



## **Cisco C880 M5 Administration 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](http://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	Preface.....	5
1.1	Concept and target groups for this manual.....	5
1.2	Documentation overview .....	6
1.3	Notational conventions .....	7
2	Overview of the iRMC functions.....	8
2.1	Standard functions .....	8
2.2	User interfaces.....	13
2.3	Application programming interfaces.....	14
2.4	Communication protocols used .....	15
2.5	Front panel LEDs controlled by the iRMC.....	16
3	First Steps.....	17
3.1	Configuration of the LAN interface .....	17
3.1.1	Prerequisites.....	17
3.1.2	Configuring the LAN interface using UEFI .....	18
3.1.3	Testing the LAN interface .....	20
3.2	Logging in to the iRMC S5 for the first time.....	20
3.2.1	Requirements .....	20
3.2.2	iRMC factory defaults.....	21
3.2.3	Logging in.....	21
3.2.4	Logging out .....	22
4	User management.....	23
4.1	User management concept.....	23
4.2	User permissions.....	26
4.3	Local user management .....	27
4.3.1	Local user management using the iRMC web interface.....	27
4.3.2	Secure Authentication via SSHv2 .....	28
4.3.2.1	Creating public and private SSHv2 keys .....	29
4.3.2.2	Uploading the public SSHv2 key.....	30
4.3.2.3	Using the public SSHv2 key .....	31
4.3.2.4	Example: Public SSHv2 key.....	32
5	Remote installation of the operating system .....	34
5.1	General procedure for installing the operating system.....	34
5.2	Connecting a storage medium as Virtual Media.....	35
5.3	Booting the managed server.....	36
6	Firmware update.....	37
6.1	Firmware selector .....	38
6.2	Firmware image downgrade.....	39

---

---

6.3	Firmware image update .....	40
-----	-----------------------------	----

---

# 1 Preface

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.

## 1.1 Concept and target groups for this manual

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

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

## 1.2 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

## 1.3 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.
<b>Bold</b>	Indicates references to names of interface elements.
monospace	Indicates system output and system elements, for example file names and paths.
<b>monospace semibold</b>	Indicates statements that are to be entered using the keyboard.
<a href="#">blue continuous text</a>	Indicates a link to a related topic.
<a href="#">purple continuous text</a>	Indicates a link to a location you have already visited.
<abc>	Indicates variables which must be replaced with real values.
[abc]	Indicates options that can be specified (syntax).
[Key]	Indicates a key on your keyboard. If you need to explicitly enter text in uppercase, the Shift key is specified, for example [Shift] + [A] for A. If you need to press two keys at the same time, this is indicated by a plus sign between the two key symbols.

### Screenshots

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

## 2 Overview 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.

### 2.1 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 and 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
- Update BIOS from remote workstation
- (BIOS update via USB)

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

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

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

## 2.2 User interfaces

The iRMC provides the following user interfaces:

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

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

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

Operation of the iRMC using the web interface is described in the "Cisco C880 M5 User Interface Guide".

- **Remote Manager:** Text-based Telnet/SSH interface via LAN You can call the Remote Manager:

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

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

## 2.3 Application programming interfaces

The iRMC S5 supports APIs (Application Programming Interface) for scripted configuration. With scripting only one iRMC has to be configured according to the requirements of the environment. This configuration is then uploaded to all other C880 M5 servers without the need to access them all one by one.

- **RESTful**

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

- **Redfish**

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

- **SCCI**

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

## 2.4 Communication protocols used

The iRMC uses the following protocols and ports for communication:

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

## 2.5 Front panel LEDs controlled by the iRMC

The iRMC controls the status LEDs which are located on the front panel of the server.

Status LEDs on the front panel:

Status of the Server	LED on the Server	
	S5 LED (green)	Power LED (green)
AC-OFF	off	off
S5 (shutdown)	on	off
S0 (power on)	off	on
iRMC not readyON	on	blinking
Power-on Delay	on	on





## 3 First Steps

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

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

### 3.1 Configuration of the LAN interface

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

After configuration you test the LAN interface.

