Cisco UCS B200 M3 Blade Server Installation and Service Note
Cisco UCS B200 M3 Blade Server

The Cisco UCS B200 M3 is an Intel-based, half-width blade supporting two CPU sockets using Intel E5-2600 series CPUs and up to 24 DIMMs; it supports one modular LOM (dedicated slot for Cisco's Virtual Interface Card) and one mezzanine adapter. At this time, the UCS B200 M2 (second generation) server is still available and is documented elsewhere. You can install up to eight UCS B200 Blade Servers to a UCS chassis, mixing with other models or Cisco UCS blade servers in the chassis if desired.

Figure 1: Cisco UCS B200 M3 Front Panel

<table>
<thead>
<tr>
<th>1 Asset tag</th>
<th>7 Network link status LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each server has a blank plastic tag that pulls out of the front panel which is provided so that you can add your own asset tracking label without interfering with the intended air flow.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2 Blade ejector handle</th>
<th>8 Blade health LED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3 Ejector captive screw</th>
<th>9 Console connector</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>4 Hard drive bay 1</th>
<th>10 Reset button access</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>5 Hard drive bay 2</th>
<th>11 Beaconing LED and button</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>6 Power button and LED</th>
</tr>
</thead>
</table>

LEDs

Server LEDs indicate whether the blade server is in active or standby mode, the status of the network link, the overall health of the blade server, and whether the server is set to give a blinking blue locator light from the locator button.

The removable drives also have LEDs indicating hard disk access activity and disk health.
Table 1: Blade Server LEDs

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Off</td>
<td>Power off.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Main power state. Power is supplied to all server components and the server is operating normally.</td>
</tr>
<tr>
<td></td>
<td>Amber</td>
<td>Standby power state. Power is supplied only to the service processor of the server so that the server can still be managed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note The front-panel power button is disabled by default. It can be re-enabled through Cisco UCS Manager. After it's enabled, if you press and release the front-panel power button, the server performs an orderly shutdown of the 12 V main power and goes to standby power state. You cannot shut down standby power from the front-panel power button. See the Cisco UCS Manager Configuration Guides for information about completely powering off the server from the software interface.</td>
</tr>
<tr>
<td>Link</td>
<td>Off</td>
<td>None of the network links are up.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>At least one network link is up.</td>
</tr>
<tr>
<td>Health</td>
<td>Off</td>
<td>Power off.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Normal operation.</td>
</tr>
<tr>
<td></td>
<td>Amber</td>
<td>Minor error.</td>
</tr>
<tr>
<td></td>
<td>Blinking Amber</td>
<td>Critical error.</td>
</tr>
<tr>
<td>Blue locator button and LED</td>
<td>Off</td>
<td>Blinking is not enabled.</td>
</tr>
<tr>
<td></td>
<td>Blinking blue 1 Hz</td>
<td>Blinking to locate a selected blade—If the LED is not blinking, the blade is not selected. You can control the blinking in UCS Manager or by using the blue locator button/LED.</td>
</tr>
</tbody>
</table>
### LED Description

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity (Disk Drive)</td>
<td>Off</td>
<td>Inactive.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Outstanding I/O to disk drive.</td>
</tr>
<tr>
<td>Health (Disk Drive)</td>
<td>Off</td>
<td>Can mean either no fault detected or the drive is not installed.</td>
</tr>
<tr>
<td></td>
<td>Flashing Amber 4 hz</td>
<td>If the Activity LED is also flashing amber, a drive rebuild is in progress.</td>
</tr>
<tr>
<td></td>
<td>Amber</td>
<td>Fault detected.</td>
</tr>
</tbody>
</table>

### Buttons

The Reset button is recessed in the front panel of the server. You can press the button with the tip of a paper clip or a similar item. Hold the button down for five seconds, and then release it to restart the server if other methods of restarting do not work.

The locator function for an individual server may get turned on or off by pressing the locator button/LED.

