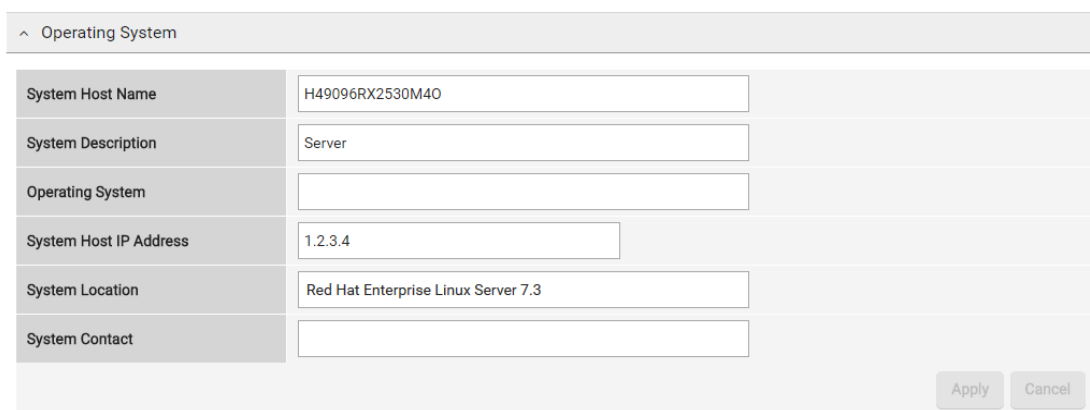
When you click one of these links, the link is enabled and the work area for that function is displayed showing any output, dialog boxes, options, links and buttons.

When you select a function menu, an **Overview** page opens. The page is always shown if a menu of the menu bar is selected.

If you select a function in the function area the **Overview** page disappears. To open the Overview page again, select the menu from the menu bar again.

Work area

In this area the page for the selected function opens. The parameters are grouped.



The screenshot shows a user interface for a function page. At the top, there is a group header 'Operating System' with a small upward-pointing triangle icon to its left. Below this header is a table of parameters, each with a label on the left and an input field on the right:

System Host Name	<input type="text" value="H49096RX2530M40"/>
System Description	<input type="text" value="Server"/>
Operating System	<input type="text"/>
System Host IP Address	<input type="text" value="1.2.3.4"/>
System Location	<input type="text" value="Red Hat Enterprise Linux Server 7.3"/>
System Contact	<input type="text"/>

At the bottom right of the form, there are two buttons: 'Apply' and 'Cancel'.

Figure 2: Group on a function page

A group consists of the following:

- ▮ Group title with an indicator and the group name
- ▮ Parameters consisting of a name and a value
- ▮ Optionally: buttons **Apply** and **Cancel**

The indicator in the group title signals the expanding status of the group:

- ^ The group is expanded.
- v The group is collapsed.

All groups are collapsed by default. You can expand each group by clicking on the group name.

* A red star close to a parameter name indicates a mandatory parameter. Unmarked parameters are optional ones.

Apply

Applies the changed settings to the related function.

Cancel

Resets the changes within the group to the previous values. No changes are made.

Logging in

All communication between the web browser and the iRMC is carried out via HTTPS.

1. Open a web browser on the remote workstation.
2. Enter the (configured) DNS name or IP address of the iRMC.
A login screen opens.
3. If no login screen appears, check the LAN connection.

i If you use Microsoft Internet Explorer, On the Tools menu of Internet Explorer, click Compatibility View Settings. Click to uncheck the **Display intranet sites in Compatibility View** check box in Compatibility View Settings dialog.

4. Type in the data for the default administrator account. User name: **admin**

Password: **admin**

Both the user name and the password are case-sensitive.

5. Click **Login** to confirm your entries.

i For reasons of security, it is recommended that you create a new administrator account once you have logged in, and then delete the default administrator account or at least change the password for it.

You can also login using the CAS service. For more information regarding CAS, refer to "[Central Authentication Service \(CAS\)](#)" on page 100.

Logging out

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

1. In the title bar open the **<User>** menu.
2. Click **Logout**.
3. Confirm that you want to log out in the dialog box.
The login screen opens again for a re-login.

Setting the language

The web interface is available in different languages:

- English
- German
- Japanese





In the title bar, you will find the **Language** menu.

1. Open the **Language** menu with a click on the arrow.
2. Select the appropriate language.
The iRMC web interface is displayed in the selected language.



2.1 System menu

The **System** menu provides information on the status of the server components and their health status.

The health status of the components is symbolized by the following icons:

	OK: Component status is okay.
	Component slot is empty.
	Warning: The status of the component has deteriorated.
	Fault: The component has a fault.

The information on the components is mostly delivered in tables. Some indicators are generally used with the following meaning:

Column	Meaning
	Opens a popup with detailed information on the related component.
	Closes the popup.
Identify LED	Indicates whether the component supports the identify LED. Clicking the ID entry activates or deactivates the Identify LED of the component.
CSS	Indicates whether the Customer Self Service (CSS) is supported for this component

Entries with Designation iRMC or BIOS

Entries with the value iRMC or BIOS in the **Designation** column indicate that the iRMC or BIOS has detected an error. It does not mean that the component itself is defective.

Entries with Designation HDD and HDD<n>, agentless HDD monitoring (out-of-band HDD monitoring)

Entries with the value HDD or HDD<n> or PCIeSSD<n> (where n = 0, 1, 2, ...) in the **Designation** column indicate the status of Hard Disk Drives (HDD):

- ▮ An entry with **Designation** HDD indicates the overall HDD status of the server by summarizing the statuses of the individual HDDs.
- ▮ An entry with **Designation** HDD<n> or PCIeSSD<n> (with n = 0, 1, 2, ...) indicates the status of an individual HDD or SSD.

Please note:

- ▮ The iRMC only supports this feature if the backplane supports it.
- ▮ This feature is deactivated if **RAID Information** is enabled.

The precise entries displayed in the tables, therefore, depend on the server state and whether the server supports "agentless HDD monitoring":

- ▮ HDD Component Status is not shown.
- ▮ **Status Prefail** is not supported for all HDDs or SSDs.
- ▮ Entries with **Designation** HDD<n> or PCIeSSD<n> (where n=0, 1, 2, ...) are only displayed if the managed server supports "agentless HDD monitoring".

2.1.1 System Overview

The **Overview** page in the **System** menu summarizes general information of the managed server.

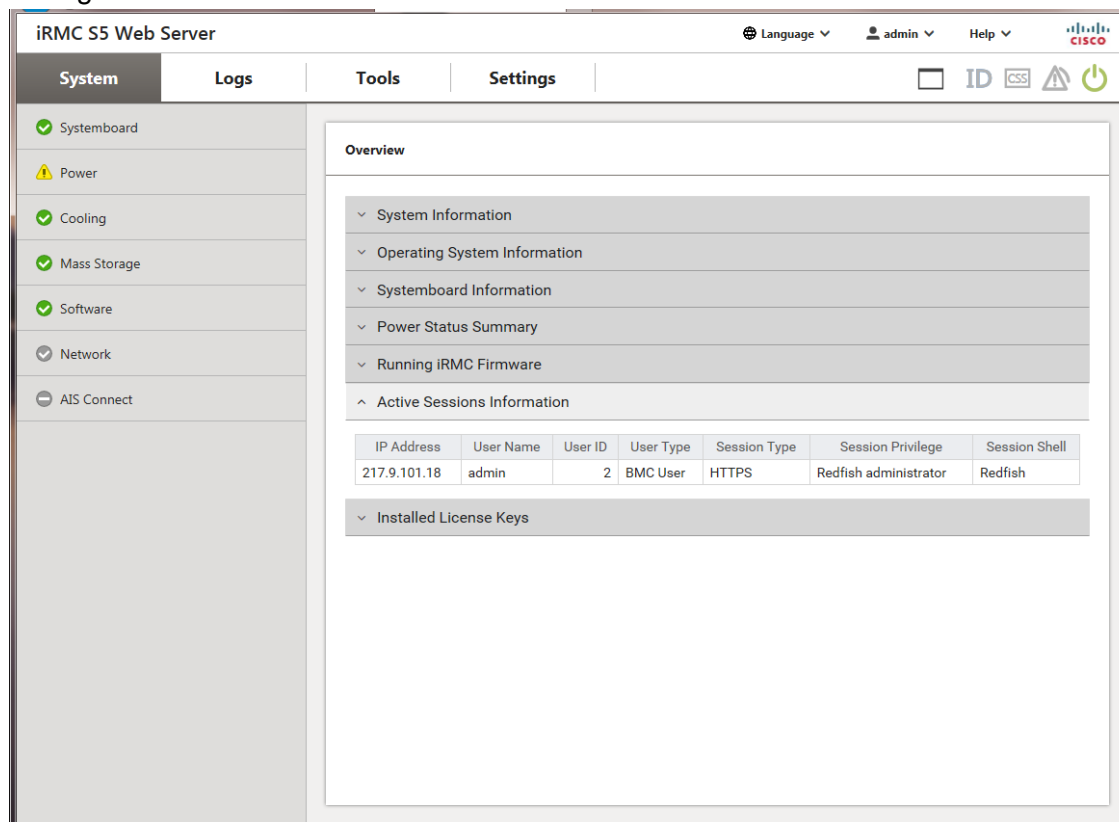


Figure 3: **Overview** page

The information is provided in several groups.

2.1.1.1 System Information

Lists general hardware information on the managed server.

Model Name

Name of the model

Chassis Type

Type of the rack

Serial Number

Serial number

Asset Tag

Additional ID, the customer-specific asset tag allows you to assign e.g. an inventory number or another identifier to the server.

System GUID

Format in which the S5 device returns UUID information.

BIOS Version

Version of the BIOS running on the managed server.

2.1.1.2 Operating System Information

Lists information on the operating system of the managed server

2.1.1.3 Systemboard Information

Lists information on the system board of the managed server.

2.1.1.4 Power Status Summary

The **Power Status Summary** group provides information on the current power status of the server and on the causes of the most recent Power On/Power Off incident. Additionally a **Power On Counter** records the total months, days and minutes during which the server has been on.

2.1.1.5 Running iRMC Firmware

Displays information on the firmware and the SDRR version of the iRMC.

2.1.1.6 Active Session Information

Displays all currently active iRMC sessions.

2.1.1.7 Installed License Keys

Displays all currently active license keys. You can install the following key types:

- KVM: License key for AVR
- Media: License key for virtual media
- eLCM: License key for embedded Lifecycle Management

The KVM and Media licenses are already installed on the C880 M5 server.

The eLCM is not supported on the C880 M5 server.

2.1.2 Systemboard

The **Systemboard** page in the **System** menu provides information on the CPU and the main memory modules. Most information is displayed in tables.

The screenshot shows the iRMC S5 Web Server interface. The top navigation bar includes 'Language', 'admin', 'Help', and the Cisco logo. The left sidebar has a 'System' menu with 'Systemboard' selected. The main content area shows the 'Systemboard' page with a 'Processors' table and several expandable sections.

Status	Socket	CPU Model	Cores (enabled / total)	Threads (enabled / total)	Identify LED	CSS
Processor detected	SB#0-CPU#0	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz	28 / 28	56 / 56		—
Processor detected	SB#0-CPU#1	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz	28 / 28	56 / 56		—
Processor detected	SB#1-CPU#0	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz	28 / 28	56 / 56		—
Processor detected	SB#1-CPU#1	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz	28 / 28	56 / 56		—
Processor detected	SB#2-CPU#0	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz	28 / 28	56 / 56		—
Processor detected	SB#2-CPU#1	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz	28 / 28	56 / 56		—
Processor detected	SB#3-CPU#0	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz	28 / 28	56 / 56		—
Processor detected	SB#3-CPU#1	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz	28 / 28	56 / 56		—

Figure 4: **Systemboard** page

The following groups are present:

2.1.2.1 Processors

Provides information on the status, IDs, CSS capability, performance etc. of the CPU(s) in the managed C880 M5 server.

2.1.2.2 Memory Modules

Provides a table of information on the status, IDs, CSS capability and performance of the main memory modules in the managed C880 M5 server.

2.1.2.3 Operating Voltages

Provides information on the status of voltage sensors assigned to the system board.

2.1.2.4 PCI Slots

Provides information on the status of PCI slots assigned to the system board.

2.1.2.5 Trusted Platform Module (TPM)

On C880 M5 servers with support for TPM, this group indicates whether TPM is enabled or disabled.

2.1.2.6 Power On Self Test (POST)

Displays the status of the last POST.

2.1.3 Power

The **Power** page of the **System** menu provides information on the power supplied by the power supply units.

The screenshot shows the iRMC S5 Web Server interface. The top navigation bar includes 'System', 'Logs', 'Tools', and 'Settings'. The left sidebar lists system components: Systemboard, Power (selected), Cooling, Mass Storage, Software, Network, and AIS Connect. The main content area is titled 'Power' and contains a sub-section 'Power Supplies' with a table of power supply units.

	Status	Designation	Model	Total Capacity [Watt]	Vendor	Part Number	Identify LED	CSS
🔍	✔ Power supply - OK	PSU#0	DPS2200AB1A	2200	DELTA	CA05954-3810/A3C40202586	ID	✔
🔍	✔ Power supply - OK	PSU#1	DPS2200AB1A	2200	DELTA	CA05954-3810/A3C40202586	ID	✔
🔍	✔ Power supply - OK	PSU#2	DPS2200AB1A	2200	DELTA	CA05954-3810/A3C40202586	ID	✔
🔍	✔ Power supply - OK	PSU#3	DPS2200AB1A	2200	DELTA	CA05954-3810/A3C40202586	ID	✔

Below the table, there are two expandable sections: 'Power Supply Redundancy and Configuration' and 'Power Consumption'.

Figure 5: **Power** page

2.1.3.1 Power Supplies

The **Power Supplies** group provides information on the power supply specifications and the IDPROM data of the FRUs (Field Replaceable Unit) of the server.

2.1.3.2 Power Supply Redundancy and Configuration

The **Power Supply Redundancy and Configuration** group show the power supply redundancy mode for the managed server. Which options are actually available depends on the server's capabilities.

2.1.3.3 Power Consumption

The **Power Consumption** group shows the current power consumption of the system components of the overall system. The tables display all the measurements of current, minimum, maximum and average power consumption for the server in the current interval.

A graphical display also shows the current power consumption of the server compared with the maximum possible power consumption.

2.1.4 Cooling

The **Cooling** page of the **System** menu displays the status of the fans and the temperature sensors.

The component with an LED can be easily identified by clicking the corresponding **ID** entry in the **Identify LED** column.

ID

Lights up the LED that is attached to the related server component. The LED's label changes to **Identify Off**.

If a server component has no LED, the **ID** entry is not set.

Status	Designation	Speed [rpm]	Fail Reaction	Fail Delay [sec]	Identify LED	CSS
✓ FAN on, running	FAN1 SYS	6000	Continue	90	ID	✓
✓ FAN on, running	FAN2 SYS	6120	Continue	90	ID	✓
✓ FAN on, running	FAN3 SYS	6120	Continue	90	ID	✓
✓ FAN on, running	FAN4 SYS	6000	Continue	90	ID	✓
✓ FAN on, running	FAN5 SYS	6120	Continue	90	ID	✓
✓ FAN on, running	FAN6 SYS	6120	Continue	90	ID	✓
✓ FAN on, running	FAN7 SYS	6120	Continue	90	ID	✓
✓ FAN on, running	FAN8 SYS	6120	Continue	90	ID	✓
✓ FAN on, running	FAN PSU1	2960	Continue	90		✓
✓ FAN on, running	FAN PSU2	2960	Continue	90		✓

Status	Designation	Temperature [°C]	Warning Level [°C]	Critical Level [°C]	Fail Reaction	CSS
✓ OK	Ambient	28	37	42	Continue	—
✓ OK	Systemboard 1	34	75	80	Continue	—
✓ OK	Systemboard 2	35	75	80	Continue	—
✓ OK	CPU1	35	91	92	Continue	—

Figure 6: Cooling page

2.1.4.1 Cooling Devices

The **Cooling Devices** group provides information on the status of the fans.

Start Fan Test

Performs the fan test at a speed similar to the currently required speed and therefore cannot be heard.

2.1.4.2 Temperature Sensors

The **Temperature Sensors** group provides information on the status of the temperature sensors which measure the temperature of the server components, such as the CPU and the memory module, and the ambient temperature.

2.1.5 Mass Storage

The **Mass Storage** page of the **System** menu provides information on controllers and devices of the managed server.

Status	Name	Entity Instance	Identify LED	CSS
OK	HDD	0		✓
OK	HDD0	1		✓
Empty or not installed	HDD1	2		✓
Empty or not installed	HDD2	3		✓
Empty or not installed	HDD3	4		✓
Empty or not installed	M.2-SSD1	62		✓
Empty or not installed	M.2-SSD2	63		✓

Figure 7: **Mass Storage** page

2.1.5.1 RAID Controllers

Displays detailed information on the RAID controllers if RAID is installed.

2.1.5.2 Directly Connected Devices

Displays the status of directly connected drives.

2.1.6 Software

The **Software** page of the **System** menu provides status information on the drivers and system management software installed on your system. This page is not available on the C880 M5 server.

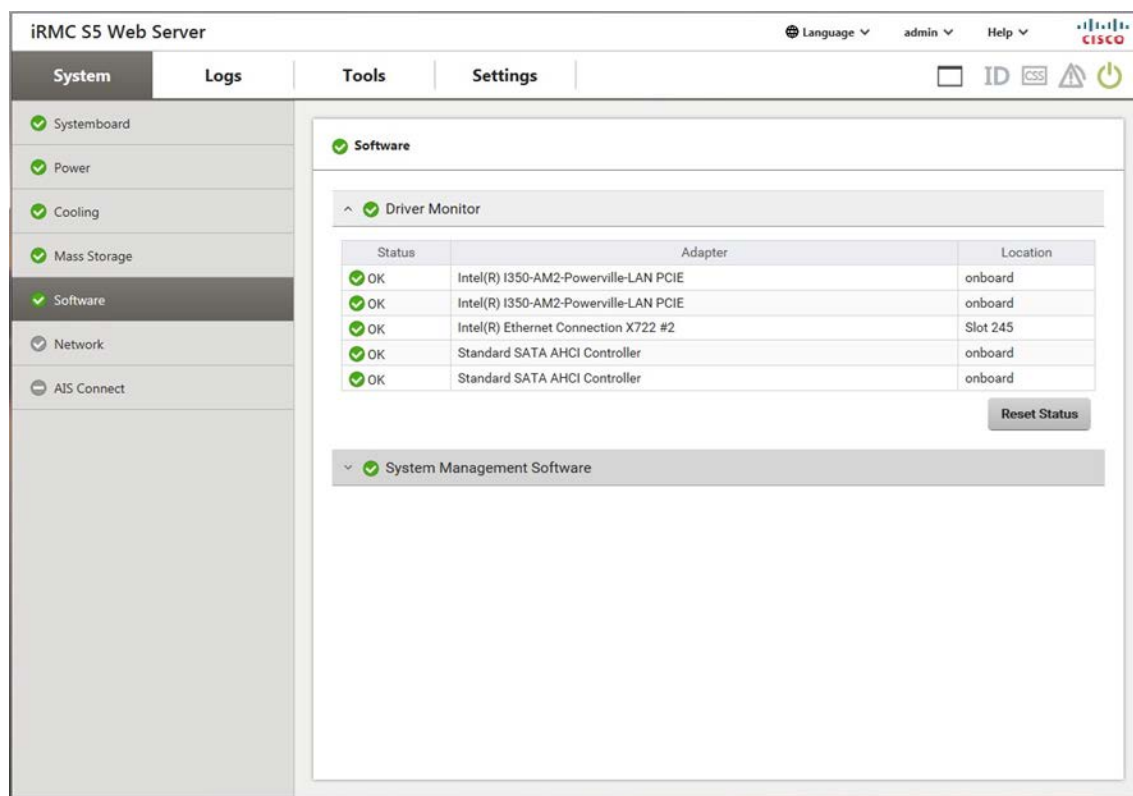


Figure 8: **Software** page

2.1.6.1 Driver Monitor

Reset Status

Resets the status of all driver components.

2.1.6.2 System Management Software

Displays the status of the installed system management software such as the iRMC itself.

2.1.7 Network

The **Network** page of the **System** menu provides information on the Ethernet ports of the iRMC. Certain information like IP address is not available on the C880 M5 server.

	Enabled	Module Name	Interface Speed [MBit]	Boot Option	VLAN Id	MAC Address	IPv4 Address	IPv6 Address
🔌	✓	Onboard LAN	1000	Uefi-Lan1	0	90:1B:0E:B0:62:C2	172.17.49.96	fe80:e10d:fe61:b373:b56d
🔌	✓	Onboard LAN	1000	Uefi-Lan2	0	90:1B:0E:B0:62:C3		
🔌	✓	Onboard LAN	0	Uefi-Lan3	0	00:00:00:00:00:00		

Figure 9: **Network** page

2.1.7.1 Ethernet Ports

Displays the status of the Ethernet ports of the iRMC.


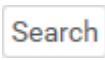

2.1.8 AIS Connect

AIS Connect is not supported on the C880 M5 server

2.2 Logs menu

The **Logs** menu summarizes the status of the logs generated and displays the entries of the log in a table.

You can sort and filter the logs table using the icons in the head of the respective column.

Icon	Meaning
	Sorts the content of the table alphabetically based on the selected column.
	Searches for a specified string or number in the selected column.
	Filters the content of the table based on the selected column.

2.2.1 Logs Overview

The **Overview** page of the **Logs** menu summarizes the current status of the event logging. You can change the settings of the logs in the **Settings** menu on the **Logging** page.

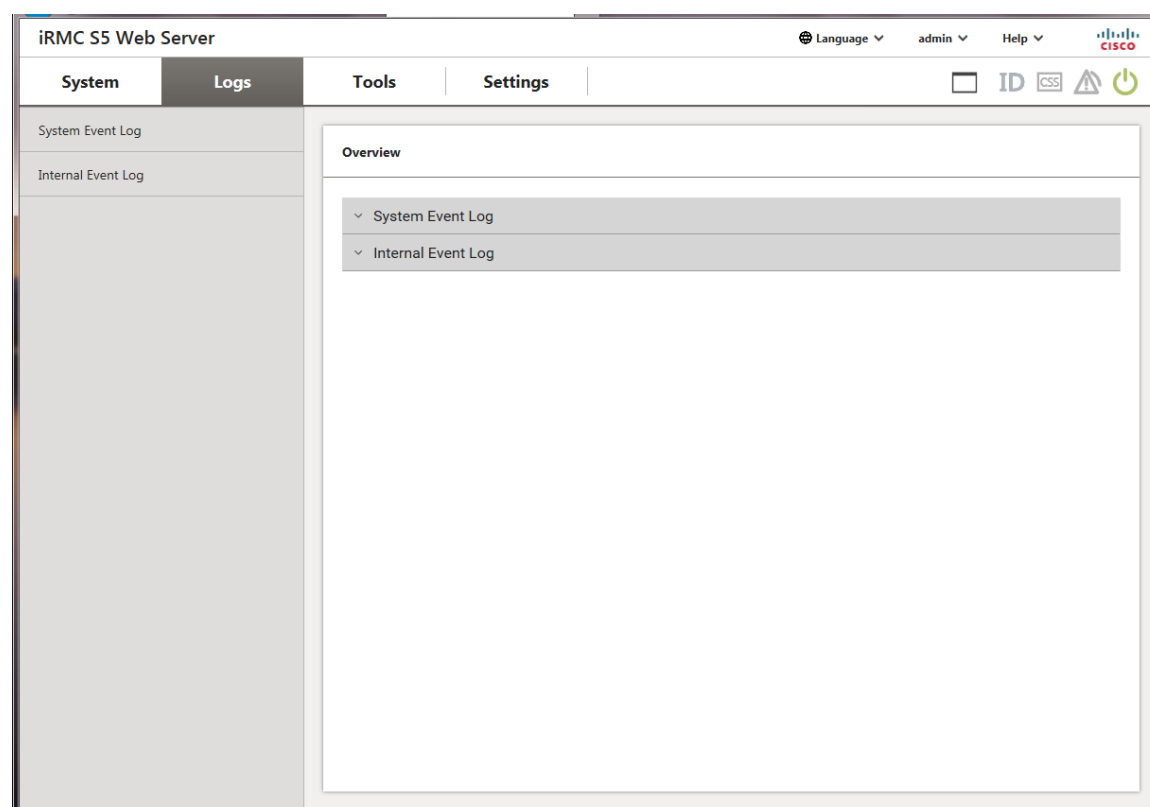


Figure 10: **Overview** page

The following groups are displayed:

2.2.1.1 System Event Log

This group summarizes the current status of the system event log.

Last Addition

Displays the point of time when the last entry was added to the log.

Last Erased

Displays the point of time when the whole log was cleared.

Records

Displays the number of entries present in the log.

Overwrite Policy

Specifies the action the iRMC performs, when the log is full:

Value	Meaning
Wraps when full	The event log is organized as a ring buffer. Once the event log is full, the iRMC overwrites the oldest entries.
Never overwrite	The event log is organized as a linear buffer. Once the event log is full, the iRMC cannot add any further entries. You have to clear the log manually to add further entries.

2.2.1.2 Internal Event Log

This group summarizes the current status of the internal event log.

Last Addition

Displays the point of time when the last entry was added to the log.

Last Erased

Displays the point of time when the whole log was cleared.

Records

Displays the number of entries present in the log.

Overwrite Policy

Specifies the action the iRMC performs, when the log is full:

Value	Meaning
Wraps when full	The event log is organized as a ring buffer. Once the event log is full, the iRMC overwrites the oldest entries.
Never overwrite	The event log is organized as a linear buffer. Once the event log is full, the iRMC cannot add any further entries. You have to clear the log manually to add further entries.

2.2.2 System Event Log

The **System Event Log** page of the **Logs** menu provides information on the SEL and displays the SEL entries. The SEL entries provide information on events like operating system boots/shutdowns, fan failures, and iRMC firmware flashes.

- i** You can modify the filter criteria for the current session on the **Logging** page of the **Settings** menu, for more information, refer to "[Logging](#)" on page 127. However, the settings you make there are only valid until the next logout, after which the default settings apply again.

The screenshot displays the 'System Event Log' page in the iRMC S5 Web Server interface. The page is divided into a left sidebar with 'System Event Log' and 'Internal Event Log' options, and a main content area. The main area shows a table of event log entries. The table has columns for Severity, Date, Code, Source, Description, and Alert Group. The entries include minor warnings for memory modules and a critical error for the OS watchdog timer.