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

#### 3.1.1 Prerequisites

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

**The LAN cable must be connected to the correct port.**

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

Depending on the server type, the system board of a C880 M5 server provides two LAN interfaces. The ports marked with a wrench symbol are assigned to the iRMC.

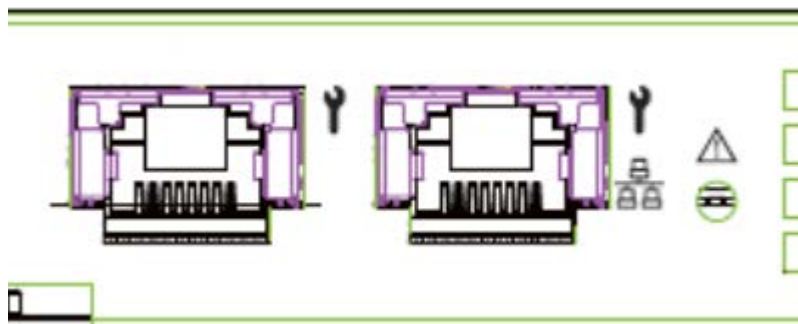




Figure 1: Ports for the iRMC (indicated by wrench symbol)

Icon	Meaning
	Dedicated Service/Management LAN (port exclusively for the iRMC; with the iRMC a LAN speed up to 1000 MBit/s is available)
	Shared LAN (iRMC and system) LAN speed setting is only available on system.

#### **Two IP addresses are required**

The LAN controller of the C880 M5 server requires a separate IP address for the iRMC in order to ensure that data packets are reliably transferred to the iRMC (and not to the operating system).