The front-panel power button is disabled by default. It can re-enabled through Cisco UCS Manager. After it's enabled, The power button allows you to manually take a server temporarily out of service but leave it in a state where it can be restarted quickly. If the desired power state for a service profile associated with a Blade server is set to "off," using the power button or Cisco UCS Manager to reset the server will cause the desired power state of the server to become out of sync with the actual power state and the server may unexpectedly shut down at a later time. To safely reboot a server from a power-down state, use the Boot Server action in Cisco UCS Manager.

### Local Console Connection

The local console connector allows a direct connection to a blade server to allow operating system installation and other management tasks to be done directly rather than remotely. The port uses the KVM dongle cable that provides a connection into a Cisco UCS blade server; it has a DB9 serial connector, a VGA connector for a monitor, and dual USB ports for a keyboard and mouse. With this cable, you can create a direct connection to the operating system and the BIOS running on a blade server. A KVM cable ships standard with each blade chassis accessory kit.

*Figure 2: KVM Cable for Blade Servers*
Drive Replacement

Each blade has up to two front-accessible, hot-swappable, 2.5-inch drives. Unused hard drive bays should always be covered with cover plates to ensure proper cooling and ventilation.

You can remove and install hard drives without removing the blade server from the chassis.

The drives supported in this blade server come with the drive sled attached. Spare drive sleds are not available. A list of currently supported drives is in the specification sheets at this URL: http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-b-series-blade-servers/datasheet-listing.html

Before upgrading or adding a drive to a running blade server, check the service profile in Cisco UCS Manager and make sure the new hardware configuration will be within the parameters allowed by the service profile.

Caution
To prevent ESD damage, wear grounding wrist straps during these procedures.

Removing a Blade Server Hard Drive

To remove a hard drive from a blade server, follow these steps:

Procedure

Step 1 Push the button to release the ejector, and then pull the hard drive from its slot.

*Figure 3: Removing the Hard Drive*

Step 2 Place the hard drive on an antistatic mat or antistatic foam if you are not immediately reinstalling it in another server.

Step 3 Install a hard disk drive blank faceplate to keep dust out of the blade server if the slot will remain empty.

Installing a Blade Server Drive

To install a drive in a blade server, follow these steps:
Procedure

Step 1  Place the drive ejector into the open position by pushing the release button.

*Figure 4: Installing a Hard Drive in a Blade Server*

Step 2  Gently slide the drive into the opening in the blade server until it seats into place.

Step 3  Push the drive ejector into the closed position.

You can use Cisco UCS Manager to format and configure RAID services. For details, see the *Configuration Guide* for the version of Cisco UCS Manager that you are using. The configuration guides are available at the following URL: [http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html](http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html)

If you need to move a RAID cluster, see the *Cisco UCS Manager Troubleshooting Reference Guide*.

---

Blade Server Removal and Installation

Before performing any internal operations on this blade server, you must remove it from the chassis.

⚠️ **Caution**

To prevent ESD damage, wear grounding wrist straps during these procedures and handle modules by the carrier edges only.

---

Powering Off a Blade Server Using the Power Button

⚠️ **Note**

The front panel power button is disabled by default to ensure that servers are decommissioned through the UCS Manager software before shutdown. If you prefer to shut down the server locally with the button, you can enable front power-button control in UCS Manager.

🔍 **Tip**

You can also shut down servers remotely using Cisco UCS Manager. For details, see the *Configuration Guide* for the version of Cisco UCS Manager that you are using. The configuration guides are available at the following URL: [http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html](http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html)
### Procedure

#### Step 1
If you are local to the server, check the color of the *Power Status* LED for each server in the chassis that you want to power off.

- Green indicates that the server is running and must be shut down before it can be safely powered off. Go to Step 2.
- Amber indicates that the server is already in standby mode and can be safely powered off. Go to Step 3.

#### Step 2
If you previously enabled front power-button control through Cisco UCS Manager, press and release the *Power* button, then wait until the *Power Status* LED changes to amber.

