

Dell™ PowerEdge™ M1000e
Systems
Configuration Guide



Dell™ PowerEdge™ M1000e
Systems
Configuration Guide



Notes, Notices, and Cautions



NOTE: A NOTE indicates important information that helps you make better use of your computer.



NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

Information in this document is subject to change without notice.

© 2008 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *PowerEdge*, and *Dell OpenManage* are trademarks of Dell Inc.; *Microsoft*, *Windows*, and *Active Directory* are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

August 2008

Contents

1	About Your System	7
	System Overview	7
	System Control Panel Features	10
	LCD Module	11
	LCD Module Menus	12
	Back-Panel Features	13
	Blades	13
	CMC Module	16
	CMC Daisy Chaining (Enclosure Stacking)	17
	iKVM Switch Module	19
2	Initial System Configuration	21
	Before You Begin	21
	Power Requirements	21
	Network Information	21
	Initial Setup Sequence	21
	Configuring the CMC	22
	Initial CMC Network Configuration	22
	Logging in to the CMC Using the Web-Based Interface	25
	Adding and Managing CMC Users	26

Configuring iDRAC Networking Using the Web-Based Interface	27
Setting the First Boot Device for Servers	28
Configuring and Managing Power	28
Installing or Updating the CMC Firmware	29
Configuring the Optional iKVM Switch Module	31
Enabling iKVM Access to the Dell CMC Console	31
Updating the iKVM Firmware	31
Tiering the Avocent iKVM Switch From an Analog KVM Switch	32
Tiering the Avocent iKVM Switch From a Digital KVM Switch	33
Viewing and Selecting Servers	34
FlexAddress	36
3 Configuring the I/O Modules	37
Overview	37
Before You Begin	39
Network Information	39
Switch Modules	39
Configuring a Switch Module Network Ethernet Port Using the Web-Based Interface	39
Cisco SFS M7000e Infiniband Switch Module	40
PowerConnect M6220 Ethernet Switch Module	42
Cisco Ethernet Switch	43
Brocade M4424 SAN I/O Module	45

Pass-through Modules	47
Ethernet Pass-through Module	47
Fibre Channel Pass-through Module	49

About Your System

System Overview

Your system can include up to 16 half-height blades (server modules), eight full-height blades, or a mixture of the two blade types (see Figure 1-1, Figure 1-2, and Figure 1-3). To function as a system, a blade is inserted into a enclosure (chassis) that supports power supplies, fan modules, a Chassis Management Controller (CMC) module, and at least one I/O module for external network connectivity. The power supplies, fans, CMC, optional iKVM module, and I/O modules are shared resources of the blades in the enclosure.

Figure 1-1. Blade Numbering – Half-Height Blades

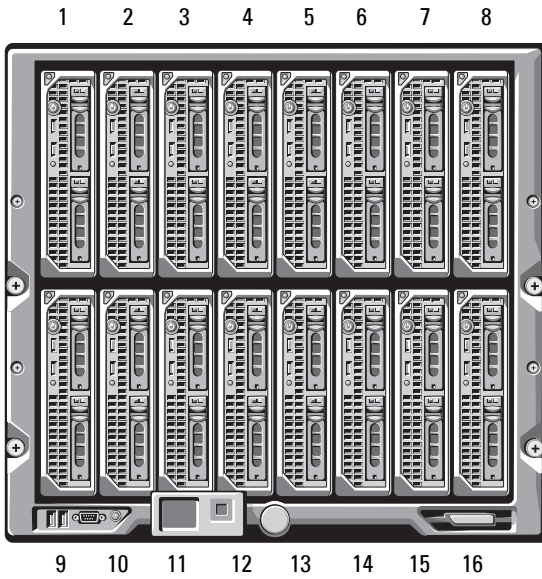


Figure 1-2. Blade Numbering - Full Height Blades

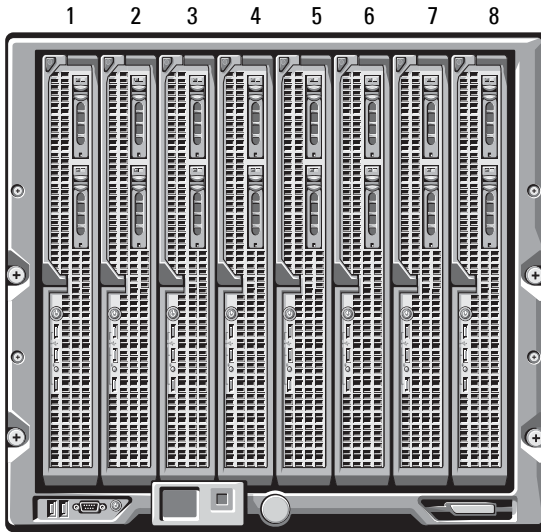
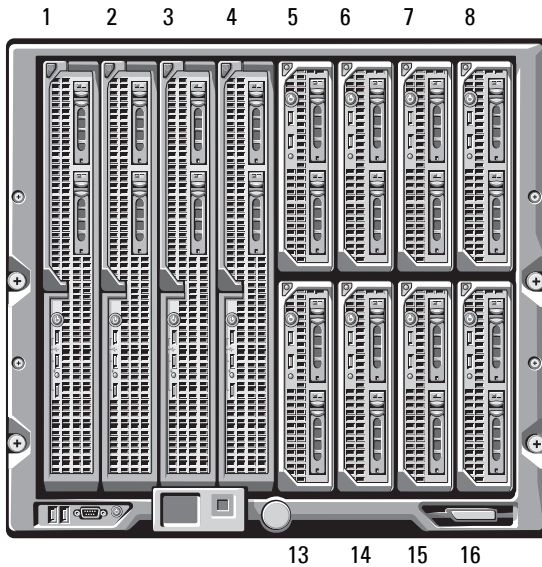


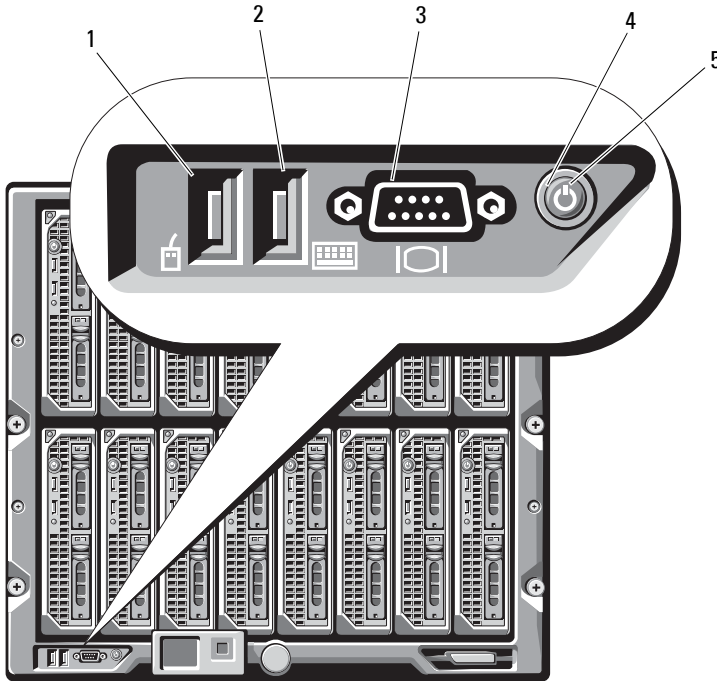
Figure 1-3. Blade Numbering - Mixed Full-Height and Half-Height Blades



System Control Panel Features

Figure 1-4 shows the control panel features on the M1000e enclosure front panel.

Figure 1-4. Control Panel Features



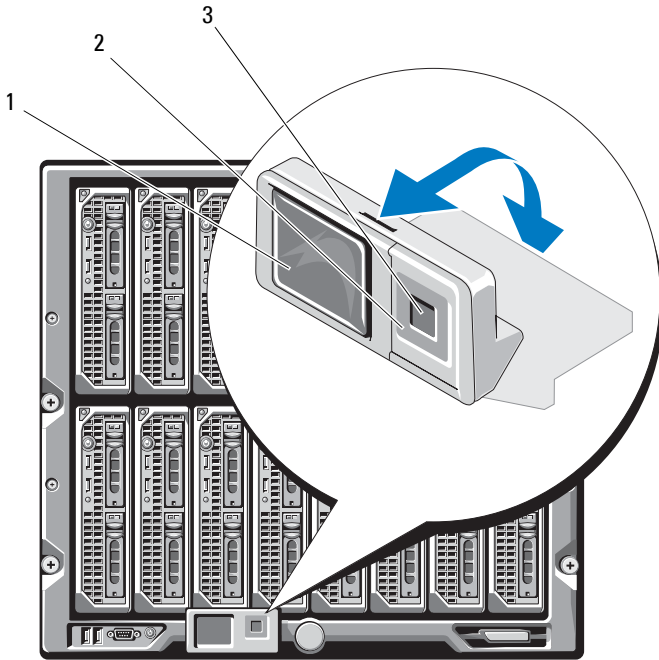
- | | | | |
|---|------------------------|---|--------------------------|
| 1 | USB port (mouse only) | 2 | USB port (keyboard only) |
| 3 | video connector | 4 | system power button |
| 5 | system power indicator | | |

NOTE: The USB and video ports are functional only if an optional iKVM module is installed.