	Severity	Date	Code	Source	Description	Alert Group
⊙	Minor	2017-05-11 09:42:08	19000B	iRMC S5	'DIMM-1D': Non Fujitsu Memory Module detected - Warranty restricted!	Memory
⊙	Minor	2017-05-11 09:42:08	19000B	iRMC S5	'DIMM-1A': Non Fujitsu Memory Module detected - Warranty restricted!	Memory
⊙	Info	2017-05-11 09:36:40	160014	iRMC S5	Online firmware flash: iRMC S5 reboot EEPROM 1 Version 91.04	Remote Management
⊙	Minor	2017-05-11 09:42:08	19000B	iRMC S5	'DIMM-1D': Non Fujitsu Memory Module detected - Warranty restricted!	Memory
⊙	Minor	2017-05-11 09:42:08	19000B	iRMC S5	'DIMM-1A': Non Fujitsu Memory Module detected - Warranty restricted!	Memory
⊙	Info	2017-05-11 09:36:40	160014	iRMC S5	Online firmware flash: iRMC S5 reboot EEPROM 1 Version 91.04	Remote Management
⊙	Info	2017-05-11 09:35:48	160013	iRMC S5	Online firmware flash EEPROM 2 Version 91.04	Remote Management
⊙	Info	2017-05-11 09:35:48	160013	iRMC S5	Online firmware flash EEPROM 1 Version 91.04	Remote Management
⊙	Critical	2017-05-10 18:25:01	080058	iRMC S5	OS Watchdog - Timer Expired	System Hang
⊙	Info	2017-05-11 09:35:48	160013	iRMC S5	Online firmware flash EEPROM 2 Version 91.04	Remote Management

Figure 11: .System Event Log page

There are the following groups for the system event log:

2.2.2.1 Event Log Information

This group summarizes the current status of the system event log.

Last Addition

Displays the point of time when the last entry was added to the log.

Last Erased

Displays the point of time when the whole log was cleared.

Records

Displays the number of entries present in the log.







Overwrite Policy

Specifies the action the iRMC performs, when the log is full:

Value	Meaning
Wraps when full	The event log is organized as a ring buffer. Once the event log is full, the iRMC overwrites the oldest entries.
Never overwrite	The event log is organized as a linear buffer. Once the event log is full, the iRMC cannot add any further entries. You have to clear the log manually to add further entries.

2.2.2.2 Event Log Content

The **Event Log Content** group displays the SEL entries in a table. The columns of the table have the following meaning:

Column	Meaning
	<p>Opens or closes a popup with the following information for the selected entry:</p> <p>CSS Indicates whether the event was triggered by a CSS component.</p> <p>Cause</p> <p>Resolutions Displays a proposed solution for the entry of severity level Critical or Major.</p>
Severity	<p>Displays the severity of the entry as an icon and as text.</p> <p>Colored icons are assigned to the various event/error categories to improve clarity:</p> <p> Major</p> <p> Minor</p> <p> Informational</p> <p> Customer self-service</p> <p> Displays cause and resolution for critical and major events.</p>
Date	Point of time the entry was added to the log.
Code	Error code of the entry
Source	Component that issued the entry
Description	Error text of the entry
Alert Group	Detailed component group the entry is related to

Clear Logs

Clears all the entries in the IPMI SEL.

2.2.3 Internal Event Log

The **Internal Event Log** page of the **Logs** menu provides information on the internal event log and displays the associated entries. The internal event log comprises audit events (login events, AVR connection events, etc.) and additional information (e.g. IPv6-related information and LDAP user names).

- i** You can modify the filter criteria for the current session on the **Logging** page of the **Settings** menu, for more information, refer to ["Logging" on page 127](#). However, the settings you make there are only valid until the next logout, after which the default settings apply again.

The screenshot displays the 'Internal Event Log' page in the iRMC S5 Web Server interface. The page is divided into a left sidebar with 'System Event Log' and 'Internal Event Log' options, and a main content area. The main content area has a search bar and a table of event log entries. The table has columns for Severity, Date, Code, Description, and Alert Group. The entries are as follows:

Severity	Date	Code	Description	Alert Group
Info	2017-02-03 12:53:28	120089	PCI: Bad TLP Bus: 58 Device: 0x00 Function: 0x00	Other
Info	2017-02-03 12:54:42	2300B1	iRMC S5 Browser http connection user 'admin' login from 10.172.44.213	Security
Info	2017-02-03 13:19:49	120089	PCI: Bad TLP Bus: 58 Device: 0x00 Function: 0x00	Other
Info	2017-02-03 13:19:51	12008C	PCI: Replay Timer Time-out Bus: 60 Device: 0x00 Function: 0x00	Other
Info	2017-02-06 07:18:02	2300E4	iRMC S5 Browser http connection user 'admin' auto-logout from 10.172.44.213	Security
Info	2017-02-06 07:22:47	2300B1	iRMC S5 Browser http connection user 'admin' login from 10.172.44.213	Security
Info	2017-02-07 11:25:56	2300B1	iRMC S5 Browser http connection user 'admin' login from 10.172.44.213	Security
Info	2017-02-07 11:31:09	2300E4	iRMC S5 Browser http connection user 'admin' auto-logout from 10.172.44.213	Security
Info	2017-02-07 11:33:57	2300B1	iRMC S5 Browser http connection user 'admin' login from 10.172.44.213	Security
Info	2017-02-09 10:30:09	2300B1	iRMC S5 Browser http connection user 'admin' login from 10.172.44.213	Security

Figure 12: .Internal Event Log page

There are the following groups for the internal event log:

2.2.3.1 Event Log Information

This group summarizes the current status of the internal event log.

Last Addition

Displays the point of time when the last entry was added to the log.

Last Erased

Displays the point of time when the whole log was cleared.

Records

Displays the number of entries present in the log.







Overwrite Policy

Specifies the action the iRMC performs, when the log is full:

Value	Meaning
Wraps when full	The event log is organized as a ring buffer. Once the event log is full, the iRMC overwrites the oldest entries.
Never overwrite	The event log is organized as a linear buffer. Once the event log is full, the iRMC cannot add any further entries. You have to clear the log manually to add further entries.

2.2.3.2 Event Log Content

The **Event Log Content** group displays the entries in a table. The columns of the table have the following meaning:

Column	Meaning
	<p>Opens or closes a popup with the following information for the selected entry:</p> <p>CSS Indicates whether the event was triggered by a CSS component.</p> <p>Cause</p> <p>Resolutions Displays a proposed solution for the entry of severity level Critical or Major.</p>
Severity	<p>Displays the severity of the entry as an icon and as text.</p> <p>Colored icons are assigned to the various event/error categories to improve clarity:</p> <p> Major</p> <p> Minor</p> <p> Informational</p> <p> Customer self-service</p> <p> Displays cause and resolution for critical and major events.</p>
Date	Point of time the entry was added to the log.
Code	Error code of the entry
Source	Component that issued the entry
Description	Error text of the entry
Alert Group	Detailed component group the entry is related to

Clear Logs

Clears all the entries in the internal event log.

2.2.3.3 Service Notice

The **Service Notice** group storing Service Notice in the Internal Event Log of the iRMC.

Submit

Stored the description of the **Add Service Notice** area in the internal event log.

2.3 Tools menu

The **Tools** menu summarizes the functions for common tasks, e.g. update, deployment, reporting, and license- and certificate management.

2.3.1 Tools Overview

The **Overview** page of the **Tools** menu displays the available functions of the menu.

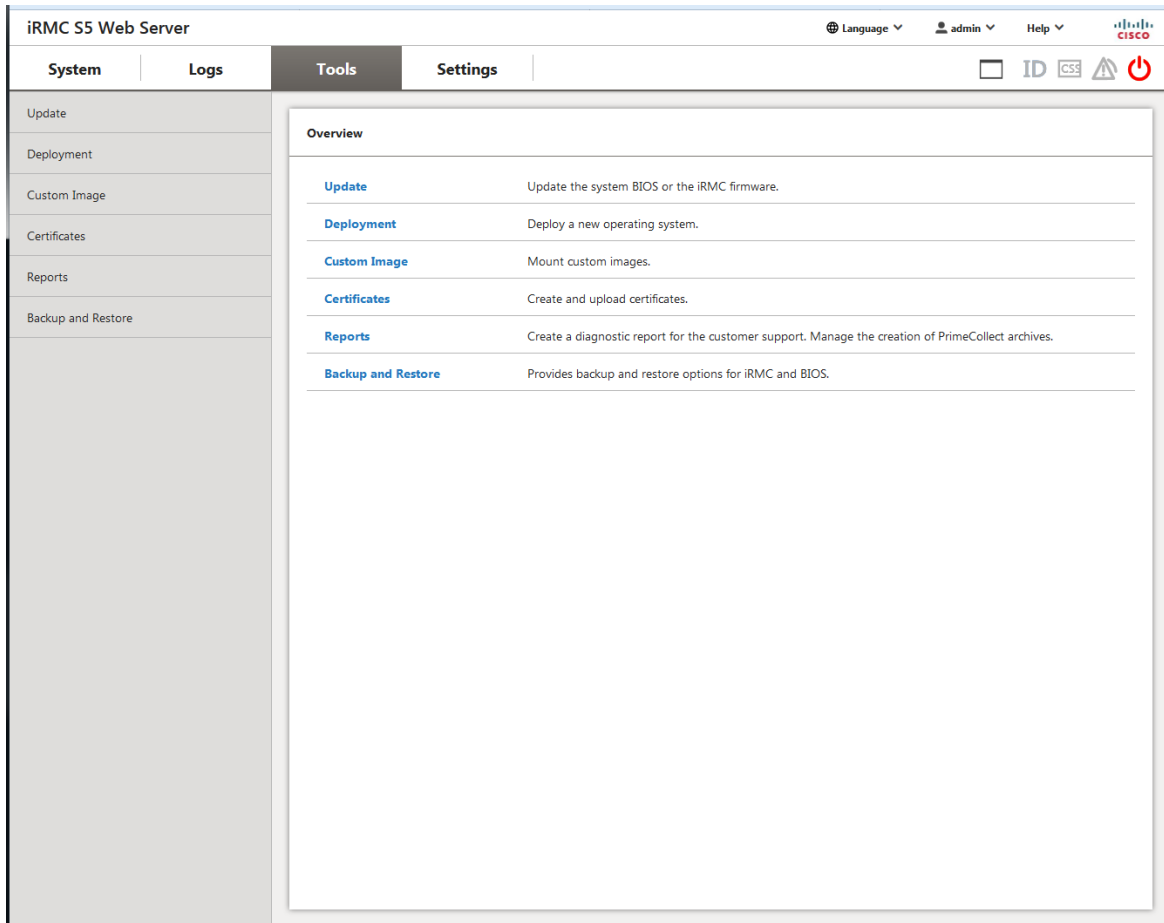


Figure 13: **Overview** page

2.3.2 Update

On the **Update** page of the **Tools** menu you configure the settings to update the iRMC firmware, BIOS and the operating system of the managed server.

The screenshot displays the iRMC S5 Web Server interface. The top navigation bar includes 'System', 'Logs', 'Tools' (selected), and 'Settings'. The left sidebar lists 'Update', 'Deployment', 'Custom Image', 'Certificates', 'Reports', and 'Backup and Restore'. The main content area is titled 'Update' and features an 'iRMC Update' section. This section contains a table with the following data:

Firmware Image	Status	Firmware Version	Booter Version	SDRR Version	SDRR ID	Firmware Date	Description
Low Firmware Image	Active	1.06P	1.14	3.07	0546	Jun 23 2017 17:20:02 JST	PRODUCTION RELEASE
High Firmware Image	Inactive	1.06P	1.14	3.07	0546	Jun 23 2017 17:20:02 JST	PRODUCTION RELEASE

Below the table, the 'Update Source' is set to 'Image file'. The 'Image to flash' is 'Low Firmware Image', and 'Boot from' is also 'Low Firmware Image'. The 'Image File' field has a 'Select...' button. The 'Stages' list includes: 1. Uploading file, 2. Checking file, 3. Flashing, and 4. iRMC Reboot. At the bottom right of the main section are 'Start Update' and 'Reboot iRMC' buttons. Below this are expandable sections for 'BIOS Update', 'Online Update', and 'Offline Update'.

Figure 14: Update page

2.3.2.1 iRMC Update

The **iRMC Update** group allows you to update the iRMC firmware online from a file. To do this, you must provide the current firmware image either locally on a remote workstation or on a TFTP server.

Only complete firmware images comprising a firmware version and an SDRR version can be used for an update (e.g. D3858_01.06P_sdr03.07.bin).

The table displays information on the iRMC firmware version and the SDRR version of the iRMC.

Image to flash

Specifies which iRMC firmware is to be updated. You have the following options:

Option	Meaning
Automatic - inactive firmware image	Selects the inactive firmware automatically.
Low Firmware Image	Selects the firmware image with the lower number (firmware image 1).
High Firmware Image	Selects the firmware image with the higher number (firmware image 2).

Boot from

Specifies the firmware image to be activated the next time the iRMC is rebooted. You have the following options:

Option	Meaning
Auto - Firmware Image with highest FW version	Automatically selects the most recent version of the firmware image.
Low Firmware Image	Selects the low firmware image.
High Firmware Image	Selects the high firmware image.
Select Firmware Image with oldest FW version	Selects the oldest version of the firmware image.
Select most recently programmed Firmware	Selects the most recently updated firmware image.
Select least recently programmed Firmware	Selects the least recently updated firmware image.

Update Source

Selects updating the iRMC firmware via Image file or TFTP.

Image File

Opens a file browser for navigating to the update file.

Start Update

Activates your settings and starts updating the iRMC firmware.

The several process stages are displayed in the **Stages** area. Every successfully passed stage is marked as ok (🟢).

Reboot iRMC

Reboots the iRMC. This button is disabled during the BIOS POST phase of the managed server.

2.3.2.2 BIOS Update

This group allows you to perform an online update of the BIOS on the managed server. To do this, you must provide the current BIOS image in a file.

Installed Version

Version of the BIOS running on the managed server

Update Source


Selects updating the BIOS via Image file or TFTP.


Image File

Opens a file browser for navigating to the update file.

Start Update

Activates your settings and starts flashing the BIOS.

 If a BIOS update is currently in progress, do not power-on the server.

The several process stages are displayed in the **Stages** area. Every successfully passed stage is marked as ok ().

2.3.2.3 Online Update

The **Online Update** group allows you to update BIOS and controller firmware while the server operating system is running. Online Update from iRMC is not supported on the C880 M5 server.


2.3.2.4 Offline Update

The **Offline Update** group allows you to update system components like network or storage controller firmware on the managed server. Offline Update from iRMC is not supported on the C880 M5 server.

2.3.2.5 Updating the BIOS

The following overview applies for both updating the BIOS via "upload from file" and TFTP. The TFTP settings can be configured/changed on the **BIOS Update Settings** group of the **System** page in the **Settings** menu, for more information, refer to "[BIOS Update Settings](#)" on page 68.

Updating the BIOS comprises the following steps:

- In the first step, you download the update file after which the following occurs:
 - If the server is powered off, it will automatically be initiate the flash process.
 - If the server is powered on, the flash process will be failed. Update the BIOS again after the server is powered off.
 -  If a BIOS update is currently in progress, do not power-on the server.
- Flash data is then transferred to memory and the status display will indicate when the transfer has successfully completed.
- Before the actual flashing process begins, the flash/update image is checked.
- Once the update/flash image is successfully verified, the actual flashing process begins. The status indication shows the completion in percent.
- Once the BIOS update has successfully completed, the following entry is written to the system event log (SEL): BIOS TFTP or HTTP/HTTPS flashOK

2.3.3 Deployment

The **Deployment** page of the **Tools** menu allows you to download or update the Service Platform. The Deployment page is not supported on the C880 M5 server.

2.3.4 Custom image

The **Custom Image** page of the **Tools** menu allows you to specify a URL from which you can download ISO images onto the iRMC SD card. The Custom Image is not supported on the C880 M5 server.


2.3.5 Certificates

The **Certificates** page of the **Tools** menu provides information on installed certificates.

The iRMC is supplied with a predefined server certificate (default certificate). If you want to access the iRMC via secure connections, it is recommended that you replace the certificate with one signed by a CA as soon as possible.

You can create a self-signed certificate using the **Generate** button within the **Current SSH/TLS Certificate** group.

The basic concept of creating and operating your own CA consists of creating a self-signed certificate whose private key will be used later on to sign the server certificates. The self-signed certificate thus serves as the Root CA certificate of your own CA.

-  When generating the new certificate, all the existing HTTPS connections are closed and the HTTPS server is automatically restarted. This can take up to five minutes depending on the length of the key. No explicit reset of the iRMC is required.

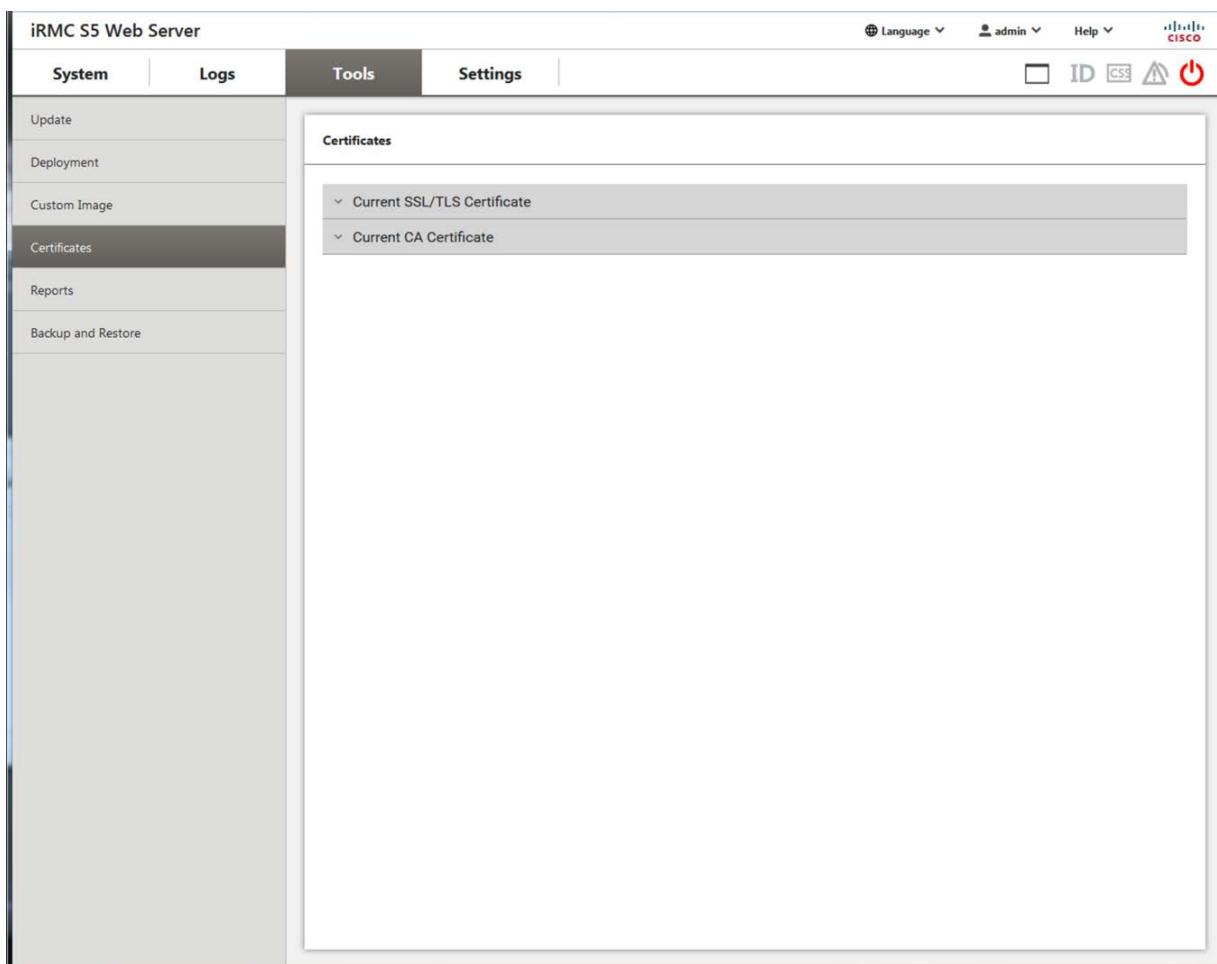


Figure 15: **Certificates** page

2.3.5.1 Current SSH/TLS Certificate

This group displays information on the currently valid SSH/TLS certificate and/or restore the default one.

Use Default

Restores the default certificate delivered with the firmware after you have confirmed that you wish to do so.

Generate

Opens the **Generate certificate** dialog in which you can enter the relevant values for the new certificate, for more information, refer to ["Generate certificate dialog" on page 53](#).

Load from file

Opens the **Upload SSH/TLS certificate** dialog, in which you enter the encryption key for the certificate, for more information, refer to ["Upload SSH/SSL certificate dialog" on page 55](#).

2.3.5.2 Current CA Certificate

This group provides information on the currently valid DSA/RSA certificate and/or restore the default one.

Use Default

Restores the default certificate delivered with the firmware after you have confirmed that you wish to do so.

Load from file

Opens the **Upload CA certificate** dialog, in which you select the file for upload, for more information, refer to ["Upload CA certificate dialog" on page 57](#).

2.3.5.3 Generate certificate dialog

In this dialog you enter the relevant parameters for a self-signed SSH/SSL certificate.

Generate certificate	
Common Name (CN)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Country (C)	<input type="text"/>
State or Province (ST)	<input type="text"/>
City or Locality (L)	<input type="text"/>
Email Address	<input type="text"/>
Valid For (days)	<input type="text" value="730"/>
Key Length (bits)	<input type="text" value="2048"/>

Generate Cancel

Figure 16: **Generate certificate** dialog

The following information can be set for a new certificate:

Common Name (CN)

Hostname, IP address

Organization (O)

Your company

Organization Unit (OU)

The department or division

Country (C)

Two letter country code, e.g. CH

State or Province (ST)

Full name of the state or province

City or Locality (L)

The city or district

Email address

Your Email address

Valid From

The date the certificate is valid from

Valid For (days)

Expiration date

Key Length (bits)

Length of the generated key


Generate

Creates the certificate with the specified parameters.

2.3.5.4 Generating a self-signed RSA Certificate

You can create a self-signed certificate using the **Certificates** page.

1. In the **Tools** menu open the **Certificates** page.
2. Open the **Current SSH/SSL Certificate** group.
3. At the end of the group click **Generate** to open the **Generate certificate** dialog.
4. In the **Generate certificate** dialog enter the required details.
5. 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 five minutes depending on the length of the key.

No explicit reset of the iRMC is required.

2.3.5.5 Upload SSH/TLS certificate dialog

With this dialog you can upload your private and the public DSA/RSA key onto the iRMC.

- i** Input format of the X.509 private DSA/RSA key: PEM-encoded format (ASCII/Base64).

Figure 17: Upload SSH/TLS certificate dialog

SSH/TLS public key

Local file with the public DSA/RSA key on the managed server

Select

Opens a dialog box for navigating to the file containing the public key.

Upload

Loads the public key onto the iRMC.

Cancel

Clears the display of the file name.

SSH/TLS private key

Local file with the private DSA/RSA key on the managed server

Select

Opens a dialog box for navigating to the file containing the private key.

- i** When you upload the private key, all the existing HTTPS connections are closed and the HTTPS server is automatically restarted. This process can take up to 30 seconds.

Upload

Loads the private key onto the iRMC.

Cancel

Clears the display of the file name.

Close

Closes the dialog without any upload.

2.3.5.6 Loading the DSA/RSA public and private key from local files

Use the **Current SSH/TLS Certificate** group to load public and private DSA/RSA keys from local files.

i The keys must be loaded onto the iRMC at the same time.

1. Save the X.509 DSA/RSA public and private DSA/RSA key in corresponding local files on the managed server.
2. In the **Tools** menu open the **Certificates** page.
3. Open the **Current SSH/TLS Certificate** group.
4. At the end of the group click **Load from file** to open the **Upload SSH/TLS certificate** dialog.
5. Specify the **SSH/TLS public key** and **SSH/TLS private key** by clicking the associated **Select** button and navigating to the file that contains the private key or the certificate.
6. Click **Upload** to load the certificate and the private key onto the iRMC.

i When you upload the certificate and private key, all the existing HTTPS connections are closed and the HTTPS server is automatically restarted. This process can take up to 30 seconds.

No explicit reset of the iRMC is required.

2.3.5.7 Upload CA certificate dialog

With this dialog you can upload a signed X.509 DSA/RSA certificate from a Certificate Authority (CA) from a local file to the iRMC.

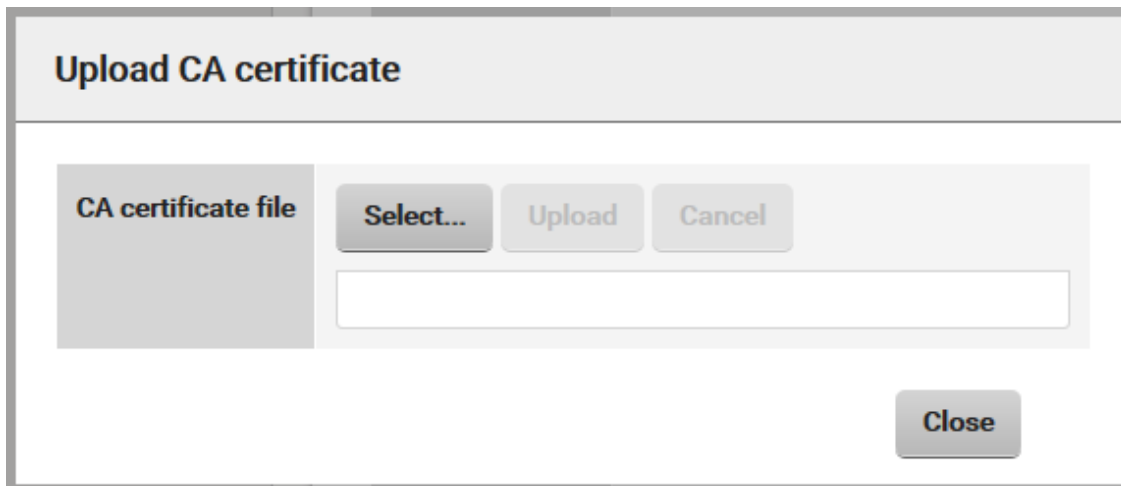


Figure 18: Upload CA certificate dialog

CA certificate file

Select

Opens a dialog box for navigating to the local file on the managed server containing the CA certificate.

Upload

Loads the certificate and/or private key onto the iRMC.

Cancel

Clears the display of the file name.


Close

Closes the dialog without any upload.

2.3.5.8 Loading a CA certificate from a local file

Use the **Current CA certificate** group to load a CA certificate from a local file.