The operating system performs a graceful shutdown and the server goes to standby mode.

**Caution** To avoid data loss or damage to your operating system, you should always invoke a graceful shutdown of the operating system.

#### Step 3
(Optional) If you are shutting down all blade servers in a chassis, disconnect the power cords from the chassis to completely power off the servers.

#### Step 4
Remove the appropriate servers from the chassis.

### Removing a Blade Server

Using UCS Manager, decommission the server before physically removing the server. To remove a blade server from the chassis, follow these steps:

#### Procedure

#### Step 1
Loosen the captive screws on the front of the blade.

#### Step 2
Remove the blade from the chassis by pulling the ejector lever on the blade until it unseats the blade server.

#### Step 3
Slide the blade part of the way out of the chassis, and place your other hand under the blade to support its weight.

#### Step 4
Once removed, place the blade on an antistatic mat or antistatic foam if you are not immediately reinstalling it into another slot.

#### Step 5
If the slot is to remain empty, install a blank faceplate (N20-CBLKB1) to maintain proper thermal temperature and keep dust out of the chassis.

### Installing a Half-width Blade Server

#### Before you begin
The blade server must have its cover installed before installing the server into the chassis to ensure adequate airflow.

#### Procedure

#### Step 1
Grasp the front of the blade server and place your other hand under the blade to support it.
Step 2  Open the ejector levers in the front of the blade server.
Step 3  Gently slide the blade into the opening until you cannot push it any farther.
Step 4  Press the ejector so that it catches the edge of the chassis and presses the blade server all the way in.
Step 5  Tighten the captive screw on the front of the blade to no more than 3 in-lbs. Tightening only with bare fingers is unlikely to lead to stripped or damaged captive screws.

Cisco UCS Manager automatically reacknowledges, reassociates, and recommissions the server, provided any hardware changes are allowed by the service profile.

Secure Digital Cards

Secure Digital (SD) card slots are provided and one or two SD cards can be populated. If two SD cards are populated, they can be used in a mirrored mode.

Note  Do not mix different capacity cards in the same server.

Note  Due to technical limitations, if the server is running a Cisco UCS Manager version earlier than release 2.2(3a) with the 32-GB SD card, only 16-GB usable capacity is available (regardless of mirroring) in the server.
Removing a Blade Server Cover

Procedure

Step 1  Press and hold the button down as shown in the figure below.

Step 2  While holding the back end of the cover, pull the cover back and then up.
Air Baffles

The air baffles direct and improve air flow for the server components. Two identical baffles ship with each B200 M3 server. No tools are necessary to install them, just place them over the DIMMs as shown, with the holes in the center of the baffles aligned with the corresponding motherboard standoffs.

Figure 8: Cisco UCS B200 M3 Air Baffles
**Internal Components**

**Figure 9: Inside View of the B200 M3 Blade Server**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hard drive bays</td>
<td>2</td>
<td>Internal USB connector</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Battery</td>
<td>4</td>
<td>CPU and heat sink</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>DIMM slots</td>
<td>6</td>
<td>Diagnostic button</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Modular LOM (shown installed)</td>
<td>8</td>
<td>Adapter card connector (Adapter not shown installed)</td>
<td></td>
</tr>
</tbody>
</table>

**Diagnostics Button and LEDs**

At blade start-up, POST diagnostics test the CPUs, DIMMs, HDDs, and rear mezzanine modules, and any failure notifications are sent to Cisco UCS Manager. You can view these notifications in the Cisco UCS Manager System Error Log or in the output of the `show tech-support` command. If errors are found, an amber diagnostic LED also lights up next to the failed component. During run time, the blade BIOS and component drivers monitor for hardware faults and will light up the amber diagnostic LED as needed.

LED states are saved, and if you remove the blade from the chassis the LED values will persist for up to 10 minutes. Pressing the LED diagnostics button on the motherboard causes the LEDs that currently show a component fault to light for up to 30 seconds for easier component identification. LED fault values are reset when the blade is reinserted into the chassis and booted, and the process begins from its start.