LCD Module

The LCD module provides an initial configuration/deployment wizard, as well as access to infrastructure and blade information and error reporting. See Figure 1-5.

Figure 1-5. LCD Module



- 1 LCD screen
- 2 scroll buttons (4)
- 3 selection ("check") button

LCD Module Menus

Main Menu

The Main Menu options include links to the **Server Menu**, the **Enclosure Menu**, and the **LCD Setup Menu**.

LCD Setup Menu

You can change the default language and startup screen for the LCD menu screens using this menu.

Server Menu

From the **Server Menu** dialog box, you can highlight each blade in the enclosure using the arrow keys, and view its status.

- A blade that is powered off or booting is designated by a gray rectangle. An active blade is indicated by a green rectangle. If a blade has errors, this condition is indicated by an amber rectangle.
- To select a blade, highlight it and press the center button. A dialog box displays the iDRAC IP address of the blade and any errors present.

Enclosure Menu

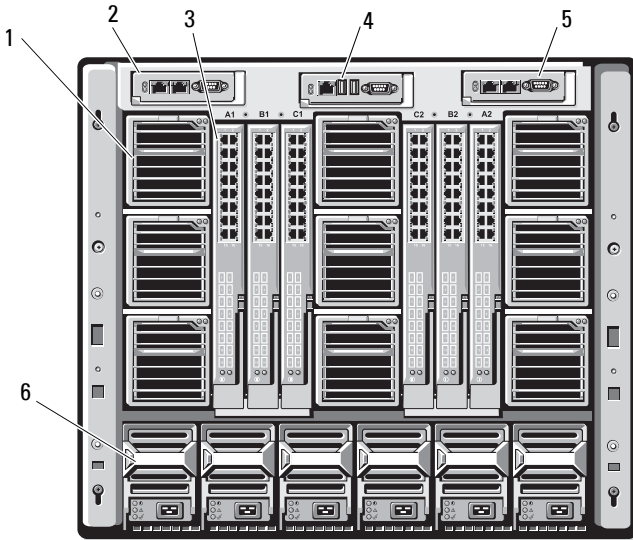
The **Enclosure Menu** includes options for **Module Status**, **Enclosure Status**, and **IP Summary**.

- In the **Module Status** dialog box, you can highlight each component in the enclosure and view its status.
 - A module that is powered off or booting is designated by a gray rectangle. An active module is indicated by a green rectangle. If a module has errors, it will be indicated by an amber rectangle.
 - If a module is selected, a dialog box displays the current status of the module and any errors present.
- In the **Enclosure Status** dialog box, you can view the enclosure status, any error conditions, and power consumption statistics.
- The **IP Summary** screen shows IP information for the CMC(s), and the iDRAC of each installed server.

Back-Panel Features

The back of the M1000e enclosure supports six I/O modules, one or two CMC modules, an optional iKVM module, nine fan modules, and six power supply modules. Figure 1-6 shows a fully configured enclosure.

Figure 1-6. Back-Panel Features

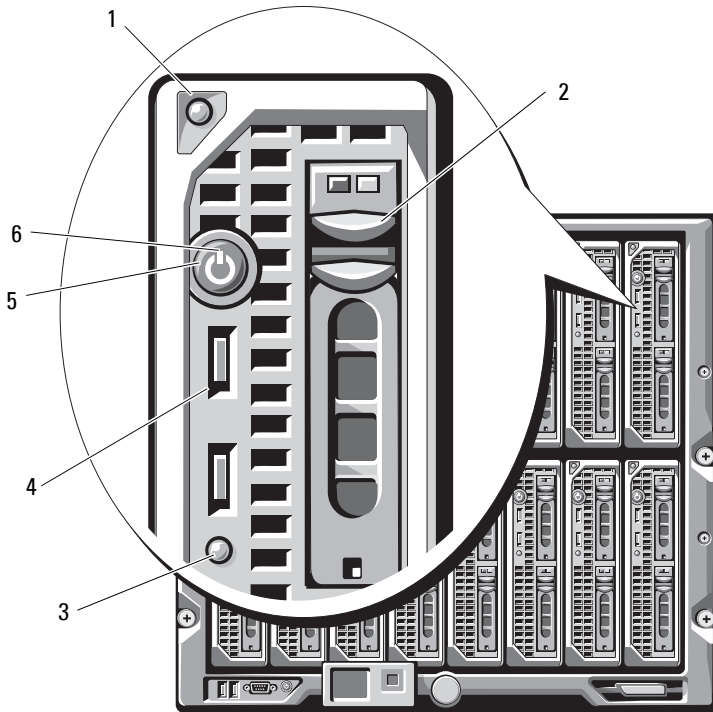


- | | | | |
|---|----------------------|---|----------------------|
| 1 | fan modules (9) | 2 | primary CMC module |
| 3 | I/O modules (6) | 4 | optional iKVM module |
| 5 | secondary CMC module | 6 | power supplies (6) |

Blades

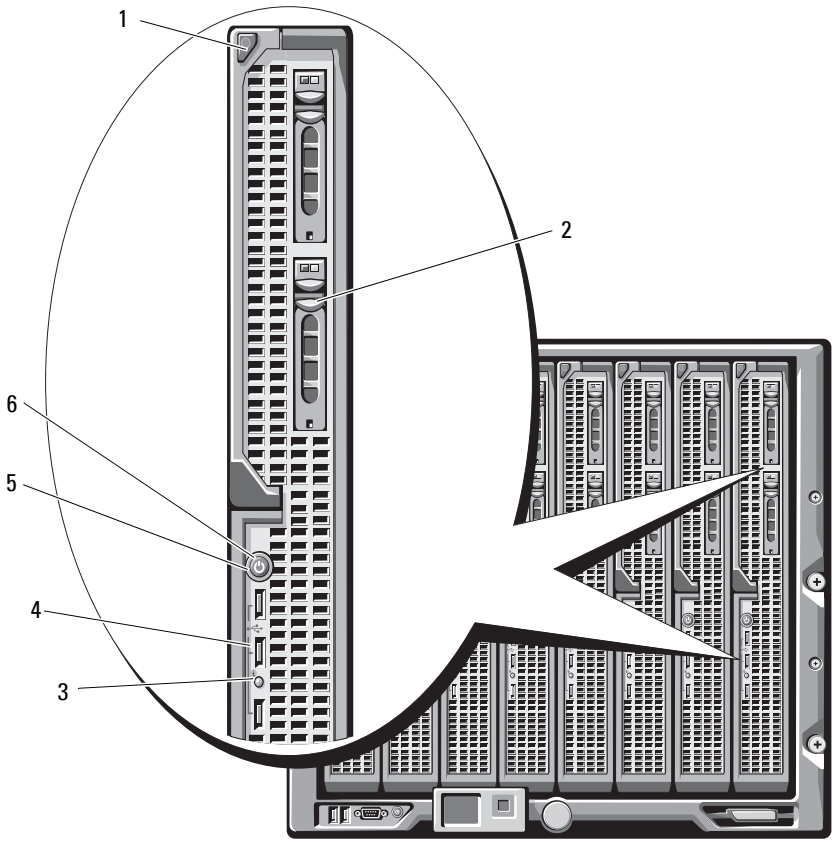
Figure 1-7 shows the front panel features on the M600 and M605 blades. Figure 1-8 shows the front panel features on the M905 and M805 blades.

