EXPLORING THE iDRAC FOR DELL POWEREDGE BLADE SERVERS

By Jon McGary

The Integrated Dell™ Remote Access Controllers (iDRACs) in Dell PowerEdge™ M-Series server blades provide powerful, easy-to-use remote management and configuration options designed to simplify management, increase flexibility, and enhance security in enterprise environments.

Related Categories:

Dell OpenManage

Dell PowerEdge servers

Dell Remote Access Controller (DRAC)

Remote access controllers (RACs)

Remote management

Systems management

Visit DELL.COM/PowerSolutions for the complete category index.

Dell PowerEdge M-Series modular blade enclosures and server blades can offer significant advantages in enterprise environments, including rapid deployment, increased rack density, and efficient energy use. Each PowerEdge M-Series server blade includes an Integrated Dell Remote Access Controller (iDRAC) that offers similar remote management and configuration capabilities as previous-generation DRACs while also introducing enhancements designed for simplified management, increased flexibility, and enhanced security.

UNDERSTANDING iDRAC MANAGEMENT AND SECURITY

Key iDRAC management features include the following:

- **Remote systems management and monitoring:** Allows administrators to remotely manage and monitor PowerEdge M-Series blades, including accessing system information and component status, through a Web browser–based graphical user interface (GUI), a local command-line interface (CLI) through console redirection, or a Server Management Command-Line Protocol (SM CLP) CLI over a Secure Shell (SSH) or Telnet connection
- **Console redirection:** Provides remote system KVM (keyboard, video, mouse) functionality
- **Virtual media:** Enables blades to access local media drives on a management station, or ISO CD or DVD images on a network share
- **Access to system logs:** Includes the system event log, the iDRAC log, and the last crash screen of a crashed or unresponsive system that is independent of the OS state
- **Platform events and alerts:** Provide warnings about potential problems through an e-mail message or Simple Network Management Protocol (SNMP) trap
- **Remote power management:** Provides power management functions, such as shutdown and reset, from a remote management console

Security is typically a top priority for enterprises, particularly in environments running remote management applications that transmit potentially sensitive data over the Internet. Key iDRAC security features include the following:

- **Support for Microsoft® Active Directory® authentication:** Centralizes iDRAC user IDs and passwords through the standard schema or an extended schema
- **Role-based authority:** Enables administrators to configure specific privileges for each user
- **Password-level security management:** Helps prevent unauthorized access to remote systems

- **Secure Web browser–based GUIs and SM CLP CLI:** Support 128-bit Secure Sockets Layer (SSL) encryption as well as 40-bit SSL encryption for countries where 128-bit encryption is not acceptable (Telnet does not support SSL encryption)
- **Session time-out configuration:** Enables administrators to set the session time-out configuration (in seconds) through a Web browser–based GUI or SM CLP CLI
- **Configurable IP ports:** Enable administrators to customize IP ports (where applicable)
- **SSH support:** Uses an encrypted transport layer to help increase security
- **Login failure limits:** Enable administrators to configure login failure limits for each IP address, including login blocking from specific IP addresses when the limit is exceeded
- **Limited IP address range configuration:** Enables administrators to restrict the IP addresses of clients connecting to the iDRAC

The iDRAC uses an integrated system-on-chip processor for remote systems monitoring and management. The iDRAC is integrated on the system board with other server components in PowerEdge M-Series server blades, which are installed in PowerEdge M1000e modular blade enclosures along with modular power supplies, cooling fans, and redundant Chassis Management Controllers (CMCs).[1] Each PowerEdge M1000e enclosure can contain up to 16 PowerEdge M-Series server blades, each equipped with its own iDRAC.

The iDRAC is responsible for managing the server blades, and the CMC is responsible for managing the enclosure. Each iDRAC combines with the CMC to coordinate the necessary power and cooling for the blades.

Similar to previous-generation DRACs, the iDRAC uses a flash file system that allows persistent administrator-defined configurations and up to 16 defined local users as well as support for Active Directory services to manage security. The iDRAC supports an integrated Web server that allows up to four DRAC administrators to be connected at the same time using a supported Web browser; at any given time, two administrators with redirection privileges may use the console redirection feature, and one administrator with virtual media privileges may use the virtual media feature.