If DIMM insertion errors are detected, they may cause the blade discovery process to fail and errors will be reported in the server POST information, which is viewable using the UCS Manager GUI or CLI. DIMMs must be populated according to specific rules. The rules depend on the blade server model. Refer to the documentation for a specific blade server for those rules.

Faults on the DIMMs or rear mezzanine modules also cause the server health LED to light solid amber for minor error conditions or blinking amber for critical error conditions.
Working Inside the Blade Server

Installing a CMOS Battery

All Cisco UCS blade servers use a CR2032 battery to preserve BIOS settings while the server is not installed in a powered-on chassis. Cisco supports the industry standard CR2032 battery that is available at most electronics stores.

⚠️ Warning ⚠️
There is danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions.

To install or replace the battery, follow these steps:

Procedure

Step 1 Remove the existing battery:
   a) Power off the blade, remove it from the chassis, and remove the top cover.
   b) Push the battery socket retaining clip away from the battery.
   c) Lift the battery from the socket. Use needle-nose pliers to grasp the battery if there is not enough clearance for your fingers.

Step 2 Install the replacement battery:
   a) Push the battery socket retaining clip away from where the battery fits in the housing.
   b) Insert the new battery into the socket with the battery’s positive (+) marking facing away from the retaining clip. Ensure that the retaining clip can click over the top of the battery to secure it in the housing.
   c) Replace the top cover.
   d) Replace the blade server in the chassis.

CPU and Heatsink Replacement

Special Information For Upgrades to Intel E5-2600 v2 Series CPUs

⚠️ Caution ⚠️
You must upgrade your server firmware to the required minimum level before you upgrade to Intel E5-2600 v2 Series CPUs. Older firmware versions cannot recognize the new CPUs and this results in a non-bootable server.

The minimum software and firmware versions required for the server to support Intel E5-2600 v2 Series CPUs are as follows:

<table>
<thead>
<tr>
<th>Software or Firmware</th>
<th>Minimum Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server CIMC</td>
<td>2.1(3)</td>
</tr>
<tr>
<td>Server BIOS</td>
<td>2.1(3)</td>
</tr>
<tr>
<td>Cisco UCS Manager</td>
<td>2.1(3)</td>
</tr>
</tbody>
</table>
Do one of the following actions:

- If your server’s firmware and/or Cisco UCS Manager software are already at the required levels shown in the table above, you can replace the CPU hardware by using the procedures in this section.
- If your server’s firmware and/or Cisco UCS Manager software is earlier than the required levels, use the instructions in the Cisco UCS B-Series Servers Upgrade Guide for Intel E5-2600 v2 Series CPUs to upgrade your firmware and software. After you upgrade, return to the procedures in this book to replace the CPU and heatsink hardware.

Removing a CPU and Heat Sink

You will use these procedures to move a CPU from one server to another, to replace a faulty CPU, or to upgrade from one CPU to another.

⚠️ Caution

The Pick-and-Place tools used in this procedure are required to prevent damage to the contact pins between the motherboard and the CPU. Do not attempt this procedure without the required tools. If you do not have the tool, you can order a spare.

- UCS-CPU-EP-PNP=; Pick n place CPU tools for M3/EP 10/8/6/4/2 core CPUs (Green)
- UCS-CPU-EP2-PNP=; Pick n place CPU tools for M3/EP v2 12 core CPUs (Purple)

Procedure

**Step 1**
Unscrew the four captive screws securing the heat sink to the motherboard.
Loosen one screw by a quarter turn, then move to the next screw. Continue loosening until the heat sink can be lifted off.

**Step 2**
Remove the heat sink.
Remove the existing thermal compound from the bottom of the heat sink using the cleaning kit included with each CPU option kit. Follow the instructions on the two bottles of cleaning solvent.