1. Save the CA certificate in a local file on the managed server.
2. In the **Tools** menu open the **Certificates** page.
3. Open the **Current CA Certificate** group.
4. At the end of the group click **Upload** from file to open the **Upload CA certificate** dialog.
5. Specify this file in the **CA certificate file** field by clicking the associated **Select** button and navigating to the file containing the CA certificate.
6. Click **Upload** to load the certificate and/or private key onto the iRMC.

-  When you upload the certificate and/or private key, all the existing HTTPS connections are closed and the HTTPS server is automatically restarted. This process can take up to 30 seconds.

No explicit reset of the iRMC is required.

2.3.5.9 Restoring the SSH/TLS certificate/CA certificate


1. In the **Tools** menu open the **Certificates** page.
2. Open the **Current SSH/TLS Certificate** group.
3. At the end of the group, click **Use Default** to restore the default certificate delivered with the firmware.
4. Open the **Current CA Certificate** group.
5. At the end of the group, click **Use Default** to restore the default certificate delivered with the firmware.

2.3.6 Reports

The **Report** page provides information on service incidents concerning server hardware/software directly out-of-band from the iRMC.

Information is provided on the following items:

- System BIOS
- PCI configuration
- IDPROM data
- Sensor data records
- Processors
- Voltages
- Fans
- Temperature sensors
- Power Supplies
- Memory modules
- Network adapters
- System Event Log (SEL)
- Internal Event Log (IEL)
- Boot status
- Management controllers
- Power consumption data

-  Alternatively, you can download and automatically evaluate the generated XML file by using a cURL or Visual Basic script. For more information, refer to the "Cisco C880 M5 Administration Guide".

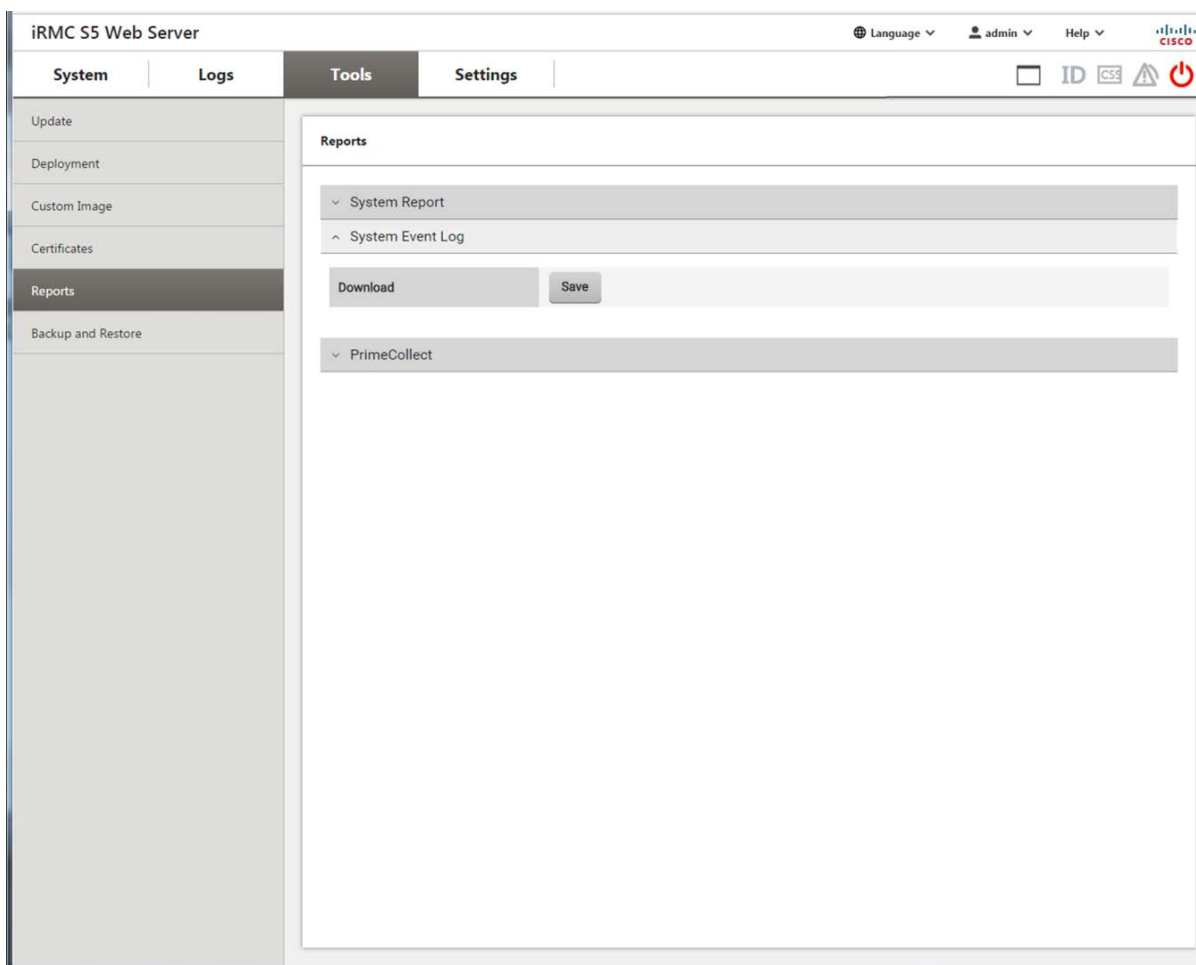


Figure 19: Reports page

2.3.6.1 System Report

Download

Downloads the XML file containing the report information.

Save

Stores a report.xml file containing the report information in the local download directory

View in Browser

Displays the XML file containing the report information in the default browser.

2.3.6.2 System Event Log

Download

Downloads the file containing the system event log.

Save

Stores a SystemEventLog file containing the system event log in the local download directory

2.3.6.3 PrimeCollect

In the **PrimeCollect** group you configure and start the creation of PrimeCollect archives. The PrimeCollect is not supported on the C880 M5 server.

2.3.7 Backup and Restore

On the **Backup and Restore** page of the **Tools** menu you can configure the settings for backing up and restoring the iRMC and the BIOS.

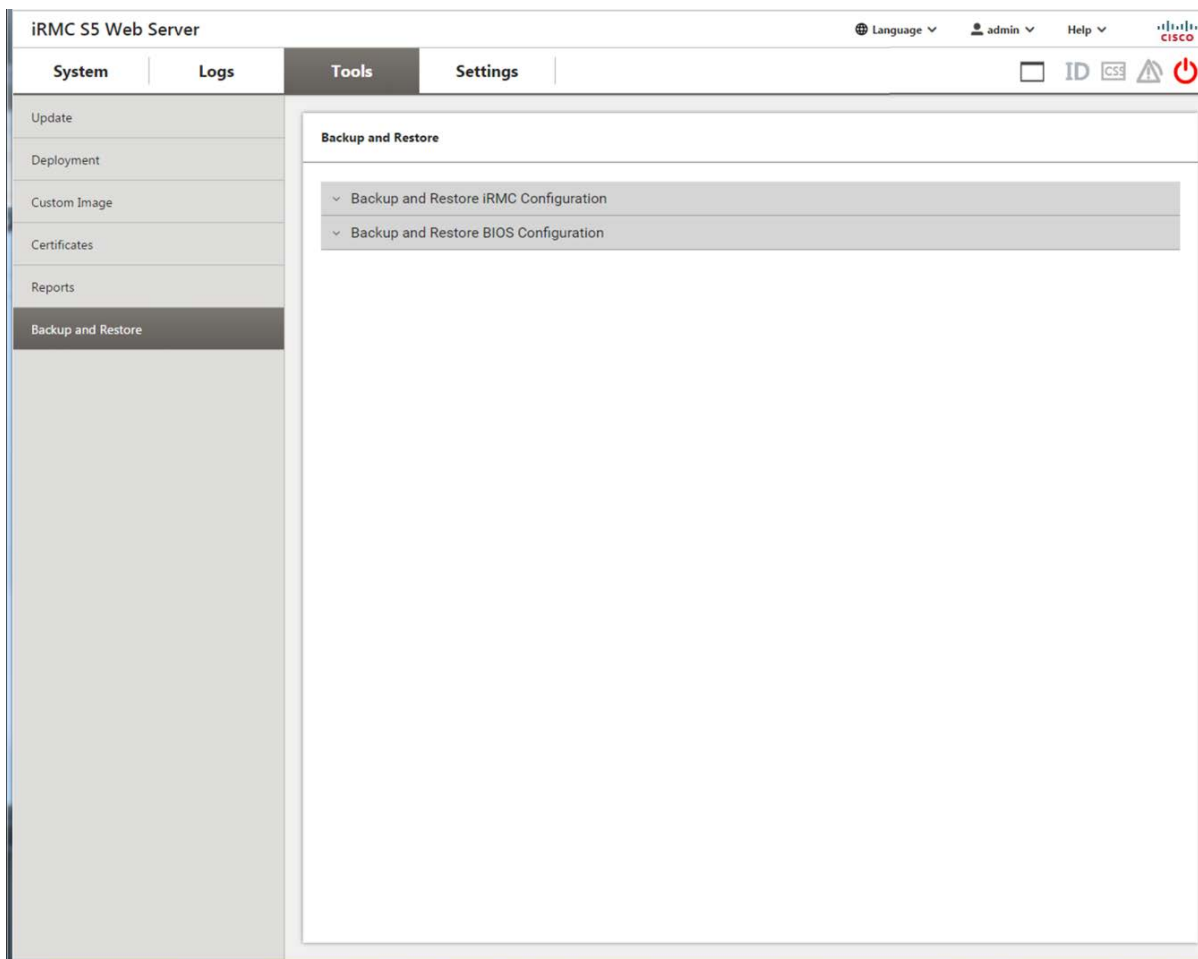


Figure 20: **Backup/Restoration of BIOS Single Parameter Settings** page

2.3.7.1 Backup and Restore iRMC Configuration

With the options of this group you save the current settings for the iRMC in a file. You can also load the firmware settings onto the iRMC again.

Backup iRMC Firmware settings to ServerView @Configuration Manager XML file

The data is exported from the iRMC in logical sections, each corresponding to a selected option.

The option **Include All other Firmware Settings** causes the firmware to export all current ConfigSpace values that have not already been exported together with another section. Newly implemented values are automatically exported with newer firmware versions.

Save

Saves the selected settings in the iRMC_settings.pre file in the default download directory on your computer.

Save all

Saves all settings in the iRMC_settings.pre file in the default download directory on your computer.

Restore iRMC Firmware settings from ServerView® Configuration Manager XML file

Provides parameters for restoring iRMC settings from a restoration file in ServerView® Configuration Manager XML file.


Settings File

Name of the restoration file

Select

Opens a browser dialog allowing you to navigate to a file (.pre) containing a backup of single BIOS parameters in the ServerView® Configuration Manager XML file.

Stages

The several process stages are displayed in the **Stages** area. Every successfully passed stage is marked as ok ().

Start Restore

Initiates the restoration of single BIOS parameter settings based on the file specified under **Restoration File**.

Once the restoration process has started, the current process status is indicated in the **Restoration Status** field.

2.3.7.2 Backup and Restore BIOS Configuration

The **Backup and Restore BIOS Configuration** group provides the following options:

- Automatic BIOS parameter backup
- Back up single BIOS parameters in ServerView® WinSCU XML format and save the backup to a file.
- Restore single BIOS parameter settings in ServerView® WinSCU XML format from a file.

Notes on the default backup process:


- During the backup process, all buttons and input fields are disabled.
- If powered off, the managed server will be automatically powered on.
- If the server is powered on, a reboot is required. Otherwise, the backup process will remain in state "Boot Pending".
- The managed server is powered off after the backup has completed.

The parameters are provided in several groups.

Backup BIOS Parameters to ServerView® Configuration Manager XML file

Provides parameters for backing up BIOS parameter settings to ServerView® Configuration Manager XML file and saving the backup to a file.

Stages

The several process stages are displayed in the **Stages** area. Every successfully passed stage is marked as ok ().

Request Backup

Initiates a backup of the BIOS parameter settings to ServerView® Configuration Manager XML file. The backup (with the name specified in the **Backup Filename** field) is stored locally on the iRMC S5.

Once the backup process has started, the current process status is displayed in the **Stages** area.

Save

Only available if a backup is available in the local storage of the iRMC S5: Opens a browser dialog allowing you to save the iRMC S5-local copy of the BIOS backup data to a file (<name-of-your-choice>.pre).


Restore BIOS Parameters from ServerView® Configuration Manager XML file

Provides parameters for restoring single BIOS parameter settings from a restoration file in ServerView® WinSCU XML format.

Parameter File

Name of the restoration file

Stages

The several process stages are displayed in the **Stages** area. Every successfully passed stage is marked as ok ().

Select

Opens a browser dialog allowing you to navigate to a file (.pre) containing a backup of single BIOS parameters in the ServerView® WinSCU XML format.

Start Restore

Initiates the restoration of single BIOS parameter settings based on the file specified under **Restoration File**.

Once the restoration process has started, the current process status is indicated in the **Restoration Status** field.

2.4 Settings menu

With the functions of the **Settings** menu you can configure all settings of the Baseboard Management Controller.

2.4.1 Settings Overview

The **Settings** page of the **Settings** menu displays the available functions of the menu.

The screenshot shows the iRMC S5 Web Server interface. The top navigation bar includes 'System', 'Logs', 'Tools', and 'Settings' (which is selected). The right side of the top bar contains 'Language', 'admin', 'Help', and the Cisco logo. Below the navigation bar, a sidebar on the left lists various system components. The main content area, titled 'Settings', provides an overview of the configuration options available.

Category	Description
System	Settings for system and operating system specific information
Network Management	Settings for network interfaces, network protocols, DNS, VLAN and Internet proxy server configuration settings
Services	Configuration settings for web based access, console access, IPMI access, video redirection and BIOS console redirection. Settings for virtual media access, SNMP access and email alerting
User Management	Settings for local user accounts, LDAP user accounts and the Central Authentication Service (CAS)
Server Management	Settings for ASR&R, Watchdogs and System UUID format
Power Management	Settings for power consumption control and system power on/off
Logging	Settings for the System Event Log, the Internal Event Log and the SysLog server
Baseboard Management Controller	BMC specific settings like time synchronisation, license management and user interface configuration

Figure 21: Overview page

2.4.2 System

On the **System** page of the **Settings** menu you can configure miscellaneous settings of the BMC.

The screenshot shows the iRMC S5 Web Server interface. The top navigation bar includes 'System', 'Logs', 'Tools', and 'Settings'. The 'Settings' menu is active, and the 'System' sub-menu is selected. The main content area is titled 'System' and contains several configuration sections:

- Asset Tag:** A section with a 'System Asset Tag' input field and 'Apply' and 'Cancel' buttons.
- Operating System Information:** A section with several fields:
 - Host Name: localhost.localdomain
 - Host IP Address(es): 192.168.122.1
 - System Description: Server
 - System Location: Server
 - System Contact: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
 - O/S Name: Red Hat Enterprise Linux Server 7.3
- A warning message: **ServerView Agents overwrite the setting on next O/S boot.**
- BIOS Update Settings**, **BIOS Backup Settings**, and **Boot Options** sections are visible but collapsed.

Figure 22: **System** page

The settings of the **System** are provided in the several groups.

2.4.2.1 Asset Tag

In the **System Asset Tag** field you can enter a customer-specific asset tag for the managed server.

- i** The customer-specific asset tag allows you to assign the server an inventory number or other identifier of your choice.

2.4.2.2 Operating System Information

Lists information on the operating system of the managed server

-  You can edit all fields of the **Operating System Information** group.

2.4.2.3 BIOS Update Settings

The **BIOS Update Settings** group allows you to perform an update of the BIOS on the managed server. To do this, you must provide the current BIOS image in a file on a TFTP server. The BIOS is flashed when TFTP is started.

TFTP Server

IP address or DNS name of the TFTP server on which the file with the BIOS image is stored.

Update Image File

File containing the BIOS image

2.4.2.4 BIOS Backup Settings

In this group you can automatize the BIOS parameter backup. When you request a BIOS parameter backup the managed server initiates a boot to read the current BIOS configuration. With **Automatic Bios Parameter Backup** enabled the BIOS configuration will be send automatically during each boot process. Thus the current BIOS configuration is always available and no additional reboot of the managed server is necessary.

-  An enabled automatic BIOS parameter backup will slow down the boot process.

Enable Parameter Backup

Enables/disables the BIOS parameter backup. Changing this option will become active after the next system boot. This system boot must be initiated manually.

Default: Disabled

2.4.2.5 Boot Options

The **Boot Options** group allows you to configure the behavior of the system the next time it is booted. You can set whether the BIOS is to interrupt the boot process for the system if errors occur during the POST phase.

- i** The options set here only apply to the next boot operation. After this, the default mechanism applies again.

POST Error Action

Specifies the BIOS behavior if an error occurs during the power on self test:

Option	Meaning
Continue	Continue the boot process if errors occur during the POST phase.
Halt on errors	Interrupt the boot process if errors occur during the POST phase.

Boot Device Selector

Storage medium you wish to boot from.

The following options are available:

Option	Meaning
No Change	The system is booted from the same storage medium as previously.
PXE/iSCSI	The system is booted from PXE/iSCSI over the network.
Hard-drive	The system is booted from HDD.
CDROM/DVD	The system is booted from CD/DVD.
Floppy	The system is booted from floppy disk.
Bios Setup	The system enters BIOS setup when booting.

Boot Type

Determines the boot mode in which the system will be started at the next boot.

Depending on the server operating system, the following options are available for selection:

Option	Meaning
PC compatible (legacy)	The system is booted in legacy BIOS-compatibility mode.
Extensible Firmware Interface Boot (EFI)	The system is booted in UEFI boot mode (only on 64-bit operating systems).

Next Boot only

Settings apply to the next boot only.

2.4.3 Network Management

On the **Network Management** page of the Settings menu you can configure several network settings of the iRMC.

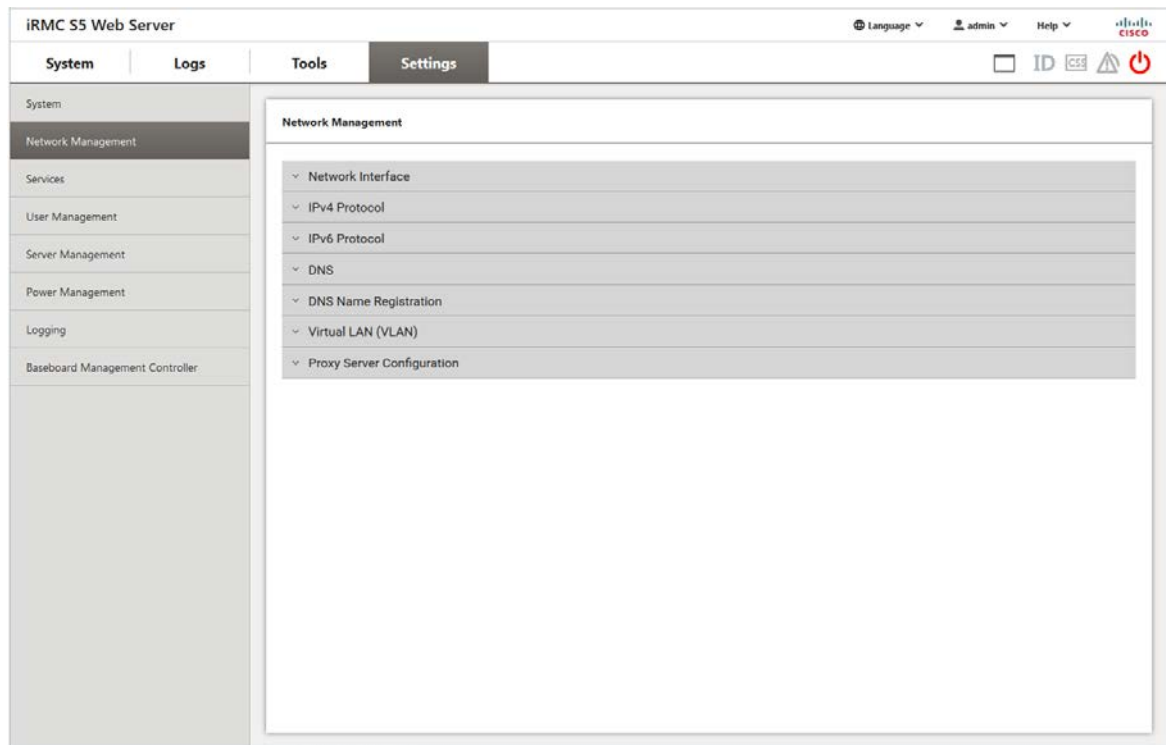




Figure 23: **Network Management** page

The network settings are provided in several groups.

2.4.3.1 Network Interface

In this group you can change the Ethernet settings for the iRMC.

-  Contact the network administrator responsible for the system before you change the Ethernet settings.
If you make illegal Ethernet settings for the iRMC, you will only be able to access the iRMC using special configuration software, the serial interface or via the BIOS.
-  Only users with Configure iRMC Settings permission are allowed to edit Ethernet settings.

MAC Address

Displays the MAC address of the iRMC.

Interface Speed

This option is disabled/not visible if network bonding is enabled.

The following options are available for the LAN speed:

- Auto Negotiation
- 1000 MBit/s Full Duplex
- 100 MBit/s Full Duplex
- 100 MBit/s Half Duplex

If **Auto Negotiation** is selected, the onboard LAN controller assigned to the iRMC autonomously determines the correct transfer speed and duplex method for the network port it is connected to. If shared LAN is selected in **Interface Port**, LAN speed setting is only available on system.

Interface Port

This option is disabled/not visible if network bonding is enabled. The LAN interface of the installed system NIC can be set up:

- As a shared LAN for shared operation with the system
- As a service LAN for exclusive use as a management LAN

Max. Transmission Unit (MTU)

Maximum packet size (in bytes) of the TCP/IP data packages that will be accepted by the TCP/IP connection (default: 3000 bytes).

Bonding

Enables/disables network bonding for the iRMC (for more information, refer to ["Network bonding" on page 77](#)).

2.4.3.2 IPv4 Protocol


The **IPv4 Protocol** group allows you to configure the IPv4 settings for the iRMC.

IPv4 Protocol

Enables/disables IPv4 addressing. IPv4 addressing is always enabled for the iRMC and cannot be disabled.

DHCP

If you activate this option, the iRMC gets its LAN settings from a DHCP server on the network.

 Do not activate the **DHCP** option if no DHCP server is available on the network.

If you activate the **DHCP** option and there is no DHCP server available on the network, the iRMC goes into a search loop (i.e. it continues searching for a DHCP server until it finds one).

The (configured) iRMC can be registered with a DNS server by an appropriately configured DHCP server.

IP Address

IPv4 address of the iRMC in the LAN. This address is different from the IP address of the managed server.

If you are working with a static address (**DHCP Enable** option not activated), you can enter the IP address here. Otherwise (if the **DHCP Enable** option is activated), the iRMC displays the address.

Subnet Mask

Subnet mask of the iRMC in the LAN

Gateway Address

IPv4 address of the default gateway in the LAN

2.4.3.3 IPv6 Protocol

The **IPv6 Protocol** group allows you to automatically or manually configure an IPv6 address for the iRMC.

IPv6 Protocol

Enables/disables IPv6 addressing for the iRMC. If IPv6 addressing is enabled, the IPv6 configuration group will be displayed.

You cannot disable IPv6 addressing if the iRMC is currently accessed via IPv6.

Manual IPv6 Configuration

This option is enabled by default.

If **Manual IPv6 Configuration** is disabled, Stateless Autoconfiguration or Stateful Address Configuration is used to automatically configure a routable IPv6 address for the iRMC:

- ▮ Stateless Autoconfiguration uses the Link Local Address, which is always assigned to the iRMC automatically, and enables the iRMC to generate its own IPv6 address.
- ▮ With Stateful Address Configuration, the iRMC obtains its IPv6 address from a DHCP server.

If you enable the **Manual IPv6 Configuration** option, the IPv6 configuration group displays additional parameters that allow you to manually configure a routable IPv6 address for the iRMC.

Interface Identifier Source

Specifies the source of the interface identifier of an IPv6 unicast address that is used to identify the interface of a link. The interface identifier needs to be unique within a subnet prefix.

Option	Meaning
Part of specified static address	Both parts of the IPv6 address (network and host) need to be configured.
EUI-64 (based on MAC Address)	The network part of the IPv6 address needs to be configured.

IPv6 Static Address

Static IPv6 address for the iRMC

Prefix Length

Length of the IPv6 prefix

IPv6 Static Gateway

Static IPv6 address of the default IPv6 gateway in the LAN

Current IPv6 Addresses

Displays the current IP settings of the iRMC.

2.4.3.4 DNS

In this group you activate the DNS for the iRMC. This makes it possible to use symbolic DNS names instead of IP addresses for configuring the iRMC.

DNS

Enables/disables DNS for the iRMC.

DNS Configuration

If you activate this option, the IP addresses of the DNS servers are obtained automatically from the DHCP server. In this case, up to three DNS servers are supported.

If you do not enable this setting, you can enter up to three DNS server addresses manually under DNS-Server 1 - DNS-Server 3.

DNS Domain

If the **Obtain DNS configuration from DHCP** option is disabled, specify the name of the default domain for requests to the DNS server(s).

DNS Search Path

List of (partially qualified) domain names, separated by one or more blanks. The DNS search list can have a maximum length of 256 characters. The **DNS Search Path** field is used to specify the domains to be searched when looking up a host name that does not have a domain-name component.

DNS Server 1 / 2 / 3

If the **Obtain DNS configuration from DHCP** option is disabled, you can enter the names of up to five DNS servers here.

DNS Retries

Number of DNS retries

DNS Timeout


Time (in seconds) the iRMC waits for a DNS response

2.4.3.5 DNS Name Registration

In this group you configure a host name for the iRMC and thus use DNS dynamically. Dynamic DNS allows DHCP servers to autonomously pass on the IP address and system name of a network component to DNS servers to facilitate identification.

Register DNS Name

Specifies how the DNS name of the iRMC is set.

Option	Meaning
None	No name is registered for the iRMC.
Register DHCP Address in DNS via DHCP Server	Enables/disables the transfer of the DHCP name to the DHCP server for the iRMC and the DNS registration via DHCP server.
Register full domain name (FQDN) via DHCP server in DNS	IPv4 addressing only: Enables/disables the transfer of the FQDN to the DHCP server for the iRMC and the DNS registration via DHCP server.
DNS Update Enabled	Enables/disables updating of DNS records via Dynamic DNS.  Only non-secure DNS is supported.

Use iRMC Name

The iRMC name specified in the **iRMC Name** entry field is used for the iRMC instead of the server name.

iRMC Name

iRMC S5 name passed to DHCP for the iRMC in place of the server name. Depending on the related options, the **iRMC Name** is used as part of the DNS name.

Use MAC Address

The last 3 bytes of the MAC address of the iRMC are appended to the DHCP name of the iRMC.

