Installing the Cisco CSP 5200

Preparing for Installation

This section contains the following topics:

Installation Warnings and Guidelines

Note Before you install, operate, or service a server, review the Regulatory Compliance and Safety Information for Cisco Cloud Services Platforms for important safety information.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

Statement 1071

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 35° C (95° F).**

Statement 1047

Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.**

Statement 1019

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 15 A.**

Statement 1005

Warning **Installation of the equipment must comply with local and national electrical codes.**

Statement 1074

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock, and key, or other means of security.**

Statement 1017

Caution To ensure proper airflow it is necessary to rack the servers using rail kits. Physically placing the units on top of one another or "stacking" without the use of the rail kits blocks the air vents on top of the servers, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your servers on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the servers. No additional spacing between the servers is required when you mount the units using rail kits.

Caution Avoid uninterruptible power supply (UPS) types that use ferroresonant technology. These UPS types can become unstable with systems such as the Cisco UCS, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

When you are installing a server, use the following guidelines:

- Plan your site configuration and prepare the site before installing the server.

- Ensure that there is adequate space around the server to allow for accessing the server and for adequate airflow. The airflow in this server is from front to back.
- Ensure that the air-conditioning meets the thermal requirements listed in the Environmental Specifications.
- Ensure that the cabinet or rack meets the requirements listed in the Rack Requirements, on page 3.
- Ensure that the site power meets the power requirements listed in the Power Specifications. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Rack Requirements

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, four-post EIA rack, with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- The rack-post holes can be square 0.38-inch (9.6 mm), round 0.28-inch (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the Cisco-supplied slide rails.
- The minimum vertical rack space per server must be one rack unit (RU), equal to 1.75 in. (44.45 mm).

Supported Cisco Slide Rail Kits

The server supports the following rail kit:

Cisco part UCSC-RAILB-M4= (ball-bearing rail kit is included with the server)

Rack Installation Tools Required

The slide rails shipped with this server do not require tools for installation.

Installing the Cisco CSP 5200 in a Rack

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Statement 1006

Procedure

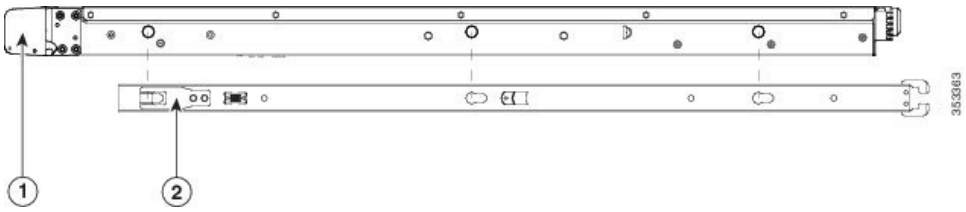
Step 1 Attach the inner rails to the sides of the Cisco CSP 5200:

a) Align an inner rail with one side of the server so that the three keyed slots in the rail align with the three pegs on the side of the Cisco CSP 5200.

b) Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.

c) Install the second inner rail to the opposite side of the Cisco CSP 5200.