**Step 3**
Unhook the first socket hook, which has the following icon: See callout 3 in the following figure.

**Step 4**
Unhook the second socket hook, which has the following icon: See callout 4 in the following figure.

**Step 5**
Open the socket latch.
Step 6  Press the central button on the CPU Pick-and-Place tool to release the catch.

Step 7  Remove an old CPU as follows:
   a) Place the CPU Pick-and-Place tool on the CPU socket aligned with the arrow pointing to the CPU registration mark.
   b) Press the button/handle on the tool to grasp the installed CPU.
   c) Lift the tool and CPU straight up.
Installing a New CPU and Heat Sink

Before installing a new CPU in a server, verify the following:

- The CPU is supported for that given server model. Refer to the Specification Sheet for this server to see the list of supported CPUs. The Specification Sheets are available at this URL: http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-b-series-blade-servers/datasheet-listing.html
- A BIOS update is available and installed that supports the CPU and the given server configuration.
- If the server will be managed by Cisco UCS Manager, the service profile for this server in Cisco UCS Manager will recognize and allow the new CPU.

Caution
The Pick-and-Place tools used in this procedure are required to prevent damage to the contact pins between the motherboard and the CPU. Do not attempt this procedure without the required tools. If you do not have the tool, you can order a spare.

- UCS-CPU-EP-PNP=; Pick n place CPU tools for M3/EP 10/8/6/4/2 core CPUs (Green)
- UCS-CPU-EP2-PNP=; Pick n place CPU tools for M3/EP v2 12 core CPUs (Purple)

Procedure
Step 1  Required: To install a CPU in an empty socket, remove the protective cap that is intended to prevent bent or touched contact pins. The pick and pull cap tool provided can be used in a manner similar to a pair of tweezers. Grasp the protective cap and pivot as shown.

Step 2  Release the catch on the pick and pull tool by pressing the handle/button.

Step 3  Remove the new CPU from the packaging, and load it into the pick and place tool as follows:

a) Confirm that the pedestal is set up correctly for your processor. The pedestal ships configured with the markings “LGA2011-R1” facing upward, and this is the correct orientation.

b) Place the CPU on the pedestal. The CPU corners should fit snugly at the pedestal corners and the notches should meet the pegs perfectly.

c) Place the CPU pick and place tool on the CPU pedestal aligned with the A1 arrow pointing to the A1 registration mark on the pedestal.

d) Press the button/handle on the tool to grasp the CPU.

e) Lift the tool and CPU straight up off of the pedestal.

Figure 12: Loading the Pick and Place Tool

Alignment mark on the pick and place tool, CPU and pedestal

Step 4  Place the CPU and tool on the CPU socket with the registration marks aligned as shown.

Step 5  Press the button/handle on the pick and place tool to release the CPU into the socket.
Step 6  Close the socket latch. See callout 1 in the following figure.

Step 7  Secure the first hook, which has the following icon: ⬇️ See callout 2 in the following figure.

Step 8  Secure the second hook, which has the following icon: ⬆️ See callout 3 in the following figure.

**Figure 14: Replacing the Heat Sink (B200 M3 Shown)**

Step 9  Using the syringe of thermal grease provided with replacement CPUs and servers, add 2 cubic centimeters of thermal grease to the top of the CPU where it will contact the heat sink. Use the pattern shown. This should require half the contents of the syringe.

**Caution** The thermal grease has very specific thermal properties. Thermal grease from other sources should not be substituted because it may lead to damage.
Note: CPU spares come with two syringes of thermal grease; one with a blue cap and one with a red cap. The syringe with the blue cap is used with this server.

Figure 15: Thermal Grease Application Pattern

---

Step 10: Replace the heat sink. See callout 4.

Caution: On certain models, heat sinks are keyed to fit into the plastic baffle extending from the motherboard. Do not force a heat sink if it is not fitting well, rotate it and re-orient the heat sink.

Step 11: Secure the heat sink to the motherboard by tightening the four captive screws a quarter turn at a time in an X pattern as shown in the upper right.