Use Extension

The extension specified in the **Extension** entry field is appended to the DHCP name of the iRMC.

Extension

Name extension for the iRMC

DNS Name

Shows the configured DNS name for the iRMC.

2.4.3.6 Virtual LAN (VLAN)

In this group you configure the VLAN settings of the iRMC.

VLAN

Enables/disables VLAN support for the iRMC.

VLAN Id

Identifier of the virtual network (VLAN) the iRMC belongs to. Permitted value range: $1 \leq \text{VLAN ID} \leq 4094$.

VLAN Priority


VLAN priority (user priority) of the iRMC S5 in the VLAN specified by VLAN ID. Permitted value range: $0 \leq \text{VLAN Priority} \leq 7$ (default: 0).

2.4.3.7 Proxy Server Configuration

In this group you can configure the settings of a proxy server which can be optionally used for establishing the connection to an update repository (for more information, refer to ["Update" on page 45](#)) and/or establishing an AIS Connect connection (for more information, refer to ["AIS Connect" on page 92](#)).

Server Address

IP address of the proxy server

-  You can activate the DNS for the iRMC (for more information, refer to ["Baseboard Management Controller" on page 131](#)). You can then use a symbolic name instead of the IP address.

Server Port

Port of the proxy service.

Default port number: 81

User Name

User name for authentication on the proxy server.

User Password

Password for authentication on the proxy server.

Confirm User Password

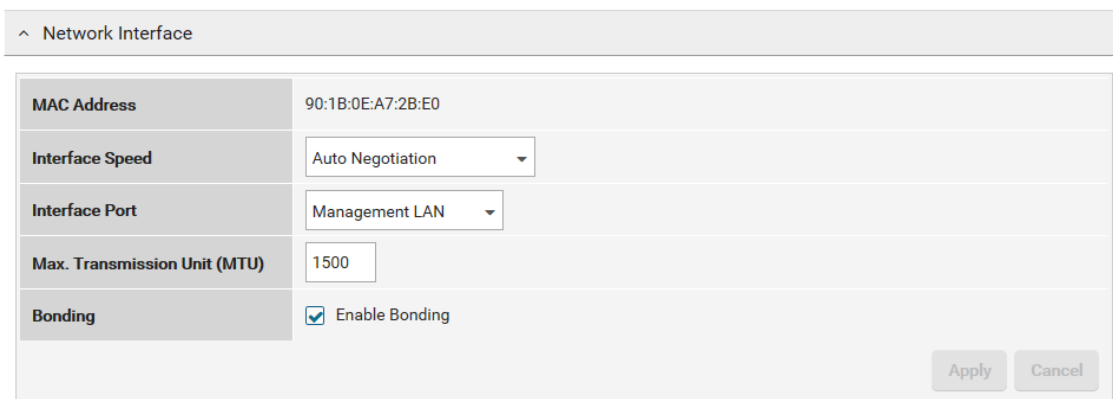
Confirm the password entered.

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

- i** For iRMC network bonding, the LAN switches involved should be located within the same network. Beyond that, iRMC network bonding does not require a special switch configuration.



The screenshot shows a 'Network Interface' settings window. It contains a table of configuration options:

MAC Address	90:1B:0E:A7:2B:E0
Interface Speed	Auto Negotiation
Interface Port	Management LAN
Max. Transmission Unit (MTU)	1500
Bonding	<input checked="" type="checkbox"/> Enable Bonding

At the bottom right of the window are 'Apply' and 'Cancel' buttons.

Figure 24: IP bonding enabled

1. Once bonding is activated, the currently used LAN port (here: Management LAN) becomes the active port and is displayed in the Active Port field. The second LAN port (here: onboard shared LAN) becomes the backup port.
2. If the currently active port (here: Management LAN) fails ("link down"), the second port (here: onboard shared LAN) becomes active.

2.4.4 Services

On the **Services** page of the **Settings** menu you can configure several services e.g. some interfaces of the iRMC.

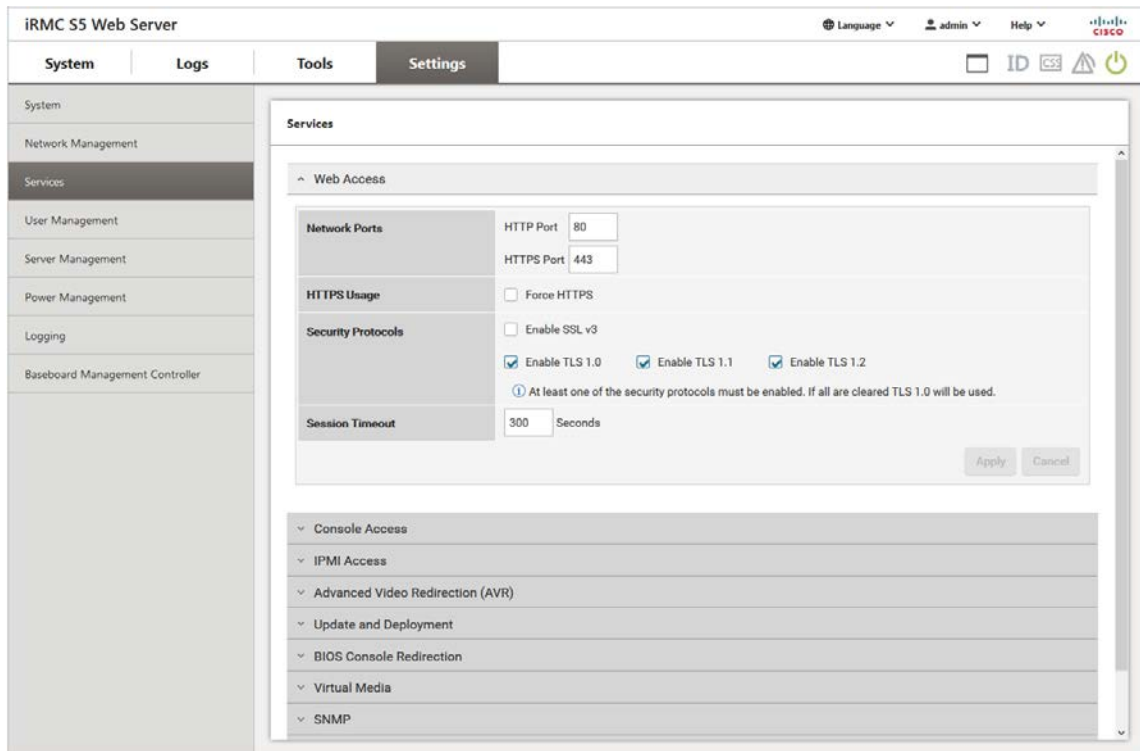


Figure 25: **Services** page

The service settings are provided in several groups.

2.4.4.1 Web Access

In this group you can view and modify the configuration settings for ports and network services.

Network Ports

In this group you select the port for the web access.

HTTP Port

HTTP port of the iRMC

Default port number: 80

Configurable: yes

Enabled by default: yes

Communication direction: inbound and outbound

HTTPS Port

HTTPS (HTTP Secure) port of the iRMC

Default port number: 443

Configurable: yes

Enabled by default: yes

Communication direction: inbound and outbound

HTTPS Usage

If you enable the **Force HTTPS** option, users can only establish a secure connection to the iRMC on the HTTPS port specified in the entry field.

If you disable the **Force HTTPS** option, users can establish a non-secure connection to the iRMC on the HTTP port specified in the entry field.

Security Protocols

In this group you specify the protocol for secure web access. If you do not select a protocol, TLS V1.0 is used.

Enable SSLv3

Allows an HTTP session via SSL V3.

-  If the SSL certificate has expired, a message to this effect is issued in the browser.

Enable TLS 1.0

Allows an HTTP session via TLS V1.0; Default

Enable TLS 1.1

Allows an HTTP session via TLS V1.1.


Enable TLS 1.2

Allows an HTTP session via TLS V1.2.

Session Timeout

Period of inactivity (in seconds) after which the session is automatically closed.

The login page of the iRMC web interface then appears, and you can log in again as required.

-  Your active session will not automatically be closed when the time specified in **Session Timeout** has elapsed.

2.4.4.2 Console Access

In this group you can view and modify the configuration settings for text based access on the managed server.

Session Drop Time

Period of inactivity (in minutes) after which a Telnet / SSH connection is automatically cleared.

Telnet

In this group you configure the text based access via Telnet.

Enable Telnet

If you enable this option, users can establish a connection to the iRMC on the Telnet port specified in the corresponding entry field.

Port

Telnet port of the iRMC

Default port number: 3172

Configurable: yes

Enabled by default: no

Communication direction: inbound and outbound

SSH

In this group you configure the text based access via SSH.

Enable SSH

If you enable this option, users can establish a connection to the iRMC on the SSH port specified in the corresponding entry field.

Port

SSH (Secure Shell) port of the iRMC

Default port number: 22

Configurable: yes

Enabled by default: yes

Communication direction: inbound and outbound

SSH Security Level

Specifies the security level for authentication via SSH if **SSH authentication mode** is set to **login using key**. The following levels are provided:

Security level	Meaning
Relaxed	A wide range of cipher suites, kexAlgorithms and data integrity (MACs) is accepted for encrypted authentication.
Intermediate	The means of encryption are restricted to a subset.
Restricted	The means of encryption are restricted to a defined set.

As a result of a setting the SSH subsystem configuration file will be modified and the SSH daemon will be restarted.

SSH Authentication Mode

Specifies the authentication method, either by password or by private key.

2.4.4.3 IPMI Access

IPMI-over-LAN is the specification of the LAN interface in the IPMI standard. This specification stipulates how IPMI messages can be sent to or from the iRMC - encapsulated in RMCP data packets. These RMCP data packets are transferred via an Ethernet LAN connection using UDP under IPv4 or IPv6.

RCMP supports the management of system statuses in systems without a running operating system.

The interface for such a connection is provided on the integrated LAN controller of the iRMC.

IPMI Over LAN

This option is enabled by default.

Allows you to disable the IPMI-over-LAN feature.

2.4.4.4 Advanced Video Redirection (AVR)

In the **Advanced Video Redirection (AVR)** group you specify various options that apply for the duration of the AVR session.

HTML5 Viewer

Specifies the medium used for video redirection:

- ▮ HTML5
- ▮ Java Applet

Both elements open a browser window containing the AVR

Active Window Title

Displays the AVR title that will be displayed in the AVR title bar.

Window Title

Title of your choice which will be displayed in the AVR title bar. The following predefined variables can be used in the AVR title:

%USER%, %BMC,_NAME%, %BMC_IP%, %CHASSIS_TYPE%, %SYSTEM_TYPE%, %SYSTEM_SERIAL%, %SYSTEM_NAME%, %SYSTEM_IP%, %SYSTEM_OS%, %ASSET_TAG%

Default Mouse Mode


Defines the default mouse mode (Absolute Mouse Mode, Relative Mouse Mode or Other Mouse Mode). For more information, refer to "[Mouse Mode](#)" on page 149.

Default: Absolute Mouse Mode

Local Monitor Off Control

The current status of the local monitor is indicated in the **AVR Video** menu and displayed via the second icon from the right on the AVR tool bar.

Enables/disables the **Local Monitor Off Control** function of the iRMC.

Option	Meaning
Enabled	Enables the Local Monitor Off Control function. In full-access mode of an AVR session, you can switch the local monitor of the server on and off from the remote workstation.
Disabled	Disables the Local Monitor Off Control function, i.e. the local monitor is always switched on and cannot be switched off.
Automatic Off when AVR is started	<p>This option only takes effect if the Local Monitor Off Control function is enabled.</p> <p>If you enable this option, the local monitor is automatically switched off for the duration of the session when an AVR session is started. After the AVR session is closed, the local monitor is automatically switched on again if no concurrent session with enabled Local Monitor Off Control is active.</p> <p> Parallel AVR sessions Even if you switch on the local monitor during your AVR session, the local monitor is automatically switched off again if a new, concurrent AVR session is started.</p> <p>The local monitor is switched on again automatically when all AVR sessions have been closed.</p>

2.4.4.5 Update and Deployment

In this group you can configure the options for the eLCM update repository. eLCM is not supported on the C880 M5 server.

2.4.4.6 BIOS Console Redirection

In the **BIOS Console Redirection** group you can configure the text console redirection. Text console redirection can also be configured in the BIOS.

Console Redirection

Enables/disables console redirection.

The operating system can also permit text console redirection irrespective of the settings in the BIOS.

Console Redirection Port

Specifies the serial port for console redirection.

Serial Port Baudrate

The following baud rates can be set: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Serial Port Flow Control

The following settings are possible:

Option	Meaning
None	Flow control is disabled.
XON/XOFF (Software)	Flow control is handled by the software.
CTS/RTS (Hardware)	Flow control is handled by the hardware.

Terminal Emulation

The following terminal emulations are available:

VT100 8Bit, ANSI 8 Bit, VT100+, UTF8

Serial 1 Multiplexer

Check the consistency of the multiplexer settings:

- Serial: System
- LAN: iRMC

2.4.4.7 Virtual Media

The Virtual Media feature provides the managed server with a “virtual” drive, which is physically located elsewhere in the network. The source for the virtual drive can be a physical drive (floppy, disk drive, CD-ROM/DVD-ROM) or an ISO image (image file).

You can make the virtual medium available as a physical drive or image file on the remote workstation. The image file may also be a network drive.

Virtual Media Options

USB Attach Mode

Attach mode of the virtual media.

The following modes are offered for selection:

Option	Meaning
Always Attach	The virtual medium is always attached to the server.
Auto Attach	The virtual medium is attached to the server only when a Virtual Media session is started.
Detach	An attached virtual medium is detached from the server.

Number of Floppy Devices

Maximum number of floppy devices that may be used in a Virtual Media session. 0 to 4 floppy devices can be configured. Default: 0.

Number of CD/DVD Devices

Maximum number of CD/DVD devices that may be used in a Virtual Media session. Up to four CD/DVD devices can be configured. Default: 2.

Number of Harddisk Devices

Maximum number of hard disk devices that may be used in a Virtual Media session. Up to four hard disk devices can be configured. Default: 1.

Remote Image Mount

Enables/disables the Remote Image Mount, which makes it possible to host CD/DVD, floppy, and hard disk ISO images on a server in the network.

Remote Image Mount**Remote Floppy Disk Devices / Remote CD/DVD Devices / Remote Harddisk Devices****Share Type**

Share type of the network share where the ISO images are located.

The following modes are offered for selection:

Option	Meaning
CIFS/SMB Common Interface File System	The share type of the network share is CIFS SMB (Common Interface File System).
NFS Network File System	The share type of the network share is NFS.

Server

IP address or DNS name of the server hosting the remote images (remote image server for short).

Share Name

Name of the network share the remote image server belongs to.

Image Name

Name of / path to the remote image.

User Name

User name required for accessing the network share.

Password

Enter the password for the user.

Confirm Password

Re-enter the password to confirm.

Domain

Domain of the user.

2.4.4.8 SNMP

In the **SNMP** group you can configure an SNMP service on the iRMC which supports SNMP v1/v2c and SNMPv3 on the following SNMP MIBs:

- SNMP MIB-2
- SNMP STATUS.MIB
- SNMP OS.MIB
- SNMP SC2.MIB

SNMP

Enables/disables the SNMP service on the iRMC S5.

When the SNMP service is enabled, information provided by these MIBs can be used by any system running an SNMP Manager. SNMPv3 provides a higher level of security than SNMPv1 or SNMPv2c.

The SNMP parameters are split into several groups.

SNMP Settings

SNMP Port

Port on which the SNMP service is listening (normally UDP 161).

SNMP Protocol

SNMP protocol version to be used. For each user, you can configure whether they are allowed to use SNMP, for more information, refer to ["Add/Edit Local User Account dialog"](#) on page 107.

Option	Meaning
All (SNMPv1/v2c/v3)	The SNMP service is available for all SNMP protocol versions (SNMP v1/v2c/v3).
SNMPv3 only	Only SNMPv3 is available.

The following two options are only displayed if **All** (SNMPv1/v2c/v3) has been selected for **SNMP Protocol**.

SNMPv1/v2c Community

Community string in the case of SNMP v1/v2c.

The community string may contain the following characters: A-Z,a-z,0-9(*/:,._?=-@&)%!

Blanks and \ are not allowed.

In SNMP terminology, a "community" denotes a group comprising one or more management platforms. Each community is identified by a community string. The community string is a non-encrypted component of every SNMP request and identifies the sender of the request as a member of the community concerned. Thus, authorization for an SNMP GET request is controlled with this community string. The community string makes a simple authentication mechanism available in SNMP.

- i Since the community string is sent in non-encrypted form with the SNMP message, it is always at risk of being used without authorization. This can be problematic for using SNMP in terms of security. On the other hand, most communities use the preset community string "public" in any case.

SNMPv1/v2c Permission

Permission for the SNMP community. The following options are possible:

Option	Meaning
ReadOnly	The user can only view the settings.

SNMP Trap Destinations

In this group you can configure the settings for SNMP trap alerting. Traps are sent regardless of whether SNMP is enabled or not. They are sent via net-snmp interface to support SNMPv1/v2c and SNMPv3 traps.

Forwarding of SNMP traps to up to seven SNMP servers is supported.

For each user, you can configure whether they are allowed to use SNMP, for more information, refer to ["Add/Edit Local User Account dialog" on page 107](#).

SNMP Community

Name of the SNMP community

SNMP User

Preconfigured SNMPv3 user for SNMPv3 trap destination

EngineID

The engineID is used for sending SNMPv3 traps. It can be changed in compliance with RFC3411. The ID needs to be unique across the set of communicating SNMPv3 Agents and Managers. The rules for an engineID are as follows:

- It must be at least five octets in length and may not be longer than 32 octets. Each octet can contain a value from 0 up to 255 (Hexadecimal: 0x00 up to 0xff).
- An SNMP Engine ID must not be set to all 0s or 255s (Hexadecimal: 0xff).
- If an engineID starts with a 0 it must be 12 octets long.
- For each engineID there must be a createUserdirective in the SNMP trap receiver configuration.

SNMP Trap Server1 to 7

DNS names or IP addresses of the servers that belong to this community and are to be configured as trap destinations together with the SNMP protocol version to be used for receiving traps.

Protocol

SNMP protocol version to be used.

Test

Traps are sent to the SNMP server for test.

Apply

Activates the SNMP server as a trap destination.

Email Alerting

The **Email Alerting** group allows you to configure the settings for email alerts.

Configuration of two mail servers is supported. Email alerting can be specified individually for each user, for more information, refer to "[Add/Edit Local User Account dialog](#)" on page 107.

2.4.4.9 Email Alerting

Enables/disables Email alerting. The options in these groups become active only, if you check this option.

SMTP Settings

SMTP Retries

Number of SMTP retries; Value range: 0 - 7

SMTP Retry Delay

Time (up to 255 in seconds) between SMTP retries

SMTP Response Timeout

Timeout (in seconds) for an SMTP response; Value range: 10 - 300

Primary SMTP Server

The **Primary SMTP Server** group allows you to configure the primary server (SMTP server).

Server Address

IP address of the mail server.

You can activate the DNS for the iRMC (for more information, refer to "[Baseboard Management Controller](#)" on page 131). You can then use a symbolic name instead of the IP address.

Network Port

SMTP port of the mail server

Auth Type

Authentication type for connecting the iRMC to the mail server:

Option	Meaning
None	No authentication for the connection.
SMTP AUTH (RFC 2554)	<p>Authentication according to RFC 2554: SMTP Service Extension for Authentication.</p> <p>In this case, the following information is required:</p> <p>Auth User Name User name for authentication on the mail server</p> <p>Auth Password Password for authentication on the mail server</p> <p>Confirm Password Confirms the password entered.</p>

Auth User Name

User name for authentication on the mail server.

Auth User Password

Password for authentication on the mail server.

Confirm Password

Confirm the password entered.

FQDN with EHLO/HELO

Enables/disables sending the FQDN with EHLO/HELO.

Secure (SSL)

Depending on the configured network port, the iRMC will either directly establish an SSL connection (SMTPS legacy port 465) or check for the presence of the STARTTLS keyword (any other configured network port):

- If STARTTLS is present in the response from the SMTP server, the iRMC switches to TLS on the existing network connection.
- If STARTTLS is not present, the mail will be sent unencrypted over the existing connection.

Email is sent SSL-encrypted.

Verify SSL Certificate

The SSL certificate from the SMTP server is verified against the stored CA certificate in the iRMC (e.g. the SMTP server certificate has to be issued/signed by this CA).

Secondary SMTP Server

The **Secondary SMTP Server** group allows you to configure the secondary server (SMTP server).

Server Address

IP address of the mail server.

You can activate the DNS for the iRMC (for more information, refer to "[Baseboard Management Controller](#)" on page 131). You can then use a symbolic name instead of the IP address.

Network Port

SMTP port of the mail server

Auth Type

Authentication type for connecting the iRMC to the mail server:

Option	Meaning
None	No authentication for the connection.
SMTP AUTH (RFC 2554)	<p>Authentication according to RFC 2554: SMTP Service Extension for Authentication.</p> <p>In this case, the following information is required:</p> <p>Auth User Name User name for authentication on the mail server</p> <p>Auth Password Password for authentication on the mail server</p> <p>Confirm Password Confirms the password entered.</p>

Auth User Name

User name for authentication on the mail server.

Auth User Password

Password for authentication on the mail server.

Confirm Password

Confirm the password entered.

FQDN with EHLO/HELO

Enables/disables sending the FQDN with EHLO/HELO.

Secure (SSL)

Depending on the configured network port, the iRMC will either directly establish an SSL connection (SMTPS legacy port 465) or check for the presence of the STARTTLS keyword (any other configured network port):

- If STARTTLS is present in the response from the SMTP server, the iRMC switches to TLS on the existing network connection.
- If STARTTLS is not present, the mail will be sent unencrypted over the existing connection.

Email is sent SSL-encrypted.

Verify SSL Certificate

The SSL certificate from the SMTP server is verified against the stored CA certificate in the iRMC (e.g. the SMTP server certificate has to be issued/signed by this CA).

Mail Format

The **Mail Format** group allows you to configure the mail-format-dependent settings. You specify the mail format for each user in the **Add/Edit User Account** dialog (for more information, refer to "[Add/Edit Local User Account dialog](#)" on page 107).

The following email formats are supported:

- Standard
- Fixed Subject
- ITS Format
- SMS Format

Some entry fields are disabled depending on the mail format.

From

Sender identification of the iRMC. Active for all mail formats.

If the string entered here contains an "@", the string is interpreted as a valid email address. Otherwise, "admin@<ip-address>" is used as the valid email address.

Subject

Fixed subject for the alert mails.

Only active for the Fixed Subject mail format.

Message

Type of message (email).

Only active for the Fixed Subject mail format.

Admin. Name

Name of the administrator responsible (optional).

Only active for the ITS mail format.

Admin. Phone

Phone number of the administrator responsible (optional).

Only active for the ITS mail format.

Country Code

Two-character country code based on ISO 3166, ISO 3166 alpha 2.

Customer Id

Identifier for the customer


Server URL

A URL under which the server is accessible under certain conditions. This must be entered manually.

Only active for the Standard mail format.

Attach Screenshot.

A screenshot generated automatically by the iRMC in the case of a critical OS stop event is attached to the corresponding 'Critical O/S Stop' event email.

-  The generation of the screenshot may fail for various reasons (e.g. unsupported graphic mode). Therefore, if no screenshot is available within 45 seconds at most, the email is sent without attachment.

2.4.4.10 AIS Connect

In this group you can configure your AIS Connect settings.

AIS Connect is not supported on the C880 M5 server.

2.4.4.11 Text console redirection

Depending on the operating system used on the managed server, you can continue to use console redirection after the BIOS / UEFI POST phase.

Requirement: The **Console Redirection** option in the **BIOS Console Redirection** group must be set to **Enhanced**, for more information, refer to "[Services](#)" on page 78.

If the managed server starts the C880 M5 ServerView Suite diagnosis software, you can operate C880 M5 ServerView Suite diagnosis using console redirection.

Linux

The settings depend on the used Linux operating system. Refer to the documentation of your operating system, and configure to output serial console to COM.

2.4.4.12 Starting AVR using Java

1. In the **Settings** menu open the **Services** page.
2. In the **Advanced Video Redirection (AVR)** group deselect the **Favor HTML5 over Java Applet**.
3. Click **Apply** to submit your changes.
4. In the title bar click to start a second 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**.

2.4.4.13 Starting AVR using HTML5

1. In the **Settings** menu open the **Services** page.
2. In the **Advanced Video Redirection (AVR)** group select the **Favor HTML5 over Java Applet**.
3. Click **Apply** to submit your changes.
4. In the title bar click to start a second AVR session.
The default browser opens with the redirection to the managed server. If there is another redirection session running, both sessions are shown in the **AVR Active Session Table**.

2.4.5 User Management

On the **User Management** page of the **Settings** menu you can configure the settings for the iRMC users and the authentication methods:

- ▮ LDAP
- ▮ CAS

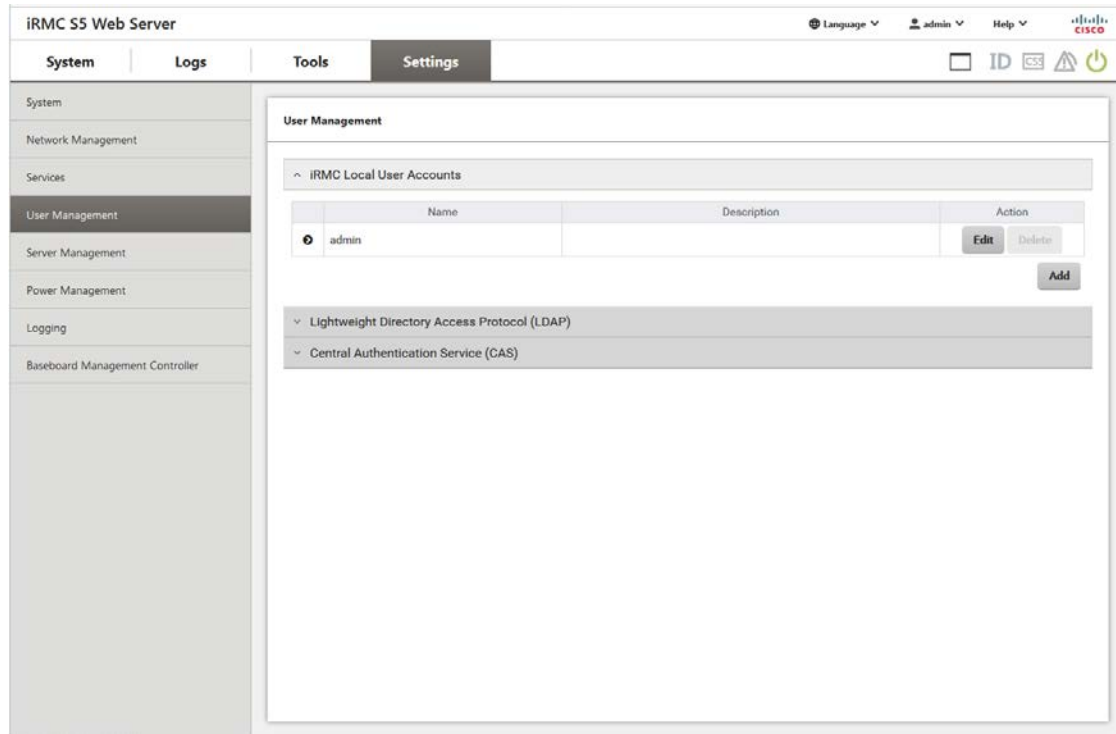



Figure 26: **User Management** page

The user settings are provided in different groups:

2.4.5.1 iRMC Local User Accounts

The **iRMC Local User Accounts** group contains a table showing all the configured users: Each line contains the data for one configured user.