Figure 1-7. Front Panel Features - PowerEdge M600 and M605



- | | | | |
|---|---------------------------------------|---|-----------------------|
| 1 | blade handle release button | 2 | hard drives (2) |
| 3 | blade status/identification indicator | 4 | USB connectors (2) |
| 5 | blade power button | 6 | blade power indicator |

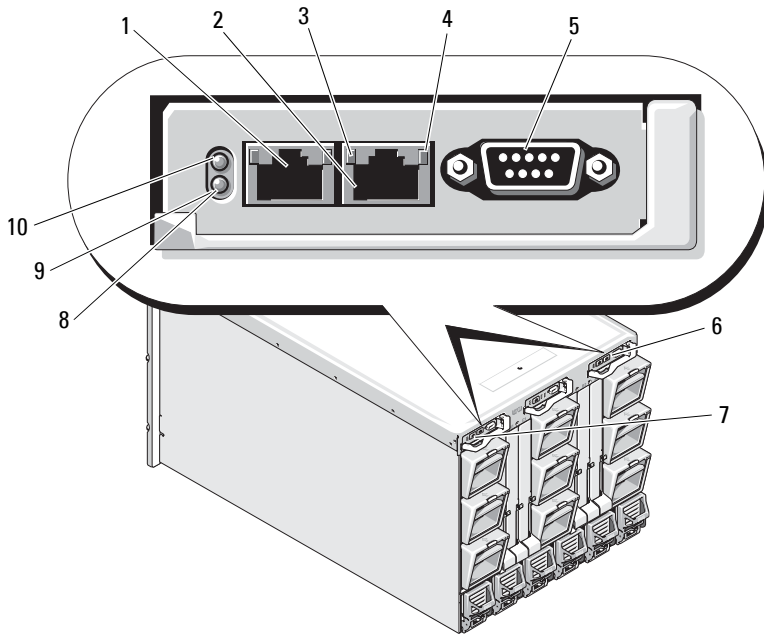
Figure 1-8. Front Panel Features - PowerEdge M905 and M805



- | | | | |
|---|---------------------------------------|---|-----------------------|
| 1 | blade handle release button | 2 | hard drives (2) |
| 3 | blade status/identification indicator | 4 | USB connectors (3) |
| 5 | blade power button | 6 | blade power indicator |

CMC Module

Figure 1-9. CMC Module Features



- | | | | |
|---|---|----|--|
| 1 | Ethernet connector Gb1 | 2 | Ethernet connector STK (used for daisy-chaining CMCs in separate enclosures) |
| 3 | link indicator (2) | 4 | activity indicator (2) |
| 5 | DB-9 serial connector for local configuration | 6 | optional secondary CMC (CMC 2) |
| 7 | primary CMC (CMC 1) | 8 | amber fault indicator |
| 9 | blue status/identification indicator | 10 | power indicator |

The CMC provides multiple systems management functions for your modular server, including the M1000e enclosure's network and security settings, I/O module and iDRAC network settings, and power redundancy and power ceiling settings.

CMC Daisy Chaining (Enclosure Stacking)

CMC daisy chaining can be utilized to minimize the number of network connections required for chassis (enclosure) management, such that only one or two network connections (depending on whether or not redundant CMCs are installed) are needed for up to four M1000e enclosures.

Cabling Guidelines

Follow these guidelines to daisy chain CMC modules from enclosure to enclosure:

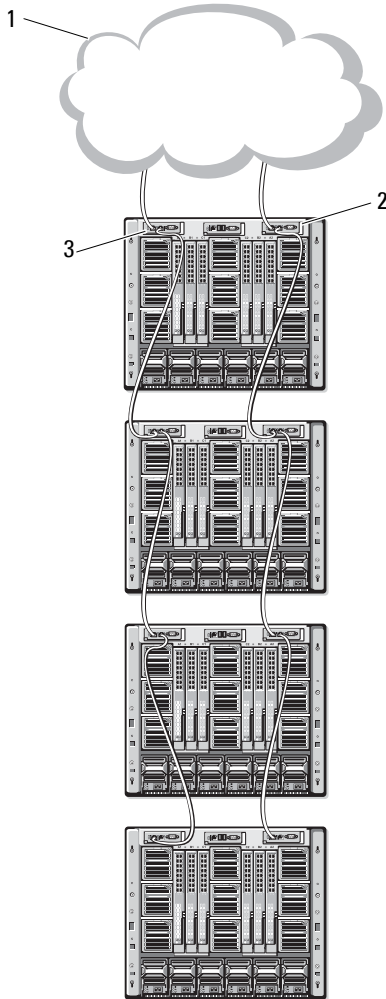
- CMC Ethernet port "GB1" is the "Uplink" port. It will uplink to either the management network, or to receive a cable from the CMC Ethernet port labeled "STK" in the adjacent enclosure.

The CMC Ethernet port labeled "STK" is the "daisy-chain" port. It will *only* connect to CMC port GB1 on the adjacent enclosure. Do not connect this cable directly to the management network.

- Up to 4 enclosures can be daisy-chained.
- Enclosures can be daisy-chained in both redundant and non-redundant deployments:
 - In a redundant CMC deployment, cable all CMC modules in the CMC primary slots together. Cable all CMC modules in the CMC secondary slots together. Do not connect the primary daisy chain with the secondary daisy chain (do not "cross cable" the two sets of CMCs).
 - In a non-redundant CMC, cable all CMC modules in the CMC primary slots together.

Figure 1-10 shows four enclosures with redundant CMC modules installed. Primary CMC port GB1 in the first enclosure connects to the management network. Primary CMC port GB1 in the adjacent enclosure is "uplinked" into the port labeled "STK" on the primary CMC in the enclosure above it. No cable is required in port STK on the fourth enclosure in line. The same cabling scheme is valid for the daisy chain of CMC modules in the secondary slot of the enclosures.

Figure 1-10. CMC Daisy-Chaining – Enclosure With Redundant CMC Modules



- 1 Management network segment
- 2 CMC1 – cable from connector Gb1 to network
- 3 CMC2 – cable from connector Gb1 to network

iKVM Switch Module

The optional Avocent iKVM analogue switch module provides connections for a keyboard, video (monitor), and mouse. It includes the following features:

- Local iKVM access can be remotely disabled on a per blade basis, using the blade's iDRAC interface (access is enabled by default).



NOTE: By default (enabled), a console session to a given blade will be available to both the iDRAC interface and a iKVM (user connected to a blade's console via iDRAC and the iKVM will see the same video and be able to type commands). The iDRAC will If this sharing is not desired, this can be disabled via the iDRAC console interface.

- The following connectors:
 - One VGA connector. The iKVM supports a video display resolution range from 640x480 at 60Hz up to 1280x1024x65,000 colors (noninterlaced) at 75Hz.
 - Two USB ports for keyboard and mouse.



NOTE: The iKVM USB ports do not support storage devices.

- RJ-45 ACI port for tiering with Dell and Avocent analog KVM and KVM over IP switches with ARI ports.



NOTE: Although the ACI port is an RJ-45 connector and uses Cat5 (or better) cabling, it is not an Ethernet network interface port. It is only used for connection to external KVM switches with Analog Rack Interface (ARI) ports, and does not support native KVM over IP.

- The iKVM can also be accessed from the front of the enclosure, providing front or rear panel KVM functionality, but not at the same time. For enhanced security, front panel access can be disabled using the CMC's interface.

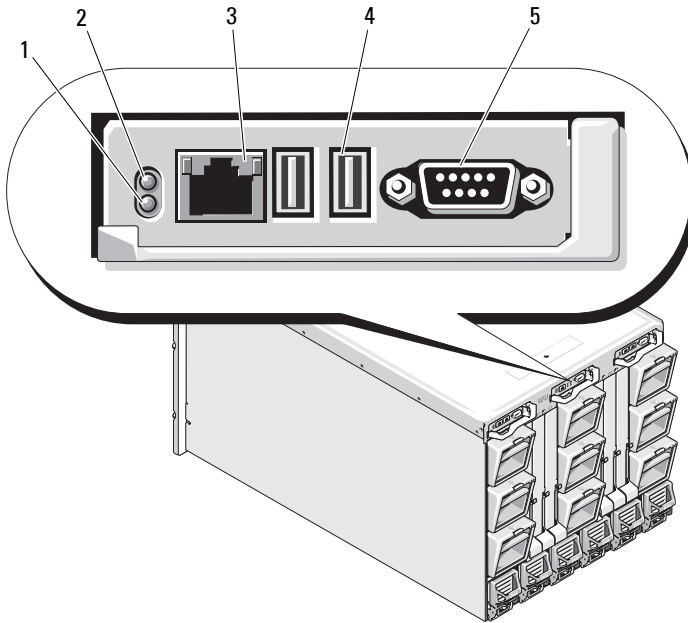


NOTE: Connecting a keyboard, video, and mouse to the enclosure front panel will disable video output to the iKVM back panel port. It will not interrupt iDRAC video and console redirection.

- You can use the iKVM to access the CMC using the Command-Line Interface. For more information, see "Using the iKVM Module" in the *CMC User's Guide*.

Figure 1-11 shows the external features of the iKVM module.

