##

DELL(TM) CHASSIS MANAGEMENT CONTROLLER (CMC)

##

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

For more information about CMC, including installation and
configuration information, see the "Dell Chassis Management Controller
Firmware Version 1.0 User's Guide" and the "Dell OpenManage(TM) Server
Administrator User's Guide." These documents are located on the Dell
Support website at "support.dell.com" and with your Product
Documentation CD.

##
TABLE OF CONTENTS
##

This file contains the following sections:

* Criticality

* Minimum Requirements

* Release Highlights

* Known Issues for CMC

* Known Issues for Documentation

##
CRITICALITY
##

2 - Recommended

##
MINIMUM REQUIREMENTS
##

The following subsections list operating systems that are compatible
with the CMC.

==
SUPPORTED SYSTEMS
==

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

* Dell PowerEdge M600 and M605.

===
SUPPORTED WEB BROWSERS
===

* Microsoft(R) Internet Explorer 6.0 (32-bit) with SP1 for Windows 2000
  Server family.

* Microsoft Internet Explorer 6.0 (32-bit) with SP2 for Windows XP and
  Windows Server(R) 2003 family.

* Microsoft Internet Explorer 7.0 for Windows Vista(R), Windows XP, and
  Windows Server 2003 family.

* Mozilla Firefox 1.5 (32-bit).

* Mozilla Firefox 2.0 (32-bit).

==
FIRMWARE VERSIONS
==

* CMC Firmware Version: 1.10

This is a maintenance release for CMC Firmware Version 1.0.

###
RELEASE HIGHLIGHTS
###

Fixes and Enhancements in 1.10
----
* Support for optional upgrade FlexAddress feature.
  The FlexAddress feature is an optional upgrade that allows the
  chassis to assign WWN/MAC (World Wide Name/Media Access Control)
  addresses to Fibre Channel and Ethernet devices. Chassis-assigned
  WWN/MAC addresses are globally unique, and specific to a server slot
  within a given chassis. This feature allows the chassis to assign a
  WWN/MAC address (Chassis Assigned IDs) that stays with a particular
  slot in the chassis. If a server is replaced, the FlexAddress for
  the slot remains the same for that given server slot. If the server
  is inserted into a new slot or chassis, the server-assigned WWN/MAC
  is used unless the FlexAddress feature is enabled for the new slot.
  If you remove the server, it will revert to the server-assigned
  address.

* CMC will block any user attempt to upload a non-Web server
  certificate. A user error will be returned.

* If a user has uploaded a non-Web server certificate using CMC
  firmware version 1.01, after a firmware install and reboot of 1.10,
  the non-Web server certificate will be removed.

```
############################################################################
FLEXADDRESS
############################################################################
```
* FlexAddress: Before installing the SD card into the CMC module,
  verify the write-protection latch is in the "unlock" position. The
  FlexAddress feature cannot be activated if the SD card is write
  protected.

* FlexAddress: The system BIOS must be upgraded prior FlexAddress
  installation. A warning icon will be displayed on the server health
  page if FlexAddress installation if performed prior to upgrading the
  system BIOS. Once the system BIOS is updated, the server module
  must be power cycled before the chassis-assigned MAC addresses will
  be accepted by the server module. The CMC will display that
  chassis-assigned MACs are configured, but the server will be using
  the server-assigned MAC configuration.

* FlexAddress: If you issue a CMCCHANGEOVER or RACRESET and then log
  into the CMC Web GUI, the FlexAddress Webpage could take a minute to update
  the changed configurations.

* FlexAddress: If a chassis with a single CMC is downgraded with
  firmware prior to 1.10, the FlexAddress feature and configuration
  will be removed. Once the CMC firmware is upgraded to 1.10 or
  later, the FlexAddress feature will need to be reactivated and
  configured by the user.

* After a CMC reset, the CMC may require up to 30 seconds after the
  serial login prompt is displayed before RACADM commands will be
  accepted. Commands issued prior to that time may receive the
  message "ERROR: Unable to perform requested operation."