Clicking  related to a user name opens a popup (for more information, refer to "[iRMC user](#)" on page 103) that displays the current settings for this user.

Edit

Opens the **Edit Local User Account** dialog where you can modify the parameters for the selected user, for more information, refer to "[Add/Edit Local User Account dialog](#)" on page 107.

Delete


Deletes the associated user after confirmation.

Add

Opens the **Add Local User Account** dialog where you can configure the parameters for a new user, for more information, refer to "[Add/Edit Local User Account dialog](#)" on page 107.

2.4.5.2 Lightweight Directory Access Protocol (LDAP)

The options in this group are only active, if you check the **Enable LDAP** option.

-  The following characters are reserved as meta characters for search strings in LDAP:
*, \, &, |, !, =, <, >, ~, : You must therefore not use these characters as components of RDNs.

Global Configuration

LDAP Support

Enables/disables authentication via LDAP for the iRMC.

If **Enable LDAP** is checked, the login information is always transferred with SSL encryption between the web browser and the iRMC (for more information, refer to ["Logging in" on page 24](#)).


LDAP SSL

Enables/disables whether the data transfer between the iRMC and the directory server is SSL-encrypted.

Enable LDAP SSL has no influence on whether or not the iRMC S5 web interface pages are SSH secured on opening.

You should only activate **LDAP SSL Enabled** if a domain controller certificate is installed.

Local Login

-  If you disable this option, all the local iRMC user identifications are locked and only the ones managed by the directory service are valid.

If **Disable Local Login** is activated and the connection to the directory service fails, it is no longer possible to log on the iRMC.

Directory Server Type

Type of directory server used. Depending on your selection, the fields of the page may change.

The following directory services are supported:

- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP
- OpenDS / OpenDJ / ApacheDS

Primary LDAP Server

LDAP directory server that is to be used.

Server

IP address or DNS name of the LDAP server

Network Port

LDAP port of the LDAP server

SSL Network Port

Secure LDAP port of the LDAP server

Backup LDAP Server

LDAP directory server which is maintained as the backup server and used as the directory server if the primary LDAP server fails.

Server

IP address or DNS name of the LDAP server

Network Port

LDAP port of the LDAP server

SSL Network Port

Secure LDAP port of the LDAP server

Directory Configuration

Depending on the selected **Directory Server Type** the irrelevant parameters are deactivated.

Authorization Type

Specifies the authorization type used. There are two possible methods:

Option	Meaning
ServerView LDAP with Authorization Settings on LDAP Server	ServerView-specific LDAP groups with authorization settings in the structure on the LDAP server are used to determine user.
Standard LDAP with Authorization Settings on iRMC	No ServerView-specific SVS structure on the LDAP server is used. Instead, user authentication is checked by means of the standard group the user belongs to. iRMC-specific user permissions for this standard LDAP group must be configured locally on the iRMC. For the Directory Service User Group Information group is displayed more information, refer to "Add/Edit LDAP User Group dialog" on page 115). This method supports group nesting. Therefore, all iRMC-specific permissions that you assign to a standard LDAP group are automatically inherited by its nested groups.

Department Name

This option is only active if the **Authorization Type** option is set to **ServerView LDAP Groups with Authorization Settings on LDAP**.

The department name is used in the directory service to determine the user permissions and alert roles. A user may have different permissions for the department X server than for the department Y server.

Domain Name

Complete DNS path name of the directory server

Base DN

Base DN is automatically derived from Domain Name.

Groups Directory as Sub-tree from Base DN

Path name of the organizational unit (OU) which, as a subtree of Base DN (Group DN Context), contains the OU SVS or iRMC groups.

User Search Context

Starting point for searching for users. A User Search Context rule is evaluated when searching for iRMC S5 users. It returns a valid LDAP distinguished name (DN), which serves as the base context for searching for users.

LDAP Group Scheme


Scheme for an LDAP group

LDAP Member Scheme

Scheme for an LDAP user

User Group Information

This group is only displayed if the **Authorization Type** option is set to **Standard LDAP Groups with Authorization Settings on iRMC**. The group displays a table with all the configured LDAP groups: Each line contains the data for one configured group.

Clicking  related to a user name opens a popup ("[LDAP user group](#)" on page [113](#)) that displays the current settings for this user.

Edit

Opens the **Edit LDAP User Group** dialog where you can modify the parameters for the selected user group, for more information, refer to "[Add/Edit LDAP User Group dialog](#)" on page [115](#).

Delete

Deletes the selected LDAP group.

Add

Opens the **Add LDAP User Group** dialog, where you can specify the parameters for a new LDAP user group with authorization settings on the iRMC, for more information, refer to "[Add/Edit LDAP User Group dialog](#)" on page [115](#).

Access Configuration

Test LDAP Access

Checks the access data to the LDAP directory server and shows the LDAP status as the result.

This test only checks the basic access data ("Is the LDAP server present?", "Is the user configured?"), but does not fully authenticate the user.

LDAP Auth Username

User name the iRMC uses to log on to the LDAP server.

LDAP Auth Password

Password the user specified under **User Name** used to authenticate themselves on the LDAP server.

Confirm Password

Repeat the password you entered under **LDAP Auth Password**.

Principal User DN

Fully distinguished name, i.e. the full description of the object path and attributes of the generic iRMC user ID (principal user), under which the iRMC queries the permissions of the iRMC users from the LDAP server.

Append Base DN to Principal User DN

If you activate this option, you do not need to specify the Base DN under **Principal User DN**. In this event, the Base DN that you specified under **Base DN** in the **Global Directory Service Configuration** group is used.

Enhanced User Login

Enhanced flexibility when users log in.

- ! Only activate this option if you are familiar with the LDAP syntax. If you inadvertently specify and activate an invalid search filter, users can only log in to the iRMC under a global login after the **Enhanced User Login** option has been deactivated.

User Login Search Filter

Contains the standard login search filter "(&(objectclass=person)(cn=%s))". At login, the placeholder %s is replaced by the associated global login. You can modify the standard filter by specifying another attribute instead of cn=. All global logins are then permitted to log in to the iRMC that meet the criteria of this search filter.

Email Alert Configuration

In this group you can configure the settings for global email alerting.

LDAP Email Alert

Enables/disables global email alerting.

LDAP Alert Table Refresh [Hours]

Defines the interval at which the email table is regularly updated.

It is strongly recommended that you specify a value >0. A value of "0" means that the table is not updated regularly.

2.4.5.3 Central Authentication Service (CAS)

The options in this group are only active, if you check the **Enable CAS** option.

The first time a user logs in to an application 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 S5 web interface as well as to any other service within the SSO domain without being prompted for login credentials again.

- i** SSO is only supported for accessing the iRMC via the web interface, and not via the Remote Manager (Telnet/SSH).

CAS Support

Enables/disables SSO using the CAS service.

The options to configure a CAS connection are divided into several groups.

CAS Server

Server

DNS name of the CAS service.

- i** It is absolutely necessary that all systems participating in the SSO domain reference the CMS via the same address representation. (An SSO Domain comprises all systems where authentication is performed using the same CAS service.) Thus, for example, if you have installed the ServerView Operations Manager using the name "my-cms.my-domain", you must specify exactly the same name for configuring the CAS service for an iRMC S5. If instead you specify only "my-cms" or another IP address of my-cms, SSO will not be enabled between the two systems.

Network Port

Port of the CAS service.

Default port number: 3170

SSL/HTTPS

Enables or disables whether all communication between the CAS service and the iRMC is SSL-encrypted.

SSL Certificate Verification

The SSL Certificate of the CAS service is checked against the CA Certificate.

Login Page Display

- i** If the **Always Display Login Page** option is not checked and the CAS service cannot be reached, type /login after the IP address of the iRMC in your browser's navigation bar.

Allows users to temporarily log in to the iRMC with privileges and permissions that differ from the authorization profile defined in the **CAS User Privilege and Permissions** group.

A user may, for instance, currently be logged in to the CAS service under a user ID with the **User** privilege and now wants to perform an action requiring the **Administrator** privilege. The user can temporarily log in to the iRMC S5 under a user ID with the required privileges. However, they cannot switch between both user IDs.

The buttons **iRMC Login** and **CAS Login** work as follows:

Butto	Meaning
iRMC S5 Login	Logs the user in to the iRMC web interface with the values specified for User name and Password . The CAS service is bypassed.
CAS Login	Logs the user in to the iRMC web interface via SSO: <ul style="list-style-type: none"> ▫ If the user has not been authenticated by the CAS service yet: The user is redirected to the CAS service for authentication with the specified values for User name and Password. ▫ If the user has already been authenticated by the CAS service: The user is logged in to the iRMC S5 without being prompted for user name and password.

Login URL

Login URL of the CAS service

Logout URL

Logout URL of the CAS service

Validate URL

Validate URL of the CAS service

Assign Permissions from

Defines the iRMC privilege and permissions for users who are logged in to the iRMC via SSO:

Option	Meaning
Local assigned permissions	The privilege and permissions defined under CAS User Privilege and Permissions apply to the user.
Permissions retrieved via LDAP	Only available if LDAP is enabled: The authorization profile defined in the LDAP directory service applies to the user.

User Access Configuration

The **User Access Configuration** group allows you to define the iRMC privileges and permissions a user is granted if they are logged in to the iRMC via SSO.

Privilege Level

Assigns an IPMI privilege group to the user:

- User
- Operator
- Administrator
- OEM

As well as the IPMI-specific permissions, you can also assign the following channel-independent permissions to individual users.

User Account Configuration

Enables/disables the permission to configure local user access data via IPMI.

iRMC Settings Configuration

Enables/disables the permission to configure the iRMC S5 settings via IPMI.

Video Redirection Usage

Enables/disables the permission to use Advanced Video Redirection (AVR) in “View Only” and “Full Control” mode.

Remote Storage Usage

Enables/disables the permission to use the Virtual Media functions.

2.4.5.4 iRMC user

User details popup

The **User details** popup displays the settings for a selected user.

User Information	
Enabled	✓
Name	admin
Description	
Role	
Access Configuration	
IPMI Enabled	—
LAN Channel Privilege	Oem
Serial Channel Privilege	Oem
Configure User Accounts	✓
Configure iRMC Settings	✓
Video Redirection Enabled	✓
Remote Storage Enabled	✓
User Shell (Text Access)	RemoteManager
SNMP Configuration	
SNMP Enabled	—
Access privilege	ReadOnly
Authentication	SHA1
Privacy	AES
Email Configuration	
Email enabled	—
Encrypted	—
Mail Format	Standard
Preferred Mail Server	Auto
Email Address	

Figure 27: User details popup

User Information

The **User Information** group displays the access data for the user.

Enabled

Displays the access status to the Redfish service. When this option is disabled, a user does not have access to the iRMC via the Redfish protocol or the web interface.

Name

Name of the local iRMC user account

Description

General description of the user account

Role

Displays the user group the user account is related to. For more information, refer to ["Required user permissions" on page 15](#).

Access Configuration

The **Access Configuration** group displays the channel-specific user privileges.

IPMI Enabled

If this option is disabled, the user will not be able to log on to the iRMC.

LAN Channel Privilege

Displays the privilege group for a LAN channel the user is allowed to use

- User
- Operator
- Administrator
- OEM

Serial Channel Privilege

Displays the privilege group for a serial channel the user is allowed to use. The same privilege groups are available as for LAN Channel Privilege.

Configure User Accounts

Displays the permission to configure local user access data.

Configure iRMC Settings

Displays the permission to configure the iRMC settings.

Video Redirection Enabled

Displays the permission to use AVR in "View Only" and "Full Control" mode.

Remote Storage Enabled

Permission to use the Remote Storage functionality.

User Shell (Text Access)

Displays the configured user shell. The following options are available:

Option	Meaning
Remote Manager	Starts a Telnet/SSH session.
None	Nothing happens.

SNMP Configuration

The **SNMP Configuration** group displays the SNMP settings for the iRMC S5 user.

SNMP Enabled

Displays if SNMP support is enabled for the user.

Access privilege

Access privilege of the user.

Authentication

Displays the authentication protocol that SNMP uses for authentication.

Option	Meaning
SHA1	Secure hash algorithm is used for authentication.
MD5	Message-Digest Algorithm 5 is used for authentication.

Privacy

Displays the privacy protocol that SNMPv3 uses for encrypting the SNMPv3 traffic.

Optio	Meaning
DES	Digital Encryption Standard is used for encrypting the SNMPv3 traffic.
AES	Advanced Encryption Standard 128-bit encryption is used for encrypting the SNMPv3 traffic.
None	No encryption is used for SNMPv3 traffic.

Email Configuration

The **Email Configuration** group allows you to configure the user-specific settings governing the email format.

Email enabled

Displays whether the user is to be informed about system statuses by email.

Encrypted

Displays whether emails should be encrypted with S/MIME.

Mail Format

The following email formats are available:

- Standard
- Fixed Subject
- ITS Format
- SMS Format

- i** As SMS format only generates emails with up to 160 characters, it is the preferred email format to the SMS gateway solution.

Preferred Mail Server

Select the preferred mail server.

You can choose one of the following options:

Option	Meaning
Automatic	If the email cannot be sent immediately, e.g. because the preferred mail server is not available, the email is sent to the second mail server.
Primary	Only the mail server which has been configured as the primary SMTP server is used as the preferred mail server.
Secondary	Only the mail server which has been configured as the secondary SMTP server is used as the preferred mail server.

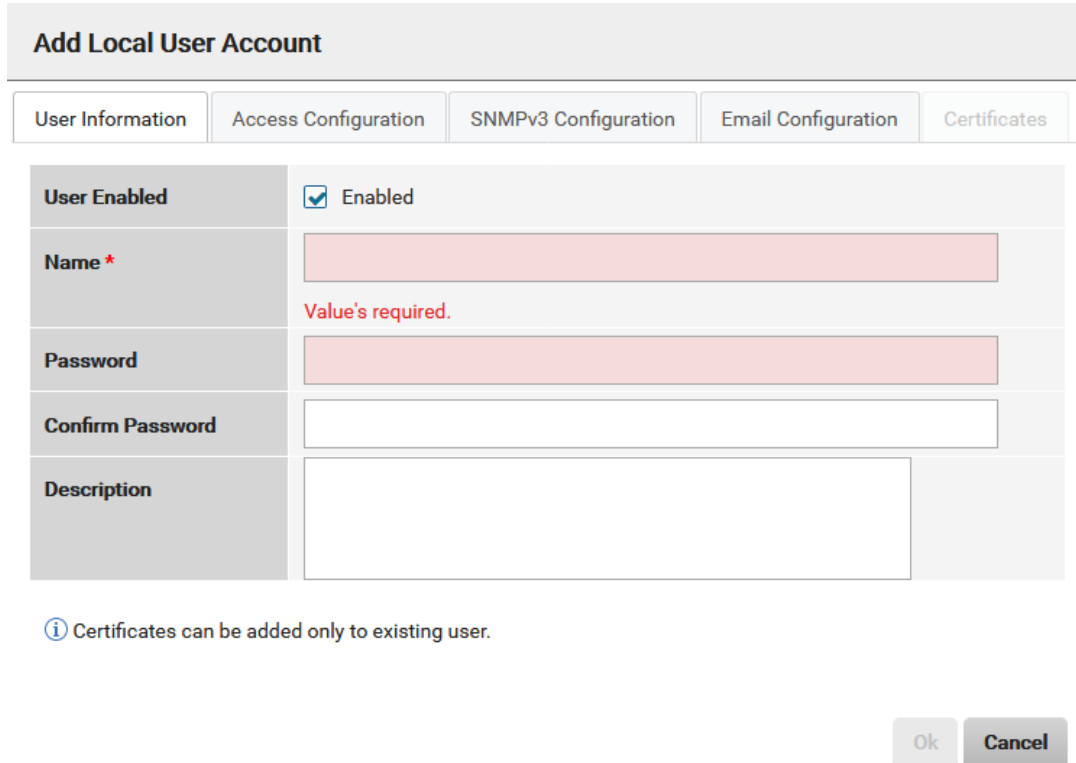
- i** Errors sending email are recorded in the event log.

Email Address

Email address of recipient

Add/Edit Local User Account dialog

With the parameters in the **Add Local User Account** or **Edit Local User Account** dialogs you configure the basic settings for a new iRMC user.



Add Local User Account

User Information Access Configuration SNMPv3 Configuration Email Configuration Certificates

User Enabled Enabled

Name *
Value's required.

Password

Confirm Password

Description

i Certificates can be added only to existing user.

Ok Cancel

Figure 28: **Add New User Account** dialog

The relevant parameters are grouped on several tabs.

User Information tab

In this tab you specify the general parameters for the user account.

User Enabled

Name

User names must be unique. Duplicate user names are not allowed.

A valid user name must start with a letter. The remaining part of the name may only contain letters, digits, underscores, dashes, periods and "at" signs (@).

Blanks are not allowed.

Password

User password. If SNMPv3 is used, the password configured for this user must have at least eight characters.

Enabling SNMPv3 for the user requires the password configured for the user to have at least eight characters.

Confirm Password

Confirm the password by entering it again here.

Description

Enter a general description of the configured user here.

Access Configuration tab

The Access Configuration tab allows you to configure the channel-specific user privileges.

Redfish/WebUI Permissions tab**Redfish/Web UI User**

Enables/disables the privilege to use the Redfish protocol and the web interface of the iRMC S5.

Redfish Role

Assigns a privilege group for using the Redfish protocol and the web interface. For more information, refer to "[Required user permissions](#)" on page 15. The following privilege groups are provided:

- Administrator
- Operator
- ReadOnly

IPMI Privileges tab**LAN Channel Privilege**

Assigns a privilege group for a LAN channel via IPMI to the user.

- User
- Operator
- Administrator
- OEM

Serial Channel Privilege

Assigns a privilege group for a serial channel via IPMI to the user. The same privilege groups are available as for LAN Channel Privilege.

Configure User Accounts

Enables/disables the permission to configure local user access data via IPMI.

Configure iRMC Settings

Enables/disables the permission to configure the iRMC settings via IPMI.

AVR Permissions tab**Video Redirection**

Enables/disables the permission to use AVR in “View Only” and “Full Control” mode.

Remote Storage

Enables/disables the permission to use the Remote Storage functionality.

Other tab**User Shell (Text Access)**

Specifies the shell the user is allowed to use. The following options are available:

Option	Meaning
Remote Manager	Starts a Telnet/SSH session.
None	No shell usage is allowed

SNMPv3 Configuration tab

On the **SNMPv3 Configuration** tab you configure the iRMC S5 user for SNMPv3. The parameters are disabled (grayed out) if the **Enabled** option for **SNMPv3** is disabled (not checked) for more information, refer to "[Services](#)" on page 78.

SNMPv3

Enables/disables SNMPv3 support for the user.

Access privilege

Specifies the access privilege of the user. The following values are possible:

Option	Meaning
ReadOnly	The user can only view the settings.

Authentication

Specifies the authentication protocol that SNMPv3 uses for authentication.

Option	Meaning
SHA	Secure hash algorithm is used for authentication.
MD5	Message-Digest Algorithm 5 is used for authentication.
None	No authentication is used for SNMP.

Privacy

Specifies the privacy protocol that SNMPv3 uses for encrypting the SNMPv3 traffic.

Optio	Meaning
DES	Digital Encryption Standard is used for encrypting the SNMPv3 traffic.
AES	Advanced Encryption Standard 128-bit encryption is used for encrypting the SNMPv3 traffic.
None	No encryption is used for SNMPv3 traffic.

Email Configuration tab

This tab contains two sub tabs for the Email parameters.

General

The **General** tab allows you to configure the user-specific settings governing the email format.

Email Alerts

Enables/disables whether the user is to be informed about system statuses by email.


Encryption

Enables/disables whether emails should be encrypted with S/MIME.

Mail Format

Specifies the mail format. The following email formats are available:


- Standard
- Fixed Subject
- ITS Format
- SMS Format

 As SMS format only generates emails with up to 160 characters, it is the preferred email format to the SMS gateway solution.

Preferred Mail Server

Specifies the preferred mail server. You can choose one of the following:

Option	Meaning
Automatic	If the email cannot be sent immediately, e.g. because the preferred mail server is not available, the email is sent to the second mail server.
Primary	Only the mail server which has been configured as the primary SMTP server is used as the preferred mail server.
Secondary	Only the mail server which has been configured as the secondary SMTP server is used as the preferred mail server.

-  Errors sending email are recorded in the event log.

Email Address

Email address of recipient

Alert Levels

This tab is only active, if you have enabled **Email Alerts**.

On this tab you specify for each of the following components the severity level for which an Email alert is sent: Fan Sensors, Temperature Sensors, Critical Hardware Errors, System Hang, POST Errors, Security, System Status, Disk Drivers & Controllers, Network Interface, Remote Management, System Power, Memory, and Others.

For each event type, the following options are available:

Option	Meaning
None	No Email is sent.
Critical	Only events with status Critical are sent.
Warning	Only events with status Critical or Warning are sent.
All	All events are sent.

Certificates tab

On this tab you can upload an SSHv2 public key or an S/MIME certificate from a local file.

SSHv2 public key

With the buttons you can upload a user SSHv2 public key from a local file.

Fingerprint

Select

Opens a file browser for navigating to the file containing the SSHv2 public key.

Upload

Loads the SSHv2 public key specified in the input field onto the iRMC.

Delete

Removes the selected file to be uploaded.

SMIME certificate

With the buttons you can upload an S/MIME certificate from a local file.

Issuer

Subject

Select

Opens a file browser for navigating to the file containing the S/MIME certificate.

Upload

Loads the S/MIME certificate specified in the input field onto the iRMC.

Delete

Removes the selected file to be uploaded.

2.4.5.5 LDAP user group

LDAP User Group details popup

The **LDAP User Group details** popup displays the settings for a selected user group.

Access Configuration	
User Shell (Text Access)	RemoteManager
Lan Channel Privilege	User
Serial Channel Privilege	User
Configure User Accounts	—
Configure iRMC Settings	—
Video Redirection Enabled	—
Remote Storage Enabled	—
Redfish Roles	
Admin	—
Operator	—
ReadOnly	—
Email Configuration	
Email enabled	—
Mail Format	UserDefined
Preferred Mail Server	Auto

Figure 29: LDAP User Group details popup

Access Configuration

The **Access Configurations** tab displays the channel-specific user privileges via the IPMI interface.

User Shell (Text Access)

Displays the set user shell.

The following options are available:

Option	Meaning
Remote Manager	Opens a Telnet/SSH session to the Remote Manager.
None	Nothing happens.

LAN Channel Privilege

Displays the set privilege group for a LAN channel via IPMI of the user:

- User
- Operator
- Administrator
- OEM

Serial Channel Privilege

Displays the set privilege group for a serial channel via IPMI of the user. The same privilege groups are available as for LAN Channel Privilege.

Configure User Accounts

Displays the set permission to configure local user access data via IPMI.

Configure iRMC Settings

Displays the set permission to configure the iRMC settings via IPMI.

Video Redirection Enabled

Displays the set permission to use AVR in "View Only" and "Full Control" mode.

Remote Storage Enabled

Displays the set permission to use the Virtual Media functions.

Redfish Roles

This group displays the role assigned to the LDAP user group for using the Redfish protocol and the web interface. For more information on Redfish privileges, refer to ["Required user permissions" on page 15](#).

Admin

Displays whether the Administrator privilege is assigned.

Operator

Displays whether the operator privilege is assigned.

ReadOnly

Displays whether the ReadOnly privilege is assigned.

Email Configuration

The **Email Configuration for LDAP User Group** group allows you to configure the user- specific settings governing the email format.

Email Enabled

Displays whether the user is to be informed about system statuses by email.

Mail Format

Displays the selected email format, you can make a number of settings in the **Email Alerting - Mail Format dependent Configuration** group.

The following email formats are available:


- Standard
- Fixed Subject
- ITS Format
- SMS Format

Preferred Mail Server

Displays the preferred mail server.

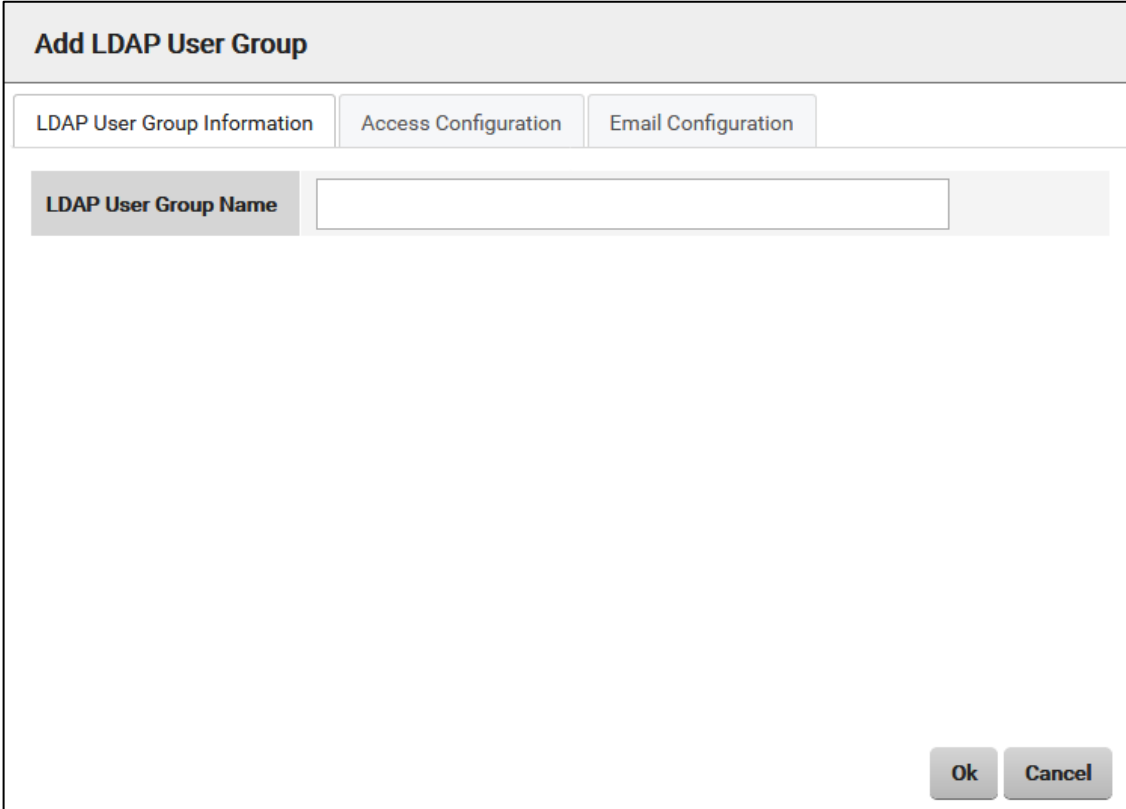
You can choose one of the following options:

Option	Meaning
Automatic	If the email cannot be sent immediately, e.g. because the preferred mail server is not available, the email is sent to the second mail server.
Primary	Only the mail server which has been configured as the primary SMTP server is used as the preferred mail server.
Secondary	Only the mail server which has been configured as the secondary SMTP server is used as the preferred mail server.

