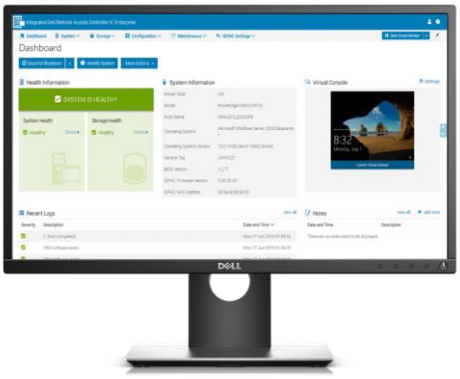
The Integrated Dell Remote Access Controller (iDRAC) Solution Brief



Full Access Management of PowerEdge Servers

Modernize with Dell EMC PowerEdge portfolio

The integrated Dell Remote Access Controller (iDRAC) delivers advanced, agent-free local and remote server administration. The iDRAC provides a secure means to automate a multitude of management tasks. Given that iDRAC is embedded in every PowerEdge server, there's no additional software to install. Once iDRAC has been enabled, you will have a complete set of server management features at your fingertips.

Manage More

With iDRAC in place across the PowerEdge portfolio, the same IT administration techniques and tools can be applied throughout. This consistent management platform allows easy scaling of PowerEdge servers as your organization's infrastructure grows. With iDRAC RESTful API, iDRAC enables support for the Redfish standard and enhances it with Dell EMC extensions to optimize at-scale management. The entire OpenManage portfolio of systems management tools allows every customer to tailor an effective, affordable solution for their environment. This portfolio includes tools, consoles and integrations that leverage iDRAC to make management easy. By extending the reach to larger numbers of servers, you can be more productive and drive down organizational costs.

Intelligent Automation

Dell's agent-free management puts you in control. Once a PowerEdge server is connected to power and networking, that system can be monitored and fully managed, whether you're standing in front of the server or remotely over a network. In fact, since iDRAC is agent free, you can monitor, manage, update, troubleshoot and remediate Dell EMC servers. With features like zero-touch deployment and provisioning, Group Manager, and System Lockdown, iDRAC is purpose-built to make server administration quick and easy. If you already have an existing management platform that utilizes in-band management, Dell EMC provides iDRAC Service Module, a lightweight service that can interact with both iDRAC and the host operating system to support legacy management platforms.

Secure Local and Remote Management

Whether iDRAC is used via the updated, HTML5-based web interface, command line interface, or a set of robust APIs such as the iDRAC RESTful API, security is ensured. SELinux and configurable options like HTTPS, TLS 1.2, Smart Card authentication, LDAP, and Active Directory integration provide security in your working environment. By providing secure access to remote servers, you can carry out critical management functions while maintaining the integrity and security of the data. Additional iDRAC security features include:

- The iDRAC allows you to protect your system from unwanted configuration changes via system lockdown mode.
- In addition to TLS 1.2 and 256-bit encryption strength, iDRAC Cipher Select provides further granular controls of the ciphers for communication.
- Additionally, the iDRAC firmware is equipped with a default security certificate, which can be replaced by one of your own.

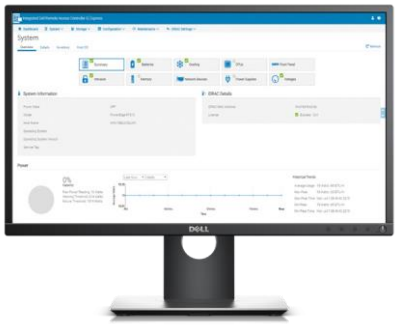
iDRAC Features and Benefits

Features	Benefits
BIOS Recovery	Detect an invalid, untrusted BIOS image when a boot is attempted and recover to an authenticated, trusted BIOS image.
Connection View	Quickly check if server LOMs/NDCs and iDRAC are connected to the correct switches and ports via the GUI or by command line interface. This helps prevent costly remote dispatch of technicians to remediate cabling errors.
Full Power Cycle	By utilizing the iDRAC Service Module, DC power, including AUX power, can be temporarily removed via local or remote control to reset all power nodes in a server, saving time when troubleshooting.
iDRAC Direct	Secure front-panel USB connection to iDRAC web interface, which eliminates the need for crash carts or a trip to the hot aisle of your data center. You can use the same port to insert a USB key to upload new system profile for secure, rapid system configuration.
iDRAC Group Manager	Provides built-in, one-to-many monitoring and inventory of local iDRACs with no software to install. Ideal for customers who don't want to install and maintain a separate monitoring console. This feature does require iDRAC Enterprise licenses.
DRAC RESTful API	With this API, iDRAC enables support for the Redfish standard and enhances it with Dell extensions.
Cipher Select	Cipher Select is an advanced user setting where the user can choose to block undesired ciphers negotiated by iDRAC, providing increased security.
OpenManage Mobile and Quick Sync 2	Use the OpenManage Mobile 2.0 (or higher) app on your handheld device to securely retrieve critical health data and easily perform bare-metal server configuration tasks via BLE/Wi-Fi connectivity. Compatible with various iOS and Android devices.
System Erase	With proper authentication, administrators can securely erase data from local storage (HDDs, SSDs, NVMes).
System Lockdown	Helps to prevent configuration or firmware changes to a server when using Dell tools. Requires iDRAC Enterprise License.
Zero touch deployment and provisioning	When ordered with Zero Touch, PowerEdge servers can be automatically configured when they are initially connected to your network. This process uses a Server Configuration Profile to ensure each server is set to your specifications.
SElinux	iDRAC code is built upon SELinux, a best-of-breed security that helps protects your system in the event of an attack.

The Heart of PowerEdge Manageability

The iDRAC provides comprehensive, embedded management across the PowerEdge family of servers, automation that lets your organization grow, and security that ensures peace of mind. From the variety of tools and technologies in the OpenManage portfolio, you can build a management solution that matches your needs, and by leveraging iDRAC, ensures optimal server management.

To view the full list of features, see the iDRAC User Guide



Learn more about iDRAC

Contact
a Dell EMC Expert

View more resources

Join the conversation with
#HashTag