USING iDRAC MANAGEMENT INTERFACES

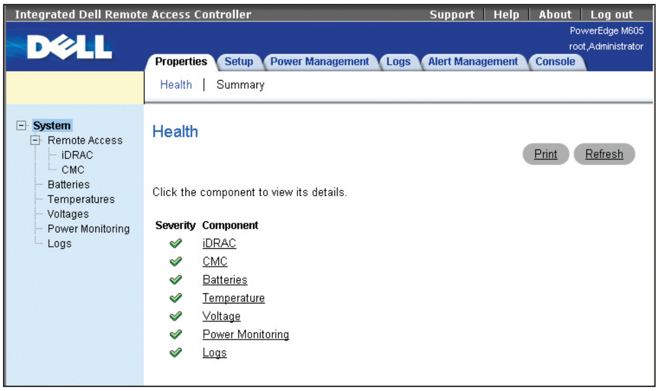
The iDRAC supports multiple management interfaces to help maximize administrator flexibility, including the following:

- **Dell OpenManage™ Server Administrator (OMSA):** Installed on the managed server, OMSA provides a comprehensive Web browser–based GUI to configure and monitor server components using alerts and sensors.
- **iDRAC Web interface:** The iDRAC provides a dedicated Web browser–based GUI to configure the iDRAC and monitor the server through the iDRAC network interface. This interface allows stand-alone operation using any supported Web browser.
- **CMC Web interface:** In addition to monitoring and managing the PowerEdge M1000e enclosure, administrators can use the CMC Web browser–based GUI to view the status of a blade, configure the iDRAC network settings, and start, stop, or reset blades.
- **Enclosure LCD panel:** The LCD panel on the PowerEdge M1000e enclosure displays the high-level status of the server blades in the enclosure. During the initial CMC configuration, a configuration wizard allows administrators to enable Dynamic Host Configuration Protocol (DHCP) configuration of the iDRAC networking.
- **Racadm CLI:** The racadm interface provides a scriptable CLI that enables administrators to configure iDRACs locally from the OS. Racadm is installed on the managed blade when administrators install OMSA. Administrators can inspect sensor data, system event log records, and current status and configuration values maintained in the iDRAC as well as alter the iDRAC configuration values, manage local users, enable and disable features, and perform functions such as shutting down or rebooting the managed server. The iDRAC does not support remote racadm.
- **iDRAC virtual media CLI (iVM-CLI):** The iVM-CLI provides managed blades access to media on the management station, which is useful for developing scripts to install operating systems on multiple blades.
- **SSH and Telnet console:** SSH (fully encrypted username and password) and Telnet connections are used to connect to the iDRAC to issue SM CLP commands. Only one SSH or Telnet client connection is supported at one time.
- **SM CLP:** Administrators can access the SM CLP CLI by logging in to the iDRAC using SSH or Telnet. SM CLP commands implement a subset of local racadm commands that are useful for scripting because administrators can execute them from a management station command line. Command output can be retrieved in well-defined formats, including XML, which is helpful for scripting and when integrating the commands with existing reporting and management tools.
- **Intelligent Platform Management Interface (IPMI):** IPMI defines a standard method for embedded management subsystems such as the iDRAC to communicate with other embedded systems and management applications. The iDRAC supports standard IPMI tools such as ipmitool and ipmishell.

[1] For more information, see "The Next-Generation Dell PowerEdge M1000e Modular Blade Enclosure," by Chad Fenner, in *Dell Power Solutions*, February 2008, DELL.COM/Downloads/Global/Power/ps1q08-20080206-Fenner.pdf.

UNDERSTANDING iDRAC FEATURE ENHANCEMENTS

The iDRAC offers several key features in addition to standard remote blade management and configuration features, including an enhanced GUI, power monitoring functionality, enhanced virtual KVM functionality, enhanced virtual media functionality, and enhanced connectivity using the SM CLP CLI.

