



Installing Cisco CSP 2100

This chapter describes how to install Cisco CSP 2100, and includes the following sections:

- [Unpacking and Inspecting Cisco CSP 2100, page 2-2](#)
- [Preparing for the Cisco CSP 2100 Installation, page 2-3](#)
- [Installing Cisco CSP 2100 In a Rack, page 2-5](#)
- [Initial Cisco CSP 2100 Setup, page 2-8](#)
- [System BIOS and CIMC Firmware, page 2-12](#)
- [Updating the BIOS and CIMC Firmware, page 2-12](#)



Note

Before you install, operate, or service Cisco CSP 2100, review the [Regulatory Compliance and Safety Information for Cisco Cloud Services Platform 2100](#) 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

Unpacking and Inspecting Cisco CSP 2100

**Caution**

When handling internal Cisco CSP 2100 components, wear an ESD strap and handle modules by the carrier edges only.

**Tip**

Keep the shipping container in case Cisco CSP 2100 requires shipping in the future.

**Note**

The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

-
- Step 1** Remove Cisco CSP 2100 from its cardboard container and save all packaging material.
- Step 2** Compare the shipment to the equipment list provided by your customer service representative. Verify that you have all items.
- Step 3** Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:
- Invoice number of shipper (see the packing slip)
 - Model and serial number of the damaged unit
 - Description of damage
 - Effect of damage on the installation
-

Preparing for the Cisco CSP 2100 Installation

This section provides information about preparing for the Cisco CSP 2100 installation, and it includes the following topics:

- [Installation Guidelines, page 2-3](#)
- [Rack Requirements, page 2-4](#)
- [Equipment Requirements, page 2-4](#)
- [Slide Rail Adjustment Range, page 2-4](#)

Installation Guidelines



Warning

To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 40° C (104° 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



Caution

To ensure proper airflow it is necessary to rack the Cisco CSP 2100s 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 Cisco CSP 2100s, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your Cisco CSP 2100s on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the Cisco CSP 2100s. No additional spacing between the Cisco CSP 2100s is required when you mount the units using rail kits.



Caution

Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with systems such as Cisco CSP 2100, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

When you are installing Cisco CSP 2100, use the following guidelines:

- Plan your site configuration and prepare the site before installing Cisco CSP 2100. The site planning for Cisco CSP 2100 is similar to that for Cisco UCS server. See the [Cisco UCS Site Preparation Guide](#) for the recommended site planning tasks.
- Ensure that there is adequate space around Cisco CSP 2100 to allow for servicing and for adequate airflow. The airflow in Cisco CSP 2100 is from front to back.
- Ensure that the air-conditioning meets the thermal requirements listed in the [Cisco CSP 2100 Specifications, page 4-1](#).
- Ensure that the cabinet or rack meets the requirements listed in the “[Rack Requirements](#)” section on [page 2-4](#).
- Ensure that the site power meets the power requirements listed in the [Cisco CSP 2100 Specifications, page 4-1](#). If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Rack Requirements

This section provides the requirements for the standard open racks. 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 supplied slide rails.
- The minimum vertical rack space per Cisco CSP 2100 must be one RU, equal to 1.75 in. (44.45 mm).

Equipment Requirements

The slide rails sold by Cisco Systems for Cisco CSP 2100 do not require tools for installation.

Slide Rail Adjustment Range

The slide rails for Cisco CSP 2100 have an adjustment range of 24 to 36 inches (610 to 914 mm).

Installing Cisco CSP 2100 In a Rack

Installing the Slide Rails

This section describes how to install Cisco CSP 2100 in a rack using the rack kits that are sold by Cisco.


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

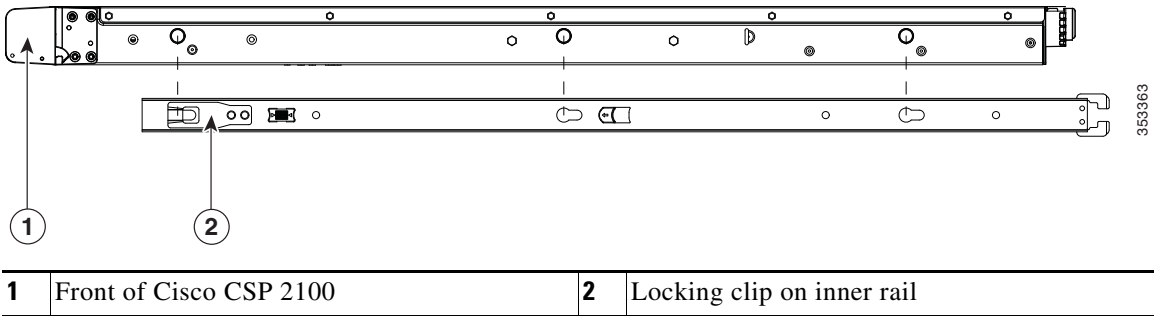
- Step 1
- Attach the inner rails to the sides of Cisco CSP 2100:
- a.