Figure 1: Attaching the Inner Rail to the Side of the Cisco CSP 5200

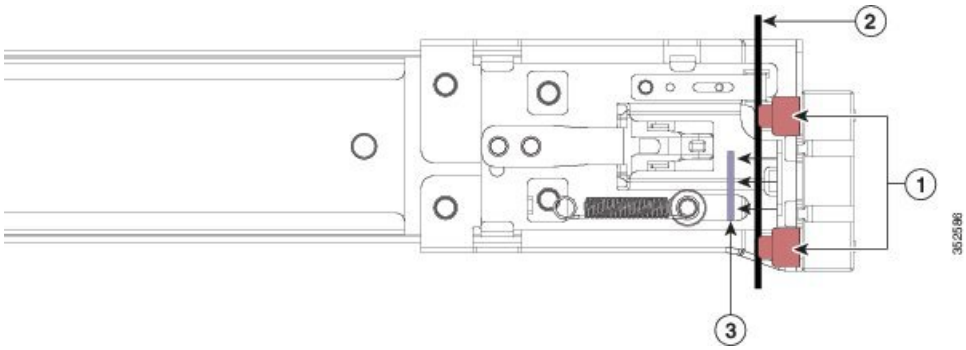


1	Front of Cisco CSP 5200	**2**	Locking clip on front of inner rail

Step 2 Open the front securing plate on both slide-rail assemblies. The front end of the slide-rail assembly has a spring-loaded securing plate that must be open before you can insert the mounting pegs into the rack-post holes.

On the *outside* of the assembly, push the green-arrow button toward the rear to open the securing plate.

Figure 2: Front Securing Mechanism, Inside of Front End



1	Front mounting pegs	**3**	Securing plate shown pulled back to the open position
2	Rack post between mounting pegs and opened securing plate	**-**	

Step 3 Install the outer slide rails into the rack:

a) Align one slide-rail assembly front end with the front rack-post holes that you want to use.

The slide rail front-end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front.

Note The rack post must be between the mounting pegs and the *open* securing plate.

b) Push the mounting pegs into the rack-post holes from the outside-front.
c) Press the securing plate release button, marked PUSH. The spring-loaded securing plate closes to lock the pegs in place.
d) Adjust the slide-rail length, and then push the rear mounting pegs into the corresponding rear rack-post holes. The slide rail must be level front-to-rear.

   The rear mounting pegs enter the rear rack-post holes from the *inside* of the rack post.

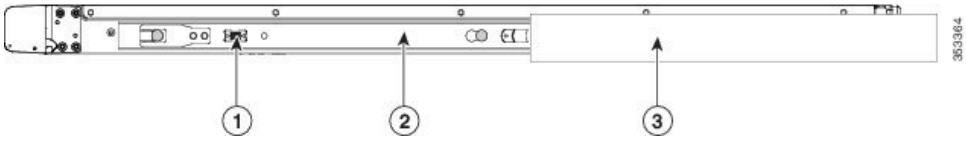
e) Attach the second slide-rail assembly to the opposite side of the rack. Ensure that the two slide-rail assemblies are at the same height and are level front-to-back.
f) Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

Step 4 Insert the server into the slide rails:

Caution This server can weigh up to 60 pounds (27 kilograms) when fully loaded with components. We recommend that you use a minimum of two people or a mechanical lift when lifting the server. Attempting this procedure alone could result in personal injury or equipment damage.

a) Align the rear ends of the inner rails that are attached to the server sides with the front ends of the empty slide rails on the rack.
b) Push the inner rails into the slide rails on the rack until they stop at the internal stops.
c) Slide the inner-rail release clip toward the rear on both inner rails, and then continue pushing the server into the rack until its front slam-latches engage with the rack posts.

Figure 3: Inner-Rail Release Clip



1	Inner-rail release clip	**3**	Outer slide rail attached to rack post
2	Inner rail attached to server and inserted into outer slide rail	**-**	

Step 5 (Optional) Secure the server in the rack more permanently by using the two screws that are provided with the slide rails. Perform this step if you plan to move the rack with Cisco CSP 5200 installed.

With the Cisco CSP 5200 fully pushed into the slide rails, open a hinged slam latch lever on the front of the Cisco CSP 5200 and insert a screw through the hole that is under the lever. The screw threads into the static part of the rail on the rack post and prevents the Cisco CSP 5200 from being pulled out. Repeat for the opposite slam latch.

Initial Cisco CSP 5200 Setup

Note This section describes how to power on the Cisco CSP 5200, assign an IP address, and connect to server management when using the Cisco CSP 5200 in standalone mode.