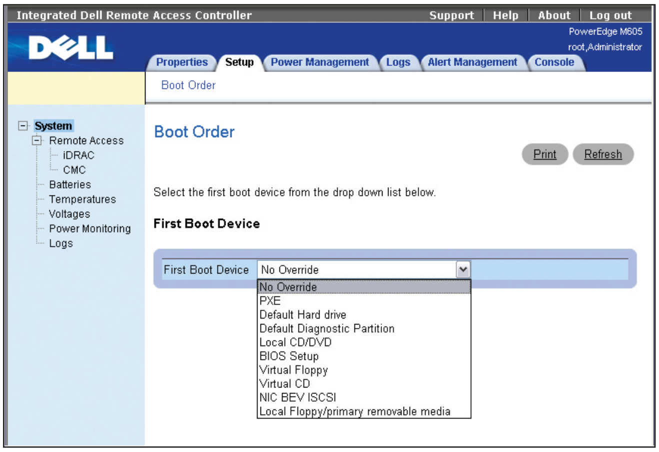


Health

Click the component to view its details.

Severity	Component
✓	iDRAC
✓	CMC
✓	Batteries
✓	Temperature
✓	Voltage
✓	Power Monitoring
✓	Logs

Figure 1. *iDRAC Health page for monitoring component health*



Boot Order

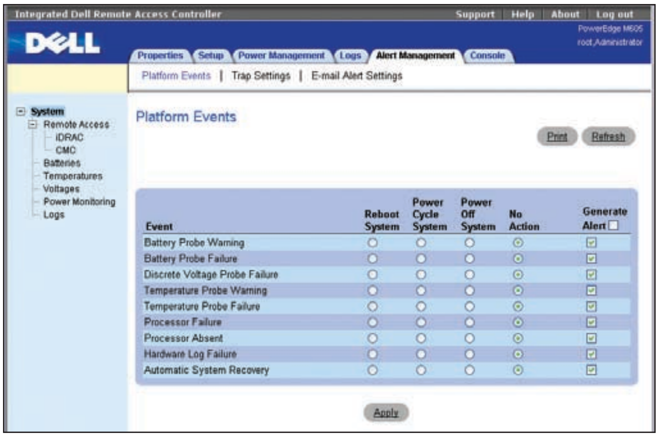
Select the first boot device from the drop down list below.

First Boot Device

First Boot Device: No Override

- No Override
- PXE
- Default Hard drive
- Default Diagnostic Partition
- Local CD/DVD
- BIOS Setup
- Virtual Floppy
- Virtual CD
- NIC BEV ISCSI
- Local Floppy/primary removable media

Figure 2. *iDRAC Boot Order page for configuring system boot order*



Platform Events

Event	Reboot System	Power Cycle System	Power Off System	No Action	Generate Alert □
Battery Probe Warning	○	○	○	●	☑
Battery Probe Failure	○	○	○	●	☑
Discrete Voltage Probe Failure	○	○	○	●	☑
Temperature Probe Warning	○	○	○	●	☑
Temperature Probe Failure	○	○	○	●	☑
Processor Failure	○	○	○	●	☑
Processor Absent	○	○	○	●	☑
Hardware Log Failure	○	○	○	●	☑
Automatic System Recovery	○	○	○	●	☑

Figure 3. *iDRAC Platform Events page for managing and configuring events and alerts*

Enhanced GUI

The iDRAC Web browser–based GUI is designed to maintain a look and feel similar to those of previous-generation DRACs while offering additional configuration pages to enhance usability. For example, the Health page provides a single location for administrators to view the overall health of the blade the iDRAC is attached to (see Figure 1). Component warnings or alerts are identified in the Severity column, and administrators can click component links to view additional information.

Another enhancement is the addition of a power-on self-test (POST) code log and the ability to configure the blade first boot device. The POST Code page displays the last system POST code—a progress indicator from the system BIOS that indicates boot sequence stages from power up to reset and provides tracing information for boot-related errors—before booting the OS. The Boot Order page enables administrators to configure the parameters that direct the system boot following a system power up or reset (see Figure 2). These settings are saved in the system BIOS until the next system boot.

