Dell Chassis Management Controller Firmware Version 4.3 Troubleshooting Guide

Notes, Cautions, and Warnings

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

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

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

Introduction

The *Dell Chassis Management Controller Firmware Version 4.3 Troubleshooting Guide* provides solutions for few issues you may see while using CMC. For additional information, see the *Dell Chassis Management Controller Firmware Version 4.3 User's Guide* at **dell.com/support/manuals**. If the problem persists, contact the Dell Technical Support.

Chassis Management Controller Stops Functioning

1. Perform one of the following:

    – If you are able to access or ping the CMC IP address, log in to CMC though the Web interface or RACADM (Telnet/SSH, Remote, or Serial RACADM) interface.

    – If you log in to CMC through the Web interface, go to **Chassis Overview** → **Troubleshooting** → **Reset components** and click **Reset/failover CMC**.

    – If you log in to CMC through RACADM (Telnet/SSH/Serial), run the **racadm cmcchangeover** command. This command is applicable only if the M1000e chassis has two CMCs, one active and the other standby. If there is only one CMC in the M1000e chassis, run the **racadm racreset** command.

    – If you log in using remote RACADM and if the chassis has two CMCs (one active and the other standby), run the following command:

    ```
    racadm -r<CMC IP address>-u<username>-p<password>cmcchangeover
    ```

    It takes around five minutes for the CMC to reboot. Log in to CMC through the Web interface or RACADM (Telnet/SSH/Serial) using the IP address and view the active errors in the CMC logs.

      * CMC Web Interface: Go to **Chassis Overview** → **Logs** to view the CMC logs.

      * RACADM: Use the **getsel**, **getraclog**, or **gettracelog** commands.

2. If the problem persists or if you are unable to access the CMC IP, connect a Serial cable to the CMC. After the login prompt is displayed, check the network settings using the following command:

    ```
    racadm getconfig -g cfglannetworking
    ```

    To change the network settings such as IP address, Subnet address, or Gateway address from DHCP to static IP or from static IP to DHCP, run the following command:

    ```
    racadm help config -g cfglannetworking
    ```

    Follow the examples provided in the output.

3. If the problem persists or if you are unable to access CMC from Serial connection, then physically remove and reinsert CMC in the chassis.

    During this operation, IP address of all servers and iDRAC is temporarily inaccessible. It takes around five minutes for the CMC to reboot. Log in to CMC through the Web interface or RACADM (Telnet/SSH/Serial) using the IP address and view the active errors in the CMC logs.

    – CMC Web Interface: Go to **Chassis Overview** → **Logs** to view the CMC logs.

    – RACADM: Use the **getsel**, **getraclog** or **gettracelog** commands.

4. Connect the network cable to the left most RJ45. If the problem persists, and you are able to access CMC through a Serial connection, then check for a recover prompt. If you see a recover prompt, type **recover** and then press <Enter>. One of the following messages is displayed:

    – `recover1[self test] CMC1 self test failure`

    – `recover2[Bad FW images] CMC2 has corrupted images`

If the prompt indicates a self test failure, there are no serviceable components on CMC. Then, replace the CMC card.

If the prompt indicates Bad Firmware Images, then recover the firmware image:

    a. At the recover prompt, type **recover** and then press <Enter>. The recover reason and available sub-commands are displayed.

    b. Run the following commands to reprogram the flash devices by uploading the firmware update file **firmimg.cmc**:

```
recover getniccfg
recover setniccfg <IP address> <Subnet address> <Gateway address>
recover ping <IP address>
recover fwupdate -g -a <IP address>
```

> **NOTE:** This is the same firmware image file that is used for normal firmware updates.

> **NOTE:** In recover mode, you cannot ping CMC normally because there is no active network stack. The **recover ping** <TFTP server IP> command allows you to ping to the TFTP server to verify the LAN connection. You may need to use the **recover reset** command after **setniccfg** on some systems.