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

#### **A gateway is configured for access from a different subnet**

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

### **3.1.2 Configuring the LAN interface using UEFI**

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

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

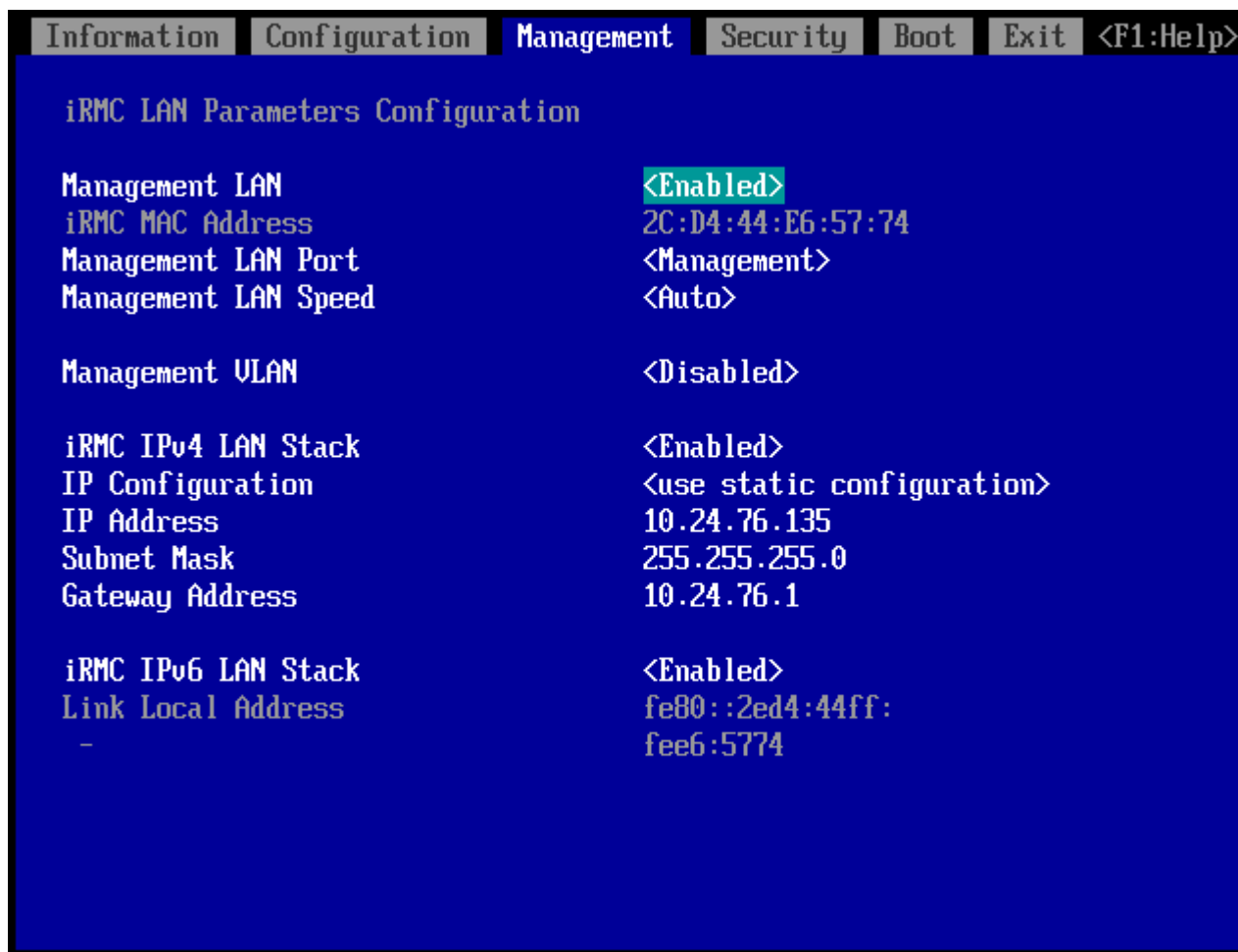


Figure 2: iRMC LAN Parameters Configuration Menu

3. In the **Management LAN** field, enter **Enabled**.
4. In the **Management LAN Port** field, enter **Management**.
  - i For more information on configuring the remaining settings, refer to the "Cisco C880 M5 User Interface Guide" and/or refer to the "Cisco C880 M5 BIOS Setup Guide".
5. Save the settings.
6. If you want to use console redirection on the iRMC, continue with configuring text console redirection.
7. If you do not want to use text console redirection on the iRMC, exit the UEFI setup and continue with testing the LAN interface ("[Testing the LAN interface](#)" on page 20).

### 3.1.3 Testing the LAN interface

You can test the LAN interface as follows:

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

## 3.2 Logging in to the iRMC S5 for the first time

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

### 3.2.1 Requirements

The following requirements must be met for a working connection: On the remote workstation:

- 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.

In your network:

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

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

## 3.2.2 iRMC factory defaults

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

### Default administrator ID

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

Administrator ID admin

Password admin

For reasons of security, it is recommended that you create a new administrator account once you have logged in, and then delete the default administrator account. At least change the password for the account ("[User management](#)" on page 23).

### Default DHCP name of the iRMC

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

IRMC<SerialNumber>

The serial number corresponds to the last three bytes of the MAC address of the iRMC. You can take the MAC address of the iRMC from the label on your C880 M5 server.

After you have logged in, the MAC address of the iRMC can be found as a read-only field in the **Network Interface** group of the **Baseboard Management Controller** page.


## 3.2.3 Logging in

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

e.g. <IP address>

or

IRMC<SerialNumber>

-  You can take the DNS name of the iRMC from the label on your C880 M5 server. A login dialog opens.

