```
################################################################################

INTEGRATED DELL(TM) REMOTE ACCESS CONTROLLER (iDRAC) Version 1.50

################################################################################
```

This document contains updated information about the Integrated Dell
Remote Access Controller (iDRAC).

For more information about iDRAC, including installation and
configuration information, see the "Integrated Dell Remote Access
Controller Version 1.5 User Guide" and the "Dell OpenManage(TM) Server
Administrator User's Guide." These documents are located on the Dell
Support site at "support.dell.com/manuals".

```
################################################################################
TABLE OF CONTENTS
################################################################################
```

This file contains the following sections:

* Criticality

* Minimum Requirements

* Release Highlights

* Known Issues

```
################################################################################
CRITICALITY
################################################################################
```

2 - Recommended

```
################################################################################
MINIMUM REQUIREMENTS
################################################################################
```

The following subsections list operating systems that are compatible
with iDRAC.

```
================================================================================
SUPPORTED SYSTEMS
================================================================================
```

iDRAC is supported on the following Dell PowerEdge(TM) systems in the
Dell PowerEdge M1000e system enclosure:

* Dell PowerEdge M600
* Dell PowerEdge M605
* Dell PowerEdge M805
* Dell PowerEdge M905

===
SUPPORTED MANAGED SERVER OPERATING SYSTEMS
===
iDRAC is supported by the following operating systems:

* Microsoft(R) Windows Server(R) 2003 family

  The Windows Server 2003 family includes
  - Windows Server 2003 R2 (Web, Standard and Enterprise Editions)
    with SP2 (x86).
  - Windows Server 2003 R2 (Standard, Enterprise and DataCenter
    Editions) with SP2 (x64).
  - Windows Server 2003 (SBS, Standard, and Premium Editions)
    with SP2.

* Microsoft Windows Server 2008 with core (Web, Standard, and
  Enterprise Editions) (x86)

* Microsoft Windows Server 2008 with core (Standard, Enterprise,
  and DataCenter Editions) (x64)

* Microsoft Windows Server 2008 SBS, EBS, Standard, and Premium
  Editions

* SUSE(R) Linux Enterprise Server (SLES) 10 SP2

* SUSE Linux Enterprise Server (SLES) 11 SP2

* Red Hat(R) Enterprise Linux (RHEL) 4.7 (x86_32, x86_64)

* RHEL 5 Update 3 (x86_32, x86_64)

* VMware(R) ESX 3.5 Update 4

* VMware ESX 4.0

* XenServer 5.5

===
SUPPORTED WEB BROWSERS
===
* Microsoft Internet Explorer(R) 6.0 with SP2 for Microsoft Windows(R)
  XP, Windows 2000 Sever, Windows 2000 Pro, Windows 2003 Server Gold,
  Windows 2003 Server SP1, and Windows 2003 Server SP2

* Microsoft Internet Explorer 7.0 for Windows 2003 Server Gold,
  Windows 2003 Server SP1, Windows 2003 Server SP2, Windows Server
  2008, and Windows Vista(R)

* Microsoft Internet Explorer 8.0 for Windows 2003 Server Gold,
  Windows 2003 Server SP1, Windows 2003 Server SP2, Windows Server
  2008, and Windows Vista. IE8 requires JRE version 1.6.14 or later

* Mozilla Firefox 2.0 on SLES 10 SP1

* Mozilla Firefox 3.0 on Windows 2003 Server Gold, Windows 2003
  Server SP1, Windows 2003 Server SP2, Windows 2000 Pro, Windows XP,
  Windows Server 2008, Windows Vista, RHEL 4, RHEL 5, SLES 10,
  SLES 11, and SLES 10 SP1

##
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.50)
##

* FlexAddress MAC for iDRAC
* VLAN Tagging
* Power Management Improvements
* Regular Maintenance

##
KNOWN ISSUES FOR (FIRMWARE VERSION 1.50)
##

This section provides additional information about known issues with
iDRAC Firmware version 1.50:

* iDRAC Linux DUPs currently do NOT support VMware ESX 4.0.

If the Linux DUP for iDRAC is executed in VMware ESX 4.0, the DUP
will fail.
Alternatively, iDRAC can be updated using the following methods:
(1) CMC GUI-based update
(2) iDRAC GUI-based update
(3) SM-CLP-based update

* iDRAC Windows DUPs currently do NOT support Win 2K8 R2.

If the Windows DUP for iDRAC is executed in Win 2K8 R2, the DUP
will fail.
Alternatively, iDRAC can be updated using the following methods:
(1) CMC GUI-based update
(2) iDRAC GUI-based update
(3) SM-CLP-based update.