Cisco CSP 5200 Default Settings

The Cisco CSP 5200 is shipped with these default settings:

- The NIC mode is *Dedicated*.
- The NIC redundancy is *None*.
- DHCP is enabled.
- IPv4 is enabled.

Connection Methods

There are two methods for connecting to the system for initial setup:

- Local setup—Use this procedure if you want to connect a keyboard and monitor directly to the system for setup. This procedure can use the included KVM cable or the ports on the rear of the server.
- Remote setup—Use this procedure if you want to perform setup through your dedicated management LAN.

Note To configure the system remotely, you must have a DHCP server on the same network as the system. Your DHCP server must be preconfigured with the range of MAC addresses for this server node. The MAC address is printed on a label that is on the pull-out asset tag on the front panel. This server node has a range of six MAC addresses assigned to the Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

This section contains the following topics:

Connecting to the Server Locally For Setup

This procedure requires the following equipment:

- VGA monitor
- USB keyboard
- Either the supported Cisco KVM cable; or a USB cable and VGA DB-15 cable

Procedure

Step 1 Attach a power cord to each power supply in your server, and then attach each power cord to a grounded power outlet.

Wait for approximately two minutes to let the server boot to standby power during the first bootup. You can verify system power status by looking at the system Power Status LED on the front panel. The system is in standby power mode when the LED is amber.

Step 2 Connect a USB keyboard and VGA monitor to the server using one of the following methods:

- Connect the included KVM cable to the KVM connector on the front panel. Connect your USB keyboard and VGA monitor to the KVM cable.
- Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear panel.

Step 3 Open the Cisco IMC Configuration Utility:

a) Press and hold the front panel power button for four seconds to boot the server.
b) During bootup, press **F8** when prompted to open the Cisco IMC Configuration Utility.

Note The first time that you enter the Cisco IMC Configuration Utility, you are prompted to change the default password. The default password is *password*. The Strong Password feature is enabled.

The following are the requirements for Strong Password:

- The password can have minimum 8 characters; maximum 14 characters.
- The password must not contain the user's name.
- The password must contain characters from three of the following four categories:
  - English uppercase letters (A through Z)
  - English lowercase letters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters !, @, #, $, %, ^, &, *, -, _, =, ‘‘

Step 4 Continue with Setting Up the System With the Cisco IMC Configuration Utility, on page 9.

Connecting to the Server Remotely For Setup

This procedure requires the following equipment:

- One RJ-45 Ethernet cable that is connected to your management LAN.

Before you begin

Note To configure the system remotely, you must have a DHCP server on the same network as the system. Your DHCP server must be preconfigured with the range of MAC addresses for this server node. The MAC address is printed on a label that is on the pull-out asset tag on the front panel. This server node has a range of six MAC addresses assigned to the Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

Procedure

Step 1 Attach a power cord to each power supply in your server, and then attach each power cord to a grounded power outlet.

Wait for approximately two minutes to let the server boot to standby power during the first bootup. You can verify system power status by looking at the system Power Status LED on the front panel. The system is in standby power mode when the LED is amber.

Step 2 Plug your management Ethernet cable into the dedicated management port on the rear panel.

Step 3 Allow your preconfigured DHCP server to assign an IP address to the server node.

Step 4 Use the assigned IP address to access and log in to the Cisco IMC for the server node. Consult with your DHCP server administrator to determine the IP address.

Note The default user name for the server is *admin*. The default password is *password*.

Step 5 From the Cisco IMC Server Summary page, click **Launch KVM Console**. A separate KVM console window opens.

Step 6 From the Cisco IMC Summary page, click **Power Cycle Server**. The system reboots.

Step 7 Select the KVM console window.

Note The KVM console window must be the active window for the following keyboard actions to work.

Step 8 When prompted, press **F8** to enter the Cisco IMC Configuration Utility. This utility opens in the KVM console window.

Note The first time that you enter the Cisco IMC Configuration Utility, you are prompted to change the default password. The default password is *password*. The Strong Password feature is enabled.