 Errors sending email are recorded in the event log.

Add/Edit LDAP User Group dialog

With the parameters in the **Add LDAP User Group** or **Edit LDAP User Group** dialogs you configure the settings for a new or existing LDAP group administered on the iRMC. These LDAP groups are used to define iRMC privileges and permissions for users who belong to standard LDAP groups on the directory server.



The screenshot shows a dialog box titled "Add LDAP User Group". It features three tabs: "LDAP User Group Information", "Access Configuration", and "Email Configuration". The "LDAP User Group Information" tab is selected and active, displaying a text input field with the label "LDAP User Group Name". At the bottom right of the dialog, there are two buttons: "Ok" and "Cancel".

Figure 30: **Add LDAP User Group** dialog

The options in this dialog are grouped on several tabs.

LDAP User Group Information tab**LDAP User Group Name**

Name of the new LDAP user group

Access Configuration tab

On the **Access Configurations** tab you can configure the user privileges for several access modes.

User Shell (Text Access)

Specifies the shell the user is allowed to use. The following options are available:

Option	Meaning
Remote Manager	Starts a Telnet/SSH session.
None	No shell usage is allowed

LAN Channel Privilege

Assigns a privilege group for a LAN channel to the user.

- User
- Operator
- Administrator
- OEM

Serial Channel Privilege

Assigns a privilege group for a serial channel to the user. The same privilege groups are available as for LAN Channel Privilege.

Configure User Accounts

Enables/disables the permission to configure local user access data.

Configure iRMC Settings

Enables/disables the permission to configure the iRMC settings.

Video Redirection

Enables/disables the permission to use AVR in “View Only” and “Full Control” mode.

Remote Storage

Enables/disables the permission to use the Remote Storage functionality.

Redfish Admin Role

Assigns the admin privilege to the LDAP user group for using the Redfish protocol.

Redfish Operator Role

Assigns the operator privilege to the LDAP user group for using the Redfish protocol.

Redfish ReadOnly Role

Assigns the read only privilege to the LDAP user group for using the Redfish protocol.

Email Configuration tab

On this tab you configure the settings of alarms send via Email. The options are grouped on two tabs.

General

Email Alerts

Enables/disables whether the user is to be informed about system statuses by email.

Mail Format

Specifies the mail format. The following email formats are available:

- Standard
- Fixed Subject
- ITS Format
- SMS Format

i As SMS format only generates emails with up to 160 characters, it is the preferred email format to the SMS gateway solution.

Preferred Mail Server

Specifies the preferred mail server. You can choose one of the following:

Option	Meaning
Automatic	If the email cannot be sent immediately, e.g. because the preferred mail server is not available, the email is sent to the second mail server.
Primary	Only the mail server which has been configured as the primary SMTP server is used as the preferred mail server.
Secondary	Only the mail server which has been configured as the secondary SMTP server is used as the preferred mail server.

i Errors sending email are recorded in the event log.

Paging Severity Configuration

On this tab you specify for each of the following components the severity level for which an Email alert is sent: Fan Sensors, Temperature Sensors, Critical Hardware Errors, System Hang, POST Errors, Security, System Status, Disk Drivers & Controllers, Network Interface, Remote Management, System Power, Memory, and Others.

The following settings are available for each event group:

Option	Meaning
None	The notification function is deactivated for this paging group.
Critical	The iRMC notifies users by email if an entry in the system event log is reported as CRITICAL.
Warning	The iRMC notifies users by email if an entry in the system event log is reported as Minor , Major or Critical .
All	The iRMC notifies users of every event in this group that causes an entry to be made in the system event log.

2.4.6 Server Management

On the **Server Management** page of the **Settings** menu you can configure several settings of the server.

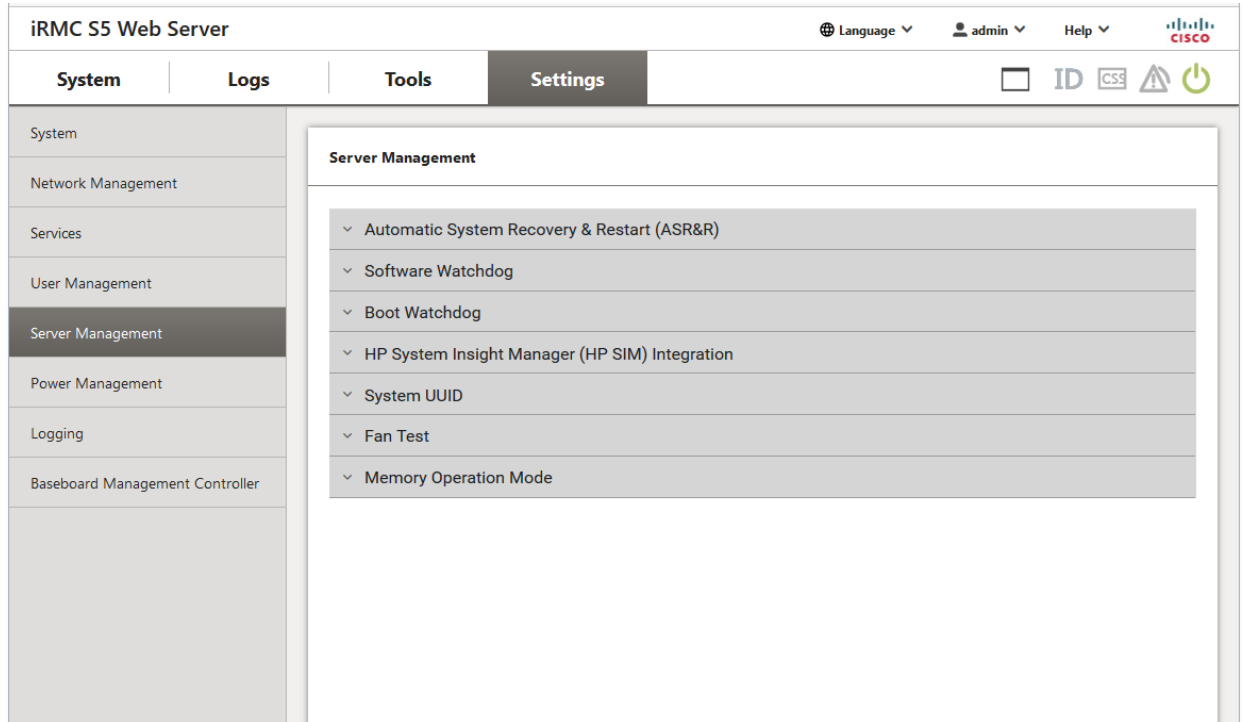


Figure 31: **Server Management** page

The server management settings are provided in several groups.

2.4.6.1 Automatic System Recovery & Restart (ASR&R)

In this group you can configure the ASR&R settings for the managed server.

Boot Delay

Delay time (in minutes) before the server restarts; Value range: 1 - 30 minutes

Retry Counter Max

Maximum number of restart attempts to be permitted for the server after a critical error; Value range: 0 - 7

Retry Counter

Number of restart attempts that a server should make after a critical error;
Value range: 0 - **Retry counter Max**

Power Cycle Delay

Time (in seconds) between powering down and powering up during a power cycle;
Value range: 7 - 15

BIOS Recovery Flash

Enables/disables the BIOS recovery flash bit:

Bit value	Meaning
Enabled	<p>The next time the system is booted, the BIOS is automatically flashed.</p> <p>The Enabled setting is of value if the operating system no longer boots after the firmware has been updated. A BIOS recovery flash is then performed automatically the next time the system is booted from the DOS floppy (or a DOS floppy image).</p> <p>After a BIOS recovery flash has been performed successfully, reset the BIOS Recovery Flash bit to disabled.</p>
Disabled	The next time the system is booted, the BIOS is not automatically flashed.

Power On on Critical Temperature

If enabled, prevents the server from being powered on if the temperature reaches a critical value.

2.4.6.2 Software Watchdog

The software watchdog monitors the activities of systems.

The software watchdog is not supported on the C880 M5 server.

Must not set 'Software Watchdog' to "Enable".

Software Watchdog Support

Enables/disables the options defined for the software watchdog.

The software watchdog is not supported on the C880 M5 server.

Must not set 'Software Watchdog' to "Enable".

Waiting Time

Time (in minutes) after which the selected behavior is to be performed following a

Timeout Delay; value range: 1 - 100

Watchdog Action

List of actions to be performed if no connection is established. The following actions are possible:

Action	Meaning
Continue	No action is performed when the watchdog expires, i.e. the server continues to run. An entry is made in the event log.
Reset	The server management software triggers a system reset.
Power Cycle	The server is powered down and immediately powered up again.

2.4.6.3 Boot Watchdog

The boot watchdog monitors the phase for start-up of the system.

The boot watchdog is not supported on the C880 M5 server.

Must not set 'Boot Watchdog' to "Enable".

Boot Watchdog Support

Enables/disables the options defined for the boot watchdog.


The boot watchdog is not supported on the C880 M5 server.

Must not set 'Boot Watchdog' to "Enable".

Waiting Time

Time (in minutes) after which the selected behavior is to be performed following a

Timeout Delay; value range: 1 - 100

-  The boot watchdog must wait until the system has been started. You must therefore specify a sufficient period for a timeout delay (1 - 100).

Watchdog Action

List of actions to be performed if no connection is established. The following actions are possible:

Action	Meaning
Continue	No action is performed when the watchdog expires, i.e. the server continues to run. An entry is made in the event log.
Reset	The server management software triggers a system reset.
Power Cycle	The server is powered down and immediately powered up again.

2.4.6.4 HP System Insight Manager (HP SIM) Integration

In this group you enable or disable HP SIM integration.

The HP SIM Integration is not supported on the C880 M5 server.

HP SIM Integration

Enables/disables HP SIM integration. This function is available after a reboot of the iRMC.

The HP SIM Integration is not supported on the C880 M5 server.

2.4.6.5 System UUID

In this group you can configure the format in which the S5 device will return UUID information.

Get System UUID Response Format

Format in which the iRMC device will return UUID information.

Option	Meaning
IPMI Specification compatible	System GUID Response Format is compatible with the IPMI Specification.
SMBIOS 2.6 Specification compatible	System GUID Response Format is compatible with the SMBIOS Reference Specification.

2.4.6.6 Fan Test

The **Fan Test** group allows you to specify a time of day when the fan test is started automatically.

Daily Fan Test

Enables/disables the daily fan test. The iRMC performs the fan test at a speed similar to the currently required speed and therefore cannot be heard.

Fan Check Time

Time at which the fan test is to be started automatically for all fans of the managed server.

2.4.6.7 Memory Operation Mode

The **Memory Operation Mode** group allows you to specify the modes of main memory modules in the managed C880 M5 server. For details, more information, refer to the "Cisco C880 M5 Installation Manual".

- i** **Apply** saves your settings to the persistent memory of the iRMC. Your settings are therefore available:
- After the next system reboot if the server is powered on.
 - After the next system power on if the server is powered off.

Memory Mode

Specifies the mode of main memory modules in the managed C880 M5 server. The following modes are offered for selection:

Option	Meaning
Normal	The setting is Normal.
Full Mirror	The setting is Full Mirror.
Address Range Mirror	The setting is Address Range Mirror.
Spare	The setting is Spare.

Lockstep Mode

Enables/disables Lockstep Mode.

Memory Mirror RAS Mode

Specifies the action after memory error in Full Mirror mode.

This setting is only available with Full Mirror mode.

The following modes are offered for selection:

Option	Meaning
Capacity Keep	The setting is Capacity Keep.
Mirror Keep	The setting is Mirror Keep.

Memory Sparing Mode

Specifies the size of spare memory in Spare mode.

This setting is only available with Spare mode.

The following modes are offered for selection:

Option	Meaning
1RANK	1RANK is used for spare memory.
Auto	Possible RANK is used for spare memory.

2.4.7 Power Management

On the **Power Management** page in the **Settings** menu you can specify the mode the iRMC S5 uses to control the power consumption of the managed server.

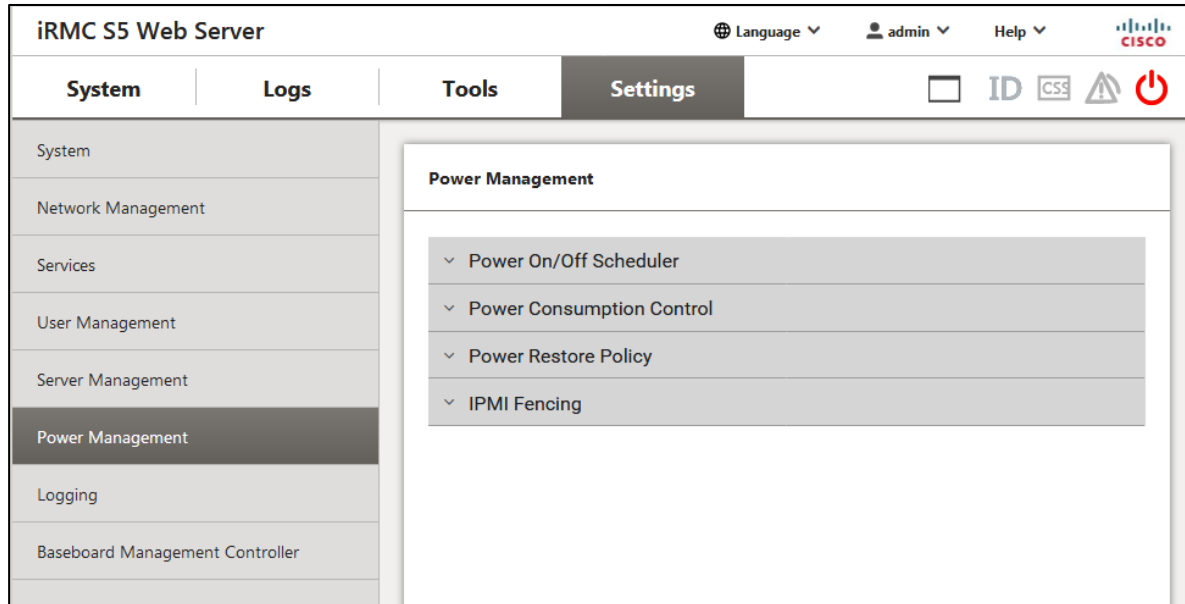


Figure 32: **Power Management** page

The power management settings are provided in several groups.

2.4.7.1 Power On/Off Scheduler

In the **Power On/Off Scheduler** group you can specify the times when the server is powered on/off for the individual days of the week or for specified times during the day.

SNMP Trap Premonition Time

Specifies, whether the iRMC sends an SNMP trap to the management console before a planned power on/off of the managed server and, if so, how many minutes before the event this should be done. No traps are sent if you specify the value "0".

2.4.7.2 Power Consumption Control

In this group you select the power control mode and specify whether the power consumption should be monitored over time.

Requirements:

The following requirements must be met in order to configure power consumption control:

- ▮ The **Enhanced SpeedStep** option must be Enabled in the **CPU Configuration** menu of the BIOS setup.
- ▮ The **Power Technology** option must be Custom in the **CPU Configuration** menu of the BIOS setup.
- ▮ The **HWPM Support** option must be Disabled in the **CPU Configuration** menu of the BIOS setup.

Power Monitoring

Enables/disables the monitoring of power consumption over time.

Power Control Mode

Mode for controlling the power consumption of the managed server:

Option	Meaning
O/S Controlled	The iRMC controls the server to achieve the best performance. In this case, power consumption is not always ideal. All other options in this group are deactivated.
Minimum Power	The iRMC controls the server to achieve the lowest possible power consumption. In this case, performance is not always ideal.
Scheduled	The iRMC uses the values specified for Scheduled Power Consumption Configuration to control power consumption.
Power limit	The iRMC uses the Power Limit to control power consumption.

Dynamic Power Control

The power limit is controlled dynamically. If this option is enabled, the iRMC lowers the server's power consumption as soon as the **Power Limit** is exceeded. The iRMC attempts to adjust power consumption to the level specified in the **Target for Power Regulation** field.

Power Limit

Maximum power consumption (in watts).

When this is reached, the action defined in the **Action Reaching Power Limit** field is performed. When the threshold is exceeded, a warning message is written to the iRMC SEL (CPU Throttling activated by Power Capping).

Target for Power Regulation

The iRMC attempts to adjust the power consumption to this value, which is to be specified as a percentage of the maximum power consumption specified in the **Power Limit** field.

Tolerance Time Before Action

Time period (in minutes) the **Power Limit** has to be exceeded before the action specified in the **Action Reaching Power Limit** field is performed.

Action Reaching Power Limit

Action to be performed when the **Power Limit** has been exceeded for at least the time specified in the **Tolerance Time Before Action** field.

Option	Meaning
Continue	No action is performed.
Graceful Power Off (Shutdown)	Shuts down the system "gracefully" and powers it down. This option is not supported on the C880 M5 server.
Immediate Power Off	The server is immediately powered down irrespective of the status of the operating system.

Scheduled Power Consumption Configuration

These parameters allow you to specify in detail the schedules and modes that the iRMC uses to control power consumption on the managed server.

- i Configuration for scheduled power control mode assumes that the **Enhanced Speed Step** option is enabled in the BIOS setup. If this is not the case, a message is displayed.

If this message appears even though **Enhanced Speed Step** is enabled, this may be because:

- The CPU (e.g. low-power CPU) of the server does not support scheduled power control.
- The system is currently in the BIOS POST phase.

Time 1

Time [hh:mm] when the iRMC starts power control as defined in **Mode 1** on the relevant day of the week.

Set Time 1 < Time 2, otherwise the power control mode specified in the **Mode 2** field will only be activated at **Time 2** on the relevant day of the following week.

Mode 1

Power consumption mode used by the iRMC for power control as of **Time 1** on the relevant day of the week.

Option	Meaning
Disabled	The iRMC does not control power consumption.
O/S Controlled	The iRMC controls the server to achieve the best performance. In this case, power consumption is not always ideal. All other options in this group are deactivated.
Minimum Power	The iRMC controls the server to achieve the lowest possible power consumption. In this case, performance is not always ideal.
Power Limit	The iRMC uses the Power Limit to control power consumption.

Time 2

Time [hh:mm] when the iRMC starts power control as defined in **Mode 2** on the relevant day of the week.

Mode 2

Power consumption mode used by the iRMC for power control as of **Time 2** on the relevant day of the week.

 Specifications in the **Everyday** field take priority.

2.4.7.3 Power Restore Policy

The **Power Restore Policy** group allows you to specify the server's power management behavior after a power outage.

The **Power Restore Policy** options have the following meanings:

Options	Meaning
Always power off	The server always remains powered off after a power outage.
Always power on	The server is always powered up again after a power outage.
Restore to powered state prior to power loss	The power up/down status of the server is restored to the status prior to the power outage.

2.4.7.4 IPMI Fencing

The option in this group shuts down a server if it is isolated or shared resources are protected from a malfunctioning server within a high availability environment. The fencing process locates the malfunctioning server and disables it.

Enable Emergency System Power off handling for Power Control

Enables/disables a shutdown of the managed server by IPMI power fencing. No backup fencing methods are used.

2.4.8 Logging

In the groups on the **Logging** page of the **Settings** menu you specify the settings for the logging functions of the iRMC.

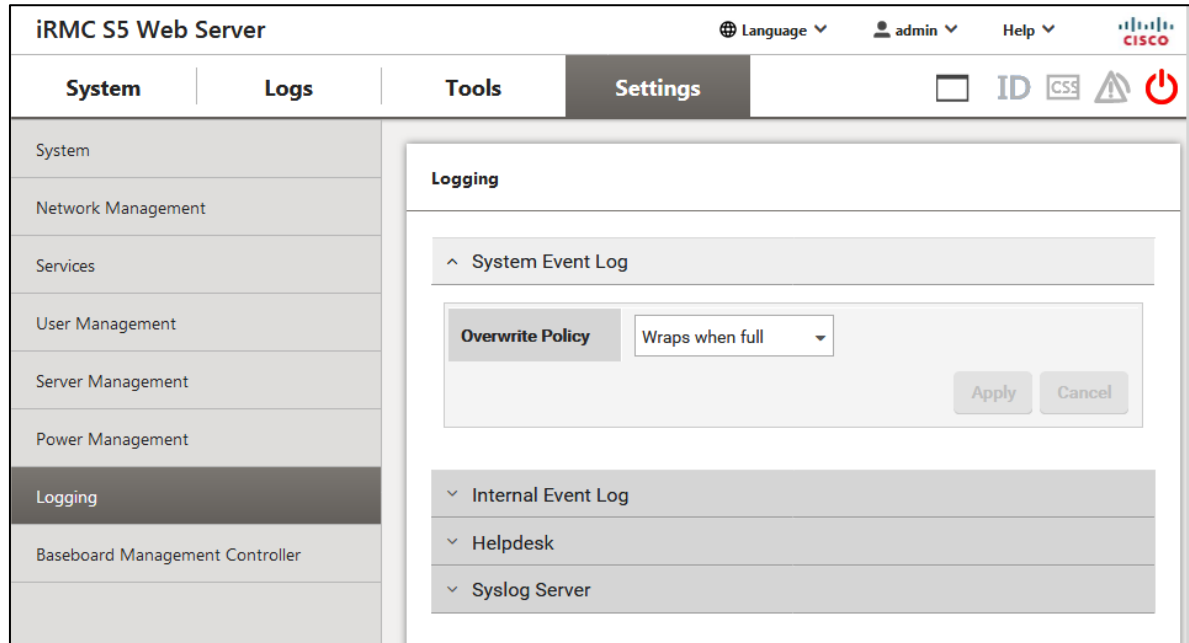


Figure 33: **Logging** page

The logging settings are provided in the following groups:

2.4.8.1 System Event Log

In this group you specify how the system event log is organized. There can be up to 455 entries in the system event log.

Overwrite Policy

Specifies the action the iRMC performs, when the log is full:

Value	Meaning
Wraps when full	The event log is organized as a ring buffer. Once the event log is full, the iRMC overwrites the oldest entries.
Never overwrite	The event log is organized as a linear buffer. Once the event log is full, the iRMC cannot add any further entries. You have to clear the log manually to add further entries.

2.4.8.2 Internal Event Log

In this group you specify how the internal event log is organized. There can be up to 455 entries in the internal event log.

Overwrite Policy

Specifies the action the iRMC performs, when the log is full:

Value	Meaning
Wraps when full	The event log is organized as a ring buffer. Once the event log is full, the iRMC overwrites the oldest entries.
Never overwrite	The event log is organized as a linear buffer. Once the event log is full, the iRMC cannot add any further entries. You have to clear the log manually to add further entries.

2.4.8.3 Helpdesk

Helpdesk Information

String used to display the Help Desk.

2.4.8.4 Syslog Server

In this group you can configure syslog forwarding, which forwards the events (entries) of SEL and/or the internal event log to dedicated syslog servers.

Event Forwarding

Enables/disables the forwarding of the events of SEL and/or the internal event log to up to three syslog servers configured below.

System Messages Forwarding

Enables/disables the forwarding of the messages of SEL and/or the internal event log to up to three syslog servers configured below.

Server 1, 2, 3

You can specify up to three servers for syslog forwarding using the following parameters.

Server Address

IP address or DNS name of the respective syslog server.

Server Port

Input port where syslog server 1 / 2 / 3 receives the forwarded events.

Protocol

Protocol (TCP or UDP) used for transferring the events to the corresponding syslog server.

Internal Event log (IEL)

Enables/disables the forwarding of the events of the internal event log to the corresponding syslog server.

System Event Log (SEL)

Enables/disables the forwarding of the events of the system event log (SEL) to the corresponding syslog server.

Filtering options**Filtering scope**

Determines the filtering granularity.

Granularit	Meaning
Basic	<p>Basic filtering which does not distinguish between the individual server components, special events, etc.</p> <p>Message severity INFORMATIONAL, MINOR, MAJOR, CRITICAL</p> <p>Here you select one or more severity levels for which event log entries should be forwarded to syslog.</p>
Extended	<p>Filtering can be configured separately for each of the following component-level or system-specific event types: Fan Sensors, Temperature Sensors, Critical Hardware Errors, System Hang, POST Errors, Security, System Status, Disk Drivers & Controllers, Network Interface, Remote Management, System Power, Memory, and Other.</p> <p>For each event type, the following options are available:</p> <p>None No event is forwarded.</p> <p>Critical Only events with status Critical are forwarded.</p> <p>Warning Only events with status Critical or Warning are forwarded.</p> <p>All All events are forwarded.</p>

Basic filtering item are provided in the following groups:

- **Critical Severity**
- **Major Severity**
- **Minor Severity**
- **Informational Severity**

Extended filtering items are provided in the following groups:

- **Fan Sensors**
- **Temperature Sensors**
- **Critical Hardware Errors**
- **System Hang**
- **POST Errors**
- **Security**
- **System Status**
- **Disk Drivers & Controllers**
- **Network Interface**
- **Remote Management**
- **System Power**
- **Memory**
- **Spare**
- **Other**

2.4.9 Baseboard Management Controller

On the **Baseboard Management Controller** page of the **Settings** menu you configure the network settings of the iRMC.