Figure 1-11. Avocent iKVM Switch Module



- | | | | |
|---|--------------------------------------|---|---|
| 1 | identification indicator | 2 | status indicator |
| 3 | ACI port for tiering connection only | 4 | USB connectors (2) for keyboard and mouse |
| 5 | video connector | | |



NOTICE: Do not connect the ACI port to a LAN device such as a network hub. Doing so may result in equipment damage.

Initial System Configuration

Before You Begin

Power Requirements

- ➡ **NOTICE:** The enclosure power supplies must be connected to a Type B or permanently-connected PDU, not directly to an electrical outlet. The power supplies require a 200–240 V power source.

Network Information

If your network uses static addressing, you will need the IP address, subnet mask, and gateway to configure the CMC and other modules in the enclosure.

Initial Setup Sequence

- 1 Unpack the enclosure and install it in a rack.


See the *Getting Started Guide* and *Rack Installation Guide* for more information.

- ➡ **NOTICE:** Do not power-on the blades (server modules) until you have configured the switch modules, as described in "Configuring the I/O Modules" on page 37.

- 2 Connect power to the power supplies.

- ➡ **NOTICE:** The power supplies must be connected to a PDU, not directly to an electrical outlet. The power supplies require a 200–240 V power source.

- 3 If an optional iKVM module is installed, connect the keyboard, video, and mouse to the enclosure control panel (see Figure 1-4) or to the iKVM module (see Figure 1-11).

 **NOTE:** Connecting a keyboard, video, and mouse to the enclosure front panel will disable video output to the iKVM back panel port.

- 4 Press the power button on the enclosure control panel. See Figure 1-4.
- 5 Configure the CMC network settings.

The LCD Configuration Wizard allows you to quickly configure the CMC and iDRAC management interfaces and on the network, so you can then manage the enclosure remotely. See "Configuring the CMC Network Settings Using the LCD Configuration Wizard" on page 23.

You can also use a management station and the RACADM CLI to configure the CMC. See "Configuring the CMC Network Settings Using a Management Station and CLI" on page 24.

- 6 Configure the IO modules at this time to allow proper network or storage management or paths. See "Configuring the I/O Modules" on page 37.
- 7 Once the Ethernet and Fibre Channel switches are configured and able to pass traffic, you can then power on your server blades. This will allow time for the Ethernet switch to boot and allow PXI \ UNDI traffic for all blade modules.

Configuring the CMC

Initial CMC Network Configuration

Connecting to the CMC Using a Network Connection and the Default IP Address, or a User-Defined IP Address

The CMC is preset for DHCP. To use a static IP address you must toggle the CMC setting from DHCP to a static address by either running the LCD Configuration Wizard, or by using a management station and CLI commands.

If toggled to use a static address, the CMC IP address will default to the standard IP address settings of 192.168.0.120, 255.255.255.0, and gateway of 192.168.0.1. You can change this address to an IP address of your choosing.

See "Configuring the CMC Network Settings Using the LCD Configuration Wizard" on page 23 for initial configuration instructions. If you prefer to use a management station and CLI, see "Configuring the CMC Network Settings Using a Management Station and CLI" on page 24.

Configuring the CMC Network Settings Using the LCD Configuration Wizard

When you first start up your system, the screen on the LCD module will direct you to configure the CMC network settings.



NOTE: The option to configure the server using the LCD Configuration Wizard is only available until the CMC is connected to the network or the default password is changed. Once the CMC is accessible from the network, the LCD panel cannot be used to reconfigure the CMC. Thereafter, use the RACADM CLI or the web-based GUI to change the CMC settings.

Table 2-1 lists the keys that you use to view or change information on the LCD module screens.

Table 2-1. LCD Module Screen Navigation Keys

Keys	Action
Left and right arrows	Move between screens.
Up arrow or down arrow	Move to the previous or next option on a screen.
Center button	Select and save an item and move to the next screen.

- 1 Choose a language from the options presented in the dialog box.
- 2 Start the LCD Configuration Wizard.
- 3 Configure the CMC network settings for your network environment



NOTE: The CMC external management network mode is set by default to DHCP. To use a static IP address, you must change the setting using the LCD Configuration Wizard.

- Network speed
- Duplex mode
- Network mode (DHCP or static)
- Static IP address, subnet mask, and gateway values (if static mode was selected)
- DNS setting, including a registered CMC name, (if DHCP mode was selected)

- 4 If desired, configure the iDRAC network setting for DHCP mode.



NOTE: You cannot set a static IP address for the iDRAC using the LCD Configuration Wizard. See "Configuring iDRAC Networking Using the Web-Based Interface" on page 27.

- 5 Review the settings on the **Network Summary** screen.
 - If the settings are correct, press the center button to close the configuration wizard and return to the **Main Menu**.
 - If the settings are not correct, use the left arrow key to return to the screen for that setting and correct it.

After you complete the LCD Configuration Wizard, you can access the CMC on the network using the Web-based CMC interface or text-based interfaces such as a serial console, Telnet, or SSH.

Note that if you intend to use static addresses rather than DHCP to access the iDRACs, you must configure them using the CMC Web-based interface or CLI.

Configuring the CMC Network Settings Using a Management Station and CLI

The LCD Configuration Wizard is the quickest way to initially configure the CMC network settings. However, you can also use a management station and a local connection to access the CMC. There are two ways to create a local connection to the CMC:

- The CMC Console via the optional iKVM. Press <Print Screen> and select blade number 17. Blade number 17 is a direct local connection to the CMC.
- Serial connection using a null modem cable (115200 bps, 8 Data bits, no parity, 1 stop bit, and no flow control).

Once you have established a connection to the CMC, you can complete the initial CMC network configuration:

- 1 Log into the CMC.
The default user name is `root` and the default password is `calvin`.
- 2 Type `getniccfg` and press <Enter> to view the current CMC network parameters.

3 Configure the CMC network settings:

- To set a static IP address, type
`setniccfg -s<IP address><network mask><gateway>`
and press <Enter>.

Use the appropriate settings for your network.

- To configure the CMC to obtain an IP address using DHCP, type
`setniccfg -d`
and press <Enter>.

4 To activate the new network settings, type

`racadm racreset`
and press <Enter>.

Logging in to the CMC Using the Web-Based Interface

1 Open a supported Web browser window.

For more information, see "Supported Web Browsers" in the *CMC User's Guide*.

2 Login to the CMC.

- If the CMC is accessed using a specific IP address, type the following URL in the **Address** field, and then press <Enter>:

`https://<CMC IP address>`

The default IP address for the CMC is 192.168.0.120. If the default HTTPS port number (port 443) has been changed, type:

`https://<CMC IP address>:<port number>`


where *<IP address>* is the IP address for the CMC and *port number* is the HTTPS port number.


- If you access the CMC using a registered DNS name, type the CMC's name:


`https://<CMC name>`

By default, the CMC name on the DNS server is `cmc-<service tag>`.

3 The CMC Login page appears.

 **NOTE:** The default CMC user name is `root`, and the password is `calvin`. The `root` account is the default administrative account that ships with the CMC. For added security, you should change the default password of the `root` account during initial setup.

 **NOTE:** The CMC does not support extended ASCII characters, such as ß, å, é, ü, or other characters used primarily in non-English languages.

 **NOTE:** You cannot log in to the Web-based interface with different user names in multiple browser windows on a single workstation.

You can log in as either a CMC user or as a Microsoft® Active Directory® user.

4 In the **Username** field, type your user name:

- CMC user name: `<user name>`
- Active Directory user name: `<domain>\<user name>`,
`<domain>/<user name>` or `<user>@<domain>`.


 **NOTE:** This field is case sensitive.

5 In the **Password** field, type your CMC user password or Active Directory user password.

 **NOTE:** This field is case sensitive.

Adding and Managing CMC Users

From the **Users** and **User Configuration** pages in the Web-based interface, you can view information about CMC users, add a new user, and change settings for an existing user.

 **NOTE:** For added security, Dell strongly recommends that you change the default password of the `root` (User 1) account. The `root` account is the default administrative account that ships with the CMC. To change the default password for the `root` account, click **User ID 1** to open the **User Configuration** page. Help for that page is available through the Help link at the top right corner of the page.

 **NOTE:** You must have **User Configuration Administrator** privileges to perform the following steps.

- 1 Log in to the Web-based interface. See "Logging in to the CMC Using the Web-Based Interface" on page 25.
- 2 Select **Chassis** in the system tree.

- 3 Click the **Network/Security** tab, and then click the **Users** sub-tab. The **Users** page appears, listing each user's user ID, login state, user name, and CMC privilege, including those of the root user. User IDs available for configuration will have no user information displayed.
- 4 Click an available user ID number. The **User Configuration** page displays.
To refresh the contents of the **Users** page, click **Refresh**. To print the contents of the **Users** page, click **Print**.
- 5 Select general settings for the users.
For details on user groups and privileges, see "Adding and Configuring Users" in the *CMC User's Guide*.
- 6 Assign the user to a CMC user group.
When you select a user privilege setting from the CMC Group drop-down menu, the enabled privileges (shown as checked boxes in the list) display according to the pre-defined settings for that group.