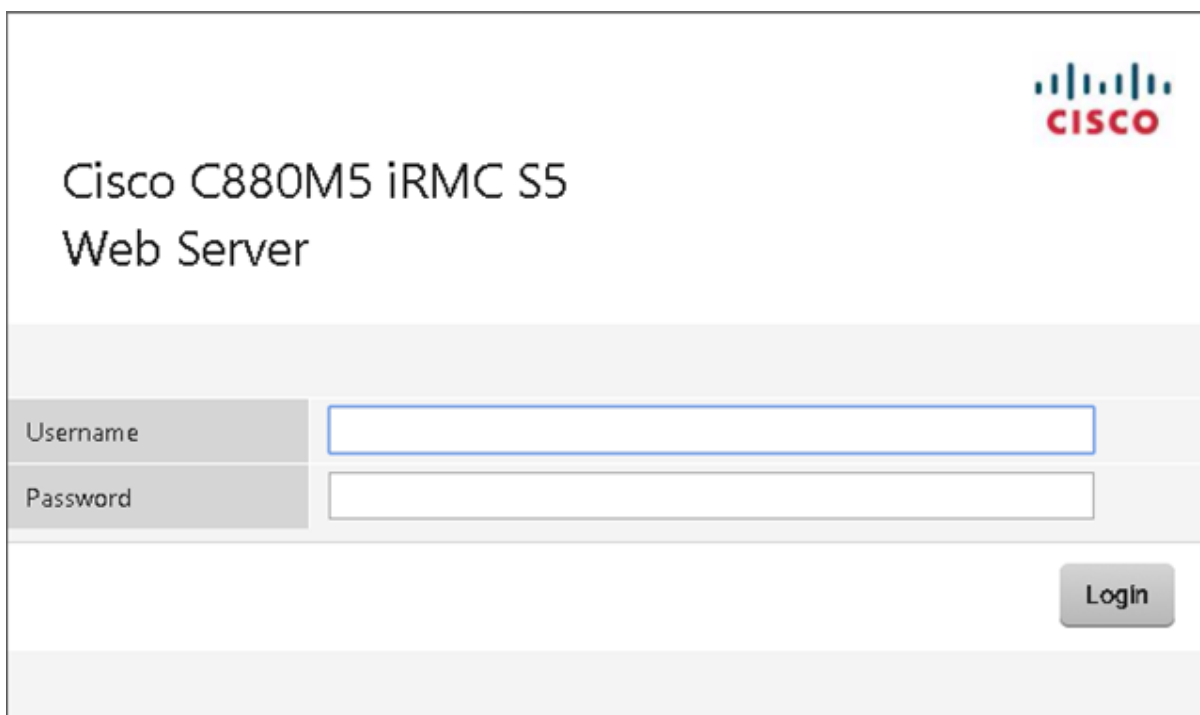


Figure 3: Login dialog for the iRMC web interface

3. If no login dialog opens, 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. Enter the data for the default administrator account.

Username: **admin**

Password: **admin**

Both the Username and the Password are case-sensitive.

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

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

For reasons of security, it is recommended that you create a new administrator account once you have logged in, and then delete the default administrator account. At least change the password for the account ("[User management](#)" on page 23).

### 3.2.4 Logging out

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

1. On the title bar open the **<User>** menu.

2. Click **logout**.

The user is logged out and the login dialog opens again. This allows you to log in again if you want.

## 4 User management

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

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

The following directory services are currently supported for global iRMC S5 user management:

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

### 4.1 User management concept

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

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

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

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

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

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

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

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

Characteristics:

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



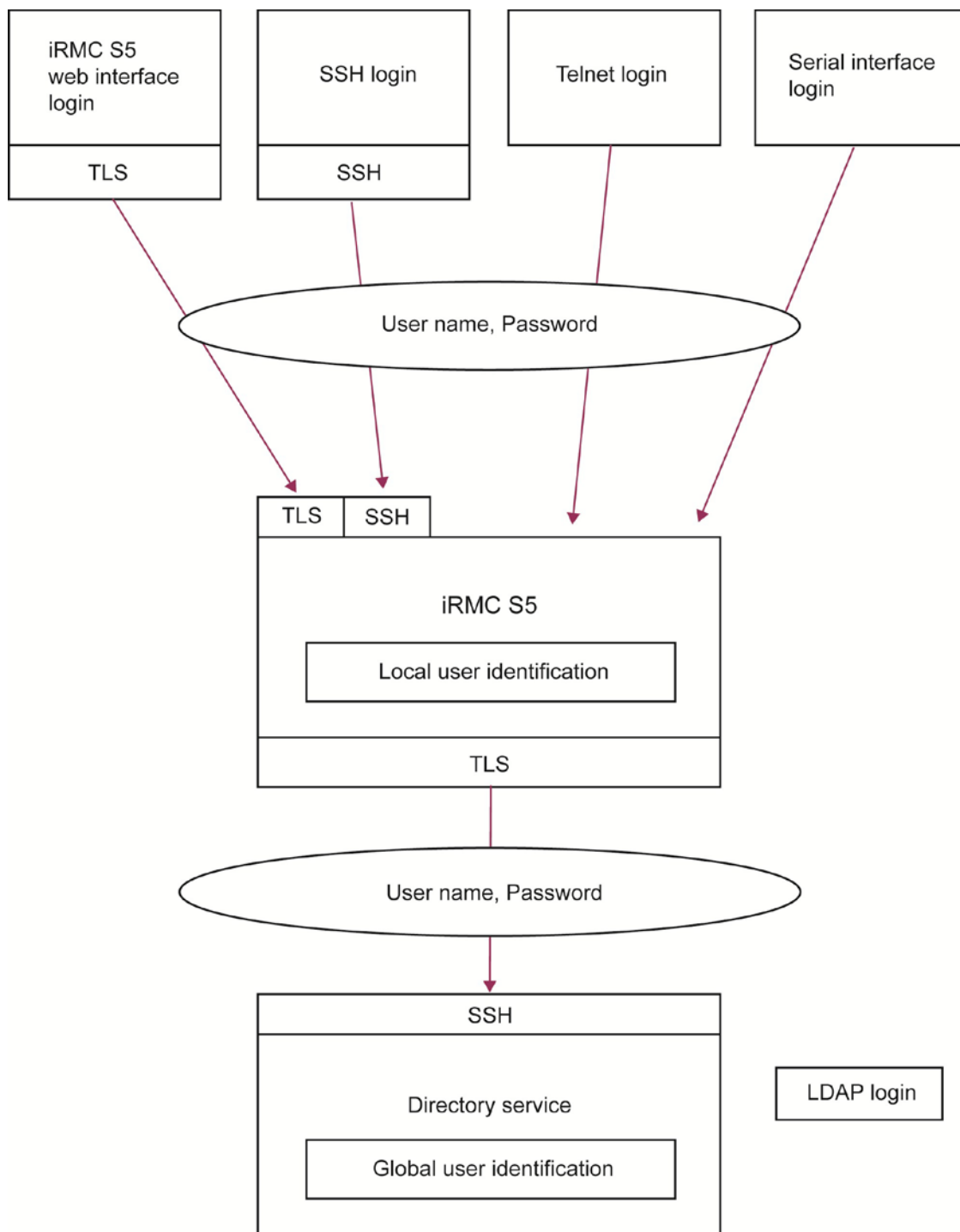


Figure 4: Login authentication via the iRMC S5

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

## 4.2 User permissions

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

**Channel-specific privileges (via assignment to channel-specific permission groups)** The iRMC assigns each user identification to one of the following four channel-specific permission groups:

- User
- Operator
- Administrator
- OEM

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

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

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

### Permissions to use special iRMC functions

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

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

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

- For the iRMC web interface in the "Cisco C880 M5 User Interface Guide"

## 4.3 Local user management

The iRMC possesses its own local user management. Up to 16 users can be configured with passwords and be assigned various rights depending on the user groups they belong to. The user identifications are stored in the local, non-volatile storage of the iRMC S5.

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

- User management via the web interface ("[Local user management using the iRMC web interface](#)" on page 27)

Additionally the iRMC also supports SSHv2-based public key authentication using pairs of public and private keys for local users ("[Secure Authentication via SSHv2](#)" on page 28).