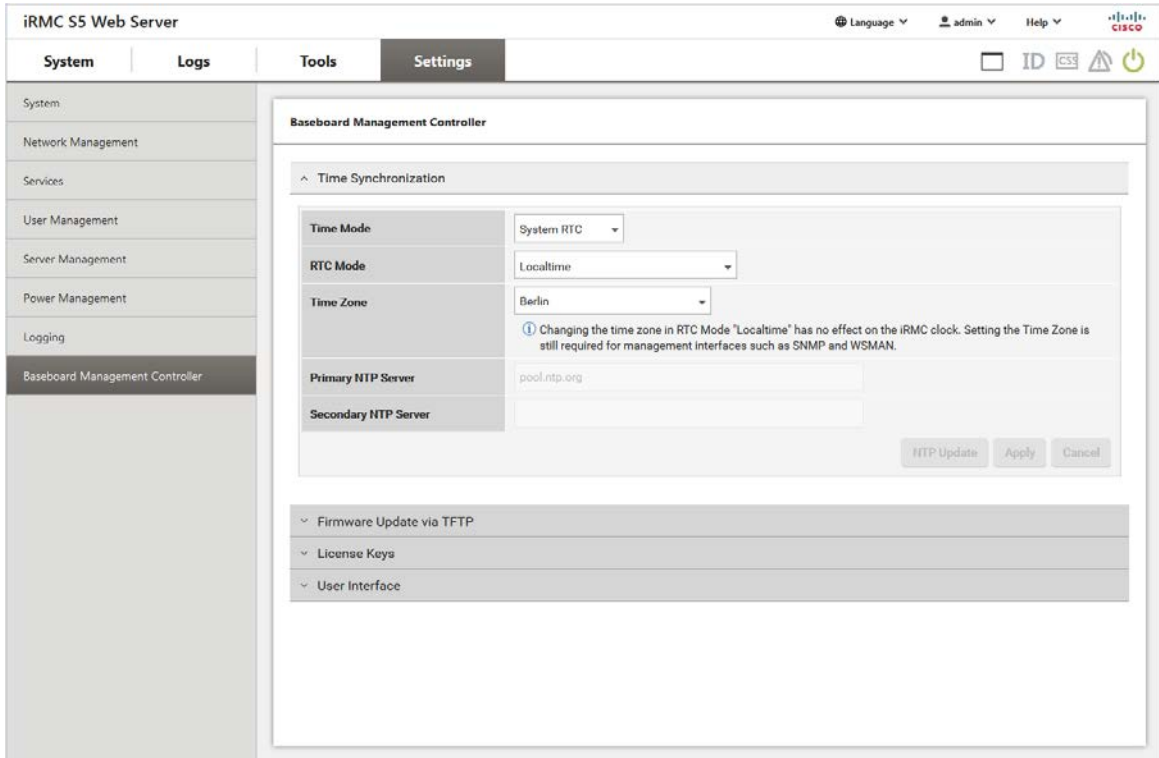


Figure 34: Baseboard Management Controller page

The Baseboard Management Controller settings are provided in several groups.

2.4.9.1 Time Synchronization

In this group you configure the time settings for the iRMC.

Time Mode

Specifies whether the iRMC gets its time settings from the managed server or from an NTP server (Network Time Protocol).

Option	Meaning
System RTC	The iRMC gets its time from the system clock of the managed server.
NTP Server	The iRMC uses NTP to synchronize its own time to an NTP server, which serves as the reference time source.

RTC Mode

Specifies whether from now on, iRMC time will be set in UTC (Universal Time Coordinated) format or Local Time format.

Option	Meaning
UTC (Universal Time Coordinated)	iRMC S5 time will be set to corrected RTC time by the time zone configuration.
Localtime	iRMC time will be set to RTC time.

Time Zone

Configures the time zone of the C880 M5 server location.

Primary NTP Server

IP address or DNS name of the primary NTP server

Secondary NTP Server

IP address or DNS name of the secondary NTP server

NTP Update

Synchronizes the clock of the iRMC to the settings of the specified NTP server.

2.4.9.2 Firmware Update via TFTP

The **Firmware Update via TFTP** group allows you to configure an update of the iRMC firmware on the managed server via TFTP. To do this, you must provide the current iRMC firmware image in a file on a TFTP server. The **iRMC Update** group on the **Update** page allows you to perform an update of the iRMC firmware on the managed server via TFTP. (for more information, refer to ["Update" on page 45](#))

TFTP Server


IP address or DNS name of the TFTP server on which the file with the iRMC firmware image is stored.

Update Image File

File containing the iRMC firmware image

2.4.9.3 License Keys

Allows you to load a license key onto the iRMC.
The eLCM is not supported on the C880 M5 server.

-  You require a valid license key to be able to use the iRMC functions **Life cycle Management**. The license key for Life cycle Management is always purchased together with the iRMC SD card.

License Key

Entry field for the license key in the format XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX.

2.4.9.4 User Interface

This group provides parameters for changing the layout of the iRMC web interface.

Power Unit

Unit of electrical power used to display power consumption:

- Watt
- BTU/h (1 BTU/h corresponds to 0.293 watts)

Temperature Units

Specifies the unit used to display temperature values on the web interface (degrees Celsius/degrees Fahrenheit). This setting applies for the current session and is preset the next time the iRMC web interface is called.

Default Language

Specifies the language (English/German/Japanese) that is set by default the next time the iRMC web interface is called.

3 Advanced Video Redirection (AVR)

Advanced Video Redirection (AVR) allows you to control the mouse and keyboard of the managed server from your remote workstation and to show the current graphical and text output from the managed server.

- i** Java caching must not be disabled. Otherwise AVR using Java cannot be started. (Java caching is enabled by default.)

3.1 Requirements for AVR

Supported graphics modes

Resolution	Refresh rates (in Hz)	Maximum color depth (bits)
640 x 480 (VGA)	60, 75, 85	32
800 x 600 (SVGA)	56, 60, 75, 85	32
1024 x 768 (XGA)	60, 70, 75, 85	32
1152 x 864	60; 70; 75	32
1280 x 800 (UXGA)	60; 70; 75; 85;	16
1280 x 1024 (UXGA)	60	24
1600 x 1200 (UXGA)	60; 65;	16
1680 x 1050	60	16
1920 x 1080	60	16
1920 x 1200	60	16

- i** Only VESA-compliant graphic modes are supported.

Supported text mode

The iRMC supports the following common text modes:

- 40 x 25
- 80 x 25
- 80 x 43
- 80 x 50

For information on the display settings, refer to the Help system of your operating system.

Keyboard settings

If the keyboard language settings on the remote workstation are different from those on the managed server, AVR keyboard language settings must be the same as on the managed server.

Mapping is possible between the following languages:

- Auto Detect (default value)
- English (United States)(*)
- English (United Kingdom)
- French
- French (Belgium)
- German (Germany) (*)
- German (Switzerland)
- Japanese(*)
- Spanish
- Italian
- Danish
- Finnish
- Norwegian (Norway)
- Portuguese (Portugal)
- Swedish
- Dutch (Netherlands)
- Dutch (Belgium)
- Turkish - F
- Turkish - Q

(*) Starting AVR using HTML5, these mapping are supported.

Supported keyboard language settings: (starting AVR using Java)
refer to ["Keyboard menu" on page 145](#).

Supported keyboard language settings: (starting AVR using HTML5)
refer to ["Keyboard menu" on page 159](#).

Not all keys can be mapped. If one key does not work, use the displayed keyboard (for more information, refer to ["Redirecting the keyboard" on page 139](#)).

3.2 Parallel AVR sessions

AVR can be used by up to two user sessions simultaneously. The AVR session started first is initially in Full access mode and has full control over the server.

Start of a second AVR session

If an AVR session is started while a previous AVR session 1 is still active and in Full access mode, the **Virtual Console Sharing Privileges** dialog box opens in the AVR window of session 1. In this dialog box you have three options to determine how to deal with the second session within 30 seconds:

Full Permission

Session 2 is switched to Full access mode. Session 1 is switched to Partial access (only Video) mode.

Virtual media connections of session 1 are cleared.

Partial Permission

Session 2 is switched to Partial access (only Video) mode. In this mode you can only passively observe keyboard and mouse operation of the server. Only the Video and Active Users functions can be used.

Session 1 remains in Full access mode.

Block Privilege Request

Session 2 is denied access and closed. Session 1 remains in Full access mode.

If the counter expires before session 1 has confirmed an option with **OK**, session 2 is switched to Full access mode and session 1 is switched to Partial access (only Video) mode.

Request Full access

If two AVR sessions are currently active and session 1 does not have Full access mode, user 1 of session 1 can request Full access by clicking **Request Full Permission** in the **Options** menu of the AVR window (for more information, refer to ["Options menu" on page 150](#)).

In this case, user 2 of the concurrent AVR session 2 is prompted to grant AVR session 1 Full access in the **Virtual Console Sharing Privileges** dialog box. In this dialog box you have two options to determine how to deal with the second session within 28 seconds:

Allow Virtual Console

Session 1 is switched to Full access mode. Session 2 is switched to Partial access (only Video) mode.

Virtual media connections of session 1 are cleared.

Allow only Video

Session 1 remains in Partial access (only Video) mode (default). In this mode you can only passively observe keyboard and mouse operation of the server. Only the Video and Active Users functions can be used.

Session 1 remains in Full access mode.

Exiting the "Full access" session

If two AVR sessions are currently active and you exit the one that is in Full access mode, the **Virtual Console Sharing Privileges** dialog box opens. This dialog box offers to select the user of the other session as the master session with Full access mode within 10 seconds:


- If you select this option, the other session will switch to Full access mode.
- If you deselect this option, the other session will remain in Partial access (only Video) mode.
- If the counter expires before you have confirmed the option with **OK**, the other session will remain in Partial access (only Video) mode.

3.3 Local Monitor Off Control function



The **Local Monitor Off Control** option of the iRMC allows you to power down the local monitor of the managed server for the duration of your AVR session. In this way, you ensure that the inputs you make and the actions you perform on the local monitor on the server using AVR cannot be seen. The identification LED flashes to indicate "Local Monitor Off" mode on the server.

You configure the **Local Monitor Off Control** function in the **Advanced Video Redirection** group of the iRMC web interface (for more information, refer to "[Services](#)" on page 78). In the **Advanced Video Redirection** group, you can also configure that the local monitor is always switched off automatically whenever a new AVR session is started.

Once you have configured the server appropriately, you can switch the local monitor of the server on and off from the remote workstation via the **Video** menu by clicking the second icon from the right on the toolbar.

-  The local monitor is always switched on and cannot be switched off if the **Local Monitor Off Control** option (for more information, refer to "[Services](#)" on page 78) is set to **disabled**.

The current status of the local monitor is indicated on the **Video** menu and displayed via the second icon from the right on the AVR toolbar (Java applet) or the AVR status bar (HTML5):

State icon	Meaning
	Indicates that the monitor of the managed server is unlocked (switched on), i.e. actions performed on the AVR console can be seen on the monitor of the managed server. Clicking this button will lock the monitor of the managed server and change the icon color to red. If the Local Monitor Off Control option (for more information, refer to " Services " on page 78) is disabled, the monitor status cannot be changed.
	Indicates that the local monitor is locked (switched off), i.e. actions performed on the AVR console cannot be seen on the monitor of the managed server. Clicking this button will unlock the monitor of the managed server and change the icon color to green.

3.4 Redirecting the keyboard

Keyboard redirection only works when the focus is on the AVR window.

- If keyboard redirection appears not to be working, simply click on the AVR window.
- If the keyboard does not respond, check that the AVR window is not in view-only mode. For how to switch to full-control mode, refer to "[Parallel AVR sessions](#)" on [page 136](#).

Special key combinations

AVR passes all normal key combinations to the server. Special keys such as Windows keys are not sent. Some special key combinations such as [Alt] + [F4] cannot be sent, because they are interrupted by the client's operating system. In such cases, you should use the integrated special keys or the hotkeys defined by yourself or the virtual keyboard.

Full keyboard support

The Full keyboard support feature allows you to use, via SoftKeyboard, all function keys of the managed server's physical keyboard.

Integrated special keys

In the bottom right of the AVR window, you will find a bar containing the special keys. These keys are implemented as "sticky keys", i.e. they remain pressed (indicated by a red label) when you click them and only return to their normal position when you click them again.

Using the integrated special keys, you can, for instance, use special key combinations which are not sent by AVR if you press them on your own keyboard.

Special key	Meaning
LALT	Left Alt(ernate) key (corresponds to the [Alt] key on your keyboard).
LCTRL	Left Ctrl key (corresponds to the left [Ctrl] key on your keyboard).
RALT	Right Alt(ernate) key / Alt(ernate) Graphic key (corresponds to the [Alt Gr] key on your keyboard).
RCTRL	Right CTRL key (corresponds to the right [Ctrl] key on your keyboard).
Num	Num Lock Key. Activates/deactivates the numeric keys on the right of your keyboard (corresponds to the [Num] key on your keyboard).
Caps	Caps Lock key (corresponds to the [Caps Lock] key on your keyboard).
Scroll	Scroll key (corresponds to the [Scroll] key on your keyboard).

SoftKeyboard (Java applet only)


In the java applet the SoftKeyboard (also known as the virtual keyboard) provides a functional representation of the keyboard. All key combinations are available when you use the SoftKeyboard. This means you can use it as a fully functional replacement for a real keyboard.

You activate the SoftKeyboard in the AVR window on the **Keyboard** menu (for more information, refer to the "[Keyboard menu](#)" on page 145).

Secure Keyboard

If you are connected to the iRMC web interface over an HTTP connection, your keystrokes and mouse clicks can be configured to be encrypted in real time before they are transferred to the managed server (for more information, refer to the relevant Options Menu).

3.5 Starting AVR using Java

1. In the **Settings** menu open the **Services** page.
2. In the **Advanced Video Redirection (AVR)** group deselect the **Favor HTML5 over Java Applet**.
3. Click **Apply** to submit your changes.
4. In the title bar click  to start a second 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**.

3.5.1 AVR window

The AVR window contains the following elements:

- The AVR menu bar provides access to the individual AVR menus (for more information, refer to ["Menus of the AVR window \(Java\)" on page 142](#)).
- The AVR toolbar provides direct access to a variety of AVR tools allowing you, among other things, to stop/resume your AVR session, use the Virtual Media function, record your AVR session and use hotkeys (for more information, refer to ["AVR toolbar" on page 153](#)).
- The zoom toolbar allows you to steplessly enlarge or reduce the AVR view.
- The integrated special keys in the bottom right of the AVR window allow you to use Windows keys or special key combinations which are not sent by AVR if you press them on your own keyboard.

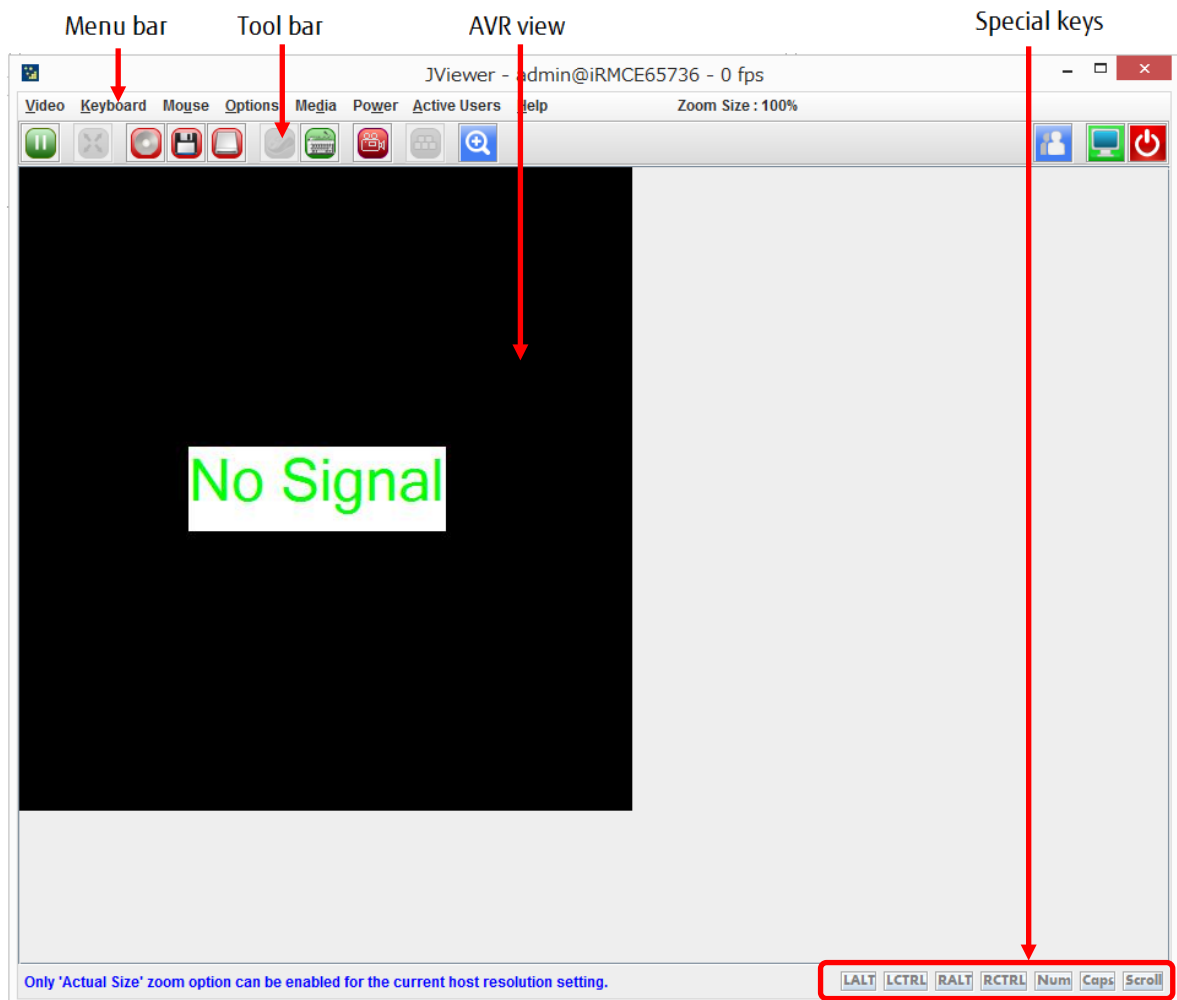


Figure 35: Structure of the AVR window

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.

3.5.2 Menus of the AVR window (Java)

The menu bar of the AVR window contains the following menus:

- "Video menu" on page 143
- "Keyboard menu" on page 145
- "Mouse menu" on page 149
- "Options menu" on page 150
- "Media menu" on page 150
- "Power menu" on page 151
- "Active Users Menu" on page 152
- "Help menu" on page 152

The icons of the AVR toolbar provide direct access to frequently used AVR functions.

3.5.2.1 Video menu

The **Video** menu allows you to configure the AVR settings and control the AVR. You can select the following commands on the **Video** menu:

Pause Redirection

Pauses AVR and freezes the AVR view. The AVR view remains frozen until AVR is resumed.

Resume Redirection

Resumes AVR and refreshes the AVR view.

Refresh Video

Refreshes the AVR view.

Turn ON Host Display

Switches on the local monitor of the managed server, depending on whether this option is selected or deselected.

- i This function is disabled in the following cases, even if the local monitor is switched off:
 - You are in view-only mode
 - A high-resolution graphics mode is set on the managed server (for more information, refer to "[Requirements for AVR](#)" on page 134). Local monitor <status> display: Local Monitor always off

Turn OFF Host Display

Switches off the local monitor of the managed server, depending on whether this option is selected or deselected.

- i If you are in view-only mode, this function is disabled, even if the local monitor is switched off.

Low Bandwidth Mode

If the data transfer rate is low, you can configure a lower bandwidth (bits per pixel, bpp) here in terms of color depth for your all AVR sessions on the same iRMC.

Option	Meaning
Normal	Default, no lower bandwidth
8 bpp	8 bpp color depth (256 colors)
8 bpp B&W	8 bpp black&white depth (256 levels of gray)
16 bpp	16 bpp color depth (65 536 colors)

Capture Screen

Makes a screenshot of the AVR view and opens a file browser that allows you to store the related CapturedScreen.jpeg file in any directory of your workstation or on a network share.

- i** The same function is also available via the **Advanced Video Redirection** page of the iRMC web interface (for more information, refer to "[Services](#)" on page 78).

Full Screen

Enables/disables full-screen mode.

- i** This option is only enabled if the screen resolution on the remote workstation is the same as the screen resolution on the managed server.

Start Video

Creates a video recording of the events that are displayed on the monitor of the managed server.

- i** This button is disabled in the following cases:
 - You have not yet configured the video settings under the **Settings** option (see below).
 - A video recording is currently running.

Stop Video

Stops video recording. This option is only enabled when a video is currently recording.

Settings

Opens the **Video Record** dialog box, allowing you to configure the settings required for recording a video (for more information, refer to "[Video Record dialog box](#)" on page 144).

Exit

Terminates your own AVR session.

Video Record dialog box

In the **Video Record** dialog box you can configure the settings required for recording a video.

You open this dialog box with **Video/Settings** in the AVR window. The dialog box has the following options:

Video Length

Duration of the video (in seconds)

Browse

Opens a browser dialog allowing you to navigate to a directory on your computer or on a network share where the video should be stored.

Video to be Saved

Shows the directory you have selected via **Browse**.

Normalized video resolution to 1024x768

In this case, a separate video file will be created for each resolution change on the monitor of the managed server.

If this option is enabled, a normalized video resolution of 1024x768 is applied to the overall video output, regardless of the actual video resolution on the monitor of the managed server. This may reduce video quality.

OK

Activates your settings and closes the dialog box. The **Start Video** button is now enabled.

Cancel

Closes the dialog box without activating your settings.

3.5.2.2 Keyboard menu

The **Keyboard** menu allows you to handle special keys when redirecting the keyboard (for more information, refer to ["Redirecting the keyboard" on page 139](#)).

You can select the following functions on the **Keyboard** menu:

Hold Right Ctrl Key

Holds down right [Ctrl] key.

Hold Right Alt Key

Holds down right [Alt] key.

Hold Left Ctrl Key

Holds down left [Ctrl] key.

Hold Left Alt key

Holds down left [Alt] key.

Left Windows Key

Holds down left Windows key if **Hold Down** is enabled. Otherwise, **Press and Release** is applied.

Right Windows Key

Holds down right Windows key if **Hold Down** is enabled. Otherwise, **Press and Release** is applied.

Ctrl+Alt+Del

Applies the key combination [Ctrl] + [Alt] + [Del].

Context Menu

Opens the appropriate context menu of the application or the operating system running on the managed server.

Hot Keys

Opens the **User Defined Macros** dialog box to define and apply your own hotkeys (for more information, refer to "[Defining a new Hotkey](#)" on page 160).

Host Physical Keyboard

Language used on the keyboard of the managed server.

The following options are available:

- Auto Detect (default value)
- English (United States)
- English (United Kingdom)
- French
- French (Belgium)
- German (Germany)
- German (Switzerland)
- Japanese
- Spanish
- Italian
- Danish
- Finnish
- Norwegian (Norway)
- Portuguese (Portugal)
- Swedish
- Dutch (Netherlands)
- Dutch (Belgium)
- Turkish - F
- Turkish - Q

If you select **AutoDetect**, the AVR assumes that the keyboard language is the same as on the managed server and the remote workstation.

SoftKeyboard

Displays the SoftKeyboard (virtual keyboard).

The following options are available:

- | English (United States)
- | English (United Kingdom)
- | Spanish
- | French
- | German (Germany)
- | Italian
- | Danish
- | Finnish
- | German (Switzerland)
- | Norwegian (Norway)
- | Portuguese (Portugal)
- | Swedish
- | Hebrew
- | French (Belgium)
- | Dutch (Netherlands)
- | Dutch (Belgium)
- | Russian (Russia)
- | Japanese (QWERTY)
- | Japanese (Hiragana)
- | Japanese (Katakana)
- | Turkish - F
- | Turkish - Q

Full Keyboard Support

If enabled, allows you to use, via SoftKeyboard, all function keys of the managed server's physical keyboard.

Linux

Select this option if the host is Linux.

Displaying the SoftKeyboard

To display the SoftKeyboard in your preferred language, proceed as follows:

1. Hover the mouse pointer over the **SoftKeyboard** item.
A list of the available SoftKeyboard languages is shown.
2. Select your preferred language from the list.
The SoftKeyboard is displayed for the selected language.

Defining a new Hotkey

To define a new hotkey, proceed as follows:

1. In the AVR window click **Hot Keys/Add Hot Key**.
The **User Defined Macros** dialog box opens showing the existing user-defined macros.
2. Click **Add** to define a new user-defined macro. The **Add Macro** dialog box opens.
3. Enter your favored combination of up to six keys by using the **Windows**, **Alt+F4**, and **Print Screen** buttons and/or the keys of your keyboard.
The entered combination is displayed in the **Add Macro** dialog box.
4. Click **Clear All** or **Clear** to remove all keys or the rightmost key from the list.
5. Click **OK** to activate the new hotkey.
The new hotkey is now displayed in the **User Defined Macros** dialog box.
6. To remove a hotkey, select the corresponding entry and click **Delete**.
7. Click **Close** to close the **User Defined Macros** dialog box.

Applying an already defined hotkey

To apply an already defined hotkey, proceed as follows:

1. Click **Hot Keys**.
2. In the list of already defined hotkeys, which is displayed below the **Add Hot Key** item, click the one you want.

3.5.2.3 Mouse menu

The **Mouse** menu allows you to configure the settings for redirecting the mouse. You can select the following functions in the Mouse menu:

Show mouse cursor

Displays/hides the mouse pointer of your remote workstation when using the AVR.

Mouse Calibration

Used for calibrating the relative mouse mode. This option is only enabled if **Relative Mouse Mode** has been set to **Mouse Mode**.

- i In **Relative Mouse Mode**, the mouse pointer of the managed server follows the mouse pointer of the remote workstation in a decelerated manner.

Show Host Cursor

Shows an extra mouse pointer in addition to the mouse pointer of the managed server.

- i If hardware acceleration of the mouse pointer is set to the maximum value and the Matrox G200e driver is installed, the hardware mouse pointer of the iRMC is activated. Only one mouse pointer is normally displayed in this mode. In this case, the **Show Host Cursor** option can be used to display a second mouse pointer which refers to the managed server.

Mouse Mode

Specifies the mouse mode.

Option	Meaning
Absolute mouse mode	Default setting, always use the Absolute mouse mode . Only in the case of an older operating system (e.g. RedHat 4) might the Absolute mouse mode not work.
Relative mouse mode	Does not display the mouse pointer of the remote workstation.
Hide mouse mode	Only for LSI WEBBIOS.

3.5.2.4 Options menu

The **Options** menu allows you to enable/disable keyboard/mouse encryption, resize the window to suit your needs, and set the language in which the menus and dialog boxes of the AVR window are to be shown.

You can select the following functions on the **Options** menu:


Window Size

Specifies whether the size of the AVR window is to be shown in its actual size or adapted to the resolution of the local monitor of the managed server or to the monitor resolution on the remote workstation.