You can customize the privileges settings for the user by checking or unchecking boxes. After you have selected a CMC Group or made Custom user privilege selections, click **Apply Changes** to keep the settings.

Configuring iDRAC Networking Using the Web-Based Interface

Follow this procedure if you did not configure the iDRAC in the LCD Configuration Wizard.



NOTE: If you did not configure the iDRAC using the LCD Configuration Wizard, the iDRAC will be disabled until you configure it using the Web-based interface



NOTE: You must have Chassis Configuration Administrator privileges to set up iDRAC network settings from the CMC.



NOTE: The default CMC user is **root** and the default password is **calvin**.

- 1 Log in to the Web-based interface. See "Logging in to the CMC Using the Web-Based Interface" on page 25.
- 2 Click the plus (+) symbol next to **Chassis** in the left column, then click **Servers**.
- 3 Click **Setup** → **Deploy**.
- 4 Enable the LAN for the iDRAC on the server by checking the checkbox next to the server beneath the **Enable Lan** heading.

- 5 Enable or disable IPMI over LAN by checking the or unchecking the checkbox next to the server beneath the **Enable IPMI over LAN** heading.
- 6 Enable or disable DHCP for the iDRAC by checking or unchecking the checkbox next to the server under the **DHCP Enabled** heading.
- 7 If DHCP is disabled, enter the static IP address, netmask, and default gateway for the iDRAC.
- 8 Click **Apply** at the bottom of the page.

Setting the First Boot Device for Servers

The **First Boot Device** page allows you to specify the boot device for each blade. You can set the default boot device and you can also set a one-time boot device so that you can boot a special image to perform tasks such as running diagnostics or reinstalling an operating system.

To set the first boot device for some or all servers in the chassis:


- 1 Log in to the CMC Web-based interface.
- 2 Click **Servers** in the system tree and then click **Setup → Deploy First Boot Device**. A list of servers is displayed, one per row.
- 3 Select the boot device you want to use for each server from the list box.
- 4 If you want the server to boot from the selected device every time it boots, unselect the **Boot Once** checkbox for the server.
If you want the server to boot from the selected device only on the next boot cycle, select the **Boot Once** checkbox for the server.
- 5 Click **Apply**.

Configuring and Managing Power

You can use the Web-based and RACADM interfaces to manage and configure power controls on the CMC, as outlined in the following sections. For detailed information on the various power management options, see "Power Management" in the *CMC User's Guide*.


Configuring Power Budget and Redundancy

The CMC's power management service optimizes power consumption for the entire chassis (the chassis, servers, I/O modules, iKVM, CMC, and PSUs) and re-allocates power to different modules based on the demand.


 **NOTE:** To perform power management actions, you must have **Chassis Control Administrator** privileges.

- 1 Log in to the CMC Web-based interface.
- 2 Select **Chassis** in the system tree.
- 3 Click the **Power Management** tab. The **Power Budget Status** page displays.
- 4 Click the **Configuration** sub-tab. The **Budget/Redundancy Configuration** page displays.
- 5 Configure the power budget and redundancy settings based on the components in the enclosure and your needs.
- 6 Click **Apply** to save your changes.

Installing or Updating the CMC Firmware

 **NOTE:** During updates of CMC or iDRAC firmware on a server, some or all of the fan units in the chassis will spin at 100%. This is normal.

Updating Firmware in a Redundant CMC Configuration

 **NOTE:** In redundant CMC configuration, care must be taken to update CMC firmware on both modules. Failure to do so may cause unexpected behavior during a CMC failover or failback. Use the following procedure for redundant CMC deployments:

- 1 Locate the secondary or standby CMC by using the RACADM `getsysinfo` command, or by using the **Chassis Summary** page in the Web-based interface. Visually, the status indicator will be solid blue on the primary or active CMC module and off on the standby or secondary CMC (see Figure 1-9).
- 2 Update the firmware on the standby CMC first. See "Updating the CMC Firmware Using the Web-based Interface" on page 30 or "Updating the CMC Firmware Using RACADM" on page 31.
- 3 Verify that the secondary or standby CMC's firmware is at the requested level with the `getsysinfo` command or through the Web-based interface.
- 4 After the standby CMC has rebooted, update the firmware on the active or primary CMC. Please allow 10 minutes for the standby CMC to boot. See "Updating the CMC Firmware Using the Web-based Interface" on page 30 or "Updating the CMC Firmware Using RACADM" on page 31.

- 5 Verify that the active or primary CMC firmware is at the requested level using the `getsysinfo` command or through the Web-based interface.
- 6 Once both CMCs are updated to the same firmware revision, use the `cmchangeover` command to reset the CMC in the left slot as primary.

Downloading the CMC Firmware

Before beginning the firmware update, download the latest firmware version from the **Dell Support** website, and save it to your local system.

The following software components are included with your CMC firmware package:

- Compiled CMC firmware code and data
- Web-based interface, JPEG, and other user interface data files
- Default configuration files

Use the **Firmware Update** page to update the CMC firmware to the latest revision. When you run the firmware update, the update retains the current CMC settings.



NOTE: The firmware update, by default, will retain the current CMC settings. During the update process, you have the option to reset the CMC configuration settings back to the factory default settings.

Updating the CMC Firmware Using the Web-based Interface

- 1 Log in to the Web-based interface. See "Logging in to the CMC Using the Web-Based Interface" on page 25.
- 2 Click **Chassis** in the system tree.
- 3 Click the **Update** tab. The **Updatable Components** page appears.
- 4 On the **Updatable Components** page, click the CMC name. The **Firmware Update** page appears.
- 5 In the **Value** field, type the path on your management station or shared network where the firmware image file resides, or click **Browse** to navigate to the file location.



NOTE: The default CMC firmware image name is **firmimg.cmc** and the filename should not be changed. Care must be taken to keep different firmware revisions separated as the file name will always be the same.

- 6 Click **Update**. A dialog box appears asking you to confirm the action.

- 7 Click **Yes** to continue. The firmware transfer process will begin and the status will display the message "Firmware Update in Progress". Once the CMC update is complete, the CMC will be reset. Once the reset is complete, you will need to refresh the User Interface page to then log in again.

Updating the CMC Firmware Using RACADM

- 1 Open a CMC command line console and log in.

- 2 Type:

```
racadm fwupdate -g -u -a <TFTP server IP address>  
-d <filepath> -m <cmc-active|cmc-standby>
```

See the latest *Dell Chassis Management Controller User's Guide* at support.dell.com for complete instructions on how to configure and operate the CMC module.

Configuring the Optional iKVM Switch Module

Enabling iKVM Access to the Dell CMC Console

Enabling access to the CMC allows you to access the CMC directly and securely through the iKVM's CMC Console option. To enable the CMC Console using the Web-based interface:

- 1 Log in to the CMC Web-based interface.
- 2 Select iKVM in the system tree. The **iKVM Status** page displays.
- 3 Click the **Setup** tab. The **iKVM Configuration** page displays.
- 4 Select **Allow access to CMC CLI from iKVM**.
- 5 Click **Apply** to save the setting.


Updating the iKVM Firmware



NOTE: The iKVM resets and becomes temporarily unavailable after the firmware has been uploaded successfully.

- 1 Log in to the CMC's Web-based interface. See "Logging in to the CMC Using the Web-Based Interface" on page 25.
- 2 Select **Chassis** in the system tree.

- 3 Click the **Update** tab. The **Updatable Components** page appears.
- 4 Click the iKVM name. The **Firmware Update** page appears.
- 5 In the **Value** field, type the path on your management station or shared network where the firmware image file resides, or click **Browse** to navigate to the file location.

 **NOTE:** The default iKVM firmware image name is **ikvm.bin**. However, the iKVM firmware image name can be renamed. If you are unable to locate **ikvm.bin**, determine whether another user has renamed the file.

- 6 Click **Update**. A dialog box appears asking you to confirm the action.
- 7 Click **Yes** to continue.

When the update is complete, the iKVM resets.

Tiering the Avocent iKVM Switch From an Analog KVM Switch

The Avocent iKVM switch can be tiered from analog KVM switches such as the Dell 2160AS and 180AS, as well as many Avocent analog KVM switches. Many switches may be tiered without the need for a Server Interface Pod (SIP) (see Table 2-2).