The following are the requirements for Strong Password:

- The password can have minimum 8 characters; maximum 14 characters.
- The password must not contain the user's name.
- The password must contain characters from three of the following four categories:
  - English uppercase letters (A through Z)
  - English lowercase letters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters !, @, #, $, %, ^, &, *, -, _, =, ‘‘

Step 9 Continue with Setting Up the System With the Cisco IMC Configuration Utility, on page 9.

Setting Up the System With the Cisco IMC Configuration Utility

Before you begin

The following procedure is performed after you connect to the system and open the Cisco IMC Configuration Utility.

Procedure

Step 1 Choose whether to enable DHCP for dynamic network settings, or to enter static network settings.

Note Before you enable DHCP, you must preconfigure your DHCP server with the range of MAC addresses for this server. The MAC address is printed on a label on the rear of the server. This server has a range of six MAC addresses assigned to Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

The *static* IPv4 and IPv6 settings include the following:

- The Cisco IMC IP address.

  For IPv6, valid values are 1 - 127.

- The gateway.

  For IPv6, if you do not know the gateway, you can set it as none by entering :: (two colons).

- The preferred DNS server address.

  For IPv6, you can set this as none by entering :: (two colons).

Step 2 (Optional) Make VLAN settings.

Step 3 Press **F1** to go to the second settings window, then continue with the next step.

From the second window, you can press **F2** to switch back to the first window.

Step 4 (Optional) Set a hostname for the server.

Step 5 (Optional) Enable dynamic DNS and set a dynamic DNS (DDNS) domain.

Step 6 (Optional) If you check the Factory Default check box, the server reverts to the factory defaults.

Step 7 (Optional) Set a default user password.

Note The factory default username for the server is *admin*. The default password is *password*.

Step 8 (Optional) Enable auto-negotiation of port settings or set the port speed and duplex mode manually.

Note Auto-negotiation is applicable only when you use the Dedicated NIC mode. Auto-negotiation sets the port speed and duplex mode automatically based on the switch port to which the server is connected. If you disable auto-negotiation, you must set the port speed and duplex mode manually.

Step 9 (Optional) Reset port profiles and the port name.

Step 10 Press **F5** to refresh the settings that you made. You might have to wait about 45 seconds until the new settings appear and the message, "Network settings configured" is displayed before you reboot the server in the next step.

Step 11 Press **F10** to save your settings and reboot the server.

Note If you chose to enable DHCP, the dynamically assigned IP and MAC addresses are displayed on the console screen during bootup.

What to do next

Use a browser and the IP address of the Cisco IMC to connect to the Cisco IMC management interface. The IP address is based upon the settings that you made (either a static address or the address assigned by your DHCP server).

Note The factory default username for the server is *admin*. The default password is *password*.

To manage the server, see the *Cisco UCS C-Series Rack-Mount Server Configuration Guide* or the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide* for instructions on using those interfaces for your Cisco IMC release. The links to the configuration guides are in the Cisco UCS C-Series Documentation Roadmap.

Updating the BIOS and Cisco IMC Firmware

Caution When you upgrade the BIOS firmware, you must also upgrade the Cisco IMC firmware to the same version or the server does not boot. Do not power off the server until the BIOS and Cisco IMC firmware are matching or the server does not boot.

Cisco provides the *Cisco UCS Host Upgrade Utility* to assist with simultaneously upgrading the BIOS, Cisco IMC, and other firmware to compatible levels.

The server uses firmware obtained from and certified by Cisco. Cisco provides release notes with each firmware image. There are several possible methods for updating the firmware:

- **Recommended method for firmware update:** Use the Cisco UCS Host Upgrade Utility to simultaneously upgrade the Cisco IMC, BIOS, and component firmware to compatible levels.

  See the *Cisco UCS Host Upgrade Utility Quick Reference Guide* for your firmware release at the documentation roadmap link below.