Align an inner rail with one side of Cisco CSP 2100 so that the three keyed slots in the rail align with the three pegs on the side of Cisco CSP 2100 (see [Figure 2-1](#)).
- 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 Cisco CSP 2100.

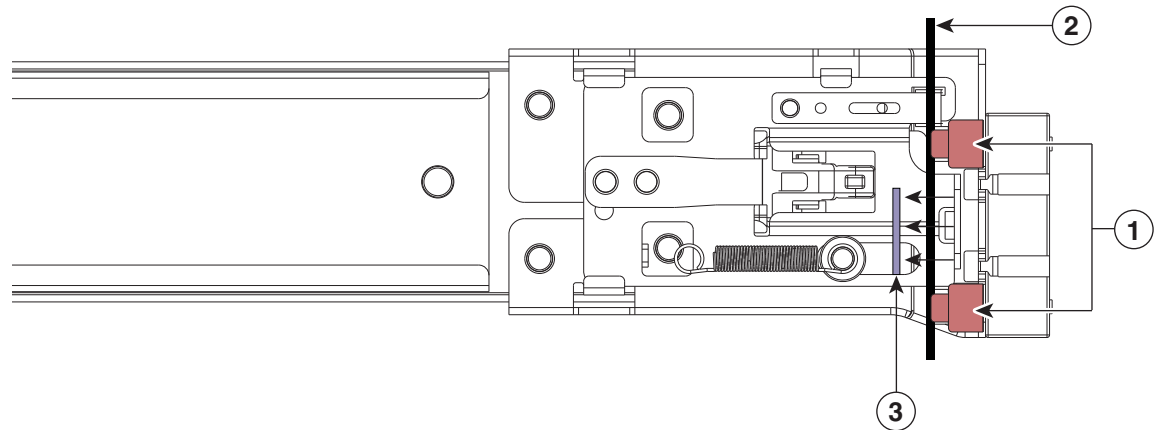
Figure 2-1 Attaching Inner Rail to Side of Cisco CSP 2100



- 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 (see [Figure 2-2](#)).

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

Figure 2-2 Front Securing Mechanism, Inside of Front End



1	Front mounting pegs	3	Securing plate shown pulled back to open position
2	Rack post		

- 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 (see [Figure 2-2](#)).



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

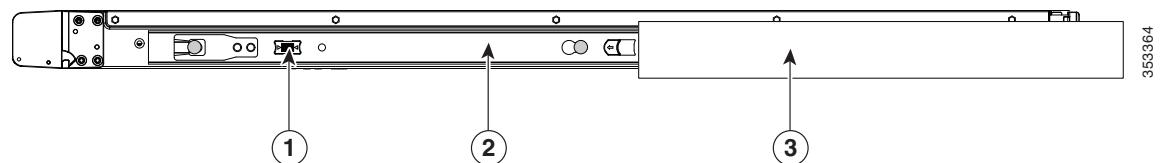
- b. Push the mounting pegs into the rack-post holes from the outside-front.
- c. Press the securing plate release button, marked PUSH. The spring-loaded securing plate closes to lock the pegs in place.
- d. Adjust the slide-rail length, and then push the rear mounting pegs into the corresponding rear 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 with each other 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 Cisco CSP 2100 into the slide rails:**Caution**

Cisco CSP 2100 can weigh up to **67 pounds (59 kilograms)** when fully loaded with components. We recommend that you use a minimum of two people or a mechanical lift when lifting Cisco CSP 2100. Attempting this procedure alone could result in personal injury or equipment damage.

- a. Align the rear of the inner rails that are attached to Cisco CSP 2100 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 release clip toward the rear on both inner rails, and then continue pushing Cisco CSP 2100 into the rack until its front slam latches engage with the rack posts.