### 4.3.1 Local user management using the iRMC web interface

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

User management on the iRMC requires Configure User Accounts permission.

#### Showing the list of configured users

A list of configured users opens in the **iRMC Local User Accounts** group on the **User Management** page in the **Settings** menu.

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

#### Configuring new users

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

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

#### Modifying the configuration of a user

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

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

#### Deleting users

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

For more information on the **User Management** page of the iRMC web interface, refer to the "Cisco C880 M5 User Interface Guide".

## 4.3.2 Secure Authentication via SSHv2

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

The iRMC supports the following types of public keys:

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

The public SSHv2 keys that you upload to the iRMC can be available either in RFC4716 format or in OpenSSH format ("[Example: Public SSHv2 key](#)" on page 32).

### Public key authentication

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

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

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

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

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

1. Create the public and private SSHv2 keys with the program `ssh-keygen` and save them in separate files ("[Creating public and private SSHv2 keys](#)" on page 29).
2. Upload the public SSHv2 key onto the iRMC from a file ("[Uploading the public SSHv2 key](#)" on page 30).
3. Configure the program `ssh` for SSHv2 access to the iRMC ("[Using the public SSHv2 key](#)" on page 31).

### 4.3.2.1 Creating public and private SSHv2 keys

You can create public and private SSHv2 keys.

#### Using the OpenSSH client program `ssh-keygen`

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

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

Proceed as follows:

1. Open a command window.
2. Call `ssh-keygen` to generate an RSA key pair:  
`ssh-keygen -t rsa`  
`ssh-keygen` logs the progress of the key generation operation. `ssh-keygen` queries the user for the file name under which the private key is to be stored and for the passphrase for the private key. `ssh-keygen` stores the resulting private and public SSHv2 keys in separate files and displays the fingerprint of the public key.

Example: Generating an RSA key pair with `ssh-keygen`

```

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

```

Explanation:

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

### 4.3.2.2 Uploading the public SSHv2 key

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

1. Login to the iRMC web interface.
2. Open the **User Management** page in the **Settings** menu.
3. In the list of configured users click **Edit** next to the relevant user.
4. In the **Edit Local User Account** dialog open the **Certificates** tab.
5. Open the **SSHv2public Key** sub tab.
6. Click **Select** in the **Upload** group and navigate to the file containing the required public key.
7. Click **Upload** to load the public key onto the iRMC.  
After the key has been successfully uploaded, the iRMC displays the key fingerprint in the **Fingerprint** field.