Option	Meaning
Actual Size	The AVR window is expanded to full monitor size.
Fit to Client Resolution	If the screen resolution on the remote workstation is higher than the screen resolution on the managed server, the AVR window is automatically adjusted. This is the normal working environment.
Fit to Host Resolution	If the screen resolution on the remote workstation is lower than or equal to the screen resolution on the managed server, the AVR window is automatically adjusted.

GUI Languages

Specifies the language in which the menus and dialog boxes of the AVR window are to be shown (English, German, Japanese).

-  The field is preset to the GUI language that was configured for the iRMC web interface from which the AVR session was started.

3.5.2.5 Media menu

Via the **Media** menu you can start the Virtual Media wizard. The Virtual Media wizard allows you to attach or detach media on the remote workstation as virtual media devices ("[Virtual Media Wizard](#)" on page 166).

Virtual Media Wizard...

Click **Virtual Media Wizard** to start the Virtual Media wizard allowing you to attach or detach media on the remote workstation as virtual media devices.

3.5.2.6 Power menu

The **Power Control** menu allows you to power the server up/down or reboot it. You can also configure the behavior of the server during the next boot operation.

Power On

Switches the server on.

Immediate Power Off

Powers the server down, regardless of the status of the operating system.

Power Cycle

Powers the server down completely and then powers it up again after a configured period. You can configure this time in the Power Cycle Delay field of the **ASR&R Options** group (for more information, refer to "[Server Management](#)" on page 118).

Press Power Button

Depending on the operating system installed and the action configured, you can trigger various actions by briefly pressing the power-off button. These actions could be shutting down the computer or switching it to standby mode.

Immediate Reset

Completely restarts the server (cold start), regardless of the status of the operating system.

Pulse NMI

Initiates a non-maskable interrupt (NMI). An NMI is a processor interrupt that cannot be ignored by standard interrupt-masking techniques in the system.

Graceful Reset (Reboot)

Graceful shutdown and reboot.

This option is not supported on the C880 M5 server.

Graceful Power Off (Shutdown)

Graceful shutdown and power off.

This option is not supported on the C880 M5 server.

Set Boot Options

Clicking this item opens the Set Boot Options dialog box for configuring the behavior of the system the next time it is booted ("[Set Boot Options dialog box](#)" on page 152).

Next Boot Only

The configured settings apply to the next boot only.

Set Boot Options dialog box

In the **Set Boot Options** dialog box you configure the behavior of the system the next time it is booted. You open the dialog box with **Power Control/Set Boot Options**.

Boot Device Selector

Storage medium you wish to boot from. The following options are available:

Option	Meaning
No Change	The system is booted from the same storage medium as previously.
PXE/iSCSI	The system is booted from PXE/iSCSI over the network.
Hard Drive	The system is booted from HDD.
CDROM/DVD	The system is booted from CD/DVD.
Floppy	The system is booted from floppy disk.
Bios Setup	The system enters BIOS setup when booting.

3.5.2.7 Active Users Menu


The **Active Users** menu shows the users currently using the AVR. The green bullet indicates your own session.

3.5.2.8 Help menu

As well as showing general information on **About JViewer**, the **Help** menu displays in the **Server Information** dialog box the information defined in the **System Information** group on the **System Overview** page of the iRMC web interface.












3.5.3 AVR toolbar





The icons of the AVR toolbar provide direct access to frequently used AVR functions. When hovering your mouse pointer over an icon, you often receive assistance in the form of tool tips.

-  In Partial access (only Video) mode, only the Video and Active Users icons can be used.

If Video Redirection is executed in **Num Lock On** mode on the server side, the client side also switches to **Num Lock On**.

The following icons reside on the toolbar of the AVR window:

Icon	Meaning
	Pauses AVR and freezes the view. The AVR view remains frozen until AVR is resumed.
	Enables/disables full-screen mode.
	Indicates whether (green) or not (red) a hard disk/USB redirection is established for this AVR session. Clicking the icon starts the Virtual Media wizard (for more information, refer to " Virtual Media Wizard " on page 166).
	Indicates whether (green) or not (red) a CD/DVD redirection is established for this AVR session. Clicking the icon starts the Virtual Media wizard.
	Indicates whether (green) or not (red) a floppy redirection is established for this AVR session. Clicking the icon starts the Virtual Media wizard.
	Indicates whether (green) or not (grayed out) the mouse pointer of the remote workstation is visible in the AVR window. Clicking the icon allows you to switch between the two modes.
	Displays the SoftKeyboard (more information, refer to " Keyboard menu " on page 145 for details).
	Displays the list of available hotkeys. To apply a hotkey, click the related item, for more information, refer to " Defining a new Hotkey " on page 160.
	Displays the zoom toolbar by click this icon.
	The zoom toolbar allows you to steplessly enlarge or reduce the AVR view.
	Displays for each currently active AVR session the iRMC user who started it and the IP address of the remote workstation from which it was started.

Icon	Meaning
	<p>If the Local Monitor Off Control option is enabled on the AVR page of the iRMC web interface, this toggle button allows you to switch between the following states:</p> <p>Indicates that the monitor of the managed server is unlocked, i.e. actions performed on the AVR console can be seen on the monitor of the managed server. Clicking this button will lock the monitor of the managed server.</p>
	<p>Indicates that the monitor of the managed server is locked, i.e. actions performed on the AVR console cannot be seen on the monitor of the managed server. Clicking this button will unlock the monitor of the managed server.</p>
	<p>This toggle button allows you to power the managed server on and off:</p> <p>Indicates that the managed server is currently powered on. Clicking this button starts a confirmation dialog for powering the managed server off (immediate power off).</p>
	<p>Indicates that the managed server is currently powered off. Clicking this button starts a confirmation dialog for powering the managed server on.</p>

3.6 Starting AVR using HTML5

1. In the **Settings** menu open the **Services** page.
2. In the **Advanced Video Redirection (AVR)** group select the **Favor HTML5 over Java Applet**.
3. Click **Apply** to submit your changes.
4. In the title bar click to start a second AVR session.
The default browser opens with the redirection to the managed server. If there is another redirection session running, both sessions are shown in the **AVR Active Session Table**.

3.6.1 HTML5 page

The redirected HTML5 page is displayed in a browser capable of HTML5.
The HTML5 page consists of the following areas:

- The menu bar provides access to the individual menus (for more information, refer to "[Menus of the AVR window \(HTML5\)](#)" on page 157).
- The status bar provides direct access to some AVR tools allowing you, among other things, to use the Virtual Media functions (for more information, refer to "[Status bar of the AVR window \(HTML5\)](#)" on page 164).
- The integrated special keys in the bottom right of the HTML5 page allow you to use Windows keys or special key combinations which are not sent by AVR if you press them on your own keyboard.

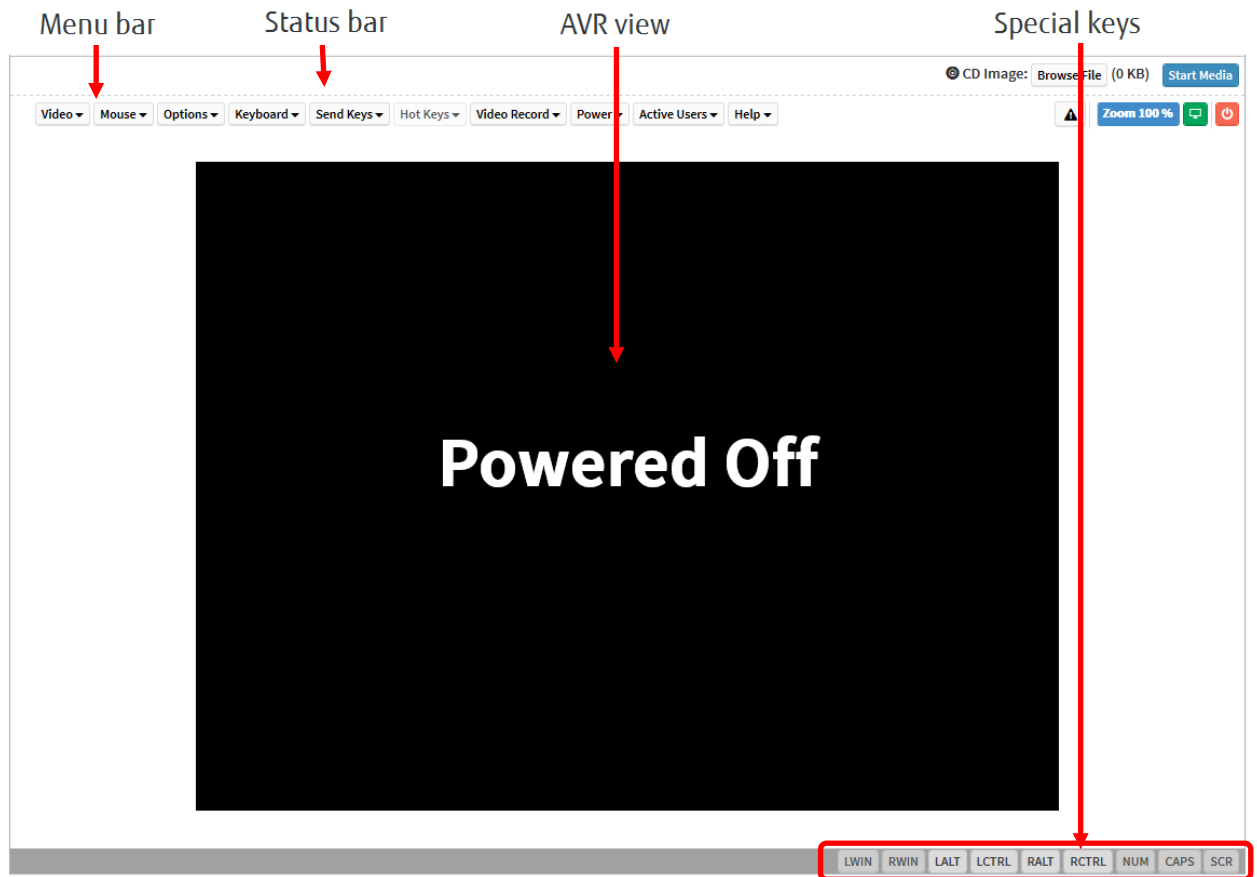


Figure 36: HTML5 page

On the bottom of the window resides a button bar with keys. Using this special keys, you can, for instance, use special key combinations which are not sent by AVR if you press them on your own keyboard.

Button	Meaning
LWIN	Presses the left Windows key (corresponds to the left [Windows] key on your keyboard).
RWIN	Presses the right Windows key (corresponds to the right [Windows] key on your keyboard).
LALT	Presses the left Alt(ernate) key (corresponds to the left [Alt] key on your keyboard).
LCTRL	Presses the left Ctrl key (corresponds to the left [Ctrl] key on your keyboard).
RALT	Presses the right Alt(ernate) key (corresponds to the right [Alt] key on your keyboard).

Button	Meaning
RCTRL	Presses the right Ctrl key (corresponds to the left [Ctrl] key on your keyboard).
NUM	Displays the current status of the [NumLock] key on your numeric keypad.
CAPS	Displays the current status of the [CapsLock] key on your keyboard.
SCR	Displays the current status of the [Print] key on your keyboard.

3.6.2 Menus of the AVR window (HTML5)

The menu bar of the AVR window contains the following menus:

- ["Video menu" on page 157](#)
- ["Mouse menu" on page 158](#)
- ["Option menu" on page 158](#)
- ["Keyboard menu" on page 159](#)
- ["Send Keys menu" on page 159](#)
- ["Hot Keys menu" on page 160](#)
- ["Video Record menu" on page 161](#)
- ["Power menu" on page 162](#)
- ["Active Users Menu" on page 163](#)
- ["Help menu" on page 163](#)

The **Request Full Access** button on the menu bar is only visible if two AVR sessions are currently active and your session is the one that is not in Full access mode. The button prompts the user of the concurrent AVR session to grant you Full access.

Depending on the decision, you will be granted Full access or remain in Partial access mode. For details, more information, refer to ["Parallel AVR sessions" on page 136](#).

The icons of the AVR status bar provide direct access to frequently used AVR functions.

3.6.2.1 Video menu

The **Video** menu allows you to configure the AVR settings and control the AVR. You can select the following commands on the **Video** menu:

Pause Video

Pauses AVR and freezes the AVR view. The AVR view remains frozen until AVR is resumed.

Resume Video

Resumes AVR and refreshes the AVR view.

Refresh Video

Refreshes the AVR view.

Host display

Display ON

Switches on the local monitor of the managed server, depending on whether this option is selected or deselected.

- i** This function is disabled in the following cases, even if the local monitor is switched off:
 - You are in view-only mode
 - A high-resolution graphics mode is set on the managed server (for more information, refer to "[Requirements for AVR](#)" on page 134). Local monitor <status> display: Local Monitor always off

Display OFF

Switches off the local monitor of the managed server, depending on whether this option is selected or deselected.

- i** If you are in view-only mode, this function is disabled, even if the local monitor is switched off.

Capture Screen

Makes a screenshot of the AVR view and opens a file browser that allows you to store the related CapturedScreen.jpeg file in any directory of your workstation or on a network share.

- i** The same function is also available via the **Advanced Video Redirection** page of the iRMC web interface (for more information, refer to "[Services](#)" on page 78).

3.6.2.2 Mouse menu

The **Mouse** menu allows you to configure the settings for redirecting the mouse.

You can select the following functions in the Mouse menu:

Show Client Cursor

Displays/hides the mouse pointer of your remote workstation when using the AVR.

3.6.2.3 Option menu

Zoom

Normal

Zoom In

Zoom out

Blok Privilege Request

Partial Permission

No Permission

3.6.2.4 Keyboard menu

In the **Keyboard** menu you can specify the language used for the keyboard layout (for more information, refer to ["Redirecting the keyboard" on page 139](#)).

Keyboard Layout

Language used on the keyboard of the managed server.

The following options are available:

- ▮ English US
- ▮ German
- ▮ Japanese

3.6.2.5 Send Keys menu

The **Send keys** menu allows you to handle special keys when redirecting the keyboard (see ["Redirecting the keyboard" on page 139](#)).

You can select the following functions on the **Send Keys** menu:

Hold down

The **Hold Down** keys are implemented as “sticky keys”, i.e. they remain pressed (indicated by a red label) when you click them and only return to their normal position when you click them again.

Right Ctrl Key

Holds down right [Ctrl] key.

Right Alt Key

Holds down right [Alt] key.

Right Windows Key

Holds down right Windows key.

Left Ctrl Key

Holds down left [Ctrl] key.

Left Alt key

Holds down left [Alt] key.

Left Windows Key

Holds down left Windows key.

Press and release

Ctrl+Alt+Del

Applies the key combination [Ctrl] + [Alt] + [Del].

Left Windows Key

Presses and releases the left Windows key.

Right Windows Key

Presses and releases the left Windows key.

Context Menu

Opens the appropriate context menu of the application or the operating system running on the managed server.

Print Screen Key

Copies a screen capture of the current screen to the clipboard.

3.6.2.6 Hot Keys menu

You can edit the **Hot Keys** menu and define any combination of keys for access via a single click.

Initially the Ctrl+Alt+Del combination is defined.

Defining a new Hotkey

To define a new hotkey, proceed as follows:

1. In the AVR window click **Hot Keys/Add Hot Key**.
The **User Defined Macros** dialog box opens showing the existing user-defined macros.
2. Click **Add** to define a new user-defined macro. The **Add Macro** dialog box opens.
3. Enter your favored combination of up to six keys by using the **Windows**, **Alt+F4**, and **Print Screen** buttons and/or the keys of your keyboard.
The entered combination is displayed in the **Add Macro** dialog box.
4. Click **Clear All** or **Clear** to remove all keys or the rightmost key from the list.
5. Click **OK** to activate the new hotkey.
The new hotkey is now displayed in the **User Defined Macros** dialog box.
6. To remove a hotkey, select the corresponding entry and click **Delete**.
7. Click **Close** to close the **User Defined Macros** dialog box.

Applying an already defined hotkey

To apply an already defined hotkey, proceed as follows:

1. Click **Hot Keys**.
2. In the list of already defined hotkeys, which is displayed below the **Add Hot Key** item, click the one you want.

3.6.2.7 Video Record menu

The **Video** menu allows you to control the AVR.

You can select the following commands on the **Video** menu:

Record Video

Creates a video recording of the events that are displayed on the monitor of the managed server.

 This button is disabled in the following cases:

- You have not yet configured the video settings under the **Settings** option.
- A video recording is currently running.

Stop Recording

Stops video recording. This option is only enabled when a video is currently recording.

Record Settings

Opens the **Video Record** dialog box, allowing you to configure the settings required for recording a video ("[Video Record dialog box](#)" on page 161).

Video Record dialog box

In the **Video Record** dialog box you can configure the settings required for recording a video.

You open this dialog box with **Video/Settings** in the AVR window.

The dialog box has the following options:

Video Length

Duration of the video (in seconds); Value range: 1-1800

Video Compression

Video Compression level; Value range: 0.1(Low quality) - 0.9 (High quality)

OK

Activates your settings and closes the dialog box. The **Start Video** button is now enabled.

Cancel

Closes the dialog box without activating your settings.

3.6.2.8 Power menu

The **Power Control** menu allows you to power the server up/down or reboot it. You can also configure the behavior of the server during the next boot operation.

Power On Server

Switches the server on.

Immediate shutdown

Powers the server down, regardless of the status of the operating system.

Power Cycle Server

Powers the server down completely and then powers it up again after a configured period. You can configure this time in the Power Cycle Delay field of the **ASR&R Options** group (for more information, refer to "[Server Management on page 118](#)").

Press Power Button

Depending on the operating system installed and the action configured, you can trigger various actions by briefly pressing the power-off button. These actions could be shutting down the computer or switching it to standby mode.

Reset Server

Completely restarts the server (cold start), regardless of the status of the operating system.

Pulse NMI

Initiates a non-maskable interrupt (NMI). An NMI is a processor interrupt that cannot be ignored by standard interrupt-masking techniques in the system.

Graceful Reset (Reboot)

Graceful shutdown and reboot.

This option is not supported on the C880 M5 server.

Graceful Power Off (Shutdown)

Graceful shutdown and power off.

This option is not supported on the C880 M5 server.

Boot Options

Clicking this item opens the Set Boot Options dialog box for configuring the behavior of the system the next time it is booted (for more information, refer to "[Set Boot Options dialog box](#)" on page 163).

Set Boot Options dialog box

In the **Set Boot Options** dialog box you configure the behavior of the system the next time it is booted. You open the dialog box with **Power Control/Set Boot Options**.

Next Boot Only

The configured settings apply to the next boot only.

Boot Device Selector

Storage medium you wish to boot from. The following options are available:

Option	Meaning
No Change	The system is booted from the same storage medium as previously.
PXE/iSCSI	The system is booted from PXE/iSCSI over the network.
Hard Drive	The system is booted from HDD.
CDROM/DVD	The system is booted from CD/DVD.
Floppy	The system is booted from floppy disk.
Bios Setup	The system enters BIOS setup when booting.

OK

Activates your settings and closes the dialog box.

Cancel

Closes the dialog box without activating your settings.

3.6.2.9 Active Users Menu

The **Active Users** menu shows the users currently using the AVR. The green bullet indicates your own session.

3.6.2.10 Help menu

The **Help** menu displays general information on H5Viewer in the **About H5Viewer** dialog box.

3.6.3 Status bar of the AVR window (HTML5)

The status bar provides direct access to some AVR tools allowing you, among other things, to use the Virtual Media functions.

CD image

Opens a dialog box to browse for an ISO image file from your computer.

Start Media

Displays a dialog box to attach or detach media on the remote workstation as virtual media devices.

CD Image

Displays the selected ISO image.

Browse

Opens a dialog to navigate to the directory of the storage medium that you want to make available as a virtual medium from your remote workstation.







Start Media Redirection

Starts media redirection and connects the provided storage medium as Virtual Media.

Close


Closes the dialog box without using the settings for media redirection.

The following icons reside below the status bar on the right of the AVR window:

Icon	Meaning
	Displays the notification received
	The zoom toolbar allows you to steplessly enlarge or reduce the AVR view.
	If the Local Monitor Off Control option is enabled on the Advanced Video Redirection (AVR) group of the iRMC web interface. This toggle button allows you to switch between the following states: Indicates that the monitor of the managed server is unlocked, i.e. actions performed on the AVR console can be seen on the monitor of the managed server. Clicking this button will lock the monitor of the managed server.
	Indicates that the monitor of the managed server is locked, i.e. actions performed on the AVR console cannot be seen on the monitor of the managed server. Clicking this button will unlock the monitor of the managed server.
	This toggle button allows you to power the managed server on and off: Indicates that the managed server is currently powered on. Clicking this button starts a confirmation dialog for powering the managed server off (immediate power off).
	Indicates that the managed server is currently powered off. Clicking this button starts a confirmation dialog for powering the managed server on.

3.6.4 Supported Browsers

The HTML5 redirection function is supported by the same browsers that are mentioned in the "[Display requirements](#)" on page 20.

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

4 Virtual Media Wizard

The Virtual Media Wizard makes a “virtual” drive available to the managed server, the source of which you provide on a remote workstation. The virtual media connection between the managed server and the remote workstation is established using the AVR Java applet. Depending on the settings made in the **Virtual Media Options** group of the **Services** page (for more information, refer to ["Services" on page 78](#)), you can connect up to 12 virtual media in total and choose between the following types:

- Physical floppies and/or floppy images (up to 4)
- Physical CD/DVDs and/or CD/DVD ISO images (up to 4 in total)
- Hard disk drives and/or hard disk/USB images (up to 4 in total)

It is not necessary for the remote media to be physically located on the remote workstation. They can also be located on any network share accessible from this remote workstation.

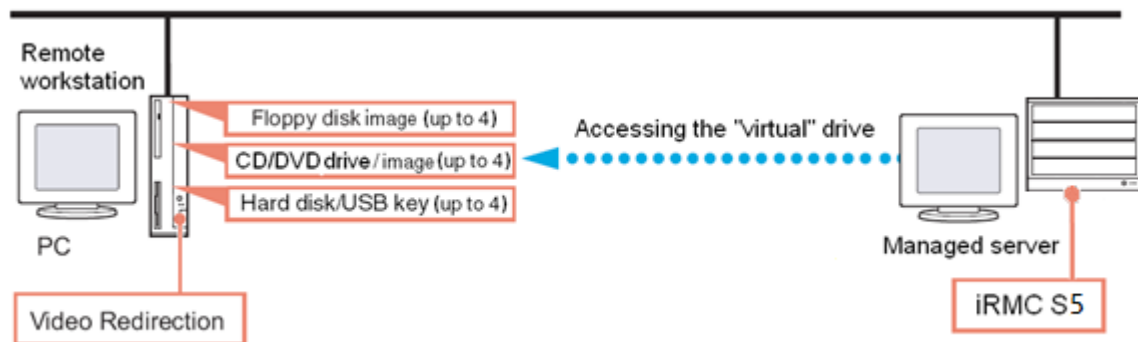


Figure 37: Virtual media provided via a remote connection

4.1 Provision of virtual media on the remote workstation

If you provide the source for a virtual drive on the remote workstation, the virtual functionality supports the following device types:

- Floppy
- CD ISO image
- DVD ISO image
- CD, DVD

i Optical storage media (CD, DVD) are automatically displayed (offered for selection).


Devices connected as virtual media are recognized as USB-connected devices by the iRMC. They cannot be used if no USB connection is available (e.g. no USB driver exists).

You can use the virtual drive to install an operating system on your C880 M5 server from the remote workstation.


4.2 Starting the Virtual Media wizard

You start the Virtual Media wizard either by using the AVR Java applet or via HTML5. You configure the settings for using Virtual Media and Advanced Redirection in the respective groups of the **Service** page (for more information, refer to ["Services" on page 78](#)).

Java applet

1. Start the iRMC web interface (for more information, refer to ["Logging in" on page 24](#)).
2. In the title bar click  to start Advanced Video Redirection. This opens the AVR window.
3. Click **Media/Virtual Media Wizard...**
or
4. Click one of the three Virtual Media icons on the toolbar. The **Virtual Media** dialog box opens.
5. Enter your settings for virtual media (for more information, refer to ["Virtual Media dialog box" on page 168](#)).


HTML5

1. Start the iRMC web interface.
2. In the title bar click  to start Advanced Video Redirection. This opens the AVR window.
3. In the status bar, select an ISO image to be displayed in the **CD image** field.
4. Click **Start Media**.
The **Virtual Media** dialog box opens.
5. Enter your settings for virtual media (for more information, refer to ["Status bar of the AVR window \(HTML5\)" on page 164](#)).

4.3 Virtual Media dialog box

Depending on the settings made on the **Services** page of the iRMC web interface, the **Virtual Media** dialog box displays between none and four panels for each of the following three media types:

- ▮ Floppy key-media (floppy images).
Default: No floppy key-medium is displayed.
- ▮ CD/DVD media ISO images
 - CD/DVD media ISO images
 - CD/DVD drives (i.e. physical CD/DVD)Default: Two CD/DVD media ISO images are displayed.
- ▮ Hard disk/USB key media
 - Hard disk/USB key images
 - Physical drive (fixed drive)Default: One Hard disk/USB key medium is displayed.

 Physical storage devices must be mounted on Linux systems.


The **Status** panel informs you about both the storage media which are currently available for virtual media connections and the ones which are currently connected as virtual storage media.

4.4 Providing storage media for virtual media


At any time during your AVR session, you have the following options:

- ▮ Add additional virtual media connections to your existing ones.
- ▮ Disconnect individual virtual media connections.

To provide a storage medium of your preferred type (e.g. a DVD image), proceed as follows:

 Physical drives are automatically displayed. Browsing is only required for providing images.

1. In the appropriate panel of the **Virtual Media** dialog box, click **Browse**.
2. The **Open** dialog box opens.
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.

3. Select the required device type under **Files of Type**.
 -  Physical storage devices must be mounted on Linux systems.
4. Specify the storage medium you wish to connect as a virtual medium under **File Name**:
 - In the case of an ISO image (ISO/NRG image), enter the file name. Alternatively, click on the file name in the Explorer.
 - In the case of a drive, enter the name of the drive, e.g.:
 - /dev/... (Linux)
5. 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.
6. Click the corresponding **Connect...** button to connect the provided storage medium as Virtual Media.

The selected storage medium is made available as a virtual medium and displayed in the corresponding panel of the **Virtual Media** dialog box.

4.5 Clearing Virtual Media connections

A virtual connection is automatically released in the following cases:

- The AVR session is disconnected.
 - The AVR session which established the virtual media connection changes to "read- only" mode due to a successful "Full Access" request from a second AVR session.
 - The settings configured on the **Virtual Media Options** page are changed ("[Services](#)" on page 78).
1. Open the **Virtual Media** dialog box ("[Virtual Media dialog box](#)" on page 168).
 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.