The recovery process displays its current activity and boots to the CMC OS upon completion. An example recover sequence may be:

```
recover getniccfg
recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1
recover ping 192.168.0.100
recover fwupdate -g -a 192.168.0.100
```

> **NOTE:** Make sure CMC has the latest revision firmware. To check the CMC version, from Telnet/SSH use the **racadm getversion** command or on the CMC Web interface, go to **Chassis Overview → Update**.
>
> To get the latest CMC firmware visit the Dell Support site at **Support → Drivers & Downloads → Enterprise IT → Servers, Storage & Networking → Poweredge → Poweredge M1000E → Chassis System Management → Dell firmware**.

Power Supply Unit Not Detected

1. Make sure that all the Power Supply Units (PSUs) are firmly connected to the chassis and status for each PSU is either online or standby. Check and replace the AC or DC cord if needed. Check to confirm the power distribution unit providing power to the PSU is operating normally.

2. Make sure that all the PSUs are operating at the same voltage. Use external tools to check and correct the voltages for the PSUs.

3. If the problem persists, perform one of the following:

    – If you are able to access or ping the CMC IP address, log in to CMC though the Web interface or RACADM (Telnet/SSH, Remote, or Serial RACADM) interface.

    – If you log in to CMC through the Web interface, go to **Chassis Overview → Troubleshooting → Reset components** and click **Reset/failover CMC**.

    – If you log in to CMC through RACADM (Telnet/SSH/Serial), run the **racadm cmcchangeover** command. This command is applicable only if the M1000e chassis has two CMCs, one active and the other standby. If there is only one CMC in the M1000e chassis, run the **racadm racreset** command.

    – If you log in using remote RACADM and if the chassis has two CMCs (one active and the other standby), run the following command:

```
racadm -r<CMC IP address>-u<username>-p<password>cmcchangeover
```

    It takes around five minutes for the CMC to reboot. Log in to CMC through the Web interface or RACADM (Telnet/SSH/Serial) using the IP address and view the active errors in the CMC logs.

* CMC Web Interface: Go to **Chassis Overview → Logs** to view the CMC logs.
* RACADM: Use the **getsel**, **getraclog** or **gettracelog** commands.

Check if the PSU comes online after this action. To verify, in the CMC Web interface, go to **Power Supplies → Properties**. The **Power Supply Status** page is displayed. The **Power Status** value should be **Online** for each PSU. If the problem persists, contact Dell Technical Support to replace the PSU.

Modular Server in the Chassis Does Not Power On

1. Make sure that all the Power Supply Units (PSUs) are firmly connected to AC or DC cord and status for each PSU should be online or standby. Check the system input power cap setting in the **Budget/Redundancy Configuration** section of the CMC Web interface (**Chassis Overview → Power → Configuration** .) If the power cap setting value is configured too low, then it does not allow any additional servers to turn on.

2. If the problem persists, check for 110V operation. If any PSU is connected to a 110V branch circuits, verify if this is a valid configuration before servers are allowed to turn on. For more details, see the Power Configuration settings in the **Budget/Redundancy Configuration** section of the CMC Web interface.

   Check if the PSU status changes to online after this action. If the problem persists, contact the Dell Technical Support to replace the PSU.

3. If the problem persists, select the **Max Power Conservation** setting in the **Budget/Redundancy Configuration** section of the CMC Web interface.

   In the **Maximum Power Conservation** mode, all servers function at their minimum power threshold, and all subsequent server power allocation requests are denied. In this mode, the performance of the powered on servers may be reduced. Additional servers cannot be powered on, regardless of server priority. The system is restored to full performance when the **Maximum Power Conservation** option is cleared. For more details, see the **Power Configuration** settings in the *Dell Chassis Management Controller Firmware Version 4.3 User's Guide* available at **dell.com/support/manuals**.

4. If the problem persists, check the server slot power priority of the slot associated with the newly inserted server, and make sure it is not lower than any other server slot power priority.

   The least priority servers lose power after a PSU failure. This is the expected behavior if the enclosure power policy was configured to **No Redundancy**.

5. To avoid a future power supply failure causing servers to turn off, make sure that the chassis has at least four PSUs. To prevent PSU failure from impacting server operation, make sure that the chassis is configured for the **Power Supply Redundancy** policy.