* After a firmware downgrade, iDRAC configuration needs to be reset
to the default values using RACADM or using iDRAC Configuration
Utility in BIOS. However, this is not required when upgrading
iDRAC firmware.

* Flashing from pre-1.2 iDRAC on VMware ESX

When attempting to flash earlier than iDRAC 1.2 releases, the Dell
Update Packages Utility does not have the logic to find the USB
devices correctly in the VMware ESX. Therefore, it is required that
other flashing methods be used instead of VMware ESX.

* Using virtual devices on VMware ESX Console, after an iDRAC Update

Reboot the managed server running VMware ESX 3.x once
after an iDRAC update is completed. This will ensure that VMware ESX
re-enumerates the virtual devices and enables virtual floppy and
virtual CDROM features of iDRAC. After that reboot, virtual devices
including Virtual Floppy work fine.

* Disabling Local Configuration Access

In order for the disabling of local configuration access to work at
iDRAC Configuration Utility level (<Ctrl-E> at bootup), the BIOS in
your system needs to be at least at the following level:

PowerEdge M600 - BIOS version 2.1.2
PowerEdge M605 - BIOS version 4.0.0
PowerEdge M805/M905 - BIOS version 0.2.3

* Possible Active Sessions versus Current Active Sessions in
  Dell OpenManage Server Administrator (OMSA)

In Dell Open Manage Server Administrator, the number of
"Current Active Sessions" displayed for iDRAC refers only to the
number of current IPMI transaction sessions active, and does not
include Web GUI or SSH/SM-CLP sessions.

* Configuring iDRAC to use Static IP using 'syscfg' utility

Given below is the method to use the syscfg utility to set iDRAC
to use a static IP address. It has to be done in 2 steps.

  Step 1: "syscfg lcp --ipaddrsrc=static"

  Wait for at least 5 seconds. After this time, the change to
  static IP will be in effect and the next syscfg command
  will succeed.

  Step 2: "syscfg lcp --gateway=(gateway IP) --ipaddress=
        (valid IP address) --subnetmask=255.255.255.0"

* Configuring the 'Host Name String' using iDRAC Configuration
  Utility

With OMSA installed:

OMSA takes precedence. OMSA sets the 'Host Name String' every time it
starts up. Given above, even if the 'Host Name String' is set using
"iDRAC Configuration Utility", it will be overwritten by OMSA when it
starts up.

With OMSA NOT installed:

iDRAC Configuration Utility can be used to configure the 'Host
Name String'.

* Updating iDRAC using DOS update utility, from a PXE network setup

iDRAC can be updated using the DOS utility when DOS is booted
using PXE. However, the new firmware image has to be on a local media
on the server for this to work properly. Local media can be a RAMDISK,
HD, or USB key on the server. Alternatively, the update of iDRACs on
multiple servers has to be sequenced, that is, done one server after
the other, with the 1st completing the update and the 2nd starting the
update, the 3rd starting the update after the 2nd is completing the
update, and so on.

* Usage of virtual CD-ROM in SLES 9

Use the auto-attach checkbox in the vMedia section of the iDRAC Web
GUI when using CD-ROM devices in SLES 9.
Another way to do the same when using SM-CLP is to set the
/system1/sp1/oemdell_vmservice1 enabledstate to VMEDIA_AUTO_ATTACH.

* RACADM restore default configuration behavior

The "racresetcfg" command in RACADM restores all properties except
"cfgDNSRacName" in the "cfgLanNetworking" group to their default
values.

* Configuring iDRAC using RACADM config

The actual time the user needs to wait after executing the
"racresetcfg" command within RACADM may vary depending on the
network speed.

* Behavior of iDRAC Virtual Media functionality, when the media
is removed

On Windows:

Once the media is removed, the Explorer window(s) for this media do
not close by themselves. User action is required. Close the Explorer
window(s), once the media is removed.

On Linux:

Once the media is removed, the file browser window(s) for this media
close by themselves. User action is NOT required.

* Using the iVMCLI tool from within a system running Windows Vista

To use iVMCLI from within a system running Windows Vista, the user
has to start up the 'cmd' with 'Run as Administrator'. (iVMCLI
requires the user has 'administrator' privileges when it is used.)

NOTE: User can log in as a non-admin user, but when using iVMCLI,
the user has to start 'cmd' with 'Run as Administrator' thereby

giving them admin privileges to enable using iVMCLI.

* If you receive a message "A webpage is not responding on the..."