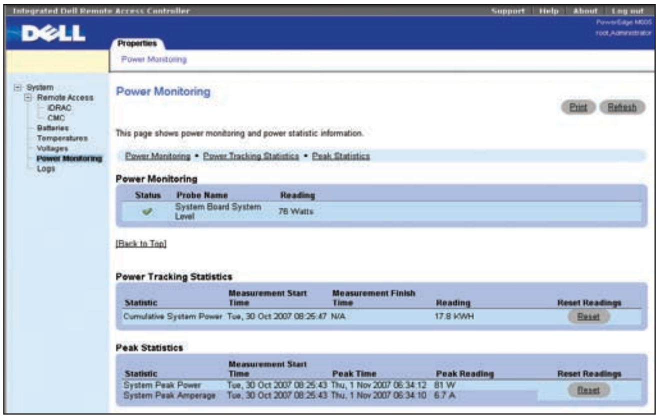
An additional page in the iDRAC Web browser–based GUI offers administrators a way to view and configure platform events and alerts, which can help reduce the platform's complexity (see Figure 3).

Power monitoring functionality

The iDRAC introduces a feature enabling administrators to monitor blade power consumption by viewing statistics for cumulative and peak power usage (see Figure 4). The cumulative system power statistic displays the total system power used by the blade, which can be reset to zero by authorized administrators. The system peak power statistic displays the maximum power (measured in watts and amps) that the server uses at one time.

Enhanced virtual KVM functionality

The Console Redirection page enables administrators to access the console redirect application and use the display, mouse,



Power Monitoring

This page shows power monitoring and power statistic information.

Power Monitoring

Status	Probe Name	Reading
✓	System Board System Level	78 Watts

Power Tracking Statistics

Statistic	Measurement Start Time	Measurement Finish Time	Reading	Reset Readings
Cumulative System Power	Tue, 30 Oct 2007 08:25:47	N/A	17.8 KWH	Reset

Peak Statistics

Statistic	Measurement Start Time	Peak Time	Peak Reading	Reset Readings
System Peak Power	Tue, 30 Oct 2007 08:25:43	Thu, 1 Nov 2007 06:34:12	81 W	Reset
System Peak Amperage	Tue, 30 Oct 2007 08:25:43	Thu, 1 Nov 2007 06:34:10	6.7 A	

Figure 4. *iDRAC Power Monitoring page for viewing system power usage and peak power statistics*

keyboard, and CD or USB drive on the local management station to control the corresponding devices on remotely managed systems. The enhanced iDRAC console redirection application supports both Microsoft ActiveX® and Java plug-ins. Administrators can typically use the Java viewer in any Web browser, including the Microsoft Internet Explorer® browser. If administrators access the iDRAC using Internet Explorer running on a Microsoft Windows® OS, they can choose either ActiveX or Java.

Enhanced virtual media functionality

The virtual media feature allows a floppy image, floppy drive, or CD drive to be available on the system's console as though the image or drive were attached and connected to the local system. For example, if administrators connect to virtual media on a blade running Windows, the virtualized drive appears in Internet Explorer as a drive with a new drive letter (such as E:\).

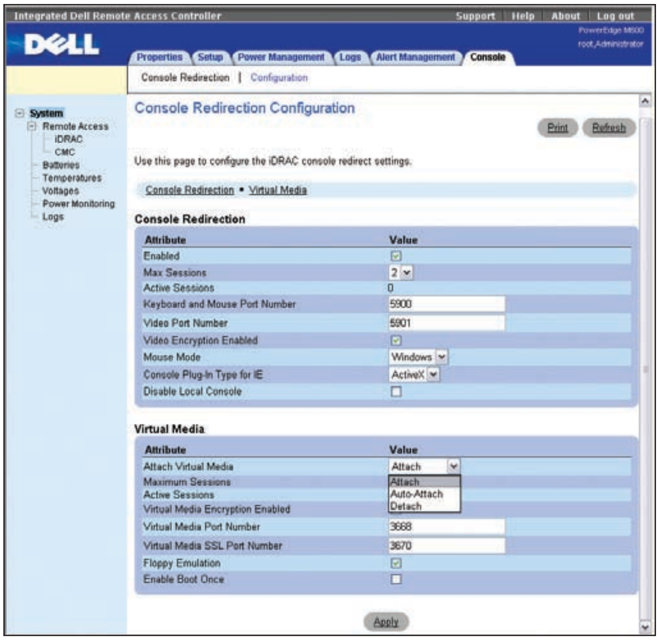
The virtual media functionality is one enhancement for the iDRAC that has been integrated into the console redirection feature. Administrators with valid credentials can access the virtual media features from within the Console Redirection Configuration page, which provides a seamless interface between the two features. Administrators can also use this page to configure virtual media drives to attach, auto-attach, or detach through the iDRAC (see Figure 5):

- **Attach:** The virtual media devices attach to the server at boot time and appear as USB drives on the blade.
- **Auto-attach:** The virtual media devices automatically attach to the server when a virtual media session starts.
- **Detach:** The virtual media devices detach from the blade; administrators cannot redirect the virtual media that uses this setting.

The iDRAC also introduces the Media Redirection wizard, which administrators can access by selecting Media > Virtual Media Wizard, then use to connect or detach individual devices without interrupting existing connections (see Figure 6).

Enhanced connectivity using the SM CLP CLI

The iDRAC supports a Distributed Management Task Force (DMTF) Systems Management Architecture for Server Hardware (SMASH)–compliant CLI accessible with the SSH and Telnet interfaces. The iDRAC SM CLP CLI is designed to provide an industry-standard interface that enables interoperability over large, heterogeneous hardware environments. The SM CLP CLI supports industry-standard commands that allow administrators with appropriate credentials to view the system event log and the blade power status; power up, power down, or reset a blade; configure iDRAC user account, LAN, and virtual media settings; configure SSL Certificate Signature Request (CSR) generation; and view Serial over LAN (SOL) redirection over SSH or Telnet.



Console Redirection Configuration

Use this page to configure the iDRAC console redirect settings.

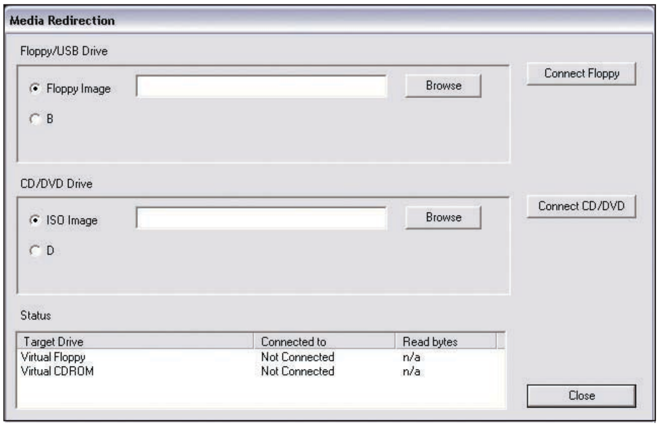
Console Redirection

Attribute	Value
Enabled	☑
Max Sessions	2
Active Sessions	0
Keyboard and Mouse Port Number	5900
Video Port Number	5901
Video Encryption Enabled	☑
Mouse Mode	Windows
Console Plug-In Type for IE	ActiveX
Disable Local Console	□

Virtual Media

Attribute	Value
Attach Virtual Media	Attach Attach Auto-Attach Detach
Maximum Sessions	
Active Sessions	
Virtual Media Encryption Enabled	
Virtual Media Port Number	3668
Virtual Media SSL Port Number	3670
Floppy Emulation	☑
Enable Boot Once	□

Figure 5. *Console Redirection Configuration page for configuring virtual media*



Target Drive	Connected to	Read bytes
Virtual Floppy	Not Connected	n/a
Virtual CDROM	Not Connected	n/a

Figure 6. *Media Redirection wizard for connecting and detaching individual devices*

MANAGING DELL POWEREDGE BLADE SERVERS

The iDRACs in Dell PowerEdge M-Series server blades provide enhanced remote management and configuration features, including enhanced Web browser–based GUIs, console redirection and virtual KVM functionality, virtual media functionality for virtual access to device images and drives, and multiple interfaces to help maximize administrator flexibility. These features are designed to offer administrators powerful yet simplified control over PowerEdge M-Series blade servers while helping increase flexibility and enhance security in their environments.

Jon McGary is a senior software developer in the Dell Remote Management Group. Before joining Dell, Jon was employed by Tandem Computers and specialized in remote management of fault-tolerant computers. He has a B.S. from Texas A&M University.