Figure 2-3 Inner Rail Release Clip



1	Inner rail release clip	3	Outer rail attached to rack post
2	Inner rail attached to Cisco CSP 2100 and inserted into outer rail		

Step 5 (Optional) Secure the Cisco CSP 2100 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 2100 installed.

With Cisco CSP 2100 fully pushed into the slide rails, open a hinged slam latch lever on the front of the Cisco CSP 2100 and insert the 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 Cisco CSP 2100 from being pulled out. Repeat for the opposite slam latch.

Initial Cisco CSP 2100 Setup

Connecting and Powering On Cisco CSP 2100 (Standalone Mode)

**Note**

This section describes how to power on Cisco CSP 2100, assign an IP address, and connect to Cisco CSP 2100 management when using the Cisco CSP 2100 *in standalone mode*.

Cisco CSP 2100 is shipped with these default settings:

- The NIC mode is Shared LOM EXT.

Shared LOM EXT mode enables the 1-Gb Ethernet ports and the ports on any installed Cisco network interface card (NIC) to access Cisco Integrated Management Interface (CIMC). If you want to use the 10/100/1000 dedicated management ports to access CIMC, you can connect to the Cisco CSP 2100 and change the NIC mode as described in [Step 1](#) of the following procedure.

- The NIC redundancy is active-active. All Ethernet ports are utilized simultaneously.
- DHCP is enabled.
- IPv4 is enabled.

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 to the system for setup. This procedure can use a KVM cable (Cisco PID N20-BKVM) or the ports on the rear of the Cisco CSP 2100. See [Local Connection Procedure, page 2-8](#).
- Remote setup—Use this procedure if you want to perform setup through your dedicated management LAN. See [Remote Connection Procedure, page 2-9](#).

**Note**

To configure the system remotely, you must have a DHCP server on the same network as the system. Your DHCP server must be pre-configured with the range of MAC addresses for this server node. The MAC address is printed on a label on the rear of the server node. This server node has a range of six MAC addresses assigned to the CIMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

Local Connection Procedure

- Step 1** Attach a power cord to each power supply in your Cisco CSP 2100, and then attach each power cord to a grounded AC power outlet. See [Power Specifications, page 4-3](#) for power specifications.
- Wait for approximately two minutes to let the Cisco CSP 2100 boot in standby power during the first bootup.
- You can verify system power status by looking at the system Power Status LED on the front panel (see [External Features Overview, page 1-1](#)). The system is in standby power mode when the LED is amber.
- Step 2** Connect a USB keyboard and VGA monitor to the Cisco CSP 2100 using one of the following methods:
- Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear panel (see [External Features Overview, page 1-1](#)).

- Connect an optional KVM cable (Cisco PID N20-BKVM) to the KVM connector on the front panel (see [External Features Overview, page 1-1](#) for the connector location). Connect your USB keyboard and VGA monitor to the KVM cable.
- Step 3** Open the CIMC Configuration Utility:
- a. Press and hold the front panel power button for four seconds to boot the Cisco CSP 2100.
 - b. During bootup, press **F8** when prompted to open the CIMC Configuration Utility.
- This utility has two windows that you can switch between by pressing F1 or F2.
- Step 4** Continue with [CIMC Configuration Utility Setup, page 2-10](#).
-

Remote Connection Procedure

- Step 1** Attach a power cord to each power supply in your Cisco CSP 2100, and then attach each power cord to a grounded AC power outlet. See [Power Specifications, page 4-3](#) for power specifications.
- Wait for approximately two minutes to let the Cisco CSP 2100 boot in standby power during the first bootup.
- You can verify system power status by looking at the system Power Status LED on the front panel (see [External Features Overview, page 1-1](#)). 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 (see [External Features Overview, page 1-1](#)).
- Step 3** Allow your pre-configured 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 CIMC 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 CIMC Server Summary page, click **Launch KVM Console**. A separate KVM console window opens.
- Step 6** From the CIMC 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 CIMC Configuration Utility. This utility opens in the KVM console window.
- This utility has two windows that you can switch between by pressing F1 or F2.
- Step 9** Continue with [CIMC Configuration Utility Setup, page 2-10](#).
-

CIMC Configuration Utility Setup

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

Step 1 Set NIC mode and NIC redundancy:

- a. Set the NIC mode to choose which ports to use to access CIMC for Cisco CSP 2100 management (see [Figure 1-2 on page 1-2](#) for identification of the ports):

- Shared LOM EXT (default)—This is the shared LOM extended mode, the factory-default setting. With this mode, the Shared LOM and Cisco Card interfaces are both enabled.