Unable to Access CMCs and Server iDRACs

1. If you are able to access or ping the CMC IP address, make sure that all network cables are connected properly and network settings are configured properly. Connect a Serial cable to the CMC. After you receive the login prompt, check the network settings using the **racadm getconfig -g cfglannetworking** command. If there is any change needed in network settings like VLAN settings, IP address, Subnet, Gateway change, from DHCP to static IP or from static IP to DHCP, run the **racadm help config -g cfglannetworking** command and follow the examples provided in the output. Also, make sure that the VLAN settings are correct in CMC and Rack switches.

2. If the problem persists or if you are unable to access CMC from Serial connection, then physically remove and reinsert CMC in the chassis.

   During this operation, IP address of all servers and iDRAC is temporarily inaccessible. It takes around five minutes for the CMC to reboot. Log in to CMC through the Web interface or RACADM (Telnet/SSH/Serial) interface using the IP address and view the active errors in the CMC logs:

   – CMC Web interface: Go to **Chassis Overview → Logs** to view the CMC logs.

– RACADM: Use the **getsel**, **getraclog**, or **gettracelog** commands.

3. If the problem persists, reset CMC to factory default settings.

> **NOTE:** This command completely erases CMC configuration. Take a backup of the chassis configuration before resetting to factory default settings. You can use this to restore the chassis configuration settings. To reset chassis configuration, run the **racadm racresetcfg** command.

> **NOTE:** Make sure CMC has the latest revision firmware. To check the CMC version, from Telnet/SSH use the **racadm getversion** command or on the CMC Web interface, go to **Chassis Overview → Update**. To get the latest CMC firmware visit the Dell Support site at **Support → Drivers & Downloads → Enterprise IT → Servers, Storage & Networking → Poweredge → Poweredge M1000E → Chassis System Management → Dell firmware** .

CMC Shows Redundancy Lost

1. A firmware or software incompatibility is detected between CMC1 and CMC2. If CMC1 and CMC2 have different firmware versions and redundancy is lost. Both CMCs should have same Firmware in order to have redundancy. To view the CMC firmware version:

   – Using CMC Web interface: Go to **Chassis Overview → Update**.
   – Using RACADM: Run the **getversion** command.

   To download the latest CMC firmware image, go to Dell support site at **Support → Drivers & Downloads → Enterprise IT → Servers, Storage & Networking → Poweredge → Poweredge M1000E → Chassis System Management → Dell firmware** .

2. If the problem persists, make sure that the network cables are connected properly to the standby CMC. Using a laptop, verify that you are able to access the IP address through that cable.

3. If the standby CMC is removed, CMC shows that redundancy is lost. Make sure that the standby CMC card is seated properly. Press the latch to unlock the module and pull the CMC module out. Reinsert the CMC module properly and lock the CMC module by closing the latch. The blue LED is enabled on the active CMC. In a redundant two-CMC configuration, only the top green LED is enabled on the standby CMC.

4. Perform one of the following:

   – If you are able to access or ping the CMC IP address, log in to CMC though the Web interface or RACADM (Telnet/SSH, Remote, or Serial RACADM) interface.
   – If you log in to CMC through the Web interface, go to **Chassis Overview → Troubleshooting → Reset components** and click **Reset/failover CMC**.
   – If you log in to CMC through RACADM (Telnet/SSH/Serial), run the **racadm cmcchangeover** command. This command is applicable only if the M1000e chassis has two CMCs, one active and the other standby. If there is only one CMC in the M1000e chassis, run the **racadm racreset** command.
   – If you log in using remote RACADM and if the chassis has two CMCs (one active and the other standby), run the following command:

   ```
   racadm -r<CMC IP address>-u<username>-p<password>cmcchangeover
   ```

   If there is only one CMC in the chassis, run the following command:

   ```
   racadm -r<CMC IP address>-u<username>-p<password>racreset
   ```

   It takes around five minutes for the CMC to reboot. After CMC is rebooted, log in to the CMC using CMC Web interface or RACADM and verify the redundancy mode:

   * CMC Web Interface: Go to **Chassis Overview → Health**. On the Graphic, place the cursor on CMCs. It must display the mode as Redundant.
   * RACADM: Use the **getredundancymode** command. Output is displayed as Redundant.
   * Remote RACADM: Run the following command:
     ```
     racadm -r<CMC IP address>-u<username>-p<password>getredundancymode
     ```

Modular Server in the Chassis is Not Accessible

1. Make sure that the modular server is in powered **ON** state. To check the modular server condition, log in to CMC Web interface. On the left pane, under **Server Overview**, click the slot where the modular server is connected. Click **Power** and verify the power status in the **Server Power Management** page. If the power state is **OFF**, under **Power Control Operations**, select **Power On Server**, and then click **Apply**.