Table 2-2. Cabling Requirements for External Analog KVM Switches

Switch	Tiering Cabling Requirements
Dell PowerConnect 180AS, 2160AS	Seamless tiering using ACI port and Cat 5 cable
Avocent Autoview 1400, 1500, 2000, 2020, 2030, Ax000R	
Avocent Autoview 200, 400, 416, 424	Avocent USB SIP (DSRIQ-USB) required with Cat 5 cable
Avocent Outlook 140ES, 180ES, 160ES	

Before connecting the iKVM switch to a supported analog switch, you must set the iKVM switch to display in slot order, and set the **Screen Delay Time** to 1 or more seconds:

- 1 Press <Print Screen> to launch the iKVM Switch OSCAR.
- 2 Click **Setup** → **Menu**. The **Menu** dialog box appears.
- 3 Select **Slot** to display servers numerically by slot number.

- 4 Enter a screen delay time of at least 1 second.
- 5 Click **OK**.

Setting the Screen Delay time to 1 second allows you to soft switch to a server without launching OSCAR.



NOTE: Soft switching allows you to switch servers using a hot key sequence. You can soft switch to a server by pressing <Print Screen> and then typing the first few characters of its name or number. If you have a Delay Time set and you press the key sequences before that time has elapsed, OSCAR will not display.

To connect the Avocent iKVM switch to a supported analog switch:

- 1 *If the switch does not require a SIP to connect to the iKVM (see Table 2-2),* connect a Cat5 (or newer) cable to the RJ-45 ACI port on the iKVM module. See Figure 1-11.

Connect the other end of this cable to the ARI port on the external switch.

If the analog switch requires a SIP (see Table 2-2), connect a Avocent USB dongle or to the iKVM, then connect a Cat5 (or newer) cable to the SIP. Connect the other end of this cable to the ARI port on the external switch.

- 2 Connect both the analog switch and the system to an appropriate power source.
- 3 Power up the system.
- 4 Power up the external analog switch.



NOTE: If the external analog switch is powered up before the system, it may result in only one blade displaying in the analog switch OSCAR, instead of 16. If this behavior occurs, shut down and restart the switch so the entire complement of blades is recognized.



NOTE: In addition to the steps outlined above, some external analog switches may require you to perform additional steps to ensure that the iKVM switch blades appear in the external analog switch OSCAR. See the external analog switch documentation for additional information.

Tiering the Avocent iKVM Switch From a Digital KVM Switch

The iKVM module may also be tiered from a digital KVM switch such as the Dell 2161DS-2 or 4161DS, or a supported Avocent digital KVM switch. Many switches may be tiered without the need for a SIP (see Table 2-3).

Table 2-3. Cabling Requirements for External Digital KVM Switches

Switch	Tiering Requirements
Dell PowerConnect 2161DS-2, 4161DS	Seamless tiering using ACI port and Cat 5 cable
Avocent DSR 800, x16x, x010, x031, x030, x035, 102x (except 1024)	
Avocent DSR 1024	Avocent USB SIP (DSRIQ-USB) required with Cat 5 cable

To tier the iKVM module from a Dell 2161DS, 180AS, or 2160AS console switch:

- *If the switch does not require a SIP to connect to the iKVM (see Table 2-3), connect a Cat5 (or newer) cable to the RJ-45 ACI port on the iKVM module. See Figure 1-11.*

Connect the other end of this cable to the ARI port on the external switch.

- *If the switch requires a USB SIP (see Table 2-2), connect an Avocent USB SIP to the iKVM, then connect a a Cat5 (or newer) cable to the SIP. Connect the other end of this cable to the ARI port on the external switch.*

Once the KVM switch is connected, the server modules appear in OSCAR.



NOTE: When the local system is set up, you must also resynchronize the server list from the Remote Console Switch software in order to see the list of blades. See "Resynchronizing the Server List at the Remote Client Workstation" on page 35."

Viewing and Selecting Servers

Use the OSCAR Main dialog box to view, configure, and manage servers in the M1000e enclosure through the iKVM. You can view the servers by name or by slot. The slot number is the chassis slot number the server occupies. The Slot column indicates the slot number in which a server is installed.



NOTE: Server names and slot numbers are assigned by the CMC.



NOTE: If you have enabled access to the CMC though the iKVM, an additional option, Dell CMC Console, is displayed. To enable this feature, see "Enabling iKVM Access to the Dell CMC Console" on page 31.

To access the **Main** dialog box:

Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.

or

If a password has been assigned, the **Password** dialog box appears. Type your password and click **OK**. The **Main** dialog box appears.

Resynchronizing the Server List at the Remote Client Workstation

Once the iKVM module is connected, the blades appear in OSCAR. You now need to resynchronize the servers on any remote workstation to ensure that the blades are available to any remote users connected to the console switch through the Remote Console Switch software.



NOTE: This procedure only resynchronizes one remote client workstation. With multiple client workstations, save the resynchronized local database and load it into the other client workstations to ensure consistency.

To resynchronize the server listing:

- 1 Click **Resync** in the **Server** category of the Management Panel (MP).
The Resync Wizard launches.

- 2 Click **Next**.

A warning message displays indicating that the database will be updated to match the current configuration of the console switch. Your current local database names will be overridden with the switch names. To include unpowered SIPs in the resynchronization, click to enable the **Include Offline SIPs** checkbox.

- 3 Click **Next**.

A **Polling Remote Console Switch** message box appears with a progress bar indicating that the switch information is being retrieved.

- 4 If no changes were detected in the appliance, a completion dialog box appears with this information.

If server changes were detected, then the **Detected Changes** dialog box will be displayed. Click **Next** to update the database.

- 5 If a cascade switch was detected, the **Enter Cascade Switch Information** dialog box appears. Select the type of switch connected to the appliance from the drop-down list. If the type you are looking for is not available, you can add it by clicking **Add**.
- 6 Click **Next**. The completion dialog box appears.

FlexAddress

FlexAddress allows you to replace the factory-assigned World Wide Name/Media Access Control (WWN/MAC) ID with a WWN/MAC ID that is persistent and mapped to a particular chassis slot. If you purchase FlexAddress with your chassis, it will be installed and active when you power up your system. If you purchase FlexAddress at a later date, you must install the SD feature card using the instructions in the *CMC Secure Digital (SD) Card Technical Specification* document. See support.dell.com for this document.

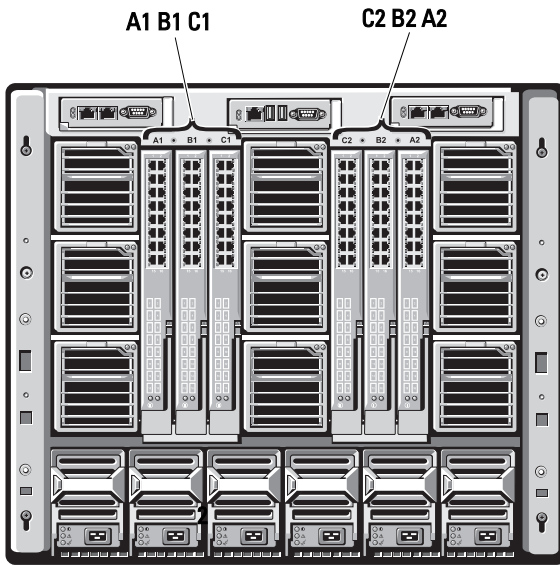
For complete information on using the FlexAddress feature, click the **Help** link in the CMC Web interface, or review the "Using FlexAddress" chapter of the *CMC User's Guide*.

Configuring the I/O Modules

Overview

The M1000e enclosure supports three redundant I/O fabrics, selectable between combinations of Ethernet and Fibre Channel modules. (Additional fabrics including Infiniband will be supported in the future.) You can install up to six hot-swappable I/O modules in the enclosure, including Fibre Channel switches, Fibre Channel pass-throughs, Ethernet switches, and Ethernet pass-through modules. Figure 3-1 shows the numbering of the I/O bays.

Figure 3-1. I/O Module Bay Numbering



Fabric A

Fabric A is a redundant Gb Ethernet fabric, supporting I/O module slots A1 and A2. The integrated Ethernet controllers in each blade dictate Fabric A as an Ethernet-only fabric.



NOTICE: Modules designed for Fabric B or Fabric C cannot be installed in slots A1 or A2. However, modules designed for Fabric A may also be installed in Fabric B and Fabric C slots.

Fabric B

Fabric B is a 1 to 10 Gb/sec dual port, quad-lane redundant fabric, supporting I/O module slots B1 and B2. Fabric B currently supports Gb Ethernet, Infiniband, and Fibre Channel modules. Additional fabric types including 10 Gb Ethernet will be supported in the future.

To communicate with an I/O module in the Fabric B slots, a blade must have a matching mezzanine card installed in a Fabric B mezzanine card location.