* FlexAddress: Using Wake-On-LAN (WOL) with FlexAddress.
  When the FlexAddress feature is deployed for the first
  time, it requires a power-down and power-up sequence for
  FlexAddress to take effect. FlexAddress on Ethernet devices is
  programmed by the server module's BIOS. In order for the
  server module's BIOS to program the address, it need to be operational
  which requires the server module to be powered up. Once the power-down
  and power-up sequence completes, the FlexAddress feature is
  available for Wake-On-LAN (WOL) function. Users may perform
  the power-down and power-up sequence on the server module to
  fully deploy FlexAddress using either the iDRAC or CMC interface.

* When changing from a server-assigned MAC address to chassis-assigned
  MAC address on Linux Based operating systems, additional configuration steps
  may be required.
  o SLES 9 and SLES 10: Users may need to run YAST (Yet another Setup
    Tool) on their Linux system to configure their Network devices
    and then restart the network services.
  o RHEL 4 and RHEL 5:   Users will need to run Kudzu, a utility to
    detect and configure new/changed hardware on the system. Kudzu
    will present the user with The Hardware Discovery Menu, it will
    detect the MAC address change as Hardware was removed and new

Hardware added.

* If a server module installed in a FlexAddress enabled slot contains a
  Qlogic or Emulex mezzanine card that has a BIOS firmware revision that
  is not the minimum version required, the server module BIOS will detect
  the incompatibility and alert the user of the problem by changing the server
  module health in the CMC to a red X. The FlexAddress Webpage for the
  server module may incorrectly show green check marks next to the
  chassis-assigned addresses for that module. The server module will use
  server-assigned MAC addresses despite the indications on the FlexAddress
  Webpage.

###
KNOWN ISSUES FOR BROWSERS
###
* In Internet Explorer Version 6, log data may not display and instead
  only a message of, "Loading Chassis Event Log..." is shown .
  Select Advanced Settings/Security and make sure the
  option, "Allow active content to run in files on My Computer" is
  NOT checked to fix this issue.

* In Internet Explorer Version 6, if the security setting is set to
  restricted, the CMC User Interface on the Alert Management pages for
  Email Alerts and SNMP Traps will display a Security Information
  message that states that the page contains both secure and non-secure
  items and will ask if you want to continue. Select "Yes". This message
  is displayed because Internet Explorer Version 6 does not allow the use
  of hidden IFRAMES on secure (SSL) pages. (183022)

###
KNOWN ISSUES FOR CMC
###

* The Chassis Asset Tag information is incorrectly displayed in the
  Service Tag field on the Chassis LCD (218411)

* RACADM CLI based command-line tool uses TFTP to transfer image files
  for all firmware updates. Only the default port for TFTP (69) is
  supported for transfers with version 1.0. (157754)

* Clearing the CMC Log can take a long time. Allow up to
  one (1) minute for this operation to complete.(152860)

* If the CMC is on a private network without access to the Internet
  and you are using Internet Explorer 6 SP 2 or Internet Explorer 7,
  you may experience delays of up to 30 seconds when using remote
  RACADM commands. (161019)

* In the CMC User Interface, under Chassis -> Network/Security tab->
  Network subtab, if the network speed is set to 1GB to match your
  network environment then the CMC will revert to Auto Negotiation
  internally to determine the network speed and Duplex Mode. It will
  not use the values set.(180871)

* Using the RACADM command line utility to set the network speed to
  1GB, will cause the CMC to revert to Auto Negotiation internally to
  determine the network speed and Duplex Mode. (180873)
  For Example, the following command will be ignored and Auto Negotiation
  will be attempted:
      racadm setniccfg -k 1000 full

* Some USB-to-serial adapters can generate a large number of
  spurious interrupts when plugged in. If the adapter is connected to
  the CMC's serial port when this happens, the CMC can become
  overloaded when attempting to service these interrupts and may reboot. This
  problem is exacerbated when the serial cable is very long, causing voltage
  levels to drop and noise on the serial line to increase. To avoid this issue,
  Dell recommends first connecting the USB-to-serial adapter into the USB
  port, before connecting to the CMC. Dell also recommends disconnecting
  the adapter from the CMC before rebooting or performing other power
  management functions on a system that is attached to the CMC.
  (180373)