   Wait for some time for the modular server to power on. If the modular server does not power on, check the:

   – Power availability and slot priority for the modular server.
   – Power redundancy configurations - Make sure the chassis has all six PSUs connected so that all the modular servers receive enough power to turn on.

   To power on the server using RACADM, run the command, **racadm help serveraction**. Follow the examples to check the power status of the modular server.

2. If the problem persists, check the connectivity to CMC. Make sure the cable from the rack switch is connected properly to CMC. If physical connectivity is fine, and the problem persists, connect a Serial cable to the CMC. After you receive a login prompt, check the network settings using the **racadm getconfig -g cfglannetworking** command. If there is any change needed in network settings such as IP address, Subnet address, or Gateway address, from DHCP to static IP or from static IP to DHCP, use the **racadm help config -g cfglannetworking** command and follow the examples provided in the output. If you are unable to access CMC using the Serial connection, then physically remove and reinsert the CMC card in the chassis.

3. If the problem persists log in to the CMC Web interface, go to **Server Overview → Setup → iDRAC → iDRAC Network Settings**, and verify the modular server network settings.

   Make sure that:

   – LAN is enabled and IPv4 or IPv6 settings are correct.
   – Verify modular server VLAN settings (**Server Overview → Setup → VLAN** .)

   In the left pane, under **Server Overview**, click on the slot where the modular server is present. Make sure the modular server gets the IP under IPv4 or IPv6 network settings.

   Ping the iDRAC IP from any management station. If this is successful, click **Launch Remote Console** option available in the same page. If the modular server has an operating system, an operating system login prompt is displayed. If the modular server is in POST condition, reboot the modular server.

   To configure the modular server network settings using RACADM, run the **racadm help setniccfg** command and follow the examples provided in the output

4. If the problem persists, reset the modular server iDRAC using the Web interface or RACADM interface:

   – CMC Web interface: Go to **Chassis Overview → Troubleshooting → Reset components** . In the **Reset** column, select **iDRAC Reset** option.

     > ![note icon] **NOTE:** Do not select the **Virtual Reseat** option as this option physically reboots the server.

   – RACADM: Through Telnet/SSH/Serial RACADM, run **racadm help racreset** and then follow the examples to reset iDRAC of the blade. For example, **racadm racreset –m server-1 -f** .

5. If the problem still persists, physically remove and reinsert the modular server.

> ![note icon] **NOTE:** Make sure you have the latest CMC firmware and latest BIOS, iDRAC, CPLD, LC and NIC firmware for the modular server. To check the CMC/modular server iDRAC version, from Telnet/SSH run the **getversion** command or from CMC Web Interface , go to **Chassis Overview → Update** or **Server Overview → Update**, and select the modular server slot from left pane. To get the latest CMC firmware visit the Dell Support site at **Support → Drivers & Downloads → Enterprise IT → Servers, Storage & Networking → Poweredge → Poweredge M1000E** or **Modular Server (M620, M820)** and so on.

Fabric Mismatch

The first modular server or IOM inserted in the chassis decides the uniformity and sequence of a Fabric type. Fabric mismatch is noticed if there is no uniformity among the Mezzanine Cards or IOMs present in B and C fabrics of previously inserted or the newly inserted modular servers or IOM. There are three types of invalid configurations and suggested solutions:

- Invalid Mezzanine Card or LOM configuration - In this configuration, a newly installed server's fabric type is different from the existing IOM fabric. An invalid Mezzanine Card (MC) configuration occurs when a single server's LOM or Mezzanine Card(MC) is not supported by its corresponding IOM. In this case, though all the other servers in the chassis are powered on, the server with the mismatched MC card is not allowed to power on. The power button on the server flashes **Amber** to alert a fabric mismatch. For example, Active working modular server-1 in SLOT-1 has a Converged network adapter (CNA) or Ethernet Mezzanine Card (MC) in Fabric B and now when you try to boot a new modular server-2 in (SLOT-2) with Fiber Channel (FC) card in Fabric B, it does not allow modular server-2 to boot and a fabric mismatch error is observed. The reason for the error is MC in Fabric B of modular server-1 in SLOT-1 does not match with MC in Fabric B of modular server-2 in SLOT-2. To fix mismatch errors, remove MC and replace with CNA or Ethernet MC in modular server-2 to allow server-2 to boot.
- Invalid IOM-Mezzanine Card configuration – In this configuration, a newly installed IOM's fabric type and the resident Mezzanine Card's fabric types do not match or they are incompatible. The mismatched IOM is in the power-off state. CMC adds an entry to CMC and hardware logs stating the invalid configuration and the IOM name. CMC causes the LED on the IOM with the error to blink. If CMC is configured to send alerts, it sends e-mail and SNMP alerts for this event. For example, if a user has Ethernet or FCoE supported IOM in B1 fabric and inserts FC Mezzanine Card in modular sever-1 of SLOT-1, modular server-1 does not boot as there is mismatch between B1 IOM and MC in modular server. To resolve the issue, either replace B1 or B2 IOMs with FC type IOMs or replace FC Mezzanine Card with Ethernet or CNA Mezzanine Card.
- Invalid IOM-IOM configuration - In this configuration, a newly installed IOM has a different or incompatible fabric type from an IOM already installed in its group. CMC holds the newly installed IOM in powered-off state, causes the IOM's error LED to blink, and entries in CMC and hardware logs about the mismatch. For example, if a user has an Ethernet or FCoE supported IOM in Fabric B1 and then inserts a FC support IOM in Fabric B2, a fabric mismatch between B1 and B2 occurs and the chassis does not allow B2 IOM to boot up. To fix the issue, insert the same type of IOMs in B1 and B2. To verify the IOMs and MC types present in the modular servers, log in to CMC using RACADM (Telnet/SSH/Serial) and run the **racadm getdcinfo** and **racadm getmodinfo** commands.

No Power for M1000e Enclosure

1. Make sure that all Power Supply Units (PSUs) in the chassis are connected to AC or DC cord and status for each PSU is online or standby. Check and replace the AC or DC cord if needed. Check and confirm that the power distribution unit providing power to the power supply is operating correctly. If the failure persists, contact Dell Technical Support to replace the PSU.
2. If the problem persists, check the system input power cap setting. If it is configured too low, any additional servers do not power on.
3. If the problem persists, check that the PSU is connected to the same voltage as the other PSUs. If CMC detects a PSU operating at a different voltage, the PSU is turned off and the status is **Failed**.
4. Open a serial/Telnet/SSH text console to CMC, log in, and run the **racadm getsysinfo** command. Make sure that Power Status is ON. Else, run the following command to power up the chassis:

   ```
   racadm chassisaction –m chassis <action>
   ```

   where <*action*> is powerup, powerdown, powercycle, nongraceshutdown or reset.

NOTE: When power supply redundancy is enabled, a PSU in the chassis is utilized as a spare, ensuring that the failure of any one PSU does not cause the servers or chassis to turn off. **Power Supply Redundancy** mode requires up to four PSUs. Additional PSUs, if present, are utilized to improve power efficiency of the system if Dynamic power supply engagement (DPSE) is enabled. Subsequent failures after loss of redundancy may cause the servers in the chassis to turn off.

CMC Disconnects From iDRAC

1. Perform one of the following:

   – If you are able to access or ping the CMC IP address, log in to CMC though the Web interface or RACADM (Telnet/SSH, Remote, or Serial RACADM) interface.

   – If you log in to CMC through the Web interface, go to **Chassis Overview → Troubleshooting → Reset components** and click **Reset/failover CMC**.

   – If you login to CMC through RACADM (Telnet/SSH/Serial), run the **racadm cmcchangeover** command. This command is applicable only if the M1000e chassis has two CMCs, one active and the other standby. If there is only one CMC in the M1000e chassis, run the **racadm racreset** command.