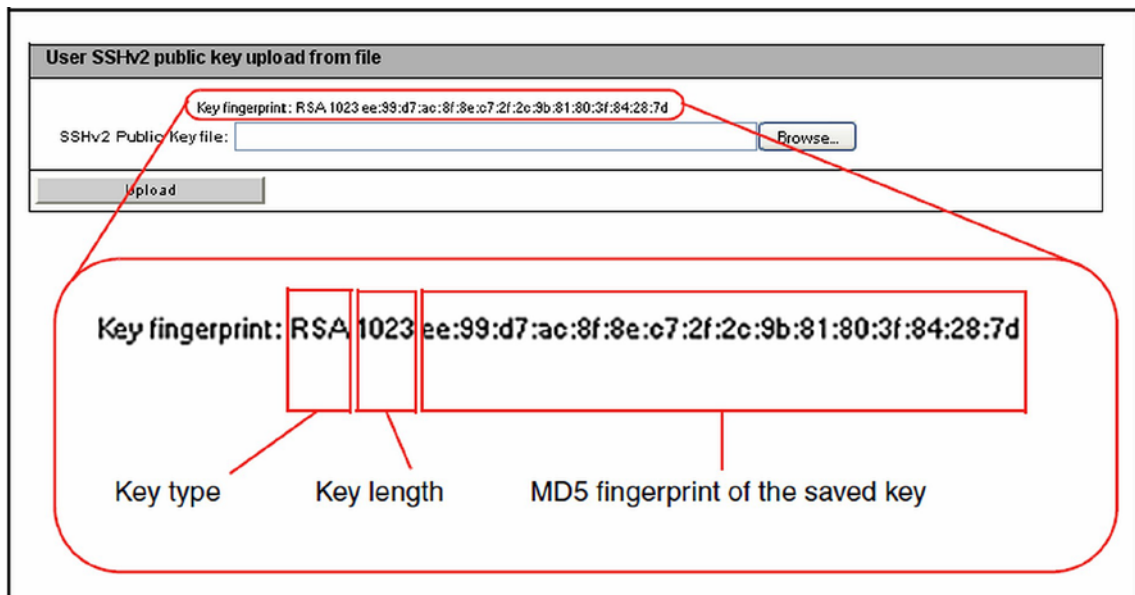


Figure 5: Display of the key fingerprint

8. For reasons of security, ensure that the fingerprint shown here matches that shown in ssh-keygen ("[Creating public and private SSHv2 keys](#)" on page 29) in the **Key fingerprint** field.

### 4.3.2.3 Using the public SSHv2 key

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

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

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

The login must have been configured as a local login on the iRMC and the associated SSHv2 key must have been loaded on the iRMC S5.

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

- Command line arguments that you specify when calling `ssh`.
- User-specific configuration file (`$HOME/.ssh/config`)
  - i** Although this file contains no security-critical information, read/write permission should only be granted to the owner. Access should be denied to all other users.
- System-wide configuration file (`/etc/ssh/ssh_config`) This file contains default values for configuration parameters:
  - If there is no user-specific configuration file
  - If the relevant parameters are not specified in the user-specific configuration file

The value found first applies for each option.

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

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

Proceed as follows:

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

```
ssh -l [<user>] <iRMC_S5>
```

or

```
ssh [<user>@]<iRMC_S5>
```

#### **<user>**

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

**<iRMC\_S5>**

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

Example: SSHv2-authenticated login on the iRMC

For the following ssh- call, it is assumed that ssh-keygen has been used to generate a public/private RSA key pair ("[Creating public and private SSHv2 keys](#)" on page 29) and that the public key User1/.ssh/id\_rsa.pub has been loaded onto the iRMC for an iRMC user user4 ("[Uploading the public SSHv2 key](#)" on page 30).

You can then log in from your local computer under \$HOME/User1 as follows on the iRMC "C880M5-iRMC" using the user name user4:

```
ssh user4@C880M5-iRMC
```

**4.3.2.4 Example: Public SSHv2 key**

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

**RFC4716 format**

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

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

```
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4  
hx
```

```
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9 Ar  
JxjlhXUzIPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsfc+F  
pGJ2iw==
```

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



### OpenSSH format

ssh-rsa

AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4  
hxv6+\ AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar  
J

xjlhXUzIPPVzuBtPaRB7+\ bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGwsfc+Fp  
GJ2iw== rsa-key- 20090401

# 5 Remote installation of the operating system

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

The chapter discusses the following specific topics:

- General procedure for the remote installation of an operating system using storage media which are provided via the "Virtual Media" feature. In the following, storage media provided via the "Virtual Media" feature are referred to as virtual storage media for short.
- Installing Linux from the remote workstation after configuration on the managed server.
- The description focuses primarily on the handling of the virtual storage media.

Prerequisites for the remote installation of the operating system via iRMC S5:

- The iRMC's LAN interface must be configured (["Configuring the LAN interface using UEFI" on page 18](#)).

## 5.1 General procedure for installing the operating system

You perform installation from the remote workstation via the AVR window using virtual media.

### Linux

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

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

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

## 5.2 Connecting a storage medium as Virtual Media


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

The source for the virtual drive can be:

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

For more information on the "virtual Media" feature, refer to the "Cisco C880 M5 User Interface Guide".