* The "connect" to server command enables the user to access the
  server's serial port through CMC's serial port. After this connection the user
  will be able to see the server's console redirection through CMC's
  serial port. The following are the prerequisites for this feature:

      1. The server should be powered on.
      2. Serial redirection must be enabled in the servers BIOS Setup.
      3. Not all keys will work, so the user has to provide appropriate
              escape sequences for "CTRL+ALT+DEL" etc. The initial
              redirection screen displays the necessary escape sequences.
   (184385)

* If you setup Active Directory (AD) on the CMC using extended schema
  and the built-in Administrator privilege object and then attempt to login to
  the CMC User Interface using this AD account, after successful AD login, the
  user name and privilege level displayed on the right hand side of the User
  Interface below the "Log out" link is as a custom user rather than as the
  privilege as created on the AD side (example: Administrator, power
  user). (183449)

* If you attempt to set the server slot name to a name greater than 15 characters
  (unsupported and documented in the CMC User's Guide) using the RACADM
  command line utility, then you will get the following generic error message:
  "ERROR: The specified object value is not valid". (181364)

* If you attempt to set the DNS CMC Name or DNS Domain Name
  without the proper rules (Rules: start with an alphabetic character
  (a-z, A-Z) and follow by an alphanumeric (a-z, A-Z, 0-9) or a valid symbol
  (such as -)) using the RACADM command line utility, then the utility will
  display the following non-specific error message:
  "ERROR: Unable to perform requested operation". Enter valid values for
  the DNS names. (173204)

* If a firmware update operation is attempted using the CMC User
  Interface that uses an invalid image file that is very small (few bytes),

there will be no error message indicating the failure of this operation.
Upload the valid image and restart the firmware update operation. (186170)

* If the standby CMC firmware was previously updated and then later
  made active, you will see an entry in the CMC log (raclog) that
  states the firmware update was successful, but with the most recent time
  stamp. This is because the standby CMC cannot register its entries to the
  logs until it becomes active. (186858)

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

This section provides additional information about known issues with
the CMC Firmware version 1.0 User Interfaces online help.

* The help for the Services Management page located in the Chassis->
  Network/Security tab->Services sub-tab of the CMC user interface in
  localized languages do not list the Telnet Port legal values.
  (179080)

* The help for the Slot Names page located in the Chassis-> Servers ->
  Setup->Slot Names sub-tab of the CMC user interface in localized
  languages do not list the rules for the slot names, which are:
  (a) The beginning of the string cannot be Switch-, Fan-, PS-, KVM,
      DRAC/MC-, Chassis and Housing-Left/Right/Center, which are case
      insensitive.
  (b) ASCII characters between 32 and 126 are allowed, but excludes 34 (").
  (c) Server-n, where n is 1 to 10, is not allowed except that Server-n is
      allowed for the n slot, which is case insensitive. Server-0n
      is different from Server-n, like Server-02 is different from
      Server-2. Therefore Server-2 is not allowed for any slot except the second
      one but Server-02 can be set in any slot. (178014)
  (d) Maximum allowed characters for the Slot Name is 15. (181364)

* The help for the Server Status page located in the Chassis-> Servers
  ->Server 1-16 -> Properties tab->Status sub-tab of the CMC user
  interface in localized languages does not list the Slot Name, Present
  properties. It also has a reference to I/O module instead of servers under Health
  -> Informational section. (179718)

* The help for the Chassis Power Management page located in the
  Chassis-> Power Management tab->Control sub-tab of the CMC user interface in
  localized languages refers to Power Off System as equivalent to pressing
  the power button when the power is "ON". This is not accurate since
  this action performs a graceful shutdown of the chassis and if any of the
  modules do not shutdown within the time period, they will remain on. (181069)

* The help for the Identify page located in the Chassis-> Troubleshooting
  tab->Identify sub-tab of the CMC user interface in localized languages
  mentions the note:
  To blink or unblink the servers, you must have Log in to iDRAC
  privilege on the iDRAC of these servers.