   – If you log in using remote RACADM and if the chassis has two CMCs (one active and the other standby), run the following command:

   ```
   racadm -r<CMC IP address>-u<username>-p<password>cmcchangeover
   ```

   It takes around five minutes for the CMC to reboot. Log in to CMC through the Web interface or RACADM (Telnet/SSH/Serial) using the IP address and view the active errors in the CMC logs.

   * CMC Web Interface: Go to **Chassis Overview → Logs** to view the CMC logs.

   * RACADM: Use the **getsel**, **getraclog** or **gettracelog** commands.

2. If the problem persists or if you are unable to access the CMC IP, make sure that network cables are connected properly and network settings are configured properly. Connect a Serial cable to the CMC. After the login prompt is displayed, check the network settings using the following command:

   ```
   racadm getconfig -g cfglannetworking
   ```

   To change the network settings such as IP address, Subnet address, or Gateway address from DHCP to static IP or from static IP to DHCP, run the following command:

   ```
   racadm help config -g cfglannetworking
   ```

   Follow the examples provided in the output.

3. If the problem persists log in to the CMC Web interface, go to **Server Overview → Setup → iDRAC → iDRAC Network Settings**, and verify the modular server network settings.
   Make sure that:

   – LAN is enabled and IPv4 or IPv6 settings are correct
   – Verify modular server VLAN settings (**Server Overview → Setup → VLAN** .)

   In the left pane, under **Server Overview**, click on the slot where the modular server is present. Make sure the modular server gets the IP under IPv4 or IPv6 network settings.

   Ping the iDRAC IP from any management station. If this is successful, click **Launch Remote Console** option available in the same page. If the modular server has an operating system, an operating system login prompt is displayed. If the modular server is in POST condition, reboot the modular server.

   To configure the modular server network settings using RACADM, run the **racadm help setniccfg** command and follow the examples provided in the output

4. If the problem persists, reset the modular server iDRAC using the Web interface or RACADM interface:

– CMC Web interface: Go to **Chassis Overview** → **Troubleshooting** → **Reset components** . In the **Reset** column, select **iDRAC Reset** option.

NOTE: Do not select the **Virtual Reseat** option as this option physically reboots the server.

– RACADM: Through Telnet/SSH/Serial RACADM, run **racadm help racreset** and then follow the examples to reset iDRAC of the blade. For example, **racadm racreset –m server-1 -f**.

5. If the problem persists or if you are unable to access CMC from Serial connection, then physically remove and reinsert CMC in the chassis.

During this operation, IP address of all servers and iDRAC is temporarily inaccessible. It takes around five minutes for the CMC to reboot. Log in to CMC through the Web interface or RACADM (Telnet/SSH/Serial) using the IP address and view the active errors in the CMC logs.

– CMC Web Interface: Go to **Chassis Overview** → **Logs** to view the CMC logs.

– RACADM: Use the **getsel**, **getraclog** or **gettracelog** commands.

NOTE: Make sure you have the latest CMC firmware, BIOS, iDRAC, CPLD, LC and NIC Firmware for the modular sever. To check the CMC or the modular sever iDRAC version, using RACADM run the **getversion** command, or from the CMC Web Interface, go to **Chassis Overview** → **Update** and **Server Overview** → **Update**, and select the modular sever slot from the left pane. To get the latest CMC firmware see the Dell Support site at **Support** → **Drivers & Downloads** → **Enterprise IT** → **Servers, Storage & Networking** → **Poweredge** → **Poweredge M1000E**.

Other Documents You May Need

In addition to this guide, you can access the following guides available at **dell.com/support/manuals**. Select **Choose from a list of all Dell products** and click **Continue**. Click **Software** → **Monitors** → **Electronics & Peripherals** → **Software** :

- Click **Remote Enterprise System Management** and then click **Dell Chassis Management Controller Version 4.3** to view:

  – The *CMC Online Help* provides information about using the Web interface.

  – The *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* provides minimum BIOS and firmware version, installation and usage information.

  – The *RACADM Command Line Reference Guide for iDRAC7 and CMC* about the RACADM sub-commands, supported interfaces, and property database groups and object definitions.

  – The *Chassis Management Controller Version 4.3 Release Notes* provides last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians.