

#####

DELL(TM) CHASSIS MANAGEMENT CONTROLLER VERSION 3.1

#####

Version: 3.1

Release Date: 7 December 2010

This document contains updated information about the Dell Chassis Management Controller (CMC).

For more information about the CMC, including installation and configuration information, see the "Dell Chassis Management Controller Firmware Version 3.1 User Guide" and the "Dell OpenManage(TM) Server Administrator User's Guide." These documents are located on the Dell Support website at "support.dell.com."

#####

TABLE OF CONTENTS

#####

This file contains the following sections:

- * Criticality
- * Minimum Requirements
- * Release Highlights
- * Known Issues

#####

CRITICALITY

#####

2 - Recommended

#####

MINIMUM REQUIREMENTS

#####

=====

SUPPORTED SYSTEMS

=====

CMC version 3.1 is supported on the following Dell PowerEdge(TM) systems in the Dell PowerEdge M1000-e system enclosure:

- * Dell PowerEdge M600
- * Dell PowerEdge M605
- * Dell PowerEdge M610
- * Dell PowerEdge M610X
- * Dell PowerEdge M710

- * Dell PowerEdge M710HD
- * Dell PowerEdge M805
- * Dell PowerEdge M905
- * Dell PowerEdge M910

SUPPORTED WEB BROWSERS

CMC version 3.1 is supported on the following web browsers:

- * Microsoft Internet Explorer 8.0 for Windows 7, Windows XP, Windows Vista, Windows Server 2008 family, and Windows Server 2003 family.
- * Microsoft Internet Explorer 8.0 (64-bit) for Windows 7 (64-bit) and Windows Server 2008 (64-bit) family.
- * Microsoft Internet Explorer 7.0 for Windows XP, Windows Vista, Windows Server 2008 family, and Windows Server 2003 family.
- * Mozilla Firefox 3.0-3.6 (32-bit), 3.5-3.6 (64-bit)

FIRMWARE VERSIONS

CMC Firmware Version: 3.1

RECOMMENDED MODULE FIRMWARE VERSIONS

The following chassis module firmware versions are recommended additionally if CMC version 3.1 is installed:

- * iDRAC Firmware Version:
 - 3.02 for Dell PowerEdge M610, M610X, M710, M710HD, M910
 - 1.53 for Dell PowerEdge M600, M605, M805, M905
- * BIOS Version:
 - 2.1.8 for Dell PowerEdge M610, M610X, M710
 - 0.1.11 for Dell PowerEdge M710HD
 - 1.1.5 for Dell PowerEdge M910

 - 2.3.1 for Dell PowerEdge M600
 - 5.4.1 for Dell PowerEdge M605
 - 2.3.3 for Dell PowerEdge M805, M905
- * CPLD Version:
 - 1.0.3 for Dell PowerEdge M610, M610X, M710
 - 1.0.0 for Dell PowerEdge M610X (Extended CPLD)
 - 1.0.0 for Dell PowerEdge M710HD
 - 1.0.1 for Dell PowerEdge M910
 - 1.1.1 for Dell PowerEdge M600

- 1.1.0 for Dell PowerEdge M605, M805, M905

RELEASE HIGHLIGHTS
#####

- * Multi-chassis management that allows up to 8 other chassis to be visible from the lead chassis.
- * Power log feature that periodically samples and displays chassis system input power (total AC consumption).
- * Server Performance over Power Redundancy, which when enabled, favors server performance and server powerup, over maintaining power redundancy. When disabled, the system favors power redundancy over server performance.
- * Provides option to use the chassis in Maximum Power Conservation Mode to extend power life while running on UPS or other backup power sources.
- * Save and restore configuration on a host.
- * Improvement of SEL log.
- * GPL/Open Source compliant.
- * Dell 8/4 Gpbs Fibre Channel Pass Thru IOM.
- * Dell M8428-k IOM.
- * Brocade BR1741M-k Dual Port Mezzanine Card.

KNOWN ISSUES FOR BROWSERS
#####

No known issues for this release.

KNOWN ISSUES FOR CMC Version 3.1
#####

- * While using the command "racadm config -f" with :
 - CMC 3.1 or later versions of firmware, ensure that the Remote RACADM client version 6.3.0 or later is installed.
 - CMC with an earlier version of 3.1 firmware, ensure that the Remote RACADM client version earlier than 6.3.0 is installed.
- * The racadm testfeature command for use with Active Directory

(Simple or Kerberos authentication), does not display diagnostic information except for simple syntax errors. Testing configuration parameters for LDAP, using the racadm testfeature command, remain fully functional (393409).

* For Single Sign-On and Smart Card login, the client system must be a part of the Active Directory domain and Kerberos Realm. On Windows 7, clients under the Local Security Policies, must ensure 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.

* 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.

KNOWN ISSUES FOR USER INTERFACE ONLINE HELP
#####

No known issues for this release.

KNOWN ISSUES FOR DOCUMENTATION
#####

No known issues for this release.

#####

Information in this document is subject to change without notice.
(C) 2010 Dell Inc. All rights reserved.

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

Trademarks used in this text: "Dell(TM)", "OpenManage(TM)", and "PowerEdge(TM)" are trademarks of Dell Inc. "Microsoft(R)", "Windows(R)", "Windows(R) 7", "Windows Vista(R)", "Windows Server(R)", "Windows(R) XP", "Internet Explorer(R)", and "Active Directory(R)" are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. "Mozilla(R)" and "Firefox(R)" are registered trademarks of the Mozilla Foundation "Red Hat(R)" and "Red Hat Enterprise Linux(R)" are registered trademarks of Red Hat,Inc. in the United States and 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.

December 2010