If you receive a message "A webpage is not responding on the
following website:" in Internet Explorer 8 (IE 8), see the
following links:

http://blogs.msdn.com/ie/archive/2009/05/04/
ie8-in-windows-7-rc-reliability-and-telemetry.aspx
http://support.microsoft.com/?kbid=970858

* Closing the remote console closes the browser without warning

IE 7 provides an advanced option setting to open new windows
as tabs with the option "Always switch to new tabs when they are
created", under "Tools-> Internet Options-> General Tab->
Tabbed Browser Settings". When using IE 7 with several tabs open
and if the iDRAC remote console is launched, all tabs are hidden
while the remote console is still open. If you close the remote
console, and if the tab warning has been turned off, that is
unchecked in Internet Properties-> Tabs-> Settings,
(Warn me when closing multiple tabs.), all the tabs including the
browser will close without any warning.

* racadm getssninfo displays information for first session only

If multiple iDRAC web GUI sessions are launched through CMC
Single Sign-On, racadm getssninfo displays information for the
first session only.

* iVMCLI requires administrator privileges with Vista

If iVMCLI is run on Windows Vista to connect a CD or ISO without
administrator privileges, it appears to be working but will
eventually timeout with a "Unable to connect" message and asks the
user to check the network/proxy settings. This same command will
work if the CMD prompt is opened with administrator privileges.
It informs the user that it will not work because it needs
administrator privileges or USB access to hardware.

* Using "Eject" option from OS to disconnect vMedia drive

If a vMedia drive is disconnected using the operating system
"Eject" option, then the drive may not be available until the
operating system re-enumerates the USB devices. In order for the
operating system to auto-detect the vMedia drive, iDRAC
vMedia device can be reattached by doing the following:

In the Web GUI under System-> Console/Media-> Configuration,
set "Attach Virtual Media" to "Detach" and click "Apply".
Next, set "Attach Virtual Media" to "Attach" and click "Apply"
again.

* Need iDRAC NIC enabled BEFORE running 'racadm getconfig'

The iDRAC NIC will be disabled if the iDRAC configuration is reset
to default settings. Ensure that the NIC is enabled before
running the commands "racadm getconfig –f <filename>" and
"racadm getconfig –g cfgLanNetworking"

* Updating iDRAC using Linux DUP on 64-bit version of RHEL 4 Update 7

The iDRAC Linux DUP can not be run on 64-bit RHEL 4 Update 7
because of known issues in that operating system.
The same DUP will update the iDRAC successfully on 64-bit RHEL
4 Update 8. Alternatively, use the RedHat KB article referenced
below to successfully update using iDRAC Linux DUP on RHEL 4
Update 7.

http://kbase.redhat.com/faq/docs/DOC-3402

##
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.40)
##

* iDRAC version 1.40 has critical security enhancements
* Support for 1:many firmware update through Chassis Management
* Single Sign-On from Chassis Management
* Active Directory performance improvements
* Regular Maintenance

##
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.20)
##

* iDRAC version 1.20 has critical security enhancements
* New operating system and browser support
* Boot Capture Replay
* Improved health status visibility

Fixes and Enhancements in 1.20
----

* Windows Server 2008 (Longhorn), ESX (latest version),
  W2K3-R2 and RHEL 5 operating system support as managed server
  operating systems

* Added support for 64-bit Firefox and IE browsers

* Generate a default Self Signed SSL certificate

* An option to disable access to iDRAC configuration by any user or
  local RACADM

* SSL 2.0 is no longer supported due to security risks

in SSL 2.0. iDRAC negotiates to use SSL 3.0 if both
(SSL 2.0 and SSL 3.0) are present

* Expanded Health Error Reporting Tree

* Java Runtime Engine and Java Development Support updated to Version
 6 Update 7 (JRE 1.6 U7)

* Two concurrent KVM Sessions are now supported
 (from different clients) to the same iDRAC

* iDRAC Console Viewer now supports mouse scrolling

* iDRAC Web Interface lists the MAC/WWN present on the server and
 supports the persistent MAC functionality of FlexAddress

* iDRAC Web Interface lists Storage Daughter card and I/O
 Mezzanine Card population

* Boot Capture console replay for last three boot sequences

* Improved Power Usage Reporting

* Improved support for non-US-ASCII keyboards

##
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.11)
##

iDRAC version 1.11 has key fixes for Active Directory,
Services (SSH, SOL) and in addition supports the FlexAddress feature.

##
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.03)
##

Enhanced TOE key detection.

##
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.02)
##

A few fixes in the version display, SM-CLP, and last crash screen
page areas are included in this release.

##
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.0)
##

* Initial release of iDRAC firmware.

##
KNOWN ISSUES FOR DOCUMENTATION

##

This section provides additional information about known issues with
iDRAC Firmware version 1.5 User Guide.

* None

##

August 2009