---

Memory and Performance

Installing Memory

To install a DIMM into the blade server, follow these steps:

Procedure

Step 1: Press the DIMM into its slot evenly on both ends until it clicks into place.

DIMMs are keyed. If a gentle force is not sufficient, make sure the notch on the DIMM is correctly aligned.

Note: Be sure that the notch in the DIMM aligns with the slot. If the notch is misaligned you may damage the DIMM, the slot, or both.

Step 2: Press the DIMM connector latches inward slightly to seat them fully.
Supported DIMMs

The DIMMs supported in this blade server are constantly being updated. A list of currently supported and available DIMMs is in the specifications sheets at:


Do not use any memory DIMMs other than those listed in the specification sheet. Doing so may irreparably damage the server and require down time.

Memory Population

The blade server contains 24 DIMM slots—12 for each CPU. Each set of 12 DIMM slots is arranged into four channels, where each channel has three DIMMs.

*Figure 16: Memory Slots within the Blade Server*

<table>
<thead>
<tr>
<th></th>
<th>Channels A-D for CPU 1</th>
<th></th>
<th>Channels E-H for CPU 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

DIMMs and Channels

Each channel is identified by a letter—A, B, C, D for CPU1, and E, F, G, H for CPU 2. Each DIMM slot is numbered 0, 1, or 2. Note that each DIMM slot 0 is blue, each slot 1 is black, and each slot 2 is off-white or beige.

The figure below shows how DIMMs and channels are physically laid out on the blade server. The DIMM slots in the upper and lower right are associated with the second CPU (CPU shown on right in the diagram), while the DIMM slots in the upper and lower left are associated with the first CPU (CPU shown on left).

*Figure 17: Physical Representation of DIMMs and Channels*
The figure below shows a logical view of the DIMMs and channels.

**Figure 18: Logical Representation of DIMMs and Channels**

DIMMs can be used in the blade server in a one DIMM per Channel (1DPC) configuration, in a two DIMMs per Channel (2DPC) configuration, or a three DIMMs per Channel (3DPC) configuration.

Each CPU in a Cisco UCS B200 M3 blade server supports four channels of three memory slots each. In a 1 DPC configuration, DIMMs are in slot 0 only. In a 2 DPC configuration, DIMMs are in both slot 0 and slot 1. In a 3 DPC configuration, DIMMs are in slot 0, slot 1, and slot 2.

**Table 3: Supported DIMM Population Order**

<table>
<thead>
<tr>
<th>DIMMs per CPU</th>
<th>CPU 1 installed slots</th>
<th>CPU 2 installed slots</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A0</td>
<td>E0</td>
</tr>
<tr>
<td>2</td>
<td>A0, B0</td>
<td>E0, F0</td>
</tr>
<tr>
<td>3</td>
<td>A0, B0, C0</td>
<td>E0, F0, G0</td>
</tr>
<tr>
<td>4 (Blue slots)</td>
<td>A0, B0, C0, D0</td>
<td>E0, F0, G0, H0</td>
</tr>
<tr>
<td>DIMMs per CPU</td>
<td>CPU 1 installed slots</td>
<td>CPU 2 installed slots</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>5</td>
<td>A0, B0, C0, D0, A1</td>
<td>E0, F0, G0, H0, E1</td>
</tr>
<tr>
<td>6</td>
<td>A0, B0, C0, A1, B1, C1</td>
<td>E0, F0, G0, E1, F1, G1</td>
</tr>
<tr>
<td>7</td>
<td>A0, B0, C0, D0, A1, B1, C1</td>
<td>E0, F0, G0, H0, E1, F1, G1</td>
</tr>
<tr>
<td>8 (Blue and black slots)</td>
<td>A0, B0, C0, D0, A1, B1, C1, D1</td>
<td>E0, F0, G0, H0, E1, F1, G1, H1</td>
</tr>
<tr>
<td>9</td>
<td>A0, B0, C0, D0, A1, B1, C1, D1, A2</td>
<td>E0, F0, G0, H0, E1, F1, G1, H1, E2</td>
</tr>
<tr>
<td>10</td>
<td>A0, B0, C0, D0, A1, B1, C1, D1, A2, B2</td>
<td>E0, F0, G0, H0, E1, F1, G1, H1, E2, F2</td>
</tr>
<tr>
<td>11</td>
<td>A0, B0, C0, D0, A1, B1, C1, D1, A2, B2, C2</td>
<td>E0, F0, G0, H0, E1, F1, G1, H1, E2, F2, G2</td>
</tr>
<tr>
<td>12 (Blue, black and beige slots)</td>
<td>A0, B0, C0, D0, A1, B1, C1, D1, A2, B2, C2</td>
<td>E0, F0, G0, H0, E1, F1, G1, H1, E2, F2, G2</td>
</tr>
</tbody>
</table>