Modules designed for Fabric A may also be installed in the Fabric B slots.

Fabric C

Fabric C is a 1 to 10 Gb/sec dual port, quad-lane redundant fabric, supporting I/O module slots C1 and C2. Fabric C currently supports Gb Ethernet, Infiniband, and Fibre Channel modules. Additional fabric types including 10 Gb Ethernet will be supported in the future.

To communicate with an I/O module in the Fabric C slots, a blade must have a matching mezzanine card installed in a Fabric C mezzanine card location.

Modules designed for Fabric A may also be installed in the Fabric C slots.

See your *Hardware Owner's Manual* for more information about I/O module installation guidelines.

Before You Begin

Network Information

You can configure your I/O switch modules using the CMC, as outlined in "Configuring a Switch Module Network Ethernet Port Using the Web-Based Interface" on page 39 (the default IP address for the CMC is 192.168.0.120), through the CMC CLI via serial console redirection, direct access to the I/O module's serial port (if supported), or using the I/O module's default IP address (if supported).

Switch Modules

Configuring a Switch Module Network Ethernet Port Using the Web-Based Interface

You can use the CMC Web-based interface to configure an I/O module's Ethernet port.



NOTE: Use this procedure to configure the switch's out-of-band Ethernet port. The switch's in-band management IP address is configured through the switch's external ports. These two IP addresses must be different, and on different networks.



NOTE: To change settings on the I/O module configuration page, you must have **Fabric Administrator** privileges for the particular Fabric in which the module is installed.



NOTE: The network IP address set on the I/O module by the CMC is not saved to a configuration file. To save the IP address configuration permanently, use the `connect switch-n RACADM` command, or use a direct interface to the I/O module GUI.



NOTE: Do not attempt to configure I/O module network settings for Ethernet passthrough or Infiniband switches.

- 1 Log in to the CMC's Web-based interface. See "Logging in to the CMC Using the Web-Based Interface" on page 25.
- 2 Select **I/O Modules** in the **Chassis** menu in the system tree.
- 3 Select the **Setup** tab. The **Configuring I/O Modules Network Settings** page appears.

- 4 Configure the switch for integration into your network.
 - Select **DHCP Mode Enabled** if your network uses a DHCP server to assign IP addresses.
 - If your network uses static IP addressing, enter an IP address, subnet mask and gateway.
- 5 When you have finished, click **Apply**.
- 6 Click the **Deploy** sub-tab.

After all I/O modules have been configured and connected, the enclosure's blades can be inserted and booted with full network communication.

Cisco SFS M7000e Infiniband Switch Module

The Cisco SFS 7000e Infiniband switch module includes 24 4x DDR Infiniband ports. Eight ports are external uplink ports, and 16 internal ports provide connectivity to the blades in the enclosure. This switch module is hot-pluggable and may be installed in Fabric B or Fabric C. See Figure 3-2.

Figure 3-2. Cisco SFS M7000e Infiniband Switch Module Features

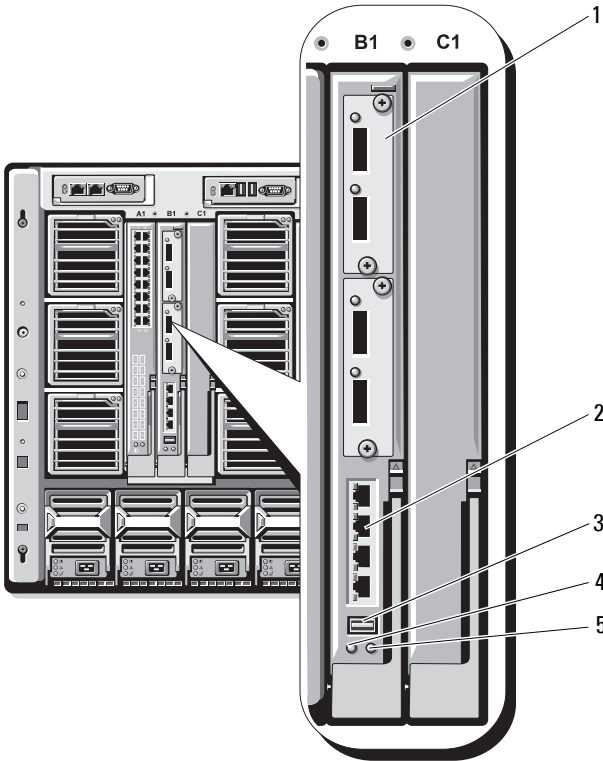


- | | | | |
|---|-----------------------------|---|---------------------------|
| 1 | Infiniband ports (8) | 2 | port status indicator (8) |
| 3 | diagnostic status indicator | 4 | power indicator |

PowerConnect M6220 Ethernet Switch Module

The PowerConnect M6220 Ethernet switch module includes four external 10/100/1000 Mbps Ethernet connectors and one USB type A form factor serial connector. See Figure 3-3.

Figure 3-3. PowerConnect M6220 Ethernet Switch Module Features



- | | | | |
|---|---|---|---|
| 1 | optional module (2) (dual 10 Gb Ethernet uplink module shown) | 2 | standard 10/100/1000 Mb Ethernet connectors (4) |
| 3 | serial connector (USB type-A form factor) | 4 | power indicator |
| 5 | status/identification indicator | | |

Two option bays support the following three module options:

- A resilient stacking module with 2 x 24 Gb stacking ports
- A 10 Gb Ethernet module with two 10 Gb optical XFP connectors
- 10 Gb Ethernet module with two copper CX4 uplinks

Cisco Ethernet Switch

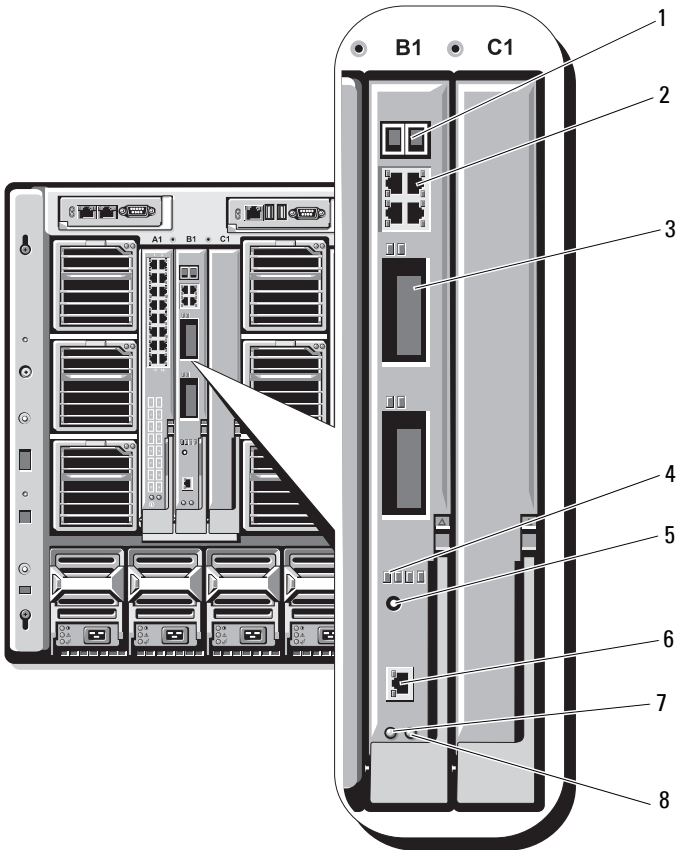
Your system supports three Cisco Catalyst Blade Switch (CBS) versions:

- The Cisco 3130G switch includes four 10/100/1000 Mb Ethernet uplink ports and two stacking ports.
- The Cisco CBS 3130X switch includes four 10/100/1000 Mb Ethernet uplink ports, two 10 Gb uplink ports, and two stacking ports.
- The Cisco CBS 3032 switch includes four 10/100/1000 Mb Ethernet uplink ports.

The two option bays support the following module options:

- Cisco X2 10 Gb transceiver modules (CBS 3130X only)
- Cisco TwinGig converter modules

Figure 3-4. Cisco Ethernet Switch Module Features



- | | |
|---|--|
| <ul style="list-style-type: none"> 1 stacking port connectors (not enabled in CBS 3032) 3 option bays (2) 5 mode button 7 power indicator | <ul style="list-style-type: none"> 2 10/100/1000 Mb Ethernet connectors (4) 4 Cisco status indicators 6 console port for switch management 8 status/identification indicator |
|---|--|

For additional information about the Cisco CBS Ethernet switch modules, see the documentation that shipped with the module.