- You can upgrade the Cisco IMC and BIOS firmware by using the Cisco IMC GUI interface.

  See the *Cisco UCS C-Series Rack-Mount Server Configuration Guide*.

- You can upgrade the Cisco IMC and BIOS firmware by using the Cisco IMC CLI interface.

  See the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide*.

For links to the documents listed above, see the Cisco UCS C-Series Documentation Roadmap.

Older NAND Flash Not Detectable By Latest Cisco IMC

Caution If your system is running Cisco IMC 4.0(1b) or later, and you have the latest NAND flash chip MT29F4G08ABAFAWP-IT:F (M70A), do not downgrade the Cisco IMC to an earlier version. Earlier versions of the BMC cannot detect this latest NAND Flash chip.

Accessing the System BIOS

Procedure

Step 1 Enter the BIOS Setup Utility by pressing the **F2** key when prompted during bootup.

Note The version and build of the current BIOS are displayed on the Main page of the utility.

Step 2 Use the arrow keys to select the BIOS menu page.

Step 3 Highlight the field to be modified by using the arrow keys.

Step 4 Press **Enter** to select the field that you want to change, and then modify the value in the field.

Step 5 Press the right arrow key until the Exit menu screen is displayed.

Step 6 Follow the instructions on the Exit menu screen to save your changes and exit the setup utility (or press **F10**). You can exit without saving changes by pressing **Esc**.

Smart Access Serial

This server supports the Smart Access Serial feature. This feature allows you to switch between host serial and Cisco IMC CLI.

- This feature has the following requirements:
  - A serial cable connection, which can use either the RJ-45 serial connector on the server rear panel, or a DB-9 connection when using the supplied KVM cable on the front-panel KVM console connector.
  - Console redirection must be enabled in the server BIOS.
  - Terminal type must be set to VT100+ or VTUFT8.
  - Serial-over-LAN (SOL) must be disabled (SOL is disabled by default).
- To switch from host serial to Cisco IMC CLI, press **Esc+9**.

  You must enter your Cisco IMC credentials to authenticate the connection.
- To switch from Cisco IMC CLI to host serial, press **Esc+8**.

Note You cannot switch to Cisco IMC CLI if the serial-over-LAN (SOL) feature is enabled.

- After a session is created, it is shown in the CLI or web GUI by the name `serial`.

Smart Access USB

This server supports the Smart Access USB feature. The board management controller (BMC) in this server can accept a USB mass storage device and access the data on it. This feature allows you to use the front-panel USB device as a medium to transfer data between the BMC and the user without need for network connectivity. This can be useful, for example, when remote BMC interfaces are not yet available, or are not accessible due to network misconfiguration.

- This feature has the following requirements:
  - The included KVM cable connected to the front panel KVM console connector.
  - A USB storage device connected to one of the USB 2.0 connectors on the KVM cable. The USB device must draw less than 500 mA to avoid disconnect by the current-protection circuit.

    Note Any mouse or keyboard that is connected to the KVM cable is disconnected when you enable Smart Access USB.

  - You can use USB 3.0-based devices, but they will operate at USB 2.0 speed.
  - We recommend that the USB device have only one partition.
  - The file system formats supported are: FAT16, FAT32, MSDOS, EXT2, EXT3, and EXT4. NTFS is not supported.
- The front-panel KVM connector has been designed to switch the USB port between Host OS and BMC.
- Smart Access USB can be enabled or disabled using any of the BMC user interfaces. For example, you can use the Cisco IMC Configuration Utility that is accessed by pressing **F8** when prompted during bootup.
  - Enabled: the front-panel USB device is connected to the BMC.
  - Disabled: the front-panel USB device is connected to the host.
- In a case where no management network is available to connect remotely to Cisco IMC, a Device Firmware Update (DFU) shell over serial cable can be used to generate and download technical support files to the USB device that is attached to front panel USB port.