**Memory Performance**

When considering the memory configuration of the blade server, there are several things to consider. For example:

- When mixing DIMMs of different densities (capacities), the highest density DIMM goes in slot 1 then in descending density.
- Besides DIMM population and choice, the selected CPU(s) can have some effect on performance.
- DIMMs can be run in a 1DPC, 2DPC, or 3DPC configuration. 1DPC and 2DPC can provide the maximum rated speed that the CPU and DIMMs are rated for. 3DPC causes the DIMMs to run at a slower speed.

**Memory Mirroring and RAS**

The Intel CPUs within the blade server support memory mirroring only when an even number of channels are populated with DIMMs. Furthermore, if memory mirroring is used, DRAM size is reduced by 50 percent for reasons of reliability.

**Installing a Virtual Interface Card Adapter**

The Cisco Virtual Interface Card (VIC) 1240 is a specialized adapter that provides dual 2 x 10 Gb of Ethernet/ or Fiber Channel over Ethernet (FCoE) connectivity to each chassis. It plugs into the dedicated slot 1 connector only. It is currently the only card that can be plugged into this connector and it will provide connectivity through either a 2100 series or 2200 series IOM.

---

**Note**

You must remove the adapter card to service it.

To install a Cisco VIC 1340 or VIC 1240 in the blade server, follow these steps:

**Procedure**

**Step 1** Position the VIC board connector above the motherboard connector and align the captive screw to the standoff post on the motherboard.

**Step 2** Firmly press the VIC board connector into the motherboard connector.
**Step 3**  Tighten the captive screw.

**Tip**  To remove a VIC, reverse the above procedure. You might find it helpful when removing the connector from the motherboard to gently rock the board along the length of the connector until it loosens.

*Figure 19: Installing a VIC mLOM Adapter*

---

**Installing an Adapter Card**

All the supported mezzanine cards have a common installation process. These cards are updated frequently. Currently supported cards and the available models for this server are listed in the specification sheets at this URL:


If you are switching from one type of adapter card to another, before you physically perform the switch make sure that you download the latest device drivers and load them into the server’s operating system. For more information, see the firmware management chapter of one of the Cisco UCS Manager software configuration guides.

**Procedure**

**Step 1**  Position the adapter board connector above the motherboard connector and align the two adapter captive screws to the standoff posts (see callout 1) on the motherboard.

**Step 2**  Firmly press the adapter connector into the motherboard connector (see callout 2).

**Step 3**  Tighten the two captive screws (see callout 3).

**Tip**  Removing an adapter card is the reverse of installing it. You might find it helpful when removing the connector from the motherboard to gently rock the board along the length of the connector until it loosens.
Installing and Enabling a Trusted Platform Module

The Trusted Platform Module (TPM) is a component that can securely store artifacts used to authenticate the server. These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments. It is a requirement for the Intel Trusted Execution Technology (TXT) security feature, which must be enabled in the BIOS settings for a server equipped with a TPM.