This is missing Server Administrator privilege on CMC and should be:

To blink or unblink the servers, you must have Server Administrator
privilege on CMC or Log in to iDRAC privilege on the iDRAC of these servers.
(175595)

* The help for the User Configuration page located in the Chassis->
  Network/Security tab-> Users sub-tab-> click User ID number of the
  CMC user interface in localized languages does not have the Super
  User listed under the CMC User Privileges section. The super user
  privilege is currently reserved for future use. (180734)

* The help for the Power Budget Status page located in the Chassis->
  Power Management tab-> Budget Status sub-tab of the CMC user
  interface in localized languages describes the Standby DC Power Capacity as:

  Indicates the amount of power (in watts) available to be provided by
  Power Supplies that are in standby mode. This power can be allocated to any
  hardware modules that are either added to the chassis or brought online.

  This needs to be:

  Indicates the amount of standby power (in watts) that is available in
  the event of a Power Supply fault or Power Supply removal from system. This
  field may show readings when the system has four or more power supplies and you have
  enabled Dynamic Power Supply Engagement.

  NOTE: It is possible to see a PSU in standby mode but not contribute
  to the Standby DC Power Capacity value. In this case the watts from this PSU are
  contributing to Total DC Power Available for Allocation value. (182571)

* The help for the Server Power Throttling Enabled on the Power
  Management Budget/Redundancy configuration page located in the Chassis-> Power
  Management tab->Configuration sub-tab of the CMC user interface in
  all languages needs to explain that the power will be siphoned from lower
  priority servers in the order of increasing slot numbers.

  Currently the help reads:
  Enables (when checked) the CMC to siphon power from lower priority servers
  when power is needed for the entire chassis. In this case, the servers are
  allowed to continue operating at a degraded performance level rather than
  shut down.

  This needs to be:
  Enables (when checked) the CMC to siphon power from lower priority servers
  in the order of increasing slot number (slot 1 to 16) when power is needed
  for the entire chassis. In this case, the servers are allowed to continue
  operating at a degraded performance level rather than shut down.
  (186703)

* The help for Power Management Budget/Redundancy configuration page
  located in the Chassis-> Power Management tab->Configuration sub-tab
  of the CMC user interface in all languages refers to "System Max AC Power
  Limit (2768 - 7928)" field displayed on the User Interface as "Enclosure

Max Power Limit" and "System AC Power Warning Threshold (2500 - 7130)"
field on the User Interface as "Power Warning Threshold".

In addition the "System Max AC Power Limit (2768 - 7928)" needs to have the
following detailed explanation:

System Max AC Power Limit is the max AC power that the system is allowed to
draw from incoming AC power supply source. It can be configured by the user
if and only if the value exceeds the AC Power equivalent (i.e. 15% higher
than the DC allocated power value) of the currently allocated DC Power to
Servers and Chassis Infrastructure. If an attempt is made by the user to
configure the value such that it falls below the AC power equivalent of the
currently allocated DC Power to Servers and Chassis Infrastructure the attempt
would not be successful. In other words, users are NOT allowed to configure
an AC power limit that is less than what is currently allocated to the servers
and infrastructure as that would result in blades being automatically powered
down. The DC power allocated to Servers and Chassis Infrastructure can be found
in the User Interface on the Chassis -> Power Management-> Power Budget status
page under Power Budgeting section or via CLI RACADM utility command (racadm
getpbinfo). User can, however, power OFF one or more server(s) to lower the
current DC Power allocation and re-attempt setting a lower value for System
Max AC Power Limit (if desired) or simply configure the limit prior to
powering on the server blades.

NOTE: Please refer to the Datacenter Capacity Planner (DCCP) tool at
www.dell.com/calc for capacity planning.(186670)

* The help for the Power Budget Status page located in the Chassis->
  Power Management tab-> Budget Status sub-tab of the CMC user interface
  describes the Priority default value as 5. This needs to be 1.
  (191163)

##
KNOWN ISSUES FOR DOCUMENTATION
##

None.

##

Information in this document is subject to change without notice.
(C) 2008 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", "Dell OpenManage", and
"PowerEdge" are trademarks of Dell Inc.; "Microsoft", "Windows",
"Windows Vista", "Windows Server", and "Active Directory" are
trademarks or registered trademarks of Microsoft Corporation.

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.

June 2008