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

1. Log into the iRMC web interface with Remote Storage Enabled permission.
2. Start the AVR with the  button in the title bar of the iRMC web interface.
3. Start Virtual Media in the AVR window. The **Virtual Media** dialog opens.
4. In the appropriate panel of the **Virtual Media** dialog, click **Browse**. The **Open** file browser dialog opens.
5. In the **Open** dialog, navigate to the directory of the storage medium that you want to make available as virtual medium from your remote workstation.
  - Installation from the vendor’s installation CD/DVD: Linux installation CD/DVD and optional drivers.
6. Select the required device type in the **Files of Type** field.
7. Specify the storage medium you want to connect as a virtual medium in the **File Name** field:
  1. In the case of an ISO image (ISO/NRG image), enter the file name. Alternatively, click on the file name in the Explorer.
  2. In the case of a drive, enter the name of the drive, e.g. /dev/... (Linux)

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

## 5.3 Booting the managed server

To boot the managed server from Linux installation CD/DVD, proceed as follows:

1. Use the options in the **Power On/Off Scheduler** group on the **Power Management** page of the iRMC web interface to start up or reboot the managed server. You can follow the progress of the boot process in the AVR window.  
During the managed server's BIOS POST phase, virtual storage media are displayed as USB 2.0 devices. Virtual storage media are represented by the following entries in the BIOS boot sequence:
  - A (physical) floppy disk is represented by a separate entry "Fujitsu RemoteStorage FD-(USB 2.0)".
  - All other virtual storage device types are represented by the shared entry "CD-ROM DRIVE".If a local CD-ROM/DVD-ROM drive and a CD-ROM/DVD-ROM drive connected as virtual media are both present at the managed server then the managed server boots from the CD-ROM/DVD-ROM drive provided via Virtual Image.
2. Press [F2] on the keyboard while the server is booting.
3. In the UEFI set-up, open the **Boot** menu in which you can define the boot sequence.
4. Specify **Boot Priority=1** (highest priority) for the Linux installation CD/DVD which is connected as virtual storage medium.
5. Save your settings and exit the UEFI setup.  
The managed server then boots from Linux installation CD/DVD which is connected as virtual storage.

If the system does not boot from the virtual storage medium (Linux installation CD/DVD):

1. Check whether the storage medium is displayed during the BIOS POST phase and connect the storage medium as a virtual medium if necessary.
2. Make sure that the correct boot sequence is specified.  
It takes about 5 minutes to boot from Linux installation CD/DVD via a virtual storage medium. The boot progress is indicated during the boot process.

## 6 Firmware update

The iRMC uses two different firmware images. The two firmware images each are stored on a 48-MB EEPROM (Electrically Erasable Programmable Read-Only Memory):

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

One of the two firmware images is active (running) at any given time, while the other is inactive. The firmware image that is active depends on the so-called firmware selector ("[Firmware selector](#)" on page 38).

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

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

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

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

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

Information on the iRMC firmware and EEPROM can be found:

- In the iRMC web interface, **System Overview** page of the **System** menu

## 6.1 Firmware selector

The firmware selector specifies the iRMC S5 firmware to be executed. Every time the iRMC is reset and restarted, the firmware selector is evaluated and processing branches to the corresponding firmware.

The firmware selector can have the following values:

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

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

You can query and explicitly set the firmware selector:

- On the **System Overview** page of the iRMC web interface in the **Running iRMC Firmware** group (for more information, refer to the "Cisco C880 M5 User Interface Guide").

## 6.2 Firmware image downgrade

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

The simplest way to downgrade the firmware is to store the previous-version firmware image as the inactive firmware image in the EEPROM of the iRMC. In this case, you only have to set the firmware selector to this previous-version image ("[Firmware selector](#)" on page 38) and subsequently restart the iRMC to activate the firmware.

## 6.3 Firmware image update

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

The following methods are available for updating the firmware images:

### **With the iRMC web interface**

The **System Overview** page allows you to update the firmware of the iRMC by providing the firmware image either:

- Locally on the remote workstation
- On a network share
- On a TFTP server (for more information, refer to the "Cisco C880 M5 User Interface Guide")