---

**Procedure**

**Step 1** Install the TPM hardware.
   a) Power off, decommission, and remove the blade server from the chassis.
   b) Remove the blade server cover.
   c) Install the TPM to the TPM socket on the server motherboard and secure it using the one-way screw that is provided. See the figure below for the location of the TPM socket.

---

**Note** TPM installation is supported after-factory. However, a TPM installs with a one-way screw and cannot be replaced or moved to another server. If a server with a TPM is returned, the replacement server must be ordered with a new TPM.
d) Return the blade server to the chassis, power it on, and allow it to be automatically reacknowledged, reassociated, and recommissioned.
e) Continue with enabling TPM support in the server BIOS in the next step.

Figure 21: TPM Socket Location

<table>
<thead>
<tr>
<th></th>
<th>Front of server</th>
<th>2</th>
<th>TPM socket on motherboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

Enable TPM Support in the BIOS.

a) Enable **Quiet Mode** in the BIOS policy of the server’s service profile.
b) Establish a direct connection to the server, either by connecting a keyboard, monitor, and mouse to the front panel using a KVM dongle (N20-BKVM) or by other means.
c) Reboot the server.
d) Press **F2** during reboot to enter the BIOS setup screens.
e) On the **Advanced** tab, select **Trusted Computing** and press **Enter** to open the TPM Security Device Configuration window.
f) Set the TPM Support option to **Enabled**.
g) Press **F10** to save and exit. Allow the server to reboot, but watch for the prompt to press F2 in the next step.

**Step 3**

Enable TPM State in the BIOS.

a) Press **F2** during reboot to enter the BIOS setup screens.
b) On the **Advanced** tab, select **Trusted Computing** and press **Enter** to open the TPM Security Device Configuration window.
c) Set the TPM State option to **Enabled**.
d) Press **F10** to save and exit. Allow the server to reboot, but watch for the prompt to press F2 in the next step.

**Step 4**

Verify that TPM Support and TPM State are enabled.

a) Press **F2** during reboot to enter the BIOS setup screens.
b) On the **Advanced** tab, select **Trusted Computing** and press **Enter** to open the TPM Security Device Configuration window.
c) Verify that TPM Support and TPM State are set to **Enabled**.
d) Continue with enabling the Intel TXT feature in the next step.

**Step 5**

Enable the Intel TXT feature in the BIOS.

a) Choose the **Advanced** tab.
b) Choose **Intel TXT (LT-SX) Configuration** to open the Intel TXT (LT-SX) Hardware Support window.
c) Set TXT Support to **Enabled**.
d) Verify that the following items are listed as Enabled:
   • VT Support (default is Enabled)
   • VT-d Support (default is Enabled)
   • TPM Support
   • TPM State
   
   If VT Support and VT-d Support are not enabled, return to the Advanced tab, select Processor Configuration, and then set Intel (R) VT and Intel (R) VT-d to Enabled.

e) Press F10 to save and exit.

---

**Server Troubleshooting**

For general troubleshooting information, see the Cisco UCS Manager Troubleshooting Reference Guide.

**Server Configuration**

Cisco UCS blade servers should be configured and managed using Cisco UCS Manager. For details, see the Configuration Guide for the version of Cisco UCS Manager that you are using. The configuration guides are available at the following URL:

**Physical Specifications for the Cisco UCS B200 M3**

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height</td>
<td>1.95 inches (50 mm)</td>
</tr>
<tr>
<td>Width</td>
<td>8.00 inches (203 mm)</td>
</tr>
<tr>
<td>Depth</td>
<td>24.4 inches (620 mm)</td>
</tr>
<tr>
<td>Weight</td>
<td>15.0 lbs (6.8 kg)</td>
</tr>
</tbody>
</table>

The system weight listed here is an estimate for a fully configured system and will vary depending on peripheral devices installed.

---

**Obtaining Documentation and Submitting a Service Request**

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Follow Cisco UCS Docs on Twitter to receive document update notifications.
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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2012 Cisco Systems, Inc. All rights reserved.
Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.