Dell Chassis Management Controller

Version 4.4

Release Notes

Release Notes

Dell Chassis Management Controller

The Dell Chassis Management Controller (CMC) is a hot-pluggable systems management hardware and software solution designed to provide the following functions for Dell PowerEdge M1000e chassis system:

- Remote management capabilities
- Power control
- Cooling control

Version

Dell Chassis Management Controller Version 4.4

Release Date

June 2013

Previous Version

Dell Chassis Management Controller Version 4.3

Importance

RECOMMENDED: Dell recommends applying this update during your next scheduled update cycle. The update contains feature enhancements or changes that will help keep your system software current and compatible with other system modules (firmware, BIOS, drivers, and software).

Platform(s) Affected

CMC version 4.4 supports the following Dell PowerEdge(TM) systems in the Dell PowerEdge M1000e system enclosure:

- Dell PowerEdge M420
- Dell PowerEdge M520
- Dell PowerEdge M600
- Dell PowerEdge M605
- Dell PowerEdge M610
- Dell PowerEdge M610X
- Dell PowerEdge M620
- Dell PowerEdge M710
- Dell PowerEdge M710HD
- Dell PowerEdge M805
- Dell PowerEdge M820
- Dell PowerEdge M905
- Dell PowerEdge M910
- Dell PowerEdge M915

What is Supported?

Supported Web Browsers and Operating Systems

CMC version 4.4 is supported on the following Web browsers:

- Microsoft Internet Explorer 8: Windows XP 32-bit SP3, Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2003 x32 and x64 SP2, Windows Server 2008 x32 and x64, Windows Server 2008 R2 x64.
- Microsoft Internet Explorer 8 (x64): Windows Vista X64 SP2, Windows 7 x64, Windows Server 2003 x64 SP2, Windows Server 2008 x64, Windows Server 2008 R2 x64.
- Microsoft Internet Explorer 9: Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2008 R2 x64.
- Microsoft Internet Explorer 9 (x64): Windows Vista x64 SP2, Windows 7 x64, Windows Server 2008 R2 x64.
- Microsoft Internet Explorer 10: Windows 8 x32 and x64, Windows Server 2012 x32 and x64.
- Safari 5.2
- Mozilla Firefox 6.0: Windows XP 32-bit SP3, Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2003 x32 and x64 SP2, Windows Server 2008 x32 and x64, Windows Server 2008 R2 x64.
- Mozilla Firefox 7.0: Windows XP 32-bit SP3, Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2003 x32 and x64 SP2, Windows Server 2008 x32 and x64, Windows Server 2008 R2 x64.
- Mozilla Firefox 15.0: Windows XP 32-bit SP3, Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2003 x32 and x64 SP2, Windows Server 2008 x32 and x64, Windows Server 2008 R2 x64.
- Mozilla Firefox 16.0: Windows XP 32-bit SP3, Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2003 x32 and x64 SP2, Windows Server 2008 x32 and x64, Windows Server 2008 R2 x64.

What's New

- Includes features released in CMC 4.31.
- Mezzanine and bNDC support:
  - Broadcom 57840S-k Quad Port 10Gbe Blade KR NDC.
  - Mellanox ConnectX -3 Dual Port 10 GbE Mezzanine card.
- DC PSU as a standard offering:
  - Firmware downgrade blocking if DC power supplies are present.
- View Chassis Server and component inventory for Chassis Group.
- Quick Deploy of Profiles to inserted servers.
- Server profile cloning (BIOS, iDRAC, NIC, LC, RAID, FC, and System).
- FCoE session information for Dell PowerEdge M1000e I/O Aggregator.
- Uplink and Downlink status for Dell PowerEdge M1000e I/O Aggregator.
- Support for PMUX mode in Dell PowerEdge M1000e I/O Aggregator.
- Management VLAN configuration for Dell PowerEdge M1000e I/O Aggregator.
- Stacking information for Dell PowerEdge M1000e I/O Aggregator.
- Use FQDN/hostname during certificate generation.
- Default credential check and display warning to user in GUI, CLI and SNMP alert.
- Mitigate password guessing with additional option to block user from any IP address.
- Launching iDRAC using DNS name.

- Additional WSMAN support for OpenManage Power Center.
- RACADM support to query active errors.
- Default key size for Certificate Signing Requests changed from 1024 to 2048.
- Security fix.

Fixes

- Resolved memory leak with Getty process.
- Resolved issue with **Email Alert Settings** page in the web interface not loading correctly when an incorrect email address is specified.

Important Notes

- While using Remote RACADM client with CMC 4.4 version, make sure that Remote RACADM client version 7.3.0 is installed.
- To retrieve default power capping values with CMC 4.4 version make sure that the following properties are used:
  - cfgChassisDefaultPowerCapUpperBound
  - cfgChassisDefaultPowerCapUpperBoundBTU
  - cfgChassisDefaultPowerCapLowerBound
  - cfgChassisDefaultPowerCapLowerBoundBTU

  Note: This information is currently not available in the iDRAC7 1.40.40 CMC 4.4 RACADM Command Line Reference Guide.
- While using the command "racadm config -f" with:
  - CMC 3.21 version of firmware, make sure that Remote RACADM client version 6.3.0 or later is installed.
  - CMC with firmware version earlier than 3.21, make sure that the Remote RACADM client version earlier than 6.3.0 is installed.