In this mode, DHCP replies are returned to both the shared LOM ports and the Cisco card ports. If the system determines that the Cisco card connection is not getting its IP address from the Cisco CSP 2100 because the Cisco CSP 2100 is in standalone mode, further DHCP requests from the Cisco card are disabled. Use the Cisco Card NIC mode if you want to connect to CIMC through a Cisco card in standalone mode.

- Shared LOM—The 1-Gb Ethernet ports are used to access CIMC. You must select a NIC redundancy and IP setting.
- Dedicated—The dedicated management port is used to access CIMC. You must select a NIC redundancy and IP setting.

- b. Use this utility to change the NIC redundancy to your preference. Cisco CSP 2100 has three possible NIC redundancy settings:

- None—The Ethernet ports operate independently and do not fail over if there is a problem. This setting can be used only with the Dedicated NIC mode.
- Active-standby—If an active Ethernet port fails, traffic fails over to a standby port.
- Active-active—All Ethernet ports are utilized simultaneously. The Shared LOM EXT mode can have only this NIC redundancy setting. Shared LOM and Cisco Card modes can have both Active-standby and Active-active settings.

Step 2 Choose whether to enable DHCP for dynamic network settings, or to enter static network settings.**Note**

Before you enable DHCP, you must pre-configure 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 CIMC. 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 CIMC IP address.
- The prefix/subnet.

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 3 (Optional) Use this utility to make VLAN settings.

Step 4 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 5 (Optional) Set a hostname for the server.

Step 6 (Optional) Enable dynamic DNS and set a dynamic DNS (DDNS) domain.

Step 7 (Optional) If you check the Factory Default check box, the server reverts to the factory defaults.

Step 8 (Optional) Set a default user password.

Step 9 (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 10 (Optional) Reset port profiles and the port name.

Step 11 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 12 Press **F10** to save your settings and reboot the Cisco CSP 2100.



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

Use a browser and the IP address of the CIMC to connect to the CIMC 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 default username for the server is *admin*. The default password is *admin*.

For information about managing the Cisco CSP 2100, see the *Cisco Cloud Services Platform 2100 Quick Start Guide* and *Cisco Cloud Services Platform 2100 Command Reference*. These guides are available at the following page:

<http://www.cisco.com/c/en/us/support/switches/cloud-services-platform-2100/tsd-products-support-series-home.html>

System BIOS and CIMC Firmware

This section includes information about the system BIOS and it includes the following sections:

- [Updating the BIOS and CIMC Firmware, page 2-12](#)
- [Accessing the System BIOS, page 2-13](#)

Updating the BIOS and CIMC Firmware



Caution

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

Cisco provides the Cisco Host Upgrade Utility to assist with simultaneously upgrading the BIOS, CIMC, 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 methods for updating the firmware:

- **Recommended method for system components firmware update:** Use the Cisco Host Upgrade Utility to simultaneously upgrade the CIMC, BIOS, LOM, and LSI storage controller to compatible levels.
See the *Cisco Host Upgrade Utility Quick Reference Guide* for your firmware level at the documentation roadmap link below.
- You can upgrade the BIOS using the EFI interface or from a Windows or a Linux platform. The procedure to upgrade the BIOS is similar to that used for the Cisco UCS C-Series Rack Mount server. For detailed information, see the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide*.
- You can upgrade the CIMC and BIOS firmware by using the CIMC GUI interface. The procedure to upgrade the CIMC and BIOS is similar to that used for the Cisco UCS C-Series Rack Mount server. For detailed information, see the *Cisco UCS C-Series Rack-Mount Server Configuration Guide*.
- You can upgrade the CIMC and BIOS firmware by using the CIMC CLI interface. The procedure to upgrade the CIMC and BIOS is similar to that used for the Cisco UCS C-Series Rack Mount server. For detailed information, see the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide*.

For links to the documents listed above, see the documentation roadmap at the following URL:

<http://www.cisco.com/go/unifiedcomputing/c-series-doc>

Accessing the System BIOS

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**.