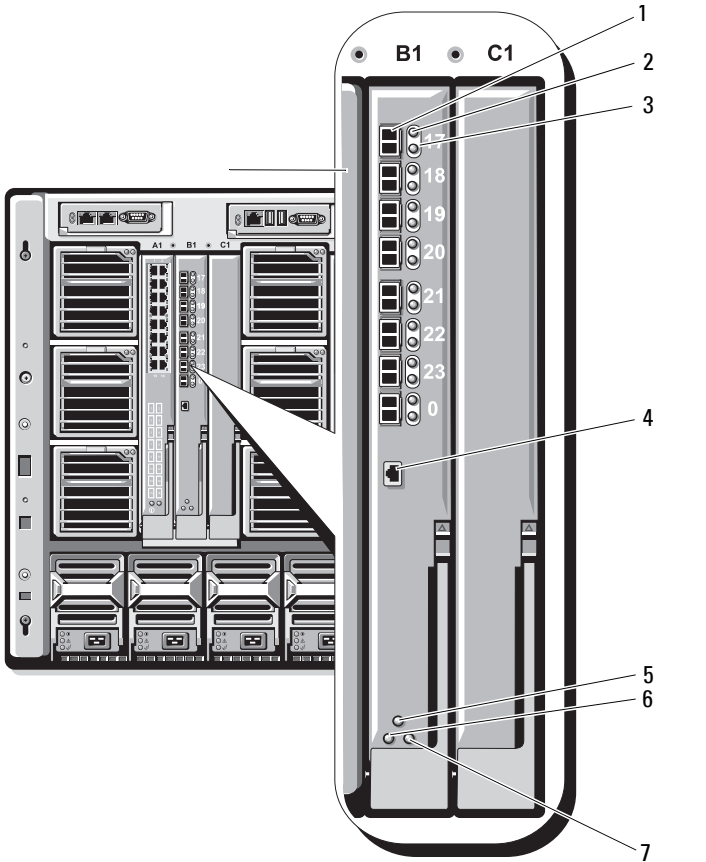
Brocade M4424 SAN I/O Module

The Brocade M4424 SAN I/O module includes eight external autosensing Fibre Channel ports (four ports are enabled in the standard configuration and four additional ports may be enabled as an optional upgrade), 16 internal ports, and one serial port with an RJ-45 connector. The external Fibre Channel ports operate at 1 Gb/sec, 2 Gb/sec, or 4 Gb/sec. The Fibre Channel switch module is hot-pluggable, and may be installed in Fabric B or Fabric C.



NOTE: The Fibre Channel switch module includes Short Wave Small Form Factor Pluggable (SFP) optical transceivers. To ensure proper functionality, use only SFPs provided with this module.

Figure 3-5. Brocade M4424 SAN I/O Module Features



- | | | | |
|---|--|---|---|
| 1 | Fibre Channel port (8) | 2 | Fibre Channel port status indicator (8) |
| 3 | Fibre Channel port speed indicator (8) | 4 | serial port (RJ-45 connector) |
| 5 | module status indicator | 6 | power indicator |
| 7 | status/identification indicator | | |

Pass-through Modules

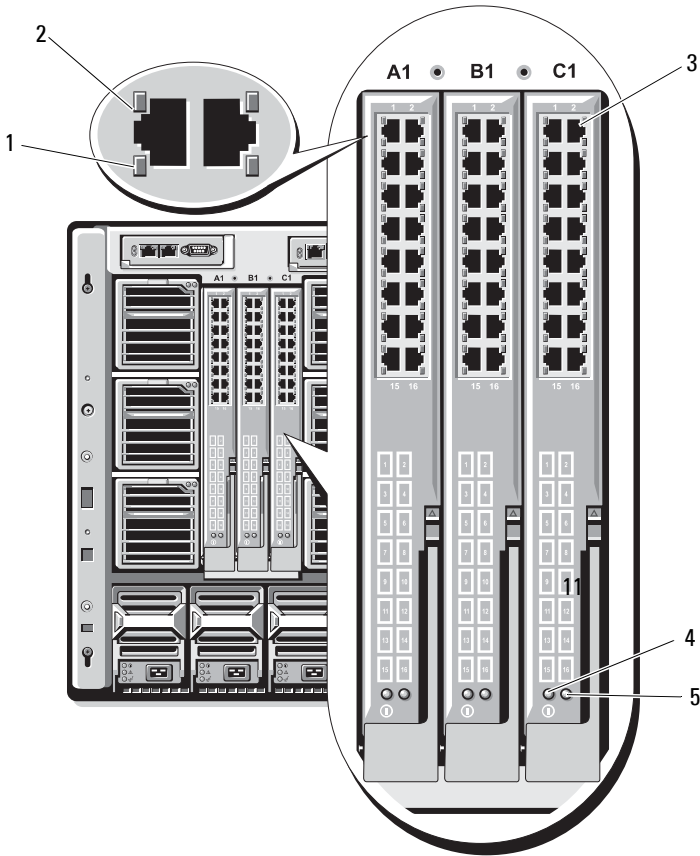
Ethernet Pass-through Module

The Ethernet pass-through module supports 10/100/1000 Mb connections, and provides a direct connection between the optional internal Ethernet mezzanine card in the blade or the integrated LOMs in the blade, and an external Ethernet device (see Figure 3-6). The Ethernet pass-through modules are hot-pluggable and may be installed in any of the three fabrics.



NOTE: No configuration is required for this module.

Figure 3-6. Ethernet Pass-through Module Features



- | | | | |
|---|---------------------------------|---|---------------------|
| 1 | activity indicator (16) | 2 | link indicator (16) |
| 3 | RJ45 Ethernet connector (16) | 4 | power indicator |
| 5 | status/identification indicator | | |

NOTE: Connectors on the Ethernet pass-through module correspond directly to the blade number. For example, blade 5 is connected to port 5 on the Ethernet pass-through module. Integrated network adapter 1 will map to I/O slot A1. Integrated network adapter 2 will map to I/O slot A2.

Fibre Channel Pass-through Module

The Fibre Channel pass-through module provides a bypass connection between a Fibre Channel mezzanine card in the blade and optical transceivers for direct connection into a Fibre Channel switch or a storage array (see Figure 3-7). The 16 pass-through ports on this module can negotiate speeds of 1-, 2-, or 4-Gbps. The Fibre Channel pass-through modules are hot-pluggable, and may be installed in Fabric B or Fabric C.

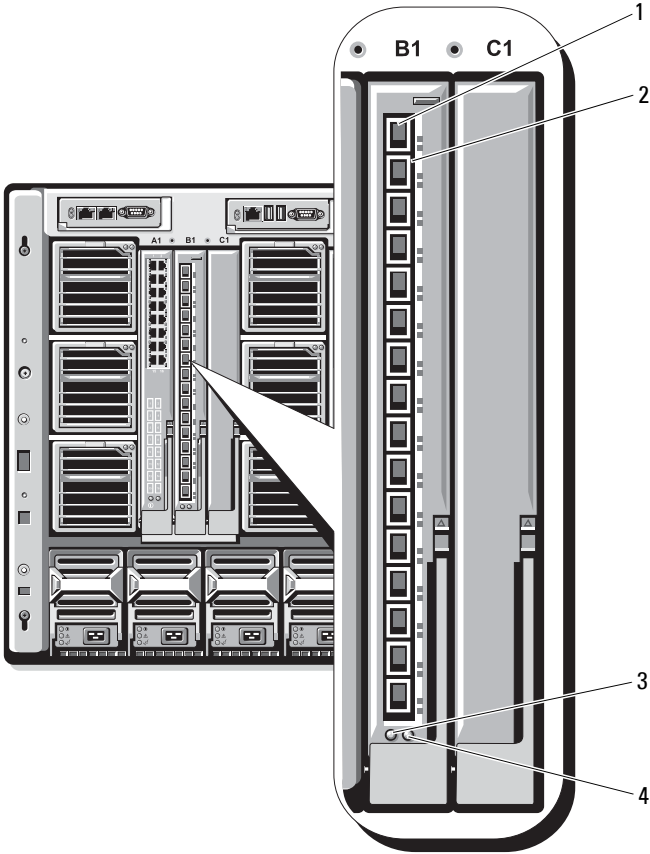


NOTE: No configuration is required for this module.



NOTE: To ensure proper functionality, use only the Short Wave Small Form Factor Pluggable (SFP) transceivers provided with this module.

Figure 3-7. Fibre Channel Pass-through Module Features



- | | | | |
|---|----------------------------------|---|---|
| 1 | SFP Fibre Channel connector (16) | 2 | Fibre Channel green/amber indicators (two per port) |
| 3 | power indicator | 4 | status/identification indicator |



www.dell.com | support.dell.com