Known Issues

Issue 1:

Description

Versions 6.0 and 7.0 of Mozilla Firefox Web Browser do not support IPv6 addresses.

Resolution

You must use URLs that contain a registered hostname when accessing a CMC or iDRAC Server that has an IPv6 address. If the CMC or iDRAC Server also has an IPv4 address, then that is supported.

Versions/Systems Affected

CMC version 2.1 or greater.

Limitations

Issue 1:

Description

The remote racadm testfeature command (racadm -r <IP Address> testfeature..) does not support the -d (debug) option.

Resolution

None

Versions/Systems Affected

All CMC versions including CMC 4.4.

Issue 2:

Description

For Single Sign-On and Smart Card login, the client system must be a part of the Active Directory domain and Kerberos Realm.

Resolution

On Windows 7 clients, under the Local Security Polices, make sure to configure the security option "Network security: Configure encryption types allowed for Kerberos." This policy setting allows you to set the encryption types that Kerberos is allowed to use.

The DES_CBC_MD5 encryption type must be selected. If this encryption type is not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications.

Versions/Systems Affected

All CMC versions including CMC 4.4.

Issue 3:

Description

When you add a member chassis to a chassis group using the Multi-Chassis Management feature, you cannot specify the group members with an IPv6 address.

Resolution

None

Versions/Systems Affected

All CMC versions including CMC 4.4.

Installation

Prerequisites

For information on pre-requisites, see the *Dell Chassis Management Controller Firmware Version 4.4 User's Guide*.

For information on Hardware and Software requirements, see the *Dell Chassis Management Controller Firmware Version 4.4 User's Guide*.

For information on Installation and Configuration, see the *Dell Chassis Management Controller Firmware Version 4.4 User's Guide*.

Installation Instructions

For information on installation, see the *Dell Chassis Management Controller Firmware Version 4.4 User's Guide*.

Upgrade

See the *Prerequisites* section for the correct version numbers.

For Flash Order on M1000e and modular systems, see support article ID 412673 at:

dell.com/support/troubleshooting/us/en/04/KCS/KcsArticles/ArticleView?c=us&l=en&s=bsd&docid=412673

NOTE: The CMC firmware must be updated prior to updating the server component firmware modules.

If using Lifecycle controller or CMC to perform the updates, iDRAC firmware version must be 3.20 or greater and the firmware should be updated in the following order:

- BIOS
- Lifecycle Controller
- iDRAC6/iDRAC7

If manually updating firmware using Dell Update Packages (DUPs) to perform the updates on the M610, M610x, M710, M710HD, M910 or M915, the firmware should be updated in the following order:

- BIOS
- Lifecycle Controller
- iDRAC6

If manually updating firmware using Dell Update Packages (DUPs) to perform the updates on the M420, M520, M620, M820, the firmware should be updated in the following order:

- Lifecycle Controller
- BIOS
- iDRAC7

NOTE: If updating iDRAC firmware to 3.0 or greater from an iDRAC version less than 2.3, the iDRAC firmware must first be updated to version 2.3 before updating to version 3.0 or greater on M610, M610x, M710, M710HD, M910, or M915.

Upgrading Dell PowerEdge M1000e I/O Aggregator

I/O Aggregator must first be updated to version 8.3.17.4 before updating to version 9.2.0.0 or greater.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area.
To contact Dell for sales, technical support, or customer service issues:

1. Visit **dell.com/ support.**
2. Select your support category.
3. Verify your country or region in the Choose a Country/Region drop-down menu at the top of the page.
4. Select the appropriate service or support link based on your need.

Accessing Documents From Dell Support Site

To access the documents from Dell Support site:

1. Go to **dell.com/support/manuals**.
2. In the **Tell us about your Dell system** section, under **No**, select **Choose from a list of all Dell products** and click **Continue**.
3. In the **Select your product type** section, click **Software, Monitors, Electronics & Peripherals**.
4. In the **Choose your Dell Software, Monitors, Electronics & Peripherals** section, click **Software**.
5. In the **Choose your Dell Software section**, click the required link from the following:
   - Client System Management
   - Enterprise System Management
   - Remote Enterprise System Management
   - Serviceability Tools
6. To view the document, click the required product version.

You can also directly access the documents using the following links:

- For Client System Management documents — **dell.com/OMConnectionsClient**
- For Enterprise System Management documents — **dell.com/openmanagemanuals**
- For Remote Enterprise System Management documents — **dell.com/esmmanuals**
- For Serviceability Tools documents — **dell.com/serviceabilitytools**