Integrated Dell Remote Access Controller 8 (iDRAC8)

Version 2.05.05.05 User's Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Copyright © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2014 - 12

Rev. A00

Contents

1 Overview....16
- Benefits of Using iDRAC With Lifecycle Controller....16
- Key Features....17
- New In This Release....20
- How To Use This User's Guide....20
- Supported Web Browsers....20
- Managing Licenses....20
  - Types of Licenses....21
  - Acquiring Licenses....21
  - License Operations....21
- Licensable Features In iDRAC8....23
- Interfaces and Protocols to Access iDRAC....28
- iDRAC Port Information....30
- Other Documents You May Need....31
- Social Media Reference....33
- Contacting Dell....33
- Accessing documents from Dell support site....33

2 Logging into iDRAC....35
- Logging into iDRAC as Local User, Active Directory User, or LDAP User....35
- Logging into iDRAC Using Smart Card....36
  - Logging Into iDRAC as a Local User Using Smart Card....36
  - Logging Into iDRAC as an Active Directory User Using Smart Card....37
- Logging into iDRAC Using Single Sign-on....37
  - Logging into iDRAC SSO Using iDRAC Web Interface....37
  - Logging into iDRAC SSO Using CMC Web Interface....38
- Accessing iDRAC Using Remote RACADM....38
  - Validating CA Certificate To Use Remote RACADM on Linux....38
- Accessing iDRAC Using Local RACADM....39
- Accessing iDRAC Using Firmware RACADM....39
- Accessing iDRAC Using SMCLP....39
- Logging in to iDRAC Using Public Key Authentication....39
- Multiple iDRAC Sessions....40
- Changing Default Login Password....40
  - Changing Default Login Password Using Web Interface....40
  - Changing Default Login Password Using RACADM....41
  - Changing Default Login Password Using iDRAC Settings Utility....41
- Enabling or Disabling Default Password Warning Message....41

Enabling or Disabling Default Password Warning Message Using Web Interface..... 41
Enabling or Disabling Warning Message to Change Default Login Password Using RACADM.....41

3 Setting Up Managed System and Management Station.....42

Setting Up iDRAC IP Address.....42
Setting Up iDRAC IP Using iDRAC Settings Utility.....43
Setting Up iDRAC IP Using CMC Web Interface..... 46
Enabling Auto-discovery.....46
Configuring Servers and Server Components Using Auto Config..... 47
Using Hash Passwords for Improved Security.....51
Setting Up Management Station.....52
Accessing iDRAC Remotely..... 52
Setting Up Managed System.....53
Modifying Local Administrator Account Settings.....53
Setting Up Managed System Location..... 53
Optimizing System Performance and Power Consumption.....54
Configuring Supported Web Browsers..... 60
Adding iDRAC to the List of Trusted Domains.....62
Disabling Whitelist Feature in Firefox..... 62
Viewing Localized Versions of Web Interface.....62
Updating Device Firmware..... 63
Downloading Device Firmware..... 65
Updating Firmware Using iDRAC Web Interface.....65
Updating Device Firmware Using RACADM.....69
Scheduling Automatic Firmware Updates.....70
Updating Firmware Using CMC Web Interface..... 71
Updating Firmware Using DUP.....71
Updating Firmware Using Remote RACADM..... 72
Updating Firmware Using Lifecycle Controller Remote Services.....72
Updating CMC Firmware From iDRAC..... 72
Viewing and Managing Staged Updates.....73
Viewing and Managing Staged Updates Using iDRAC Web interface.....73
Viewing and Managing Staged Updates Using RACADM.....73
Rolling Back Device Firmware..... 74
Rollback Firmware Using iDRAC Web Interface.....74
Rollback Firmware Using CMC Web Interface..... 75
Rollback Firmware Using RACADM.....75
Rollback Firmware Using Lifecycle Controller.....76
Rollback Firmware Using Lifecycle Controller-Remote Services.....76
Recovering iDRAC..... 76
Using TFTP Server.....76

Backing Up Server Profile....76
Backing Up Server Profile Using iDRAC Web Interface....77
Backing Up Server Profile Using RACADM....77
Scheduling Automatic Backup Server Profile....77
Importing Server Profile....79
Importing Server Profile Using iDRAC Web Interface....79
Importing Server Profile Using RACADM....80
Restore Operation Sequence....80
Monitoring iDRAC Using Other Systems Management Tools....80

4 Configuring iDRAC....81
Viewing iDRAC Information....82
Viewing iDRAC Information Using Web Interface....82
Viewing iDRAC Information Using RACADM....82
Modifying Network Settings....82
Modifying Network Settings Using Web Interface....83
Modifying Network Settings Using Local RACADM....83
Configuring IP Filtering....84
Configuring Services....85
Configuring Services Using Web Interface....86
Configuring Services Using RACADM....86
Enabling or Disabling HTTPs Redirection....87
Using VNC Client to Manage Remote Server....87
Configuring VNC Server Using iDRAC Web Interface....88
Configuring VNC Server Using RACADM....88
Setting Up VNC Viewer With SSL Encryption....88
Setting Up VNC Viewer Without SSL Encryption....88
Configuring Front Panel Display....89
Configuring LCD Setting....89
Configuring System ID LED Setting....90
Configuring Time Zone and NTP....91
Configuring Time Zone and NTP Using iDRAC Web Interface....91
Configuring Time Zone and NTP Using RACADM....91
Setting First Boot Device....91
Setting First Boot Device Using Web Interface....92
Setting First Boot Device Using RACADM....92
Setting First Boot Device Using Virtual Console....92
Enabling Last Crash Screen....92
Enabling or Disabling OS to iDRAC Pass-through....93
Supported Cards for OS to iDRAC Pass-through....94
Supported Operating Systems for USB NIC....94
Enabling or Disabling OS to iDRAC Pass-through Using Web Interface....96

Enabling or Disabling OS to iDRAC Pass-through Using RACADM... 97
Enabling or Disabling OS to iDRAC Pass-through Using iDRAC Settings Utility... 97
Obtaining Certificates... 97
SSL Server Certificates... 98
Generating a New Certificate Signing Request... 99
Uploading Server Certificate... 100
Viewing Server Certificate... 101
Uploading Custom Signing Certificate... 101
Downloading Custom SSL Certificate Signing Certificate... 102
Deleting Custom SSL Certificate Signing Certificate... 102
Configuring Multiple iDRACs Using RACADM... 103
Creating an iDRAC Configuration File... 104
Parsing Rules... 105
Modifying the iDRAC IP Address... 106
Disabling Access to Modify iDRAC Configuration Settings on Host System... 106

5 Viewing iDRAC and Managed System Information... 108
Viewing Managed System Health and Properties... 108
Viewing System Inventory... 108
Viewing Sensor Information... 109
Monitoring Performance Index of CPU, Memory, and I/O Modules... 111
Monitoring Performance Index for of CPU, Memory, and I/O Modules Using Web Interface... 112
Monitoring Performance Index for of CPU, Memory, and I/O Modules Using RACADM... 113
Checking the System for Fresh Air Compliance... 113
Viewing Historical Temperature Data... 113
Viewing Historical Temperature Data Using iDRAC Web Interface... 114
Viewing Historical Temperature Data Using RACADM... 114
Configuring Warning Threshold for Inlet Temperature... 114
Viewing Network Interfaces Available On Host OS... 115
Viewing Network Interfaces Available on Host OS Using Web Interface... 115
Viewing Network Interfaces Available on Host OS Using RACADM... 115
Viewing FlexAddress Mezzanine Card Fabric Connections... 116
Viewing or Terminating iDRAC Sessions... 116
Terminating iDRAC Sessions Using Web Interface... 116
Terminating iDRAC Sessions Using RACADM... 117

6 Setting Up iDRAC Communication... 118
Communicating With iDRAC Through Serial Connection Using DB9 Cable... 119
Configuring BIOS For Serial Connection... 120
Enabling RAC Serial Connection... 120
Enabling IPMI Serial Connection Basic and Terminal Modes... 120

Switching Between RAC Serial and Serial Console While Using DB9 Cable... 123
Switching From Serial Console to RAC Serial... 123
Switching From RAC Serial to Serial Console... 123
Communicating With iDRAC Using IPMI SOL... 123
Configuring BIOS For Serial Connection... 124
Configuring iDRAC to Use SOL... 124
Enabling Supported Protocol... 125
Communicating With iDRAC Using IPMI Over LAN... 129
Configuring IPMI Over LAN Using Web Interface... 129
Configuring IPMI Over LAN Using iDRAC Settings Utility... 130
Configuring IPMI Over LAN Using RACADM... 130
Enabling or Disabling Remote RACADM... 130
Enabling or Disabling Remote RACADM Using Web Interface... 130
Enabling or Disabling Remote RACADM Using RACADM... 131
Disabling Local RACADM... 131
Enabling IPMI on Managed System... 131
Configuring Linux for Serial Console During Boot... 131
Enabling Login to the Virtual Console After Boot... 132
Supported SSH Cryptography Schemes... 134
Using Public Key Authentication For SSH... 134

7 Configuring User Accounts and Privileges... 138

Configuring Local Users... 138
Configuring Local Users Using iDRAC Web Interface... 138
Configuring Local Users Using RACADM... 139
Configuring Active Directory Users... 141
Prerequisites for Using Active Directory Authentication for iDRAC... 142
Supported Active Directory Authentication Mechanisms... 144
Standard Schema Active Directory Overview... 144
Configuring Standard Schema Active Directory... 146
Extended Schema Active Directory Overview... 149
Configuring Extended Schema Active Directory... 151
Testing Active Directory Settings... 161
Configuring Generic LDAP Users... 162
Configuring Generic LDAP Directory Service Using iDRAC Web-Based Interface... 162
Configuring Generic LDAP Directory Service Using RACADM... 163
Testing LDAP Directory Service Settings... 163

8 Configuring iDRAC for Single Sign-On or Smart Card Login... 165

Prerequisites for Active Directory Single Sign-On or Smart Card Login... 165
Registering iDRAC as a Computer in Active Directory Root Domain... 166
Generating Kerberos Keytab File... 166

Creating Active Directory Objects and Providing Privileges....167
Configuring Browser to Enable Active Directory SSO....167
Configuring iDRAC SSO Login for Active Directory Users....168
Configuring iDRAC SSO Login for Active Directory Users Using Web Interface....168
Configuring iDRAC SSO Login for Active Directory Users Using RACADM....168
Configuring iDRAC Smart Card Login for Local Users....168
Uploading Smart Card User Certificate....169
Uploading Trusted CA Certificate For Smart Card....169
Configuring iDRAC Smart Card Login for Active Directory Users....170
Enabling or Disabling Smart Card Login....170
Enabling or Disabling Smart Card Login Using Web Interface....171
Enabling or Disabling Smart Card Login Using RACADM....171
Enabling or Disabling Smart Card Login Using iDRAC Settings Utility....171

9 Configuring iDRAC to Send Alerts....172

Enabling or Disabling Alerts....172
Enabling or Disabling Alerts Using Web Interface....173
Enabling or Disabling Alerts Using RACADM....173
Enabling or Disabling Alerts Using iDRAC Settings Utility....173
Filtering Alerts....173
Filtering Alerts Using iDRAC Web Interface....173
Filtering Alerts Using RACADM....174
Setting Event Alerts....174
Setting Event Alerts Using Web Interface....174
Setting Event Alerts Using RACADM....175
Setting Alert Recurrence Event....175
Setting Alert Recurrence Events Using iDRAC Web Interface....175
Setting Alert Recurrence Events Using RACADM....175
Setting Event Actions....175
Setting Event Actions Using Web Interface....175
Setting Event Actions Using RACADM....176
Configuring Email Alert, SNMP Trap, or IPMI Trap Settings....176
Configuring IP Alert Destinations....176
Configuring Email Alert Settings....178
Configuring WS Eventing....180
Alerts Message IDs....180

10 Managing Logs....184

Viewing System Event Log....184
Viewing System Event Log Using Web Interface....184
Viewing System Event Log Using RACADM....184
Viewing System Event Log Using iDRAC Settings Utility....185

Viewing Lifecycle Log 185
Viewing Lifecycle Log Using Web Interface..... 186
Viewing Lifecycle Log Using RACADM..... 186
Exporting Lifecycle Controller Logs..... 186
Exporting Lifecycle Controller Logs Using Web Interface..... 187
Exporting Lifecycle Controller Logs Using RACADM..... 187
Adding Work Notes..... 187
Configuring Remote System Logging..... 187
Configuring Remote System Logging Using Web Interface..... 187
Configuring Remote System Logging Using RACADM..... 188

11 Monitoring and Managing Power..... 189
Monitoring Power..... 189
Monitoring Power Using Web Interface..... 189
Monitoring Power Using RACADM..... 190
Setting Warning Threshold for Power Consumption..... 190
Setting Warning Threshold for Power Consumption Using Web Interface..... 190
Executing Power Control Operations..... 190
Executing Power Control Operations Using Web Interface..... 190
Executing Power Control Operations Using RACADM..... 191
Power Capping..... 191
Power Capping in Blade Servers..... 191
Viewing and Configuring Power Cap Policy..... 191
Configuring Power Supply Options..... 193
Configuring Power Supply Options Using Web Interface..... 193
Configuring Power Supply Options Using RACADM..... 193
Configuring Power Supply Options Using iDRAC Settings Utility..... 194
Enabling or Disabling Power Button..... 194

12 Inventory, Monitoring, and Configuring Network Devices..... 195
Inventory and Monitoring Network Devices..... 195
Monitoring Network Devices Using Web Interface..... 195
Monitoring Network Devices Using RACADM..... 195
Inventory and Monitoring FC HBA Devices..... 196
Monitoring FC HBA Devices Using Web Interface..... 196
Monitoring FC HBA Devices Using RACADM..... 196
Dynamic Configuration of Virtual Addresses, Initiator, and Storage Target Settings..... 196
Supported Cards for I/O Identity Optimization..... 197
Supported BIOS Version for I/O Identity Optimization..... 198
Supported NIC Firmware Versions for I/O Identity Optimization..... 198
System Behavior for FlexAddress and IO Identity 199
Enabling or Disabling I/O Identity Optimization..... 199

Configuring Persistence Policy Settings....200

13 Managing Storage Devices....204

Understanding RAID Concepts....205
What Is RAID?....206
Organizing Data Storage For Availability And Performance....207
Choosing RAID Levels....207
Comparing RAID Level Performance....214
Supported Controllers....216
Supported RAID Controllers....216
Supported Non-RAID Controllers....216
Supported Enclosures....216
Summary of Supported Features for Storage Devices....216
Inventory and Monitoring Storage Devices....219
Monitoring Storage Device Using Web Interface....219
Monitoring Storage Device Using RACADM....220
Monitoring Backplane Using iDRAC Settings Utility....220
Viewing Storage Device Topology....220
Managing Physical Disks....220
Assigning or Unassigning Physical Disk as Global Hot spare....220
Convert To RAID Capable Disk....221
Convert To Non-RAID Disk....222
Managing Virtual Disks....222
Creating Virtual Disks....222
Editing Virtual Disk Cache Policies....224
Deleting Virtual Disks....225
Checking Virtual Disk Consistency....225
Initializing Virtual Disks....226
Encrypting Virtual Disks....227
Assigning or Unassigning Dedicated Hot Spares....227
Managing Virtual Disks Using Web Interface....227
Managing Virtual Disks Using RACADM....228
Managing Controllers....228
Configuring Controller Properties....229
Importing or Auto Importing Foreign Configuration....232
Clearing Foreign Configuration....233
Resetting Controller Configuration....234
12Gbps SAS HBA Adapter Operations....235
Monitoring Predictive Failure Analysis On Drives....235
Controller Operations in Non-RAID (HBA) Mode....236
Running RAID Configuration Jobs On Multiple Storage Controllers....236
Managing PCIe SSDs....236

Inventory and Monitoring PCIe SSDs... 237
Preparing to Remove PCIe SSD... 238
Erasing PCIe SSD Device Data... 239
Managing Enclosures or Backplanes... 240
Configuring Backplane Mode... 241
Viewing Universal Slots... 243
Setting SGPIO Mode... 244
Choosing Operation Mode to Apply Settings... 244
Choosing Operation Mode Using Web Interface... 244
Choosing Operation Mode Using RACADM... 245
Viewing and Applying Pending Operations... 245
Viewing, Applying, or Deleting Pending Operations Using Web Interface... 245
Viewing and Applying Pending Operations Using RACADM... 246
Storage Devices — Apply Operation Scenarios... 247
Case 1: Selected an Apply Operation (Apply Now, At Next Reboot, or At Scheduled Time) and there are no existing pending operations Case 2: Selected an Apply Operation (Apply Now, At Next Reboot, or At Scheduled Time) and there are existing pending operations Case 3: Selected Add to Pending Operations and there are no existing pending operationsCase 4: Selected Add to Pending Operations and there are prior existing pending operations... 247
Blinking or Unblinking Component LEDs... 248
Blinking or Unblinking Component LEDs Using Web Interface... 248
Blinking or Unblinking Component LEDs Using RACADM... 249

14 Configuring and Using Virtual Console... 250

Supported Screen Resolutions and Refresh Rates... 250
Configuring Web Browsers to Use Virtual Console... 251
Configuring Web Browser to Use Java Plug-in... 251
Configuring IE to Use ActiveX Plug-in... 252
Importing CA Certificates to Management Station... 254
Configuring Virtual Console... 254
Configuring Virtual Console Using Web Interface... 255
Configuring Virtual Console Using RACADM... 255
Previewing Virtual Console... 255
Launching Virtual Console... 255
Launching Virtual Console Using Web Interface... 256
Launching Virtual Console Using URL... 257
Disabling Warning Messages While Launching Virtual Console Or Virtual Media Using Java or ActiveX Plug-in... 257
Using Virtual Console Viewer... 257
Synchronizing Mouse Pointers... 258
Passing All Keystrokes Through Virtual Console... 259

15 Managing Virtual Media..... 263
Supported Drives and Devices..... 264
Configuring Virtual Media..... 264
Configuring Virtual Media Using iDRAC Web Interface..... 264
Configuring Virtual Media Using RACADM..... 265
Configuring Virtual Media Using iDRAC Settings Utility..... 265
Attached Media State and System Response..... 265
Accessing Virtual Media..... 265
Launching Virtual Media Using Virtual Console..... 266
Launching Virtual Media Without Using Virtual Console..... 266
Adding Virtual Media Images..... 267
Viewing Virtual Device Details..... 267
Resetting USB..... 268
Mapping Virtual Drive..... 268
Unmapping Virtual Drive..... 269
Setting Boot Order Through BIOS..... 269
Enabling Boot Once for Virtual Media..... 270

16 Installing and Using VMCLI Utility..... 271
Installing VMCLI..... 271
Running VMCLI Utility..... 271
VMCLI Syntax..... 272
VMCLI Commands to Access Virtual Media..... 272
VMCLI Operating System Shell Options..... 273

17 Managing vFlash SD Card..... 274
Configuring vFlash SD Card..... 274
Viewing vFlash SD Card Properties..... 275
Enabling or Disabling vFlash Functionality..... 275
Initializing vFlash SD Card..... 276
Getting the Last Status Using RACADM..... 277
Managing vFlash Partitions..... 277
Creating an Empty Partition..... 278
Creating a Partition Using an Image File..... 279
Formatting a Partition..... 280
Viewing Available Partitions..... 280
Modifying a Partition..... 281
Attaching or Detaching Partitions..... 282
Deleting Existing Partitions..... 283
Downloading Partition Contents..... 284
Booting to a Partition..... 284

18 Using SMCLP 286
System Management Capabilities Using SMCLP 286
Running SMCLP Commands 287
iDRAC SMCLP Syntax 287
Navigating the MAP Address Space 290
Using Show Verb 290
Using the -display Option 290
Using the -level Option 291
Using the -output Option 291
Usage Examples 291
Server Power Management 291
SEL Management 292
MAP Target Navigation 294

19 Using iDRAC Service Module 295
Installing iDRAC Service Module 295
Supported Operating Systems for iDRAC Service Module 295
iDRAC Service Module Monitoring Features 295
Operating System Information 296
Replicate Lifecycle Logs to OS Log 296
Automatic System Recovery Options 296
Windows Management Instrumentation Providers 297
Co-existence of OpenManage Server Administrator and iDRAC Service Module 298
Using iDRAC Service Module From iDRAC Web Interface 298
Using iDRAC Service Module From RACADM 299

20 Using USB Port for Server Management 300
Accessing iDRAC Interface over Direct USB Connection 300
Configuring iDRAC Using Server Configuration Profile on USB Device 301
Configuring USB Management Port Settings 301
Importing Server Configuration Profile From USB Device 303

21 Using iDRAC Quick Sync 306
Configuring iDRAC Quick Sync 307
Configuring iDRAC Quick Sync Settings Using Web Interface 307
Configuring iDRAC Quick Sync Settings Using RACADM 307
Configuring iDRAC Quick Sync Settings Using iDRAC Settings Utility 308
Using Mobile Device to View iDRAC Information 308

22 Deploying Operating Systems 309
Deploying Operating System Using VMCLI 309

Deploying Operating System Using Remote File Share... 310
Managing Remote File Share... 311
Configuring Remote File Share Using Web Interface... 312
Configuring Remote File Share Using RACADM... 313
Deploying Operating System Using Virtual Media... 313
Installing Operating System From Multiple Disks... 314
Deploying Embedded Operating System On SD Card... 314
Enabling SD Module and Redundancy in BIOS... 314

23 Troubleshooting Managed System Using iDRAC... 316

Using Diagnostic Console... 316
Scheduling Remote Automated Diagnostics... 317
Scheduling Remote Automated Diagnostics Using RACADM... 318
Viewing Post Codes... 318
Viewing Boot and Crash Capture Videos... 318
Configuring Video Capture Settings... 318
Viewing Logs... 319
Viewing Last System Crash Screen... 319
Viewing Front Panel Status... 319
Viewing System Front Panel LCD Status... 319
Viewing System Front Panel LED Status... 320
Hardware Trouble Indicators... 320
Viewing System Health... 321
Generating Technical Support Report... 321
Generating Technical Support Report Automatically... 322
Generating Technical Support Report Manually... 323
Checking Server Status Screen for Error Messages... 325
Restarting iDRAC... 325
Resetting iDRAC Using iDRAC Web Interface... 325
Resetting iDRAC Using RACADM... 325
Erasing System and User Data... 325
Resetting iDRAC to Factory Default Settings... 326
Resetting iDRAC to Factory Default Settings Using iDRAC Web Interface... 326
Resetting iDRAC to Factory Default Settings Using iDRAC Settings Utility... 326

24 Frequently Asked Questions... 327

System Event Log... 327
Network Security... 328
Active Directory... 328
Single Sign-On... 331
Smart Card Login... 332
Virtual Console... 332

Virtual Media..... 336
vFlash SD Card..... 339
SNMP Authentication..... 339
Storage Devices..... 339
iDRAC Service Module..... 339
RACADM..... 341
Miscellaneous..... 342

25 Use Case Scenarios..... 345
Troubleshooting An Inaccessible Managed System..... 345
Obtaining System Information and Assess System Health..... 346
Setting Up Alerts and Configuring Email Alerts..... 346
Viewing and Exporting Lifecycle Log and System Event Log..... 346
Interfaces to Update iDRAC Firmware..... 346
Performing Graceful Shutdown..... 347
Creating New Administrator User Account..... 347
Launching Server's Remote Console and Mounting a USB Drive..... 347
Installing Bare Metal OS Using Attached Virtual Media and Remote File Share..... 347
Managing Rack Density..... 348
Installing New Electronic License..... 348
Applying I/O Identity Configuration Settings for Multiple Network Cards in Single Host System Reboot..... 348

1

Overview

The Integrated Dell Remote Access Controller (iDRAC) is designed to make server administrators more productive and improve the overall availability of Dell servers. iDRAC alerts administrators to server issues, helps them perform remote server management, and reduces the need for physical access to the server.

iDRAC with Lifecycle controller technology is part of a larger datacenter solution that helps keep business critical applications and workloads available at all times. The technology allows administrators to deploy, monitor, manage, configure, update, troubleshoot and remediate Dell servers from any location, and without the use of agents. It accomplishes this regardless of operating system or hypervisor presence or state.

Several products work in conjunction with the iDRAC and Lifecycle controller to simplify and streamline IT operations, such as:

- Dell Management plug-in for VMware vCenter
- Dell Repository Manager
- Dell Management Packs for Microsoft System Center Operations Manager (SCOM) and Microsoft System Center Configuration Manager (SCCM)
- BMC Bladelogic
- Dell OpenManage Essentials
- Dell OpenManage Power Center

The iDRAC is available in the following variants:

- Basic Management with IPMI (available by default for 200-500 series servers)
- iDRAC Express (available by default on all 600 and higher series of rack or tower servers, and all blade servers)
- iDRAC Enterprise (available on all server models)

For more information, see the *iDRAC Overview and Feature Guide* available at **dell.com/support/manuals**.

Benefits of Using iDRAC With Lifecycle Controller

The benefits include:

- Increased Availability — Early notification of potential or actual failures that help prevent a server failure or reduce recovery time after failure.
- Improved Productivity and Lower Total Cost of Ownership (TCO) — Extending the reach of administrators to larger numbers of distant servers can make IT staff more productive while driving down operational costs such as travel.

- Secure Environment — By providing secure access to remote servers, administrators can perform critical management functions while maintaining server and network security.
- Enhanced Embedded Management through Lifecycle Controller – Lifecycle Controller provides deployment and simplified serviceability through Lifecycle Controller GUI for local deployment and Remote Services (WS-Management) interfaces for remote deployment integrated with Dell OpenManage Essentials and partner consoles.

For more information on Lifecycle Controller GUI, see *Lifecycle Controller User's Guide* and for remote services, see *Lifecycle Controller Remote Services User's Guide* available at **dell.com/support/manuals**.

Key Features

The key features in iDRAC include:

NOTE: Some of the features are available only with iDRAC Enterprise license. For information on the features available for a license, see Managing Licenses.

Inventory and Monitoring

- View managed server health.
- Inventory and monitor network adapters and storage subsystem (PERC and direct attached storage) without any operating system agents.
- View and export system inventory.
- View sensor information such as temperature, voltage, and intrusion.
- Monitor CPU state, processor automatic throttling, and predictive failure.
- View memory information.
- Monitor and control power usage.
- Support for SNMPv3 gets.
- For blade servers: launch Chassis Management Controller (CMC) Web interface, view CMC information, and WWN/MAC addresses.

  NOTE: CMC provides access to iDRAC through the M1000E Chassis LCD panel and local console connections. For more information, see *Chassis Management Controller User's Guide* available at **dell.com/support/manuals**.
- View network interfaces available on host operating systems.
- View inventory and monitor information and configure basic iDRAC settings using iDRAC Quick Sync feature and a mobile device.

Deployment

- Manage vFlash SD card partitions.
- Configure front panel display settings.
- Manage iDRAC network settings.
- Configure and use virtual console and virtual media.
- Deploy operating systems using remote file share, virtual media, and VMCLI.
- Enable auto-discovery.
- Perform server configuration using the export or import XML profile feature through RACADM and WS-MAN. For more information, see the *Lifecycle Controller Remote Services Quick Start Guide*.
- Configure persistence policy for virtual addresses, initiator, and storage targets.
- Remotely configure storage devices attached to the system at run-time.

- Perform the following operations for storage devices:
  - Physical disks: Assign or unassign physical disk as a global hot spare.
  - Virtual disks:
    * Create virtual disks.
    * Edit virtual disks cache policies.
    * Check virtual disk consistency.
    * Initialize virtual disks.
    * Encrypt virtual disks.
    * Assign or unassign dedicated hot spare.
    * Delete virtual disks.
  - Controllers:
    * Configure controller properties.
    * Import or auto-import foreign configuration.
    * Clear foreign configuration.
    * Reset controller configuration.
    * Create or change security keys.
  - PCIe SSD devices:
    * Inventory and remotely monitor the health of PCIe SSD devices in the server.
    * Prepare the PCIe SSD to be removed.
    * Securely erase the data.
  - Set the backplane mode (unified or split mode).
  - Blink or unblink component LEDs.
  - Apply the device settings immediately, at next system reboot, at a scheduled time, or as a pending operation to be applied as a batch as part of the single job.

Update

- Manage iDRAC licenses.
- Update BIOS and device firmware for devices supported by Lifecycle Controller.
- Update or rollback iDRAC firmware and lifecycle controller firmware using a single firmware image.
- Manage staged updates.
- Backup and restore server profile.
- Access iDRAC interface over direct USB connection.
- Configure iDRAC using Server Configuration Profiles on USB device.

Maintenance and Troubleshooting

- Perform power related operations and monitor power consumption.
- Optimize system performance and power consumption by modifying the thermal settings.
- No dependency on OpenManage Server Administrator for generation of alerts.
- Log event data: Lifecycle and RAC logs.
- Set email alerts, IPMI alerts, remote system logs, WS eventing logs, and SNMP traps (v1, v2c, and v3) for events and improved email alert notification.
- Capture last system crash image.

- View boot and crash capture videos.
- Out-of-band monitor and alert the performance index of CPU, memory, and I/O modules.
- Configure warning threshold for inlet temperature and power consumption.
- Use iDRAC Service Module to:
  - View Operating System (OS) information.
  - Replicate Lifecycle Controller logs to operating system logs.
  - Automatic system recovery options.
  - Populate Windows Management Instrumentation (WMI) information.
  - Integrate with Technical Support Report. This is applicable only if iDRAC Service Module Version 2.0 or later is installed. For more information, see Generating Tech Support Report.
  - Prepare to Remove NVMe PCIe SSD. For more information, see Preparing to Remove PCIe SSD.
- Generate technical support report in the following ways:
  - Automatic — Using iDRAC Service Module that automatically invokes the OS Collector tool.
  - Manual — Using OS Collector tool.

Secure Connectivity

Securing access to critical network resources is a priority. iDRAC implements a range of security features that includes:

- Custom signing certificate for Secure Socket Layer (SSL) certificate.
- Signed firmware updates.
- User authentication through Microsoft Active Directory, generic Lightweight Directory Access Protocol (LDAP) Directory Service, or locally administered user IDs and passwords.
- Two-factor authentication using the Smart–Card logon feature. The two-factor authentication is based on the physical smart card and the smart card PIN.
- Single Sign-on and Public Key Authentication.
- Role-based authorization, to configure specific privileges for each user.
- SNMPv3 authentication for user accounts stored locally in the iDRAC. It is recommended to use this, but it is disabled by default.
- User ID and password configuration.
- Default login password modification.
- Set user passwords and BIOS passwords using one way hash format for improved security.
- SMCLP and Web interfaces that support 128-bit and 40-bit encryption (for countries where 128 bit is not acceptable), using the SSL 3.0 standard.
- Session time-out configuration (in seconds).
- Configurable IP ports (for HTTP, HTTPS, SSH, Telnet, Virtual Console, and Virtual Media).

  NOTE: Telnet does not support SSL encryption and is disabled by default.
- Secure Shell (SSH) that uses an encrypted transport layer for higher security.
- Login failure limits per IP address, with login blocking from that IP address when the limit is exceeded.
- Limited IP address range for clients connecting to iDRAC.
- Dedicated Gigabit Ethernet adapter available on rack and tower servers (additional hardware may be required).

New In This Release

- Support for the following PowerEdge systems:
  - PowerEdge T430
  - PowerEdge R530
  - PowerEdge R430
  - PowerEdge M630
  - PowerEdge FC630
- Configure CMC firmware update settings to perform firmware update for CMC and its shared components from iDRAC. This is applicable for FX2/FX2s chassis
- Update to the list of licensable features.
- Support for DNS domain name in SNMP traps.

How To Use This User's Guide

The contents of this User's Guide enable you to perform the tasks by using:

- iDRAC Web interface — Only the task-related information is provided here. For information about the fields and options, see the *iDRAC Online Help* that you can access from the Web interface.
- RACADM — The RACADM command or the object that you must use is provided here. For more information, see the *RACADM Command Line Reference Guide* available at **dell.com/support/manuals**.
- iDRAC Settings Utility — Only the task-related information is provided here. For information about the fields and options, see the *iDRAC Settings Utility Online Help* that you can access when you click **Help** in the iDRAC Settings GUI (press <F2> during boot, and then click **iDRAC Settings** on the **System Setup Main Menu** page).

Supported Web Browsers

iDRAC is supported on the following browsers:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

For the list of versions, see the *iDRAC8 Release Notes* available at **dell.com/support/manuals**.

Managing Licenses

iDRAC features are available based on the purchased license (Basic Management, iDRAC Express, or iDRAC Enterprise). Only licensed features are available in the interfaces that allow you to configure or use iDRAC. For example, iDRAC Web interface, RACADM, WS-MAN, OpenManage Server Administrator, and so on. Some features, such as dedicated NIC or vFlash requires iDRAC ports card. This is optional on 200-500 series servers.

iDRAC license management and firmware update functionality is available through iDRAC Web interface and RACADM.

Types of Licenses

The types of licenses offered are:

- 30 day evaluation and extension — The license expires after 30 days and can be extended for 30 days. Evaluation licenses are duration based, and the timer runs when power is applied to the system.
- Perpetual — The license is bound to the service tag and is permanent.

Acquiring Licenses

Use any of the following methods to acquire the licenses:

- E-mail — License is attached to an email that is sent after requesting it from the technical support center.
- Self-service portal — A link to the Self-Service Portal is available from iDRAC. Click this link to open the licensing Self-Service Portal on the internet. Currently, you can use the License Self-Service Portal to retrieve licenses that were purchased with the server. You must contact the sales representative or technical support to buy a new or upgrade license. For more information, see the online help for the self-service portal page.
- Point-of-sale — License is acquired while placing the order for a system.

License Operations

Before you perform the license management tasks, make sure to acquire the licenses. For more information, see the *Overview and Feature Guide* available at **dell.com/support/manuals**.

NOTE: If you have purchased a system with all the licenses pre-installed, then license management is not required.

You can perform the following licensing operations using iDRAC, RACADM, WS-MAN, and Lifecycle Controller-Remote Services for one-to-one license management, and Dell License Manager for one-to-many license management:

- View — View the current license information.
- Import — After acquiring the license, store the license in a local storage and import it into iDRAC using one of the supported interfaces. The license is imported if it passes the validation checks.

  NOTE: For a few features, a system restart is required to enable the features.
- Export — Export the installed license into an external storage device for backup or to reinstall it again after a part or motherboard replacement. The file name and format of the exported license is **<EntitlementID>.xml**.
- Delete — Delete the license that is assigned to a component if the component is missing. After the license is deleted, it is not stored in iDRAC and the base product functions are enabled.
- Replace — Replace the license to extend an evaluation license, change a license type such as an evaluation license with a purchased license, or extend an expired license.
  - An evaluation license may be replaced with an upgraded evaluation license or with a purchased license.
  - A purchased license may be replaced with an updated license or with an upgraded license.
- Learn More — Learn more about an installed license, or the licenses available for a component installed in the server.

NOTE: For the Learn More option to display the correct page, make sure that ***.dell.com** is added to the list of Trusted Sites in the Security Settings. For more information, see the Internet Explorer help documentation.

For one-to-many license deployment, you can use Dell License Manager. For more information, see the *Dell License Manager User's Guide* available at **dell.com/support/manuals**.

Importing License After Replacing Motherboard

You can use the Local iDRAC Enterprise License Installation Tool if you have recently replaced the motherboard and need to reinstall the iDRAC Enterprise license locally (with no network connectivity) and activate the dedicated NIC. This utility installs a 30-day trial iDRAC Enterprise license and allows you to reset the iDRAC to change from shared NIC to dedicated NIC.

For more information about this utility and to download this tool, click here.

License Component State or Condition and Available Operations

The following table provides the list of license operations available based on the license state or condition.

Table 1. License Operations Based on State and Condition

License/ Component state or condition	Import	Export	Delete	Replace	Learn More
Non-administrator login	No	No	No	No	Yes
Active license	Yes	Yes	Yes	Yes	Yes
Expired license	No	Yes	Yes	Yes	Yes
License installed but component missing	No	Yes	Yes	No	Yes

NOTE: In the iDRAC Web interface, on the **Licenses** page, expand the device to view the **Replace** option in the drop-down menu.

Managing Licenses Using iDRAC Web Interface

To manage the licenses using the iDRAC Web interface, go to **Overview → Server → Licenses** .

The **Licensing** page displays the licenses that are associated to devices, or the licenses that are installed but the device is not present in the system. For more information on importing, exporting, deleting, or replacing a license, see the *iDRAC Online Help*.

Managing Licenses Using RACADM

To manage licenses using RACADM, use the **license** subcommand. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Licensable Features In iDRAC8

The following table provides the iDRAC8 features that are enabled based on the license purchased.

Feature	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express for Blades	iDRAC8 Enterprise
Interfaces / Standards				
IPMI 2.0	Yes	Yes	Yes	Yes
DCMI 1.5	Yes	Yes	Yes	Yes
Web-based GUI	Yes	Yes	Yes	Yes
Racadm command line (local/remote)	Yes	Yes	Yes	Yes
SMASH-CLP (SSH-only)	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes
SSH	Yes	Yes	Yes	Yes
WSMAN	Yes	Yes	Yes	Yes
Network Time Protocol	No	Yes	Yes	Yes
Connectivity				
Shared NIC	Yes	Yes	N/A	Yes[1]
Dedicated NIC[2]	Yes	Yes	Yes	Yes[2]
VLAN tagging	Yes	Yes	Yes	Yes
IPv4	Yes	Yes	Yes	Yes
IPv6	Yes	Yes	Yes	Yes
DHCP	Yes	Yes	Yes	Yes
Dynamic DNS	Yes	Yes	Yes	Yes
OS pass-through	Yes	Yes	Yes	Yes
Front panel USB	Yes	Yes	Yes	Yes
Security				
Role-based authority	Yes	Yes	Yes	Yes

Feature	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express for Blades	iDRAC8 Enterprise
Local users	Yes	Yes	Yes	Yes
SSL encryption	Yes	Yes	Yes	Yes
IP blocking	No	Yes	Yes	Yes
Directory services (AD, LDAP)	No	No	No	Yes
Two-factor authentication (smart card)	No	No	No	Yes
Single sign-on (kerberos)	No	No	No	Yes
PK authentication (for SSH)	No	Yes	Yes	Yes
Remote Presence				
Power control	Yes	Yes	Yes	Yes
Boot control	Yes	Yes	Yes	Yes
Serial-over-LAN	Yes	Yes	Yes	Yes
Virtual Media	No	No	Yes	Yes
Virtual Folders	No	No	No	Yes
Remote File Share	No	No	No	Yes
Virtual Console	No	No	Yes	Yes
VNC connection to OS	No	No	No	Yes
Quality/bandwidth control	No	No	Yes	Yes
Virtual Console collaboration (up to six simultaneous users)	No	No	No	Yes
Virtual Console chat	No	No	No	Yes
Virtual Flash partitions	No	No	No	Yes [2,3]
Power and Thermal				

Feature	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express for Blades	iDRAC8 Enterprise
Automatic power on after loss	Yes	Yes	Yes	Yes
Real-time power meter	Yes	Yes	Yes	Yes
Power thresholds and alerts (includes headroom)	No	Yes	Yes	Yes
Real-time power graphing	No	Yes	Yes	Yes
Historical power counters	No	Yes	Yes	Yes
Power capping	No	No	No	Yes
Power Center integration	No	No	No	Yes
Temperature monitoring	Yes	Yes	Yes	Yes
Temperature graphing	No	Yes	Yes	Yes
Health Monitoring				
Full agent-free monitoring	Yes	Yes	Yes	Yes
Predictive failure monitoring	Yes	Yes	Yes	Yes
SNMPv1, v2, and v3 (traps and gets)	Yes	Yes	Yes	Yes
Email Alerting	No	Yes	Yes	Yes
Configurable thresholds	Yes	Yes	Yes	Yes
Fan monitoring	Yes	Yes	Yes	Yes
Power Supply monitoring	Yes	Yes	Yes	Yes
Memory monitoring	Yes	Yes	Yes	Yes
CPU monitoring	Yes	Yes	Yes	Yes
RAID monitoring	Yes	Yes	Yes	Yes
NIC monitoring	Yes	Yes	Yes	Yes

Feature	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express for Blades	iDRAC8 Enterprise
HD monitoring (enclosure)	Yes	Yes	Yes	Yes
Out of Band Performance Monitoring	No	No	No	Yes
Update				
Remote agent-free update	Yes	Yes	Yes	Yes
Embedded update tools	Yes	Yes	Yes	Yes
Sync with repository (scheduled updates)	No	No	No	Yes
Auto-update	No	No	No	Yes
Deployment and Configuration				
Embedded OS deployment tools	Yes	Yes	Yes	Yes
Embedded configuration tools (iDRAC Settings Utility)	Yes	Yes	Yes	Yes
Embedded configuration wizards (Lifecycle Controller wizards)	Yes	Yes	Yes	Yes
Auto-Discovery	No	Yes	Yes	Yes
Remote OS deployment	No	Yes	Yes	Yes
Embedded driver pack	Yes	Yes	Yes	Yes
Full configuration inventory	Yes	Yes	Yes	Yes
Inventory export	Yes	Yes	Yes	Yes
Remote configuration	Yes	Yes	Yes	Yes
Zero-touch configuration	No	No	No	Yes
System Retire/Repurpose	Yes	Yes	Yes	Yes
Diagnostics, Service, and Logging				

Feature	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express for Blades	iDRAC8 Enterprise
Embedded diagnostic tools	Yes	Yes	Yes	Yes
Part Replacement	No	Yes	Yes	Yes
Server Configuration Backup	No	No	No	Yes
Server Configuration Restore	Yes	Yes	Yes	Yes
Easy Restore (system configuration)	Yes	Yes	Yes	Yes
Health LED / LCD	Yes	Yes	Yes	Yes
Quick Sync (require NFC bezel)	Yes	Yes	N/A	Yes
iDRAC Direct (front USB management port)	Yes	Yes	Yes	Yes
iDRAC Service Module (iSM)	Yes	Yes	Yes	Yes
Embedded Tech Support Report	Yes	Yes	Yes	Yes
Crash screen capture	No	Yes	Yes	Yes
Crash video capture	No	No	No	Yes
Boot capture	No	No	No	Yes
Manual reset for iDRAC	Yes	Yes	Yes	Yes
Virtual NMI	Yes	Yes	Yes	Yes
OS watchdog	Yes	Yes	Yes	Yes
Embedded Health Report	Yes	Yes	Yes	Yes
System Event Log	Yes	Yes	Yes	Yes
Lifecycle Log	Yes	Yes	Yes	Yes
Work notes	Yes	Yes	Yes	Yes
Remote Syslog	No	No	No	Yes

Feature	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express for Blades	iDRAC8 Enterprise
License management	Yes	Yes	Yes	Yes

[1] Not available with blade servers.

[2] 500 series and lower rack and tower servers require a hardware card to enable this feature; this hardware is offered at additional cost.

[3] Requires vFlash SD card media.

Interfaces and Protocols to Access iDRAC

The following table lists the interfaces to access iDRAC.

NOTE: Using more than one interface at the same time may generate unexpected results.

Table 2. Interfaces and Protocols to Access iDRAC

Interface or Protocol	Description
iDRAC Settings Utility	Use the iDRAC Settings utility to perform pre-OS operations. It has a subset of the features that are available in iDRAC Web interface along with other features. To access iDRAC Settings utility, press <F2> during boot and then click **iDRAC Settings** on the **System Setup Main Menu** page.
iDRAC Web Interface	Use the iDRAC Web interface to manage iDRAC and monitor the managed system. The browser connects to the Web server through the HTTPS port. Data streams are encrypted using 128-bit SSL to provide privacy and integrity. Any connection to the HTTP port is redirected to HTTPS. Administrators can upload their own SSL certificate through an SSL CSR generation process to secure the Web server. The default HTTP and HTTPS ports can be changed. The user access is based on user privileges.
RACADM	Use this command line utility to perform iDRAC and server management. You can use RACADM locally and remotely. • Local RACADM command line interface runs on the managed systems that have Server Administrator installed. Local RACADM communicates with iDRAC through its in-band IPMI host interface. Since it is installed on the local managed system, users are required to log in to the operating system to run this utility. A user must have a full administrator privilege or be a root user to use this utility. • Remote RACADM is a client utility that runs on a management station. It uses the out-of-band network interface to run RACADM commands on the managed system and uses the HTTPs channel. The **–r** option runs the RACADM command over a network. • Firmware RACADM is accessible by logging in to iDRAC using SSH or telnet. You can run the firmware RACADM commands without specifying the iDRAC IP, user name, or password. • You do not have to specify the iDRAC IP, user name, or password to run the firmware RACADM commands. After you enter the RACADM prompt, you can directly run the commands without the racadm prefix.

Interface or Protocol	Description
Server LCD Panel/ Chassis LCD Panel	Use the LCD on the server front panel to: • View alerts, iDRAC IP or MAC address, user programmable strings. • Set DHCP • Configure iDRAC static IP settings. For blade servers, the LCD is on the chassis front panel and is shared between all the blades. To reset iDRAC without rebooting the server, press and hold the System Identification button for 16 seconds.
CMC Web Interface	In addition to monitoring and managing the chassis, use the CMC Web interface to: • View the status of a managed system • Update iDRAC firmware • Configure iDRAC network settings • Log in to iDRAC Web interface • Start, stop, or reset the managed system • Update BIOS, PERC, and supported network adapters
Lifecycle Controller	Use Lifecycle Controller to perform iDRAC configurations. To access Lifecycle Controller, press <F10> during boot and go to **System Setup → Advanced Hardware Configuration → iDRAC Settings**. For more information, see *Lifecycle Controller User's Guide* available at **dell.com/support/manuals**.
Telnet	Use Telnet to access iDRAC where you can run RACADM and SMCLP commands. For details about RACADM, see *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**. For details about SMCLP, see Using SMCLP. **NOTE:** Telnet is not a secure protocol and is disabled by default. Telnet transmits all data, including passwords in plain text. When transmitting sensitive information, use the SSH interface.
SSH	Use SSH to run RACADM and SMCLP commands. It provides the same capabilities as the Telnet console using an encrypted transport layer for higher security. The SSH service is enabled by default on iDRAC. The SSH service can be disabled in iDRAC. iDRAC only supports SSH version 2 with DSA and the RSA host key algorithm. A unique 1024-bit DSA and 1024-bit RSA host key is generated when you power-up iDRAC for the first time.
IPMITool	Use the IPMITool to access the remote system's basic management features through iDRAC. The interface includes local IPMI, IPMI over LAN, IPMI over Serial, and Serial over LAN. For more information on IPMITool, see the *Dell OpenManage Baseboard Management Controller Utilities User's Guide* at **dell.com/support/manuals**. **NOTE:** IPMI version 1.5 is not supported.

Interface or Protocol	Description
VMCLI	Use the Virtual Media Command Line Interface (VMCLI) to access a remote media through the management station and deploy operating systems on multiple managed systems.
SMCLP	Use Server Management Workgroup Server Management-Command Line Protocol (SMCLP) to perform systems management tasks. This is available through SSH or Telnet. For more information about SMCLP, see Using SMCLP.
WS-MAN	The LC-Remote Services is based on the WS-Management protocol to do one-to-many systems management tasks. You must use WS-MAN client such as WinRM client (Windows) or the OpenWSMAN client (Linux) to use the LC-Remote Services functionality. You can also use Power Shell and Python to script to the WS-MAN interface. Web Services for Management (WS-Management) is a Simple Object Access Protocol (SOAP)–based protocol used for systems management. iDRAC uses WS–Management to convey Distributed Management Task Force (DMTF) Common Information Model (CIM)–based management information. The CIM information defines the semantics and information types that can be modified in a managed system. The data available through WS-Management is provided by iDRAC instrumentation interface mapped to the DMTF profiles and extension profiles. For more information, see the following: • Lifecycle Controller-Remote Services User's Guide available at **dell.com/support/manuals**. • Lifecycle Controller Integration Best Practices Guide available at **dell.com/support/manuals**. • Lifecycle Controller page on Dell TechCenter — **delltechcenter.com/page/Lifecycle+Controller** • Lifecycle Controller WS-Management Script Center — **delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller** • MOFs and Profiles — **delltechcenter.com/page/DCIM.Library** • DTMF Web site — **dmtf.org/standards/profiles/**

iDRAC Port Information

The following ports are required to remotely access iDRAC through firewalls. These are the default ports iDRAC listens to for connections. Optionally, you can modify most of the ports. To do this, see Configuring Services.

Table 3. Ports iDRAC Listens for Connections

Port Number	Function
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS

Port Number	Function
623	RMCP/RMCP+
161*	SNMP
5900*	Virtual Console keyboard and mouse redirection, Virtual Media, Virtual Folders, and Remote File Share
5901	VNC When VNC feature is enabled, the port 5901 opens.

* Configurable port

The following table lists the ports that iDRAC uses as a client.

Table 4. Ports iDRAC Uses as Client

Port Number	Function
25*	SMTP
53	DNS
68	DHCP-assigned IP address
69	TFTP
162*	SNMP trap
445	Common Internet File System (CIFS)
636	LDAP Over SSL (LDAPS)
2049	Network File System (NFS)
123	Network Time Protocol (NTP)
3269	LDAPS for global catalog (GC)

* Configurable port

Other Documents You May Need

In addition to this guide, the following documents available on the Dell Support website at **dell.com/support/manuals** provides additional information about the setup and operation of iDRAC in your system.

- The *iDRAC Online Help* provides detailed information about the fields available on the iDRAC Web interface and the descriptions for the same. You can access the online help after you install iDRAC.

- The *iDRAC8 RACADM Command Line Interface Reference Guide* provides information about the RACADM sub-commands, supported interfaces, and iDRAC property database groups and object definitions.
- The *iDRAC RACADM Support Matrix* provides the list of sub commands and objects that are applicable for a particular iDRAC version.
- The *Systems Management Overview Guide* provides brief information about the various software available to perform systems management tasks.
- The *Dell Lifecycle Controller Graphical User Interface For 13th Generation Dell PowerEdge Servers User's Guide* provides information on using Lifecycle Controller Graphical User Interface (GUI).
- The *Dell Lifecycle Controller Remote Services For 13th Generation Dell PowerEdge Servers Quick Start Guide* provides an overview of the Remote Services capabilities, information on getting started with Remote Services, Lifecycle Controller API, and provides references to various resources on Dell Tech Center.
- The *Dell Remote Access Configuration Tool User's Guide* provides information on how to use the tool to discover iDRAC IP addresses in your network and perform one-to-many firmware updates and active directory configurations for the discovered IP addresses.
- The *Dell Systems Software Support Matrix* provides information about the various Dell systems, the operating systems supported by these systems, and the Dell OpenManage components that can be installed on these systems.
- The *iDRAC Service Module Installation Guide* provides information to install the iDRAC Service Module.
- The *Dell OpenManage Server Administrator Installation Guide* contains instructions to help you install Dell OpenManage Server Administrator.
- The *Dell OpenManage Management Station Software Installation Guide* contains instructions to help you install Dell OpenManage management station software that includes Baseboard Management Utility, DRAC Tools, and Active Directory Snap-In.
- The *Dell OpenManage Baseboard Management Controller Management Utilities User's Guide* has information about the IPMI interface.
- The *Release Notes* provides last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians.
- The *Glossary* provides information about the terms used in this document.

The following system documents are available to provide more information:

- The *iDRAC Overview and Feature Guide* provides information about iDRAC, its licensable features, and license upgrade options.
- The safety instructions that came with your system provide important safety and regulatory information. For additional regulatory information, see the Regulatory Compliance home page at **dell.com/regulatory_compliance**. Warranty information may be included within this document or as a separate document.
- The *Rack Installation Instructions* included with your rack solution describe how to install your system into a rack.
- The *Getting Started Guide* provides an overview of system features, setting up your system, and technical specifications.
- The *Owner's Manual* provides information about system features and describes how to troubleshoot the system and install or replace system components.

Related Links

Contacting Dell

Accessing documents from Dell support site

Social Media Reference

To know more about the product, best practices, and information about Dell solutions and services, you can access the social media platforms such as Dell TechCenter. You can access blogs, forums, whitepapers, how-to videos, and so on from the iDRAC wiki page at **www.delltechcenter.com/idrac**.

For iDRAC and other related firmware documents, see **www.dell.com/esmmanuals**.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to **dell.com/support**.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.

Accessing documents from Dell support site

You can access the required documents in one of the following ways:

- Using the following links:
  - For all Enterprise Systems Management documents — **dell.com/softwaresecuritymanuals**
  - For Enterprise Systems Management documents — **dell.com/openmanagemanuals**
  - For Remote Enterprise Systems Management documents — **dell.com/esmmanuals**
  - For OpenManage Connections Enterprise Systems Management documents — **dell.com/OMConnectionsEnterpriseSystemsManagement**
  - For Serviceability Tools documents — **dell.com/serviceabilitytools**
  - For Client Systems Management documents — **dell.com/clientsystemsmanagement**
  - For OpenManage Connections Client Systems Management documents — **dell.com/connectionsclientsystemsmanagement**
- From the Dell Support site:
  a. Go to **dell.com/support/home**.
  b. Under **General support** section, click **Software & Security**.
  c. In the **Software & Security** group box, click the required link from the following:
     - **Enterprise Systems Management**
     - **Remote Enterprise Systems Management**
     - **Serviceability Tools**

- **Client Systems Management**
- **Connections Client Systems Management**

d. To view a document, click the required product version.

- Using search engines:
  - Type the name and version of the document in the search box.

2

Logging into iDRAC

You can log in to iDRAC as an iDRAC user, as a Microsoft Active Directory user, or as a Lightweight Directory Access Protocol (LDAP) user. The default user name and password is root and calvin, respectively. You can also log in using Single Sign-On or Smart Card.

NOTE: You must have Login to iDRAC privilege to log in to iDRAC.

Related Links

Logging into iDRAC as Local User, Active Directory User, or LDAP User
Logging into iDRAC Using Smart Card
Logging into iDRAC Using Single Sign-on
Changing Default Login Password

Logging into iDRAC as Local User, Active Directory User, or LDAP User

Before you log in to iDRAC using the Web interface, make sure that you have configured a supported Web browser and the user account is created with the required privileges.

NOTE: The user name is *not* case-sensitive for an Active Directory user. The password is case-sensitive for all users.

NOTE: In addition to Active Directory, openLDAP, openDS, Novell eDir, and Fedora based directory services are supported.

To log in to iDRAC as local user, Active Directory user, or LDAP user:

1. Open a supported Web browser.
2. In the **Address** field, type `https://[iDRAC-IP-address]` and press <Enter>.

   NOTE: If the default HTTPS port number (port 443) was changed, enter: `https://[iDRAC-IP-address]:[port-number]` where, `[iDRAC-IP-address]` is the iDRAC IPv4 or IPv6 address and `[port-number]` is the HTTPS port number.

   The **Login** page is displayed.
3. For a local user:
   - In the **Username** and **Password** fields, enter your iDRAC user name and password.
   - From the **Domain** drop-down menu, select **This iDRAC**.
4. For an Active Directory user, in the **Username** and **Password** fields, enter the Active Directory user name and password. If you have specified the domain name as a part of the username, select **This iDRAC** from the drop-down menu. The format of the user name can be: <domain>\<username>, <domain>/<username>, or <user>@<domain>.

   For example, dell.com\john_doe, or JOHN_DOE@DELL.COM.

If the domain is not specified in the user name, select the Active Directory domain from the **Domain** drop-down menu.

5. For an LDAP user, in the **Username** and **Password** fields, enter your LDAP user name and password. Domain name is not required for LDAP login. By default, **This iDRAC** is selected in the drop-down menu.
6. Click **Submit**. You are logged into iDRAC with the required user privileges.

   If you log in with Configure Users privileges and the default account credentials, and if the default password warning feature is enabled, the **Default Password Warning** page is displayed allowing you to easily change the password.

Related Links

Configuring User Accounts and Privileges
Changing Default Login Password
Configuring Supported Web Browsers

Logging into iDRAC Using Smart Card

You can log in to iDRAC using a smart card. Smart cards provide Two Factor Authentication (TFA) that provide two-layers of security:

- Physical smart card device.
- Secret code such as, a password or a PIN.

Users must verify their credentials using the smart card and the PIN.

Related Links

Logging Into iDRAC as a Local User Using Smart Card
Logging Into iDRAC as an Active Directory User Using Smart Card

Logging Into iDRAC as a Local User Using Smart Card

Before you log in as a local user using Smart Card, make sure to:

- Upload user smart card certificate and the trusted Certificate Authority (CA) certificate to iDRAC
- Enable smart card logon.

The iDRAC Web interface displays the smart card logon page for users who are configured to use the smart card.

NOTE: Depending on the browser settings, you are prompted to download and install the smart card reader ActiveX plug-in when using this feature for the first time.

To log in to iDRAC as a local user using smart card:

1. Access the iDRAC Web interface using the link `https://[IP address]`.

   The **iDRAC Login** page is displayed prompting you to insert the smart card.

   NOTE: If the default HTTPS port number (port 443) has been changed, type: `https://[IP address]:[port number]` where, `[IP address]` is the IP address for the iDRAC and `[port number]` is the HTTPS port number.
2. Insert the Smart Card into the reader and click **Login**.

   A prompt is displayed for the Smart Card's PIN. A password in not required.

3. Enter the Smart Card PIN for local Smart Card users.
   You are logged into the iDRAC.

   NOTE: If you are a local user for whom **Enable CRL check for Smart Card Logon** is enabled, iDRAC attempts to download the CRL and checks the CRL for the user's certificate. The login fails if the certificate is listed as revoked in the CRL or if the CRL cannot be downloaded for some reason.

Related Links

Enabling or Disabling Smart Card Login
Configuring iDRAC Smart Card Login for Local Users

Logging Into iDRAC as an Active Directory User Using Smart Card

Before you log in as a Active Directory user using Smart Card, make sure to:

- Upload a Trusted Certificate Authority (CA) certificate (CA-signed Active Directory certificate) to iDRAC.
- Configure the DNS server.
- Enable Active Directory login.
- Enable Smart Card login.

To log in to iDRAC as an Active Directory user using smart card:

1. Log in to iDRAC using the link `https://[IP address]`.
   The **iDRAC Login** page is displayed prompting you to insert the Smart Card.

   NOTE: If the default HTTPS port number (port 443) is changed, type: `https://[IP address]:[port number]` where, `[IP address]` is the iDRAC IP address and `[port number]` is the HTTPS port number.
2. Insert the Smart Card and click **Login**.
   The **PIN** pop-up is displayed.
3. Enter the PIN and click **Submit**.
   You are logged in to iDRAC with your Active Directory credentials.

   NOTE:

   If the smart card user is present in Active Directory, an Active Directory password is not required.

Related Links

Enabling or Disabling Smart Card Login
Configuring iDRAC Smart Card Login for Active Directory Users

Logging into iDRAC Using Single Sign-on

When Single Sign-On (SSO) is enabled, you can log in to iDRAC without entering your domain user authentication credentials, such as user name and password.

Related Links

Configuring iDRAC SSO Login for Active Directory Users

Logging into iDRAC SSO Using iDRAC Web Interface

Before logging into iDRAC using Single Sign-on, make sure that:

- You have logged into your system using a valid Active Directory user account.
- Single Sign-On option is enabled during Active Directory configuration.

To login to iDRAC using Web interface:

1. Log in to your management station using a valid Active Directory account.
2. In a Web browser, type `https://[FQDN address]`

   NOTE: If the default HTTPS port number (port 443) has been changed, type: `https://[FQDN address]:[port number]` where, `[FQDN address]` is the iDRAC FQDN (iDRACdnsname.domain. name) and `[port number]` is the HTTPS port number.

   NOTE: If you use IP address instead of FQDN, SSO fails.

   iDRAC logs you in with appropriate Microsoft Active Directory privileges, using your credentials that were cached in the operating system when you logged in using a valid Active Directory account.

Logging into iDRAC SSO Using CMC Web Interface

Using the SSO feature, you can launch iDRAC Web interface from CMC Web interface. A CMC user has the CMC user privileges when launching iDRAC from CMC. If the user account is present in CMC and not in iDRAC, the user can still launch iDRAC from CMC.

If iDRAC network LAN is disabled (LAN Enabled = No), SSO is not available.

If the server is removed from the chassis, iDRAC IP address is changed, or there is a problem in iDRAC network connection, the option to Launch iDRAC is grayed-out in the CMC Web interface.

For more information, see the *Chassis Management Controller User's Guide* available at **dell.com/support/manuals**.

Accessing iDRAC Using Remote RACADM

You can use remote RACADM to access iDRAC using RACADM utility.

For more information, see the *RACADM Reference Guide for iDRAC and CMC* available at **dell.com/support/manuals**.

If the management station has not stored the iDRAC's SSL certificate in its default certificate storage, a warning message is displayed when you run the RACADM command. However, the command is executed successfully.

NOTE: The iDRAC certificate is the certificate iDRAC sends to the RACADM client to establish the secure session. This certificate is either issued by a CA or self-signed. In either case, if the management station does not recognize the CA or signing authority, a warning is displayed.

Related Links

Validating CA Certificate To Use Remote RACADM on Linux

Validating CA Certificate To Use Remote RACADM on Linux

Before running remote RACADM commands, validate the CA certificate that is used for secure communications.

To validate the certificate for using remote RACADM:

1. Convert the certificate in DER format to PEM format (using openssl command line tool):

   ```
   openssl x509 -inform pem -in [yourdownloadedderformatcert.crt] -outform pem
   -out [outcertfileinpemformat.pem] -text
   ```
2. Find the location of the default CA certificate bundle on the management station. For example, for RHEL5 64-bit, it is **/etc/pki/tls/cert.pem**.
3. Append the PEM formatted CA certificate to the management station CA certificate.

   For example, use the `cat command: - cat testcacert.pem >> cert.pem`
4. Generate and upload the server certificate to iDRAC.

Accessing iDRAC Using Local RACADM

For information to access iDRAC using local RACADM, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Accessing iDRAC Using Firmware RACADM

You can use SSH or Telnet interfaces to access iDRAC and run firmware RACADM commands. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Accessing iDRAC Using SMCLP

SMCLP is the default command line prompt when you log in to iDRAC using Telnet or SSH. For more information, see Using SMCLP.

Logging in to iDRAC Using Public Key Authentication

You can log into the iDRAC over SSH without entering a password. You can also send a single RACADM command as a command line argument to the SSH application. The command line options behave similar to remote RACADM since the session ends after the command is completed.

For example:

Logging in:

```
ssh username@<domain>
```

or

```
ssh username@<IP_address>
```

where `IP_address` is the IP address of the iDRAC.

Sending RACADM commands:

```
ssh username@<domain> racadm getversion
```

```
ssh username@<domain> racadm getsel
```

Related Links

Using Public Key Authentication For SSH

Multiple iDRAC Sessions

The following table provides the list of multiple iDRAC sessions that are possible using the various interfaces.

Table 5. Multiple iDRAC Sessions

Interface	Number of Sessions
iDRAC Web Interface	6
Remote RACADM	4
Firmware RACADM / SMCLP	SSH - 2 Telnet - 2 Serial - 1

Changing Default Login Password

The warning message that allows you to change the default password is displayed if:

- You log in to iDRAC with Configure User privilege.
- Default password warning feature is enabled.
- Credentials for any currently enabled account are root/calvin.

A warning message is also displayed when you log in to iDRAC using SSH, Telnet, remote RACADM, or the Web interface. For Web interface, SSH, and Telnet, a single warning message is displayed for each session. For remote RACADM, the warning message is displayed for each command.

Related Links

Enabling or Disabling Default Password Warning Message

Changing Default Login Password Using Web Interface

When you log in to iDRAC Web interface, if the **Default Password Warning** page is displayed, you can change the password. To do this:

1. Select the **Change Default Password** option.
2. In the **New Password** field, enter the new password.
   The maximum characters for the password are 20. The characters are masked. The following characters are supported:
   - 0-9
   - A-Z
   - a-z
   - Special characters: +, &, ?, >, -, }, |, ., !, (, ', ,, _,[, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, I, \
3. In the **Confirm Password** field, enter the password again.
4. Click **Continue**. The new password is configured and you are logged in to iDRAC.

NOTE: **Continue** is enabled only if the passwords entered in the **New Password** and **Confirm Password** fields match.

For information about the other fields, see the *iDRAC Online Help*.

Changing Default Login Password Using RACADM

To change the password, run the following RACADM command:

```
racadm set iDRAC.Users.<index>.Password <Password>
```

where, `<index>` is a value from 1 to 16 (indicates the user account) and `<password>` is the new user—defined password.

For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide*.

Changing Default Login Password Using iDRAC Settings Utility

To change the default login password using iDRAC Settings Utility:

1. In the iDRAC Settings utility, go to **User Configuration**.
   The **iDRAC Settings.User Configuration** page is displayed.
2. In the **Change Password** field, enter the new password.
3. Click **Back**, click **Finish**, and then click **Yes**.
   The details are saved.

Enabling or Disabling Default Password Warning Message

You can enable or disable the display of the default password warning message. To do this, you must have Configure Users privilege.

Enabling or Disabling Default Password Warning Message Using Web Interface

To enable or disable the display of the default password warning message after logging in to iDRAC:

1. Go to **Overview → iDRAC Settings → User Authentication → Local Users** .
   The **Users** page is displayed.
2. In the **Default Password Warning** section, select **Enable**, and then click **Apply** to enable the display of the **Default Password Warning** page when you log in to iDRAC. Else, select **Disable**.
   Alternatively, if this feature is enabled and you do not want to display the warning message for subsequent log-ins, on the **Default Password Warning** page, select the **Do not show this warning again** option, and then click **Apply**.

Enabling or Disabling Warning Message to Change Default Login Password Using RACADM

To enable the display of the warning message to change the default login password using RACADM, use `idrac.tuning.DefaultCredentialWarning` object. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

3

Setting Up Managed System and Management Station

To perform out-of-band systems management using iDRAC, you must configure iDRAC for remote accessibility, set up the management station and managed system, and configure the supported Web browsers.

NOTE: In case of blade servers, install CMC and I/O modules in the chassis and physically install the system in the chassis before performing the configurations.

Both iDRAC Express and iDRAC Enterprise ship from the factory with a default static IP address. However, Dell also offers two options-Auto-discovery that allows you to access the iDRAC, and remotely configure your server, and DHCP:

- Auto Discovery — Use this option if you have a provisioning server installed in your data center environment. A provisioning server manages and automates the deployment or upgrade of an operating system and applications to a Dell PowerEdge server. By enabling Auto Discovery, the servers — upon first boot — searches for a provisioning server to take control and begin the automated deployment or update process.
- DHCP — Use this option if you have a Dynamic Host Configuration Protocol (DHCP) server installed in the data center environment. The DHCP server automatically assigns the IP address, gateway, and subnet mask for iDRAC.

You can enable Auto-discovery or DHCP when you place an order for the server. There is no charge to enable either of these features. Only one setting is possible.

Related Links

Setting Up iDRAC IP Address
Setting Up Managed System
Updating Device Firmware
Rolling Back Device Firmware
Setting Up Management Station
Configuring Supported Web Browsers

Setting Up iDRAC IP Address

You must configure the initial network settings based on your network infrastructure to enable the communication to and from iDRAC. You can set up the IP address using one of the following interfaces:

- iDRAC Settings utility
- Lifecycle Controller (see *Lifecycle Controller User's Guide*)
- Dell Deployment Toolkit (see *Dell Deployment Toolkit User's Guide*)
- Chassis or Server LCD panel (see the system's *Hardware Owner's Manual*)

NOTE: In case of blade servers, you can configure the network setting using the Chassis LCD panel only during initial configuration of CMC. After the chassis is deployed, you cannot reconfigure iDRAC using the Chassis LCD panel.

- CMC Web interface (see *Dell Chassis Management Controller Firmware User's Guide)*

In case of rack and tower servers, you can set up the IP address or use the default iDRAC IP address 192.168.0.120 to configure initial network settings, including setting up DHCP or the static IP for iDRAC.

In case of blade servers, the iDRAC network interface is disabled by default.

After you configure iDRAC IP address:

- Make sure to *change the default user name and password after setting up the iDRAC IP address*.
- Access it through any of the following interfaces:
  - iDRAC Web interface using a supported browser (Internet Explorer, Firefox, Chrome, or Safari)
  - Secure Shell (SSH) — Requires a client such as PuTTY on Windows. SSH is available by default in most of the Linux systems and hence does not require a client.
  - Telnet (must be enabled, since it is disabled by default)
  - IPMITool (uses IPMI command) or shell prompt (requires Dell customized installer in Windows or Linux, available from *Systems Management Documentation and Tools* DVD or **support.dell.com**)

Related Links

Setting Up iDRAC IP Using iDRAC Settings Utility
Setting Up iDRAC IP Using CMC Web Interface
Enabling Auto-discovery
Configuring Servers and Server Components Using Auto Config

Setting Up iDRAC IP Using iDRAC Settings Utility

To set up the iDRAC IP address:

1. Turn on the managed system.
2. Press <F2> during Power-on Self-test (POST).
3. In the **System Setup Main Menu** page, click **iDRAC Settings**.
   The **iDRAC Settings** page is displayed.
4. Click **Network**.
   The **Network** page is displayed.
5. Specify the following settings:
   - Network Settings
   - Common Settings
   - IPv4 Settings
   - IPv6 Settings
   - IPMI Settings
   - VLAN Settings
6. Click **Back**, click **Finish**, and then click **Yes**.
   The network information is saved and the system reboots.

Related Links

Network Settings
Common Settings

IPv4 Settings
IPv6 Settings
IPMI Settings
VLAN Settings

Network Settings

To configure the Network Settings:

NOTE: For information about the options, see the *iDRAC Settings Utility Online Help*.

1. Under **Enable NIC**, select the **Enabled** option.
2. From the **NIC Selection** drop-down menu, select one of the following ports based on the network requirement:
   - Dedicated — Enables the remote access device to use the dedicated network interface available on the Remote Access Controller (RAC). This interface is not shared with the host operating system and routes the management traffic to a separate physical network, enabling it to be separated from the application traffic.

     This option implies that iDRAC's dedicated network port routes its traffic separately from the Server's LOM or NIC ports. With respect to managing network traffic, the Dedicated option allows iDRAC to be assigned an IP address from the same subnet or different subnet in comparison to the IP addresses assigned to the Host LOM or NICs.

     NOTE: The option is available only on rack or tower systems.
   - LOM1
   - LOM2
   - LOM3
   - LOM4

     NOTE: In the case of rack and tower servers, two LOM options (LOM1 and LOM2) or all four LOM options are available depending on the server model. Blade servers do not use LOM for iDRAC communication.
3. From the **Failover Network** drop-down menu, select one of the remaining LOMs. If a network fails, the traffic is routed through the failover network.

   NOTE: If you have selected **Dedicated** in **NIC Selection** drop-down menu, the option is grayed-out .

   For example, to route the iDRAC network traffic through LOM2 when LOM1 is down, select **LOM1** for **NIC Selection** and **LOM2** for **Failover Network**.
4. Under **Auto Negotiation**, select **On** if iDRAC must automatically set the duplex mode and network speed. This option is available only for dedicated mode. If enabled, iDRAC sets the network speed to 10, 100, or 1000 Mbps based on the network speed.
5. Under **Network Speed**, select either 10 Mbps or100 Mbps.

   NOTE: You cannot manually set the Network Speed to 1000 Mbps. This option is available only if **Auto Negotiation** option is enabled.
6. Under **Duplex Mode**, select **Half Duplex** or **Full Duplex** option.

   NOTE: If you enable **Auto Negotiation**, this option is grayed-out.

Common Settings

If network infrastructure has DNS server, register iDRAC on the DNS. These are the initial settings requirements for advanced features such as Directory services——Active Directory or LDAP, Single Sign On, and smart card.

To register iDRAC:

1. Enable **Register DRAC on DNS**.
2. Enter the **DNS DRAC Name**.
3. Select **Auto Config Domain Name** to automatically acquire domain name from DHCP. Else, provide the **DNS Domain Name**.

IPv4 Settings

To configure the IPv4 settings:

1. Select **Enabled** option under **Enable IPv4** .
2. Select **Enabled** option under **Enable DHCP** , so that DHCP can automatically assign the IP address, gateway, and subnet mask to iDRAC. Else, select **Disabled** and enter the values for:
   - Static IP Address
   - Static Gateway
   - Static Subnet Mask
3. Optionally, enable **Use DHCP to obtain DNS server address**, so that the DHCP server can assign the **Static Preferred DNS Server** and **Static Alternate DNS Server**. Else, enter the IP addresses for **Static Preferred DNS Server** and **Static Alternate DNS Server**.

IPv6 Settings

Alternately, based on the infrastructure setup, you can use IPv6 address protocol.

To configure the IPv6 settings:

1. Select **Enabled** option under **Enable IPv6**.
2. For the DHCPv6 server to automatically assign the IP address, gateway, and subnet mask to iDRAC, select **Enabled** option under **Enable Auto-configuration**. If enabled, the static values are disabled. Else, proceed to the next step to configure using the static IP address.
3. In the **Static IP Address 1** box, enter the static IPv6 address.
4. In the **Static Prefix Length** box, enter a value between 0 and 128.
5. In the **Static Gateway** box, enter the gateway address.
6. If you are using DHCP, enable **DHCPv6 to obtain DNS Server addresses** to obtain Primary and Secondary DNS server addresses from DHCPv6 server. Else, select **Disabled** and do the following:
   - In the **Static Preferred DNS Server** box, enter the static DNS server IPv6 address.
   - In the **Static Alternate DNS Server** box, enter the static alternate DNS server.

IPMI Settings

To enable the IPMI Settings:

1. Under **Enable IPMI Over LAN**, select **Enabled**.
2. Under **Channel Privilege Limit**, select **Administrator**, **Operator**, or **User**.
3. In the **Encryption Key** box, enter the encryption key in the format 0 to 40 hexadecimal characters (without any blanks characters.) The default value is all zeros.

VLAN Settings

You can configure iDRAC into the VLAN infrastructure. To configure VLAN Settings:

1. Under **Enable VLAN ID**, select **Enabled**.
2. In the **VLAN ID** box, enter a valid number from 1 to 4094.
3. In the **Priority** box, enter a number from 0 to 7 to set the priority of the VLAN ID.

   NOTE: After enabling VLAN, the idrac IP is not accessible for sometime.

Setting Up iDRAC IP Using CMC Web Interface

To set up the iDRAC IP address using CMC Web interface:

NOTE: You must have Chassis Configuration Administrator privilege to set up iDRAC network settings from CMC.

1. Log in to CMC Web interface.
2. Go to **Server Overview → Setup → iDRAC**.

   The **Deploy iDRAC** page is displayed.
3. Under **iDRAC Network Settings**, select **Enable LAN** and other network parameters as per requirements. For more information, see *CMC online help*.
4. For additional network settings specific to each blade server, go to **Server Overview → <server name>**.

   The **Server Status** page is displayed.
5. Click **Launch iDRAC** and go to **Overview → iDRAC Settings → Network**.
6. In the **Network** page, specify the following settings:
   - Network Settings
   - Common Settings
   - IPV4 Settings
   - IPV6 Settings
   - IPMI Settings
   - VLAN Settings

   NOTE: For more information, see *iDRAC Online Help*.
7. To save the network information, click **Apply**.

   For more information, see the *Chassis Management Controller User's Guide* available at **dell.com/support/manuals**.

Enabling Auto-discovery

The auto-discovery feature allows newly installed servers to automatically discover the remote management console that hosts the provisioning server. The *provisioning server* provides custom administrative user credentials to iDRAC, so that the unprovisioned server can be discovered and managed from the management console. For more information about auto-discovery, see the *Lifecycle Controller Remote Services User's Guide* available at **dell.com/support/manuals**.

Auto-discovery works with a static IP. DHCP, DNS server, or the default DNS host name discovers the provisioning server. If DNS is specified, the provisioning server IP is retrieved from DNS and the DHCP settings are not required. If the provisioning server is specified, discovery is skipped so neither DHCP nor DNS is required.

You can enable auto-discovery using iDRAC Settings Utility or using Lifecycle Controller. For information on using Lifecycle Controller, see *Lifecycle Controller User's Guide* available at **dell.com/support/manuals**.

If auto-discovery feature is not enabled on the factory-shipped system, the default administrator account (user name as root and password as calvin) is enabled. Before enabling auto-discovery, make sure to disable this administrator account. If the auto-discovery in Lifecycle Controller is enabled, all the iDRAC user accounts are disabled until the provisioning server is *discovered*.

To enable auto-discovery using iDRAC Settings utility:

1. Turn on the managed system.
2. During POST, press <F2 >, and go to **iDRAC Settings → Remote Enablement**.
   The **iDRAC Settings Remote Enablement** page is displayed.
3. Enable auto-discovery, enter the provisioning server IP address, and click **Back**.

   NOTE: Specifying the provisioning server IP is optional. If it is not set, it is discovered using DHCP or DNS settings (step 7).
4. Click **Network**.
   The **iDRAC Settings Network** page is displayed.
5. Enable NIC.
6. Enable IPv4.

   NOTE: IPv6 is not supported for auto-discovery.
7. Enable DHCP and get the domain name, DNS server address, and DNS domain name from DHCP.

   NOTE: Step 7 is optional if the provisioning server IP address (step 3) is provided.

Configuring Servers and Server Components Using Auto Config

The Auto Config feature allows you to configure and provision all the components in a server (example, iDRAC, PERC, and RAID) in a single operation by automatically importing an XML configuration file. All the configurable parameters are specified in the XML file. The DHCP server that assigns the IP address also provides the XML file details to configure the iDRAC.

You can create the XML file based on the service tag of the servers or create a generic XML file that you can use to configure all iDRACs serviced by the DHCP server. This XML file is stored in a shared location (CIFS or NFS) that is accessible by the DHCP server and iDRAC(s) of the server being configured. The DHCP server uses a DHCP server option to specify the XML file name, XML file location, and the user credentials to access the file location.

When the iDRAC or CMC obtains an IP address from the DHCP server, the XML file is used to configure the devices. Auto-config is invoked only after the iDRAC gets its IP address from the DHCP server. If it does not get a response or an IP address from the DHCP server, then auto-config is not invoked.

NOTE:
- You can enable Auto Config only if **DHCPv4** and the **Enable IPv4** options are enabled.
- Auto Config and auto-discovery features are mutually exclusive. You must disable auto-discovery for the Auto Config feature to work.

If all the Dell PowerEdge servers in the DHCP server pool are of the same Model type and number, then a single xml file (**config.xml**) is required. (This is the default XML file name.)

You can configure individual servers using different configuration files mapped using individual host names. In an environment that has different servers with specific requirements, you can use different XML filenames to distinguish each server. For example, if there are two servers – a PowerEdge R720 and a PowerEdge R520, you must use two XML files, **R720-config.xml** and **R520-config.xml**.

The server-config-agent uses the rules in the following sequence to determine which XML file(s) on the File Share to apply for each iDRAC/PowerEdge server:

1. The filename specified in DHCP option 60.
2. **<ServiceTag>-config.xml** - If a filename is not specified in DHCP option 60, use the system service tag to uniquely identify the XML config file for the system. For example, **<servicetag>-config.xml**
3. **<Model number>-config.xml** - If the option 60 filename is not specified and the **<ServiceTag>-config.xml** file is not found, then use the system Model number as the basis for the XML config file name to use. For example, **R520-config.xml**.
4. **config.xml** – If the option 60 filename, service tag-based, and model number—based files are not available, use the default **config.xml** file.

Related Links

Auto Config Sequence
DHCP Options
Enabling Auto Config Using iDRAC Web Interface
Enabling Auto Config Using RACADM

Auto Config Sequence

1. Create or modify the XML file that configures the attributes of Dell servers.
2. Place the XML file in a share location that is accessible by the DHCP server and all the Dell servers that are assigned IP address from the DHCP server.
3. Specify the XML file location in vendor-option 43 field of DHCP server.
4. The iDRAC as part of acquiring IP address advertises vendor class identifier iDRAC. (Option 60)
5. The DHCP server matches the vendor class to the vendor option in the **dhcpd.conf** file and sends the XML file location and XML file name to the iDRAC.
6. The iDRAC processes the XML file and configures all the attributes listed in the file

DHCP Options

DHCPv4 allows a large number of globally defined parameters to be passed to the DHCP clients. Each parameter is known as a DHCP option. Each option is identified with an option tag, which is a 1 byte value. Option tags 0 and 255 are reserved for padding and end of options, respectively. All other values are available for defining options.

The DHCP Option 43 is used to send information from the DHCP server to the DHCP client. The option is defined as a text string. This text string is set to contain the values of the XML filename, share location and the credentials to access the location. For example,

```
option myname code 43 = text;
option myname "-l 10.35.175.88://xmlfiles –f dhcpProv.xml -u root -p calvin";
```

where, -l is the location of the Remote File Share and –f is the file name in the string along with the credentials to the Remote File Share. In this example, *root* and *calvin* are the username and password to the RFS.

The DHCP Option 60 identifies and associates a DHCP client with a particular vendor. Any DHCP server configured to take action based on a client's vendor ID should have Option 60 and Option 43 configured.

With Dell PowerEdge servers, the iDRAC identifies itself with vendor ID: *iDRAC*. Therefore, you must add a new 'Vendor Class' and create a 'scope option' under it for 'code 60,' and then enable the new scope option for the DHCP server.

Related Links

Configuring Option 43 on Windows
Configuring Option 60 on Windows
Configuring Option 43 and Option 60 on Linux

Configuring Option 43 on Windows

To configure option 43 on Windows:

1. On the DHCP server, go to **Start** → **Administration Tools** → **DHCP** to open the DHCP server administration tool.
2. Find the server and expand all items under it.
3. Right-click on **Scope Options** and select **Configure Options**.

   The **Scope Options** dialog box is displayed.
4. Scroll down and select **043 Vendor Specific Info**.
5. In the **Data Entry** field, click anywhere in the area under **ASCII** and enter the IP address of the server that has the share location, which contains the XML configuration file.

   The value appears as you type it under the **ASCII**, but it also appears in binary to the left.
6. Click **OK** to save the configuration.

Configuring Option 60 on Windows

To configure option 60 on Windows:

1. On the DHCP server, go to **Start** → **Administration Tools** → **DHCP** to open the DHCP server administration tool.
2. Find the server and expand the items under it.
3. Right-click on **IPv4** and choose **Define Vendor Classes**.
4. Click **Add** and enter the following:
   - **Display name** — iDRAC (read-only)
   - **Description** — Vendor Class
   - Under **ASCII**, click and enter iDRAC.
5. Click **OK**.
6. On the DHCP window, right-click on **IPv4** and choose **Set Predefined Options**.
7. From the **Option class** drop-down menu,select **iDRAC** (created in step 4) and click **Add**.
8. In the **Option Type** dialogue box, enter the following information:
   - **Name** — iDRAC
   - **Data Type** — String
   - **Code** – 1
   - **Description** — Dell vendor class identifier
9. Click **OK** twice to return to the **DHCP** window.
10. Expand all items under the server name, right-click on **Scope Options** and select **Configure Options**.
11. Click on the **Advanced** tab.
12. From the **Vendor class** drop-down menu, select **iDRAC**. The 060iDRAC appears in the **Available Options** column.

13. Select **060iDRAC** option.
14. Enter the string value that must be sent to the iDRAC (along with a standard DHCP provided IP address). The string value will help in importing the correct XML configuration file.

    For the option's **DATA entry, String Value** setting, use a text parameter that has the following letter options and values:

    - Filename – iDRAC_Config.XML or iDRAC_Config-<service-tag>.XML. (-f)
    - Sharename – (-n)
    - ShareType – -s (0 = NFS, 2 = CIFS)
    - IPAddress – IP address of the file share. (-i)
    - Username – Required for CIFS (-u)
    - Password – Required for CIFS (-p)
    - ShutdownType – Specify Graceful or Forced. (-d)
    - Timetowait - Default is 300 (-t)
    - EndHostPowerState - (-e)

Configuring Option 43 and Option 60 on Linux

Update the **/etc/dhcpd.conf** file. Similar to Windows, the steps are :

1. Set aside a block or pool of addresses that this DHCP server can allocate.
2. Set the option 43 and use the name vendor class identifier for option 60.

For example,

```
option myname code 43 = text;
subnet 192.168.0.0 netmask 255.255.0.0  {
#default gateway
    option routers            192.168.0.1;
    option subnet-mask        255.255.255.0;
    option nis-domain        "domain.org";
    option domain-name        "domain.org";
    option domain-name-servers    192.168.1.1;
    option time-offset        -18000;    # Eastern Standard Time
#    option ntp-servers        192.168.1.1;
#    option netbios-name-servers    192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#    option netbios-node-type 2;
    option vendor-class-identifier "iDRAC";
    set vendor-string = option vendor-class-identifier;
    option myname "2001::9174:9611:5c8d:e85//xmlfiles/dhcpProv.xml -u root -p
calvin";
    range dynamic-bootp 192.168.0.128 192.168.0.254;
    default-lease-time 21600;
    max-lease-time 43200;
    # we want the nameserver to appear at a fixed address
    host ns {
        next-server marvin.redhat.com;
        hardware ethernet 12:34:56:78:AB:CD;
        fixed-address 207.175.42.254;
    }
}
```

Enabling Auto Config Using iDRAC Web Interface

Make sure that DHCPv4 and the Enable IPv4 options are enabled and Auto-discovery is disabled.

To enable Auto Config:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network**.
   The **Network** page is displayed.
2. In the **Auto Config** section, select one of the following options to enable **Auto Config**:
   - **Enable Once** — Configures the component only once using the XML file referenced by the DHCP server. After this, Auto Config is disabled.
   - **Enable Once After Reset** — After the iDRAC is reset, configures the components only once using the XML file referenced by the DHCP server. After this, Auto Config is disabled.

   To disable the Auto Config feature, select **Disable**.
3. Click **Apply** to apply the setting.

Enabling Auto Config Using RACADM

To enable Auto Config feature using RACADM, use the `iDRAC.NIC.AutoConfig` object. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide*.

Using Hash Passwords for Improved Security

For iDRAC in 13th generation servers, you can set user passwords and BIOS passwords using a one way hash format. The user authentication mechanism is not affected (except for SNMPv3 and IPMI) and you can provide the password in plain text format.

With the new password hash feature:

- You can generate your own SHA256 hashes to set iDRAC user passwords and BIOS passwords. This allows you to have the SHA256 values in the server configuration profile, RACADM, and WSMAN. When you provide the SHA256 password values, you cannot authenticate through SNMPv3 and IPMI.
- You can set up a template server including all the iDRAC user accounts and BIOS passwords using the current plain text mechanism. After the server is set up, you can export the server configuration profile with the password that has hash values. The export includes the hash values required for SNMPv3 and IPMI authentication.

You can generate the hash password with and without Salt using SHA256.

You must have Server Control privileges to include and export hash passwords.

If access to all accounts is lost, use iDRAC Settings Utility or local RACADM and perform reset iDRAC to default task.

If the iDRAC user account's password is set with the SHA256 password hash only and not the other hashes (SHA1v3Key or MD5v3Key), then authentication through SNMP v3 and IPMI is not available.

Hash Password Using RACADM

Use the following objects with the **set** racadm sub command to set hash passwords:

- iDRAC.Users.SHA256Password
- iDRAC.Users.SHA256PasswordSalt

Use the following command to include the hash password in the exported server configuration profile:

```
racadm get -f <file name> -l <NFS / CIFS share> -u <username> -p <password>  -t
<filetype> --includePH
```

You must set the Salt attribute when the associated hash is set.

NOTE: The attributes are not applicable to the INI configuration file.

Hash Password in Server Configuration Profile

The new hash passwords can be optionally exported in the server configuration profile.

When importing server configuration profile, you can uncomment the existing password attribute or the new password hash attribute(s). If both are uncommented an error is generated and the password is not set. A commented attribute is not applied during an import.

Generating Hash Password Without SNMPv3 and IPMI Authentication

To generate hash password without SNMPv3 and IPMI authentication:

1. For iDRAC user accounts, you must salt the password using SHA256.

   When you salt the password, a 16 byte binary string is appended. The Salt is required to be 16 bytes long, if provided.
2. Provide hash value and salt in the imported server configuration profile, RACADM commands, or WSMAN.
3. After setting the password, the normal plain text password authentication works except that SNMP v3 and IPMI authentication fails for iDRAC user accounts that had passwords updated with hash.

Setting Up Management Station

A management station is a computer used for accessing iDRAC interfaces to remotely monitor and manage the PowerEdge server(s).

To set up the management station:

1. Install a supported operating system. For more information, see the readme.
2. Install and configure a supported Web browser (Internet Explorer, Firefox, Chrome, or Safari).
3. Install the latest Java Runtime Environment (JRE) (required if Java plug-in type is used to access iDRAC using a Web browser).
4. From the *Dell Systems Management Tools and Documentation* DVD, install Remote RACADM and VMCLI from the SYSMGMT folder. Else, run **Setup** on the DVD to install Remote RACADM by default and other OpenManage software. For more information about RACADM, see *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.
5. Install the following based on the requirement:
   - Telnet
   - SSH client
   - TFTP
   - Dell OpenManage Essentials

Related Links

Installing and Using VMCLI Utility

Configuring Supported Web Browsers

Accessing iDRAC Remotely

To remotely access iDRAC Web interface from a management station, make sure that the management station is in the same network as iDRAC. For example:

- Blade servers — The management station must be on the same network as CMC. For more information on isolating CMC network from the managed system's network, see *Chassis Management Controller User's Guide* available at **dell.com/support/manuals**.
- Rack and tower servers — Set the iDRAC NIC to Dedicated or LOM1 and make sure that the management station is on the same network as iDRAC.

To access the managed system's console from a management station, use Virtual Console through iDRAC Web interface.

Related Links

Launching Virtual Console
Network Settings

Setting Up Managed System

If you need to run local RACADM or enable Last Crash Screen capture, install the following from the *Dell Systems Management Tools and Documentation* DVD:

- Local RACADM
- Server Administrator

For more information about Server Administrator, see *Dell OpenManage* Server Administrator User's Guide available at **dell.com/support/manuals**.

Related Links

Modifying Local Administrator Account Settings

Modifying Local Administrator Account Settings

After setting the iDRAC IP address, you can modify the local administrator account settings (that is, user 2) using the iDRAC Settings utility. To do this:

1. In the iDRAC Settings utility, go to **User Configuration**.
   The **iDRAC Settings User Configuration** page is displayed.
2. Specify the details for **User Name**, **LAN User Privilege**, **Serial Port User Privilege**, and **Change Password**.
   For information about the options, see the *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
   The local administrator account settings are configured.

Setting Up Managed System Location

You can specify the location details of the managed system in the data center using the iDRAC Web interface or iDRAC Settings utility.

Setting Up Managed System Location Using Web Interface

To specify the system location details:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Properties** → **Details**.
   The **System Details** page is displayed.
2. Under **System Location**, enter the location details of the managed system in the data center.

For information about the options, see the *iDRAC Online Help*.

3. Click **Apply**. The system location details is saved in iDRAC.

Setting Up Managed System Location Using RACADM

To specify the system location details, use the `System.Location` group objects. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Setting Up Managed System Location Using iDRAC Settings Utility

To specify the system location details:

1. In the iDRAC Settings utility, go to **System Location**.
   The **iDRAC Settings System Location** page is displayed.
2. Enter the location details of the managed system in the data center. For information about the options, see the *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
   The details are saved.

Optimizing System Performance and Power Consumption

The power required to cool a server can contribute a significant amount to the overall system power. Thermal control is the active management of system cooling through fan speed and system power management to make sure that the system is reliable while minimizing system power consumption, airflow, and system acoustic output. You can adjust the thermal control settings and optimize against the system performance and performance-per-Watt requirements.

Using the iDRAC Web interface, RACADM, or the iDRAC Settings Utility, you can change the following thermal settings:

- Optimize for performance
- Optimize for minimum power
- Set the maximum air exhaust temperature
- Increase airflow through a fan offset, if required
- Increase airflow through increasing minimum fan speed

Modifying Thermal Settings Using iDRAC Web Interface

To modify the thermal settings:

1. In the iDRAC Web interface, go to **Overview → Hardware → Fans → Setup**.
   The **Fan Setup** page is displayed.
2. Specify the following:
   - **Thermal Profile** — Select the thermal profile:
     - **Default Thermal Profile Settings** — Implies that the thermal algorithm uses the same system profile settings that is defined under **System BIOS → System BIOS Settings.System Profile Settings** page.

     By default, this is set to **Default Thermal Profile Settings**. You can also select a custom algorithm, which is independent of the BIOS profile. The options available are:

– **Maximum Performance (Performance Optimized)** :

  * Reduced probability of memory or CPU throttling.
  * Increased probability of turbo mode activation.
  * Generally, higher fan speeds at idle and stress loads.

– **Minimum Power (Performance per Watt Optimized)**:

  * Optimized for lowest system power consumption based on optimum fan power state.
  * Generally, lower fan speeds at idle and stress loads.

NOTE: Selecting **Maximum Performance** or **Minimum Power**, overrides thermal settings associated to System Profile setting under **System BIOS → System BIOS Settings.System Profile Settings** page.

- **Maximum Exhaust Temperature Limit** — From the drop-down menu, select the maximum exhaust air temperature. The values are displayed based on the system.

  The default value is **Default, 70°C (158 °F)**.

  This option allows the system fans speeds to change such that the exhaust temperature does not exceed the selected exhaust temperature limit. This cannot always be guaranteed under all system operating conditions due to dependency on system load and system cooling capability.
- **Fan Speed Offset** — Selecting this option allows additional cooling to the server. In case hardware is added (example, new PCIe cards), it may require additional cooling. A fan speed offset causes fan speeds to increase (by the offset % value) over baseline fan speeds calculated by the Thermal Control algorithm. Possible values are:

  – **Low Fan Speed** — Drives fan speeds to a moderate fan speed.
  – **Medium Fan Speed** — Drives fan speeds close to medium.
  – **High Fan Speed** — Drives fan speeds close to full speed.
  – **Max Fan Speed** — Drives fan speeds to full speed.
  – **Off** — Fan speed offset is set to off. This is the default value. When set to off, the percentage does not display. The default fan speed is applied with no offset. Conversely, the maximum setting will result in all fans running at maximum speed.

  The fan speed offset is dynamic and based on the system. The fan speed increase for each offset is displayed next to each option.

  The fan speed offset increases all fan speeds by the same percentage. Fan speeds may increase beyond the offset speeds based on individual component cooling needs. The overall system power consumption is expected to increase.

  Fan speed offset allows you to increase the system fan speed with four incremental steps. These steps are equally divided between the typical baseline speed and the maximum speed of the server system fans. Some hardware configurations results in higher baseline fan speeds, which results in offsets other than the maximum offset to achieve maximum speed.

  The most common usage scenario is non-standard PCIe adapter cooling. However, the feature can be used to increase system cooling for other purposes.
- **Minimum Fan Speed in PWM (% of Max)** — Select this option to fine tune the fan speed. Using this option, you can set a higher baseline system fan speed or increase the system fan speed if other custom fan speed options are not resulting in the required higher fan speeds.

  – **Default** — Sets minimum fan speed to default value as determined by the system cooling algorithm.

– **Custom** — Enter the percentage value.

The allowable range for minimum fan speed PWM is dynamic based on the system configuration. The first value is the idle speed and the second value is the configuration max (which may or may not be 100% based on system configuration).

System fans can run higher than this speed as per thermal requirements of the system but not lower than the defined minimum speed. For example, setting Minimum Fan Speed at 35% limits the fan speed to never go lower than 35% PWM.

NOTE: 0% PWM does not indicate fan is off. It is the lowest fan speed that the fan can achieve.

The settings are persistent, which means that once they are set and applied, they do not automatically change to the default setting during system reboot, power cycling, iDRAC, or BIOS updates. A few Dell servers may or may not support some or all of these custom user cooling options. If the options are not supported, they are not displayed or you cannot provide a custom value.

3. Click **Apply** to apply the settings.
   The following message is displayed:

   ```
   It is recommended to reboot the system when a thermal profile change has
   been made. This is to ensure all power and thermal settings are activated.
   ```

   Click **Reboot Later** or **Reboot Now**.

   NOTE: You must reboot the system for the settings to take effect.

Modifying Thermal Settings Using RACADM

To modify the thermal settings, use the objects in the **system.thermalsettings** group with the **set** sub command as provided in the following table.

Object	Description	Usage	Example

`AirExhaustTemp`	Allows to set the maximum air exhaust temperature limit.	Set to any of the following values (based on the system):
		• 0 - Indicates 40°C
		• 1 - Indicates 45°C
		• 2 - Indicates 50°C
		• 3 - Indicates 55°C
		• 4 - Indicates 60°C
		• 255 - Indicates 70°C (default)
			To check the existing setting on the system:
			`racadm get system.thermalsettings.AirExhaustTemp`
			The output is:
			`AirExhaustTemp=70`
			This means that the system is set to limit the air exhaust temperature to 70°C.
			To set the exhaust temperature limit to 60°C:
			`racadm set system.thermalsettings.AirExhaustTemp 4`

Object	Description	Usage	Example

			The output is:
			`Object value modified successfully.`
			If a system does not support a particular air exhaust temperature limit, then when you run the following command:
			`racadm set system.thermalsettings.AirExhaustTemp 0`
			The following error message is displayed:
			`ERROR: RAC947: Invalid object value specified.`
			Make sure to specify the value depending on the type of object.
			For more information, see RACADM help.
			To set the limit to the default value:
			`racadm set system.thermalsettings.AirExhaustTemp 255`

`FanSpeedHighOffsetVal`	• Getting this variable reads the fan speed offset value in %PWM for High Fan Speed Offset setting.
	• This value depends on the system.
	• Use `FanSpeedOffset` object to set this value using index value 1.
		Values from 0-100	`racadm get system.thermalsettings FanSpeedHighOffsetVal`
			This returns a value such as “66”. This means that when you use the following command, it applies a fan speed offset of High (66% PWM) over the baseline fan speed
			`racadm set system.thermalsettings FanSpeedOffset 1`

`FanSpeedLowOffsetVal`	• Getting this variable reads the fan speed offset value in %PWM for Low Fan Speed Offset setting.
	• This value depends on the system.
	• Use `FanSpeedOffset` object to set this value using index value 0.
		Values from 0-100	`racadm get system.thermalsettings FanSpeedLowOffsetVal`
			This returns a value such as “23”. This means that when you use the following command, it applies a fan speed offset of Low (23% PWM) over baseline fan speed
			`racadm set system.thermalsettings FanSpeedOffset 0`

Object	Description	Usage	Example
FanSpeedMaxOffsetVal	• Getting this variable reads the fan speed offset value in %PWM for Max Fan Speed Offset setting. • This value depends on the system. • Use FanSpeedOffset to set this value using index value 3	Values from 0-100	racadm get system.thermalsettings FanSpeedMaxOffsetVal This returns a value such as "100". This means that when you use the following command, it applies a fan speed offset of Max (meaning full speed, 100% PWM). In most cases, this offset results in fan speeds increasing to full speed. racadm set system.thermalsettings FanSpeedOffset 3
FanSpeedMediumOffsetVal	• Getting this variable reads the fan speed offset value in %PWM for Medium Fan Speed Offset setting. • This value depends on the system. • Use FanSpeedOffset object to set this value using index value 2	Values from 0-100	racadm get system.thermalsettings FanSpeedMediumOffsetVal This returns a value such as "47". This means that when you use the following command, it applies a fan speed offset of Medium (47% PWM) over baseline fan speed racadm set system.thermalsettings FanSpeedOffset 2
FanSpeedOffset	• Using this object with get command displays the existing Fan Speed Offset value. • Using this object with set command allows setting the required fan speed offset value. • The index value decides the offset that is applied and the FanSpeedLowOffsetVal, FanSpeedMaxOffsetVal, FanSpeedHighOffsetVal, and FanSpeedMediumOffsetVal objects (defined earlier) are the values at which the offsets are applied.	Values are: • 0 - Low Fan Speed • 1 - High Fan Speed • 2 - Medium Fan Speed • 3 - Max Fan Speed • 255 - None	To view the existing setting: racadm get system.thermalsettings.FanSpeedOffset To set the fan speed offset to High value (as defined in FanSpeedHighOffsetVal) racadm set system.thermalsettings.FanSpeedOffset 1
MFSMaximumLimit	Read Maximum limit for MFS	Values from 1 - 100	To display the highest value that can be set using MinimumFanSpeed option: racadm get system.thermalsettings.MFSMaximumLimit

Object	Description	Usage	Example
MFSMinimumLimit	Read Minimum limit for MFS	Values from 0 to MFSMaximumLimit Default is 255 (means None)	To display the lowest value that can be set using MinimumFanSpeed option. racadm get system.thermalsettings.MFSMinimumLimit
MinimumFanSpeed	• Allows configuring the Minimum Fan speed that is required for the system to operate. • It defines the baseline (floor) value for fan speed and system allows fans to go lower than this defined fan speed value. • This value is %PWM value for fan speed.	Values from MFSMinimumLimit to MFSMaximumLimit When get command reports 255, it means user configured offset is not applied.	To make sure that the system minimum speed does not decrease lower than 45% PWM (45 must be a value between MFSMinimumLimit to MFSMaximumLimit): racadm set system.thermalsettings.MinimumFanSpeed 45
ThermalProfile	• Allows to specify the Thermal Base Algorithm. • Allows to set the system profile as required for thermal behavior associated to the profile.	Values: • 0 — Auto • 1 — Maximum performance • 2 — Minimum Power	To view the existing thermal profile setting: racadm get system.thermalsettings.ThermalProfile To set the thermal profile to Maximum Performance: racadm set system.thermalsettings.ThermalProfile 1

Modifying Thermal Settings Using iDRAC Settings Utility

To modify the thermal settings:

1. In the iDRAC Settings utility, go to **Thermal**.
   The **iDRAC Settings Thermal** page is displayed.
2. Specify the following:
   - Thermal Profile
   - Maximum Exhaust Temperature Limit
   - Fan Speed Offset
   - Minimum Fan Speed

   For information about the fields, see the Modifying Thermal Settings Using Web Interface.

   The settings are persistent, which means that once they are set and applied, they do not automatically change to the default setting during system reboot, power cycling, iDRAC, or BIOS updates. A few Dell servers may or may not support some or all of these custom user cooling options. If the options are not supported, they are not displayed or you cannot provide a custom value.
3. Click **Back**, click **Finish**, and then click **Yes**.

The thermal settings are configured.

Configuring Supported Web Browsers

iDRAC is supported on Internet Explorer, Mozilla Firefox, Google Chrome, and Safari Web browsers. For information about the versions, see the *Readme* available at **dell.com/support/manuals**.

If you are connecting to iDRAC Web interface from a management station that connects to the Internet through a proxy server, you must configure the Web browser to access the Internet from through this server. This section provides information to configure Internet Explorer.

To configure the Internet Explorer Web browser:

1. Set IE to **Run As Administrator**.
2. In the Web browser, go to **Tools** → **Internet Options** → **Security** → **Local Network**.
3. Click **Custom Level**, select **Medium-Low**, and click **Reset**. Click **OK** to confirm. Click **Custom Level** to open the dialog.
4. Scroll down to the section labeled ActiveX controls and plug-ins and set the following:

   NOTE: The settings in the Medium-Low state depend on the IE version.

   - Automatic prompting for ActiveX controls: Enable
   - Binary and script behaviors: Enable
   - Download signed ActiveX controls: Prompt
   - Initialize and script ActiveX controls not marked as safe: Prompt
   - Run ActiveX controls and plug-ins: Enable
   - Script ActiveX controls marked safe for scripting: Enable

   Under **Downloads**:

   - Automatic prompting for file downloads: Enable
   - File download: Enable
   - Font download: Enable

   Under **Miscellaneous**:

   - Allow META-REFRESH: Enable
   - Allow scripting of Internet Explorer Web browser control: Enable
   - Allow script-initiated windows without size or position constraints: Enable
   - Do not prompt for client certificate selection when no certificates or only one certificate exists: Enable
   - Launching programs and files in an IFRAME: Enable
   - Open files based on content, not file extension: Enable
   - Software channel permissions: Low safety
   - Submit non-encrypted form data: Enable
   - Use Pop-up Blocker: Disable

   Under **Scripting**:

   - Active scripting: Enable
   - Allow paste operations via script: Enable

- Scripting of Java applets: Enable

5. Go to **Tools** → **Internet Options** → **Advanced**.
6. Under **Browsing**:
   - Always send URLs as UTF-8: selected
   - Disable script debugging (Internet Explorer): selected
   - Disable script debugging: (Other): selected
   - Display a notification about every script error: cleared
   - Enable Install On demand (Other): selected
   - Enable page transitions: selected
   - Enable third-party browser extensions: selected
   - Reuse windows for launching shortcuts: cleared

   Under **HTTP 1.1 settings**:
   - Use HTTP 1.1: selected
   - Use HTTP 1.1 through proxy connections: selected

   Under **Java (Sun)**:
   - Use JRE 1.6.x_yz: selected (optional; version may differ)

   Under **Multimedia**:
   - Enable automatic image resizing: selected
   - Play animations in Web pages: selected
   - Play videos in Web pages: selected
   - Show pictures: selected

   Under **Security**:
   - Check for publishers' certificate revocation: cleared
   - Check for signatures on downloaded programs: selected
   - Use SSL 2.0: cleared
   - Use SSL 3.0: selected
   - Use TLS 1.0: selected
   - Warn about invalid site certificates: selected
   - Warn if changing between secure and not secure mode: selected
   - Warn if forms submittal is being redirected: selected

   NOTE: To modify the settings, it is recommended that you learn and understand the consequences. For example, if you block pop-ups, parts of iDRAC Web interface may not function properly.
7. Click **Apply**, and then click **OK**.
8. Click the **Connections** tab.
9. Under **Local Area Network (LAN) settings**, click **LAN Settings**.
10. If you are using IE9 and IPv6 address to access iDRAC, clear the **Use automatic configuration script** option.
11. If the **Use a proxy server** box is selected, select the **Bypass proxy server for local addresses** box.
12. Click **OK** twice.
13. Close and restart your browser to make sure all changes take effect.

NOTE: When you log in to iDRAC Web interface using Internet Explorer 9.x, sometimes contents in few pages are not shown properly. To resolve this, press <F12>. In the **Internet Explorer 9 Debug** window, select **Document Mode** as **Internet Explorer 7**. The browser refreshes and the iDRAC **Login** page is displayed.

Related Links

Viewing Localized Versions of Web Interface
Adding iDRAC to the List of Trusted Domains
Disabling Whitelist Feature in Firefox

Adding iDRAC to the List of Trusted Domains

When you access iDRAC Web interface, you are prompted to add iDRAC IP address to the list of trusted domains if the IP address is missing from the list. When completed, click **Refresh** or relaunch the Web browser to establish a connection to iDRAC Web interface.

On some operating systems, Internet Explorer (IE) 8 may not prompt you to add iDRAC IP address to the list of trusted domains if the IP address is missing from the list.

NOTE: When connecting to the iDRAC Web interface with a certificate the browser does not trust, the browser's certificate error warning may display a second time after you acknowledge the first warning. This is the expected behavior to for security.

To add iDRAC IP address to the list of trusted domains in IE8, do the following:

1. Select **Tools** → **Internet Options** → **Security** → **Trusted sites** → **Sites**.
2. Enter iDRAC IP address to the **Add this website to the zone**.
3. Click **Add**, click **OK**, and then click **Close**.
4. Click **OK** and then refresh your browser.

Disabling Whitelist Feature in Firefox

Firefox has a "whitelist" security feature that requires user permission to install plug-ins for each distinct site that hosts a plug-in. If enabled, the whitelist feature requires you to install a Virtual Console viewer for each iDRAC you visit, even though the viewer versions are identical.

To disable the whitelist feature and avoid unnecessary plug-in installations, perform the following steps:

1. Open a Firefox Web browser window.
2. In the address field, enter `about:config` and press <Enter>.
3. In the **Preference Name** column, locate and double-click **xpinstall.whitelist.required**.
   The values for **Preference Name**, **Status**, **Type**, and **Value** change to bold text. The **Status** value changes to user set and the **Value** changes to false.
4. In the **Preferences Name** column, locate **xpinstall.enabled**.
   Make sure that **Value** is **true**. If not, double-click **xpinstall.enabled** to set **Value** to **true**.

Viewing Localized Versions of Web Interface

iDRAC Web interface is supported in the following languages:

- English (en-us)
- French (fr)
- German (de)

- Spanish (es)
- Japanese (ja)
- Simplified Chinese (zh-cn)

The ISO identifiers in parentheses denote the supported language variants. For some supported languages, resizing the browser window to 1024 pixels wide is required to view all features.

iDRAC Web interface is designed to work with localized keyboards for the supported language variants. Some features of iDRAC Web interface, such as Virtual Console, may require additional steps to access certain functions or letters. Other keyboards are not supported and may cause unexpected problems.

NOTE: See the browser documentation on how to configure or setup different languages and view localized versions of iDRAC Web interface.

Updating Device Firmware

Using iDRAC, you can update the iDRAC, BIOS, and all device firmware that is supported through Lifecycle Controller update such as:

- Lifecycle Controller
- Diagnostics
- Operating System Driver Pack
- Network Interface Card (NIC)
- RAID Controller
- Power Supply Unit (PSU)
- PCIe Solid State Drives (SSDs)

You must upload the required firmware to iDRAC. After the upload is complete, the current version of the firmware installed on the device and the version being applied is displayed. If the firmware being uploaded is not valid, an error message is displayed. Updates that do not require a reboot are applied immediately. Updates that require a system reboot are staged and committed to run on the next system reboot. Only one system reboot is required to perform all updates.

After the firmware is updated, the **System Inventory** page displays the updated firmware version and logs are recorded.

The supported firmware image file types are:

- **.exe** — Windows based Dell Update Package (DUP)
- **.d7** — Contains both iDRAC and Lifecycle Controller firmware.

For files with **.exe** extension, you must have System Control privilege. The Remote Firmware Update licensed feature and Lifecycle Controller must be enabled.

For files with **.d7** extension, you must have Configure privilege.

You can perform firmware updates using the following methods:

- Using a firmware image file on a local system or on a network share.
- Connecting to the FTP, TFTP, or HTTP site or a network repository that contains a catalog of available updates. You can create custom repositories using Repository Manager. For more information, see

Repository Manager User's Guide. iDRAC automatically provides a difference between the BIOS and the firmware that is installed on the server and the repository location or FTP site. All applicable updates contained in the repository are applied to the system. This feature is available with iDRAC Enterprise license.

- Scheduling recurring automated firmware updates using the catalog file in the FTP site or the network repository location.

The following table provides information on whether a system restart is required or not when firmware is updated for a particular component.

NOTE: When multiple firmware updates are applied through out-of-band methods, the updates are ordered in the most efficient possible manner to reduce unnecessary system restart.

Table 6. Firmware Update – Supported Components

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band—System Restart Required?	In-band—System Restart Required?	Lifecycle Controller GUI—Restart Required?
Diagnostics	No	No	No	No
OS Driver Pack	No	No	No	No
Lifecycle Controller	No	No	No	Yes
BIOS	Yes	Yes	Yes	Yes
RAID Controller	Yes	Yes	Yes	Yes
Backplanes	Yes	Yes	Yes	Yes
Enclosures	Yes	Yes	No	Yes
NIC	Yes	Yes	Yes	Yes
iDRAC	Yes	**No	*No	*No
Power Supply Unit	Yes	Yes	Yes	Yes
CPLD	No	Yes	Yes	Yes
FC Cards	Yes	Yes	Yes	Yes
PCIe SSD	Yes	Yes	Yes	Yes

* Indicates that though a system restart is not required, iDRAC must be restarted to apply the updates. iDRAC communication and monitoring will temporarily be interrupted.

** When iDRAC is updated from version 1.30.30 or later, a system restart is not necessary. However, firmware versions of iDRAC earlier than 1.30.30 require a system restart when applied using the out-of-band interfaces.

Related Links

Downloading Device Firmware
Updating Single Device Firmware
Updating Firmware Using Repository
Updating Firmware Using FTP
Updating Device Firmware Using TFTP
Updating Device Firmware Using HTTP
Updating Device Firmware Using RACADM

Scheduling Automatic Firmware Updates
Updating Firmware Using CMC Web Interface
Updating Firmware Using DUP
Updating Firmware Using Remote RACADM
Updating Firmware Using Lifecycle Controller Remote Services

Downloading Device Firmware

The image file format that you download depends on the method of update:

- iDRAC Web interface — Download the binary image packaged as a self-extracting archive. The default firmware image file is **firmimg.d7**.

  NOTE: The same file format is used to recover iDRAC using CMC Web interface.
- Managed System — Download the operating system-specific Dell Update Package (DUP). The file extensions are **.bin** for Linux Operating systems and **.exe** for Windows operating systems.
- Lifecycle Controller — Download the latest catalog file and DUPs and use the *Platform Update* feature in Lifecycle Controller to update the device firmware. For more information about Platform Update, see *Lifecycle Controller User's Guide* available at **dell.com/support/manuals**.

Updating Firmware Using iDRAC Web Interface

You can update the device firmware using firmware images available on the local system, from a repository on a network share (CIFS or NFS), or from FTP.

Updating Single Device Firmware

Before updating the firmware using single device update method, make sure that you have downloaded the firmware image to a location on the local system.

To update single device firmware using iDRAC Web interface:

1. Go to **Overview → iDRAC Settings → Update and Rollback** .

   The **Firmware Update** page is displayed.
2. On the **Update** tab, select **Local** as the **File Location**.
3. Click **Browse**, select the firmware image file for the required component, and then click **Upload**.
4. After the upload is complete, the **Update Details** section displays each firmware file uploaded to iDRAC and its status.

   If the firmware image file is valid and was successfully uploaded, the **Contents** column displays a icon next to the firmware image file name. Expand the name to view the **Device Name**, **Current**, and **Available firmware version** information.
5. Select the required firmware file to be updated and do one of the following:
   - For firmware images that do not require a host system reboot, click **Install**. For example, iDRAC firmware file.
   - For firmware images that require a host system reboot, click **Install and Reboot** or **Install Next Reboot**.
   - To cancel the firmware update, click **Cancel**.

   NOTE: If you have uploaded the same firmware image file more than once, only the latest firmware file is available for selection. The check box for the earlier firmware image files is disabled.

When you click **Install**, **Install and Reboot** or **Install Next Reboot**, the message `Updating Job Queue` is displayed.

6. Click **Job Queue** to display the **Job Queue** page, where you can view and manage the staged firmware updates or click **OK** to refresh the current page and view the status of the firmware update.

   NOTE: If you navigate away from the page without committing the updates, an error message is displayed and all the uploaded content is lost.

Related Links

Updating Device Firmware
Viewing and Managing Staged Updates
Downloading Device Firmware

Updating Firmware Using Repository

You can perform multiple firmware updates by specifying a network share containing a valid repository of DUPs and a catalog describing the available DUPs. When iDRAC connects to the network share location and checks for available updates, a comparison report is generated that lists all available updates. You can then select and apply the required updates contained in the repository to the system.

Before performing an update using the repository, make sure that:

- A repository containing Windows based update packages (DUPs) and a catalog file is created in the network share (CIFS or NFS). If a user-defined catalog file is not available, by default Catalog.xml is used.
- Lifecycle Controller is enabled.
- You have Server Control privilege to update firmware for devices other than iDRAC.

To update device firmware using a repository:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Update and Rollback** .
   The **Firmware Update** page is displayed.
2. On the **Update** tab, select **Network Share** as the **File Location**.
3. In the **Catalog Location** section, enter the network setting details.
   While specifying the network share settings, it is recommended to avoid special characters for user name and password or percent encode the special characters.

   For information about the fields, see the *iDRAC Online Help*.
4. Click **Check for Update**.
   The **Update Details** section displays a comparison report showing the current firmware versions and the firmware versions available in the repository.

   NOTE: Any update in the repository that is not applicable to the system or the installed hardware or not supported is not included in the comparison report.
5. Select the required updates and do one of the following:
   - For firmware images that do not require a host system reboot, click **Install**. For example, .d7 firmware file.
   - For firmware images that require a host system reboot, click **Install and Reboot** or **Install Next Reboot**.
   - To cancel the firmware update, click **Cancel**.

When you click **Install**, **Install and Reboot** or **Install Next Reboot**, the message `Updating Job Queue` is displayed.

6. Click **Job Queue** to display the **Job Queue** page, where you can view and manage the staged firmware updates or click **OK** to refresh the current page and view the status of the firmware update.

Related Links

Updating Device Firmware
Viewing and Managing Staged Updates
Downloading Device Firmware
Scheduling Automatic Firmware Updates

Updating Firmware Using FTP

You can directly connect to the Dell FTP site or any other FTP site from iDRAC to perform the firmware updates. You can use the Windows based update packages (DUPs) and a catalog file available on the FTP site instead of creating custom repositories.

Before performing an update using the repository, make sure that:

- Lifecycle Controller is enabled.
- You have Server Control privilege to update firmware for devices other than iDRAC.

To update device firmware using FTP:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Update and Rollback** .
   The **Firmware Update** page is displayed.
2. On the **Update** tab, select **FTP** as the **File Location**.
3. In the **FTP Server Settings** section, enter the FTP details.
   For information about the fields, see the *iDRAC Online Help*.
4. Click **Check for Update**.
5. After the upload is complete, the **Update Details** section displays a comparison report showing the current firmware versions and the firmware versions available in the repository.

   NOTE: Any update in the repository that is not applicable to the system or the installed hardware or is not supported is not included in the comparison report.
6. Select the required updates and do one of the following:
   - For firmware images that do not require a host system reboot, click **Install**. For example, **.d7** firmware file.
   - For firmware images that require a host system reboot, click **Install and Reboot** or **Install Next Reboot**.
   - To cancel the firmware update, click **Cancel**.

   When you click **Install**, **Install and Reboot** or **Install Next Reboot**, the message `Updating Job Queue` is displayed.
7. Click **Job Queue** to display the **Job Queue** page, where you can view and manage the staged firmware updates or click **OK** to refresh the current page and view the status of the firmware update.

Related Links

Updating Device Firmware
Viewing and Managing Staged Updates
Downloading Device Firmware
Scheduling Automatic Firmware Updates

Updating Device Firmware Using TFTP

You can directly connect to the TFTP site from iDRAC to perform the firmware updates. You can use the Windows based update packages (DUPs) and a catalog file available on the TFTP site instead of creating custom repositories.

Before performing an update, make sure that:

- Lifecycle Controller is enabled.
- You have Server Control privilege to update firmware for devices other than iDRAC.

To update device firmware using TFTP:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Update and Rollback** .
   The **Firmware Update** page is displayed.
2. On the **Update** tab, select **TFTP** as the **File Location**.
3. In the **TFTP Server Settings** section, enter the TFTP details.
   For information about the fields, see the *iDRAC Online Help*.
4. Click **Check for Update**.
5. After the upload is complete, the **Update Details** section displays a comparison report showing the current firmware versions and the firmware versions available in the repository.

   NOTE: Any update in the repository that is not applicable to the system or the installed hardware or is not supported is not included in the comparison report.
6. Select the required updates and do one of the following:
   - For firmware images that do not require a host system reboot, click **Install**. For example, **.d7** firmware file.
   - For firmware images that require a host system reboot, click **Install and Reboot** or **Install Next Reboot**.
   - To cancel the firmware update, click **Cancel**.

   When you click **Install**, **Install and Reboot** or **Install Next Reboot**, the message `Updating Job Queue` is displayed.
7. Click **Job Queue** to display the **Job Queue** page, where you can view and manage the staged firmware updates or click **OK** to refresh the current page and view the status of the firmware update.

Related Links

Downloading Device Firmware
Updating Device Firmware
Viewing and Managing Staged Updates
Downloading Device Firmware
Scheduling Automatic Firmware Updates

Updating Device Firmware Using HTTP

You can directly connect to the HTTP site from iDRAC to perform the firmware updates. You can use the Windows based update packages (DUPs) and a catalog file available on the HTTP site instead of creating custom repositories.

Before performing an update using the repository, make sure that:

- Lifecycle Controller is enabled.

- You have Server Control privilege to update firmware for devices other than iDRAC.

To update device firmware using HTTP:

1. In the iDRAC Web interface, go to **Overview** → **iDRAC Settings** → **Update and Rollback** .
   The **Firmware Update** page is displayed.
2. On the **Update** tab, select **HTTP** as the **File Location**.
3. In the **HTTP Server Settings** section, enter the HTTP details.
   For information about the fields, see the *iDRAC Online Help*.
4. Click **Check for Update**.
5. After the upload is complete, the **Update Details** section displays a comparison report showing the current firmware versions and the firmware versions available in the repository.

   NOTE: Any update in the repository that is not applicable to the system or the installed hardware or is not supported is not included in the comparison report.
6. Select the required updates and do one of the following:
   - For firmware images that do not require a host system reboot, click **Install**. For example, **.d7** firmware file.
   - For firmware images that require a host system reboot, click **Install and Reboot** or **Install Next Reboot**.
   - To cancel the firmware update, click **Cancel**.

   When you click **Install**, **Install and Reboot** or **Install Next Reboot**, the message `Updating Job Queue` is displayed.
7. Click **Job Queue** to display the **Job Queue** page, where you can view and manage the staged firmware updates or click **OK** to refresh the current page and view the status of the firmware update.

Enter the tasks the user should do after finishing this task (optional).

Related Links

Downloading Device Firmware
Updating Device Firmware
Viewing and Managing Staged Updates
Downloading Device Firmware
Scheduling Automatic Firmware Updates

Updating Device Firmware Using RACADM

To update device firmware using RACADM, use the **update** subcommand. For more information, see the *RACADM Reference Guide for iDRAC and CMC* available at **dell.com/support/manuals**.

Examples:

- To generate a comparison report using an update repository:
  ```
  racadm update –f catalog.xml –l //192.168.1.1 –u test –p passwd --
  verifycatalog
  ```
- To perform all applicable updates from an update repository using **myfile.xml** as a catalog file and perform a graceful reboot:
  ```
  racadm update –f “myfile.xml” –b “graceful” –l //192.168.1.1 –u test –p
  passwd
  ```
- To perform all applicable updates from an FTP update repository using **Catalog.xml** as a catalog file:
  ```
  racadm update –f “Catalog.xml” –t FTP –e 192.168.1.20/Repository/Catalog
  ```

Scheduling Automatic Firmware Updates

You can create a periodic recurring schedule for iDRAC to check for new firmware updates. At the scheduled day and time, iDRAC connects to the specified network share (CIFS or NFS) or the FTP, checks for new updates and applies or stages all applicable updates. A log file on the remote server contains information about server access and staged firmware updates.

Automatic updates is available only with the iDRAC Enterprise license.

You can schedule automatic firmware updates using the iDRAC Web interface or RACADM.

NOTE: IPv6 address is not supported for scheduling automatic firmware updates.

Related Links

Downloading Device Firmware
Updating Device Firmware
Viewing and Managing Staged Updates

Scheduling Automatic Firmware Update Using Web Interface

To schedule automatic firmware update using Web Interface:

NOTE: Do not create the next scheduled occurrence of an automatic update job if a job is already Scheduled. It overwrites the current scheduled job.

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Update and Rollback** .
   The **Firmware Update** page is displayed.
2. Click the **Automatic Update** tab.
3. Select the **Enable Automatic Update** option.
4. Select any of the following options to specify if a system reboot is required after the updates are staged:
   - **Schedule Updates** — Stage the firmware updates but do not reboot the server.
   - **Schedule Updates and reboot Server** — Enables server reboot after the firmware updates are staged.
5. Select any of the following to specify the location of the firmware images:
   - **Network** — Use the catalog file from a network share (CIFS or NFS). Enter the network share location details.

     NOTE: While specifying the network share settings, it is recommended to avoid special characters for user name and password or percent encode the special characters.
   - **FTP** — Use the catalog file from the FTP site. Enter the FTP site details.
6. Based on the selection in step 5, enter the network settings or the FTP settings.
   For information about the fields, see the *iDRAC Online Help*.
7. In the **Update Window Schedule** section, specify the start time for the firmware update and the frequency of the updates (daily, weekly, or monthly).
   For information about the fields, see the *iDRAC Online Help*.
8. Click **Schedule Update**.
   The next scheduled job is created in the job queue. Five minutes after the first instance of the recurring job starts, the job for the next time period is created.

Scheduling Automatic Firmware Update Using RACADM

To schedule automatic firmware update, use the following commands:

- To enable automatic firmware update:

  ```
  racadm set lifecycleController.lcattributes.AutoUpdate.Enable 1
  ```

- To view the status of automatic firmware update:

  ```
  racadm get lifecycleController.lcattributes.AutoUpdate
  ```

- To schedule the start time and frequency of the firmware update:

  ```
  racadm AutoUpdateScheduler create -u username -p password -l <location>  [-f
  catalogfilename -pu <proxyuser> -pp<proxypassword> -po <proxy port> -pt
  <proxytype>] -time < hh:mm> [-dom < 1 - 28,L,'*'> -wom <1-4,L,'*'> -dow <sun-
  sat,'*'>] -rp <1-366> -a <applyserverReboot (1-enabled | 0-disabled)>
  ```

  For example,

  – To automatically update firmware using a CIFS share:

    ```
    racadm AutoUpdateScheduler create -u admin -p pwd -l //1.2.3.4/CIFS-share
    -f cat.xml -time 14:30 -wom 1 -dow sun -rp 5 -a 1
    ```

  – To automatically update firmware using FTP:

    ```
    racadm AutoUpdateScheduler create -u admin -p pwd -l ftp.mytest.com -pu
    puser -pp puser -po 8080 -pt http -f cat.xml -time 14:30 -wom 1 -dow sun -
    rp 5 -a 1
    ```

- To view the current firmware update schedule:

  ```
  racadm AutoUpdateScheduler view
  ```

- To disable automatic firmware update:

  ```
  racadm set lifecycleController.lcattributes.AutoUpdate.Enable 0
  ```

- To clear the schedule details:

  ```
  racadm AutoUpdateScheduler clear
  ```

Updating Firmware Using CMC Web Interface

You can update iDRAC firmware for blade servers using the CMC Web interface.

To update iDRAC firmware using the CMC Web interface:

1. Log in to CMC Web interface.
2. Go to **Server** → **Overview** → **<server name>**.

   The **Server Status** page is displayed.
3. Click **Launch iDRAC** Web interface and perform **iDRAC Firmware Update**.

Related Links

Updating Device Firmware
Downloading Device Firmware
Updating Firmware Using iDRAC Web Interface

Updating Firmware Using DUP

Before you update firmware using Dell Update Package (DUP), make sure to:

- Install and enable the IPMI and managed system drivers.
- Enable and start the Windows Management Instrumentation (WMI) service if your system is running Windows operating system,

NOTE: While updating the iDRAC firmware using the DUP utility in Linux, if you see error messages such as `usb 5-2: device descriptor read/64, error -71` displayed on the console, ignore them.

- If the system has ESX hypervisor installed, then for the DUP file to run, make sure that the "usbarbitrator" service is stopped using command: `service usbarbitrator stop`

To update iDRAC using DUP:

1. Download the DUP based on the installed operating system and run it on the managed system.
2. Run the DUP.

   The firmware is updated. A system restart is not required after firmware update is complete.

Updating Firmware Using Remote RACADM

To update using remote RACADM:

1. Download the firmware image to the TFTP or FTP server. For example, C:\downloads\firmimg.d7
2. Run the following RACADM command:

   TFTP server:

   - Using **fwupdate** command: `racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -g -u -a <path>`

     where *path* is the location on the TFTP server where **firmimg.d7** is stored.
   - Using **update** command: `racadm -r <iDRAC IP address> -u <username> -p <password> update —f <filename>`

   FTP server:

   - Using **fwupdate** command: `racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -f <ftpsrever IP> <ftpserver username> <ftpserver password> -d <path>`

     where *path* is the location on the FTP server where **firmimg.d7** is stored.
   - Using **update** command: `racadm -r <iDRAC IP address> -u <username> -p <password> update —f <filename>`

   For more information, see **fwupdate** command in the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Updating Firmware Using Lifecycle Controller Remote Services

For information to update the firmware using Lifecycle Controller–Remote Services, see *Lifecycle Controller Remote Services Quick Start Guide* available at **dell.com/support/manuals**.

Updating CMC Firmware From iDRAC

In FX2/FX2s chassis, you can update the firmware for the Chassis Management Controller and any component that can be updated by CMC and shared by the servers from iDRAC.

Before applying the update, make sure that:

- Servers are not allowed to power-up by CMC.
- Chassis with LCD must display a message indicating “update is in-progress”.
- Chassis without LCD must indicate the update progress using LED blinking pattern.

- During the update, chassis action power commands are disabled.

The updates for components such as Programmable System-on-Chip (PSoC) of IOM that requires all the servers to be idle, the update is applied on the next chassis power-up cycle.

CMC Settings to Update CMC Firmware from iDRAC

In FX2/FX2s chassis, before performing the firmware update from iDRAC for CMC and its shared components, do the following:

1. Launch the CMC Web interface
2. Navigate to **Chassis Overview → Setup → General**.
3. From the **Chassis Management at Server Mode** drop-down menu, select **Manage and Monitor**, and the click **Apply**.

iDRAC Settings to Update CMC Firmware

In FX2/FX2s chassis, before updating the firmware for CMC and its shared components from iDRAC, do the following settings in iDRAC:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Update and Rollback → Settings**
   The **Chassis Management Controller Firmware Update Settings** page is displayed.
2. For **Allow CMC Updates Through OS and Lifecycle Controller**, select **Enabled** to enable CMC firmware update from iDRAC.
3. Under **Current CMC Setting**, make sure that **Chassis Management at Server Mode** option displays **Manage and Monitor**. You can set this in CMC.

Viewing and Managing Staged Updates

You can view and delete the scheduled jobs including configuration and update jobs. This is a licensed feature. All jobs queued to run during the next reboot can be deleted.

Related Links

Updating Device Firmware

Viewing and Managing Staged Updates Using iDRAC Web interface

To view the list of scheduled jobs using iDRAC Web interface, go to **Overview → Server → Job Queue**. The **Job Queue** page displays the status of jobs in the Lifecycle Controller job queue. For information about the displayed fields, see the *iDRAC Online Help*.

To delete job(s), select the job(s) and click **Delete**. The page is refreshed and the selected job is removed from the Lifecycle Controller job queue. You can delete all the jobs queued to run during the next reboot. You cannot delete active jobs, that is, jobs with the status *Running* or *Downloading*.

You must have Server Control privilege to delete jobs.

Viewing and Managing Staged Updates Using RACADM

To view the staged updates using RACADM, use **jobqueue** subcommand. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Rolling Back Device Firmware

You can rollback the firmware for iDRAC or any device that is supported by Lifecycle Controller even if the update was previously performed using another interface. For example, if the firmware was updated using the Lifecycle Controller GUI, you can rollback the firmware using the iDRAC Web interface. You can perform firmware rollback for multiple devices with one system reboot.

In 13th generation servers that have a single iDRAC and Lifecycle Controller firmware, rolling back iDRAC firmware will also rollback Lifecycle Controller firmware.

You can perform firmware rollback for the following components:

- iDRAC with Lifecycle Controller
- BIOS
- Network Interface Card (NIC)
- Power Supply Unit (PSU)
- RAID Controller
- Backplane

NOTE: You cannot perform firmware rollback for Diagnostics, Driver Packs, and CPLD.

Before you rollback the firmware, make sure that:

- You have Configure privilege to rollback iDRAC firmware.
- You have Server Control privilege and have enabled Lifecycle Controller to rollback firmware for any other device other than the iDRAC.

You can rollback the firmware to the previously installed version using any of the following methods:

- iDRAC Web interface
- CMC Web interface
- RACADM CLI (iDRAC and CMC)
- Lifecycle Controller
- Lifecycle Controller-Remote Services

Related Links

Rollback Firmware Using iDRAC Web Interface
Rollback Firmware Using CMC Web Interface
Rollback Firmware Using RACADM
Rollback Firmware Using Lifecycle Controller
Rollback Firmware Using Lifecycle Controller-Remote Services

Rollback Firmware Using iDRAC Web Interface

To roll back device firmware:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Update and Rollback → Rollback**.

The **Rollback** page displays the devices for which you can rollback the firmware. You can view the device name, associated devices, currently installed firmware version, and the available firmware rollback version.

2. Select one or more devices for which you want to rollback the firmware.
3. Based on the selected devices, click **Install and Reboot** or **Install Next Reboot**. If only iDRAC is selected, then click **Install**.

   When you click **Install and Reboot** or **Install Next Reboot**, the message "Updating Job Queue" is displayed.
4. Click **Job Queue**.

   The **Job Queue** page is displayed, where you can view and manage the staged firmware updates.

   NOTE:
   - While in rollback mode, the rollback process continues in the background even if you navigate away from this page.
   - If iDRAC configuration is reset to default values, the iDRAC IP address is reset to 192.168.0.120. You can access iDRAC using this IP, or reconfigure the iDRAC address using local RACADM or F2 (remote RACADM requires network access).

   An error message appears if:

   - You do not have Server Control privilege to rollback any firmware other than the iDRAC or Configure privilege to rollback iDRAC firmware.
   - Firmware rollback is already in-progress in another session.
   - Updates are staged to run or already in running state.

   If Lifecycle Controller is disabled or in recovery state and you try to perform a firmware rollback for any device other than iDRAC, an appropriate warning message is displayed along with steps to enable Lifecycle Controller.

Rollback Firmware Using CMC Web Interface

To roll back using the CMC Web interface:

1. Log in to CMC Web interface.
2. Go to **Server Overview** → **<server name>**.

   The **Server Status** page is displayed.
3. Click **Launch iDRAC** and perform device firmware rollback as mentioned in the Rollback Firmware Using iDRAC Web Interface section.

Rollback Firmware Using RACADM

To rollback device firmware using racadm:

1. Check the rollback status and the FQDD using the `swinventory` command:

   ```
   racadm swinventory
   ```

   For the device for which you want to rollback the firmware, the `Rollback Version` must be `Available`. Also, make a note of the FQDD.
2. Rollback the device firmware using:

   ```
   racadm rollback <FQDD>
   ```

For more information, see *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Rollback Firmware Using Lifecycle Controller

For information, see *Lifecycle Controller User's Guide* available at **dell.com/support/manuals**.

Rollback Firmware Using Lifecycle Controller-Remote Services

For information, see *Lifecycle Controller Remote Services Quick Start Guide* available at **dell.com/support/manuals**.

Recovering iDRAC

iDRAC supports two operating system images to make sure a bootable iDRAC. In the event of an unforeseen catastrophic error and you lose both boot paths:

- iDRAC bootloader detects that there is no bootable image.
- System Health and Identify LED is flashed at ~1/2 second rate. (LED is located on the back of a rack and tower servers and on the front of a blade server.)
- Bootloader is now polling the SD card slot.
- Format an SD card with FAT using a Windows operating system, or EXT3 using a Linux operating system.
- Copy **firmimg.d7** to the SD card.
- Insert the SD card into the server.
- Bootloader detects the SD card, turns the flashing LED to solid amber, reads the firmimg.d7, reprograms iDRAC, and then reboots iDRAC.

Using TFTP Server

You can use Trivial File Transfer Protocol (TFTP) server to upgrade or downgrade iDRAC firmware or install certificates. It is used in SM-CLP and RACADM command line interfaces to transfer files to and from iDRAC. The TFTP server must be accessible using an iDRAC IP address or DNS name.

NOTE: If you use iDRAC Web interface to transfer certificates and update firmware, TFTP server is not required.

You can use the `netstat –a`command on Windows or Linux operating systems to see if a TFTP server is running. The default port for TFTP is 69. If TFTP server is not running, do one of the following:

- Find another computer on the network running a TFTP service.
- Install a TFTP server on the operating system.

Backing Up Server Profile

You can backup the system configuration, including the installed firmware images on various components such as BIOS, RAID, NIC, iDRAC, Lifecycle Controller, and Network Daughter Cards (NDCs) and the configuration settings of those components. The backup operation also includes the hard disk configuration data, motherboard, and replaced parts. The backup creates a single file that you can save to a vFlash SD card or network share (CIFS or NFS).

You can also enable and schedule periodic backups of the firmware and server configuration based on a certain day, week, or month.

Backup feature is licensed and is available with iDRAC Enterprise license.

NOTE: In 13th generation servers, this feature is automatically enabled.

Before performing a backup operation, make sure that:

- Collect System Inventory On Reboot (CSIOR) option is enabled. If CSIOR is disabled and if you initiate a backup operation, the following message is displayed:
  `System Inventory with iDRAC may be stale,start CSIOR for updated inventory`
- To perform backup on a vFlash SD card:
  - A Dell supported vFlash SD card is inserted, enabled, and initialized.
  - vFlash SD card has enough space to store the backup file.

The backup file contains encrypted user sensitive data, configuration information, and firmware images that you can use for import server profile operation.

Backup events are recorded in the Lifecycle Log.

Related Links

Scheduling Automatic Backup Server Profile
Importing Server Profile

Backing Up Server Profile Using iDRAC Web Interface

To back up the server profile using iDRAC Web interface:

1. Go to **Overview → iDRAC Settings → Server Profile**.
   The **Backup and Export Server Profile** page is displayed.
2. Select one of the following to save the backup file image:
   - **Network** to save the backup file image on a CIFS or NFS share.
   - **vFlash** to save the backup file image on the vFlash card.
3. Enter the backup file name and encryption passphrase (optional).
4. If **Network** is selected as the file location, enter the network settings.

   NOTE: While specifying the network share settings, it is recommended to avoid special characters for user name and password or percent encode the special characters.

   For information about the fields, see the *iDRAC Online Help*.
5. Click **Backup Now**.
   The backup operation is initiated and you can view the status on the **Job Queue** page. After a successful operation, the backup file is created in the specified location.

Backing Up Server Profile Using RACADM

To backup the server profile using RACADM, use **systemconfig backup** subcommand. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Scheduling Automatic Backup Server Profile

You can enable and schedule periodic backups of the firmware and server configuration based on a certain day, week, or month.

Before scheduling automatic backup server profile operation, make sure that:

- Lifecycle Controller and Collect System Inventory On Reboot (CSIOR) option is enabled.
- Network Time Protocol (NTP) is enabled so that time drift does not affect the actual times of scheduled jobs running and when the next scheduled job is created.
- To perform backup on a vFlash SD card:
  - A Dell supported vFlash SD card is inserted, enabled, and initialized.
  - vFlash SD card has enough space to store the backup file.

NOTE: IPv6 address is not supported for scheduling automatic backup server profile.

Scheduling Automatic Backup Server Profile Using Web Interface

To schedule automatic backup server profile:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Server Profile**.
   The **Backup and Export Server Profile** page is displayed.
2. Click the **Automatic Backup** tab.
3. Select the **Enable Automatic Backup** option.
4. Select one of the following to save the backup file image:
   - **Network** to save the backup file image on a CIFS or NFS share.
   - **vFlash** to save the backup file image on the vFlash card.
5. Enter the backup file name and encryption passphrase (optional).
6. If **Network** is selected as the file location, enter the network settings.

   NOTE: While specifying the network share settings, it is recommended to avoid special characters for user name and password or percent encode the special characters.

   For information about the fields, see the *iDRAC Online Help*
7. In the **Backup Window Schedule** section, specify the backup operation start time and frequency of the operation (daily, weekly, or monthly).
   For information about the fields, see the *iDRAC Online Help*.
8. Click **Schedule Backup**.
   A recurring job is represented in the job queue with a start date and time of the next scheduled backup operation. Five minutes after the first instance of the recurring job starts, the job for the next time period is created. The backup server profile operation is performed at the scheduled date and time.

Scheduling Automatic Backup Server Profile Using RACADM

To enable automatic backup use the command:

```
racadm set lifecyclecontroller.lcattributes.autobackup Enabled
```

To schedule a backup server profile operation:

```
racadm systemconfig backup –f <filename> <target> [-n <passphrase>] -time
<hh:mm> -dom <1-28,L,’*’> -dow<*,Sun-Sat> -wom <1-4, L,’*’> -rp  <1-366>-mb
<Max Backups>
```

To view the current backup schedule:

```
racadm systemconfig getbackupscheduler
```

To disable automatic backup use the command:

```
racadm set LifeCycleController.lcattributes.autobackup Disabled
```

To clear the backup schedule:

```
racadm systemconfig clearbackupscheduler
```

For more information, see the iDRAC8 RACADM Command Line Interface Reference Guide available at **dell.com/support/manuals**.

Importing Server Profile

You can use the back up image file to import (restore) the configuration and firmware for the same server without rebooting the server.

In 13th generation servers, this feature automates the entire motherboard replacement process. After replacing the motherboard and reinstalling the memory, HDDs, and other hardware, a special boot screen is displayed that provides an option to restore all saved configuration, service tag and license settings, and diagnostic programs. The iDRAC on the new motherboard reads this information and restores the saved configuration.

Import feature is not licensed.

NOTE: For the restore operation, the system service tag and the service tag in the backup file must be identical. The restore operation applies to all system components that are same and present in the same location (example, in the same slot) as captured in the backup file. If components are different or not in the same location, they are not modified and restore failures is logged to the Lifecycle Log.

Before performing an import operation, make sure that Lifecycle Controller is enabled. If Lifecycle Controller is disabled, and if you initiate the import operation, the following message is displayed:

```
Lifecycle Controller is not enabled, cannot create Configuration job.
```

When import is already in-progress, and if you initiate a import operation again, the following error message is displayed:

```
Restore is already running
```

Import events are recorded in the Lifecycle Log.

Related Links

Restore Operation Sequence

Importing Server Profile Using iDRAC Web Interface

To import the server profile using iDRAC Web interface:

1. Go to **Overview → iDRAC Settings → Server Profile → Import**.
   The **Import Server Profile** page is displayed.
2. Select one of the following to specify the location of the backup file:
   - **Network**
   - **vFlash**
3. Enter the backup file name and decryption passphrase (optional).

4. If **Network** is selected as the file location, enter the network settings.

   NOTE: While specifying the network share settings, it is recommended to avoid special characters for user name and password or percent encode the special characters.

   For information about the fields, see the *iDRAC Online Help*.
5. Select one of the following for **Virtual disks configuration and hard disk data**:
   - **Preserve** - Preserves the RAID level, virtual disk, controller attributes, and hard disk data in the system and restores the system to a previously known state using the backup image file.
   - **Delete and Replace** - Deletes and replaces the RAID level, virtual disk, controller attributes, and hard disk configuration information in the system with the data from the backup image file.
6. Click **Import**.

   The import server profile operation is initiated.

Importing Server Profile Using RACADM

To import the server profile using RACADM, use **systemconfig restore** command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Restore Operation Sequence

The restore operation sequence is:

1. Host system shuts down.
2. Backup file information is used to restore the Lifecycle Controller.
3. Host system turns on.
4. Firmware and configuration restore process for the devices is completed.
5. Host system shuts down.
6. iDRAC firmware and configuration restore process is completed.
7. iDRAC restarts.
8. Restored host system turns on to resume normal operation.

Monitoring iDRAC Using Other Systems Management Tools

You can discover and monitor iDRAC using Dell Management Console or Dell OpenManage Essentials. You can also use Dell Remote Access Configuration Tool (DRACT) to discover iDRACs, update firmware, and set up Active Directory. For more information, see the respective user's guides.

4

Configuring iDRAC

iDRAC enables you to configure iDRAC properties, set up users, and set up alerts to perform remote management tasks.

Before you configure iDRAC, make sure that the iDRAC network settings and a supported browser is configured, and the required licenses are updated. For more information about the licensable feature in iDRAC, see Managing Licenses.

You can configure iDRAC using:

- iDRAC Web Interface
- RACADM
- Remote Services (see *Lifecycle Controller Remote Services User's Guide*)
- IPMITool (see *Baseboard Management Controller Management Utilities User's Guide*)

To configure iDRAC:

1. Log in to iDRAC.
2. Modify the network settings if required.

   NOTE: If you have configured iDRAC network settings, using iDRAC Settings utility during iDRAC IP address setup, then ignore this step.
3. Configure interfaces to access iDRAC.
4. Configure front panel display.
5. Configure System Location if required.
6. Configure time zone and Network Time Protocol (NTP) if required.
7. Establish any of the following alternate communication methods to iDRAC:
   - IPMI or RAC serial
   - IPMI serial over LAN
   - IPMI over LAN
   - SSH or Telnet client
8. Obtain the required certificates.
9. Add and configure iDRAC users with privileges.
10. Configure and enable e-mail alerts, SNMP traps, or IPMI alerts.
11. Set the power cap policy if required.
12. Enable the Last Crash Screen.
13. Configure virtual console and virtual media if required.
14. Configure vFlash SD card if required.
15. Set the first boot device if required.
16. Set the OS to iDRAC Pass-through if required.

Related Links

Logging into iDRAC

Modifying Network Settings
Configuring Services
Configuring Front Panel Display
Setting Up Managed System Location
Configuring Time Zone and NTP
Setting Up iDRAC Communication
Configuring User Accounts and Privileges
Monitoring and Managing Power
Enabling Last Crash Screen
Configuring and Using Virtual Console
Managing Virtual Media
Managing vFlash SD Card
Setting First Boot Device
Enabling or Disabling OS to iDRAC Pass-through
Configuring iDRAC to Send Alerts

Viewing iDRAC Information

You can view the basic properties of iDRAC.

Viewing iDRAC Information Using Web Interface

In the iDRAC Web interface, go to **Overview → iDRAC Settings → Properties** to view the following information related to iDRAC. For information about the properties, see *iDRAC Online Help*.

- Hardware and firmware version
- Last firmware update
- RAC time
- IPMI version
- User interface title bar information
- Network settings
- IPv4 Settings
- IPv6 Settings

Viewing iDRAC Information Using RACADM

To view iDRAC information using RACADM, see `getsysinfo` or `get` subcommand details provided in the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Modifying Network Settings

After configuring the iDRAC network settings using the iDRAC Settings utility, you can also modify the settings through the iDRAC Web interface, RACADM, Lifecycle Controller, Dell Deployment Toolkit, and Server Administrator (after booting to the operating system). For more information on the tools and privilege settings, see the respective user's guides.

To modify the network settings using iDRAC Web interface or RACADM, you must have **Configure** privileges.

NOTE: Changing the network settings may terminate the current network connections to iDRAC.

Modifying Network Settings Using Web Interface

To modify the iDRAC network settings:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network**.
   The **Network** page is displayed.
2. Specify the network settings, common settings, IPv4, IPv6, IPMI, and/or VLAN settings as per your requirement and click **Apply**.
   If you select **Auto Dedicated NIC** under **Network Settings**, when the iDRAC has its NIC Selection as shared LOM (1, 2, 3, or 4) and a link is detected on the iDRAC dedicated NIC, the iDRAC changes its NIC selection to use the dedicated NIC. If no link is detected on the dedicated NIC, then the iDRAC uses the shared LOM. The switch from shared to dedicated time-out is five seconds and from dedicated to shared is 30 seconds. You can configure this time-out value using RACADM or WS-MAN.

   For information about the various fields, see the *iDRAC Online Help*.

Modifying Network Settings Using Local RACADM

To generate a list of available network properties, type the following:

NOTE: You can use either **getconfig** and **config** commands or **get** and **set** commands with the RACADM objects.

- Using **getconfig** command: `racadm getconfig -g cfgLanNetworking`
- Using **get** command: `racadm get iDRAC.Nic`

To use DHCP to obtain an IP address, use the following command to write the object **cfgNicUseDhcp** or **DHCPEnable** and enable this feature:

- Using **config** command: `racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1`
- Using **set** command: `racadm set iDRAC.IPv4.DHCPEnable 1`

The following is an example of how the command may be used to configure the required LAN network properties:

- Using **config** command:

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0
racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002
racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

- Using **set** command:

```
racadm set iDRAC.Nic.Enable 1
racadm set iDRAC.IPv4.Address 192.168.0.120
```

```
racadm set iDRAC.IPv4.Netmask 255.255.255.0
racadm set iDRAC.IPv4.Gateway 192.168.0.120
racadm set iDRAC.IPv4.DHCPEnable 0
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNS1 192.168.0.5
racadm set iDRAC.IPv4.DNS2 192.168.0.6
racadm set iDRAC.Nic.DNSRegister 1
racadm set iDRAC.Nic.DNSRacName RAC-EK00002
racadm set iDRAC.Nic.DNSDomainFromDHCP 0
racadm set iDRAC.Nic.DNSDomainName MYDOMAIN
```

NOTE: If **cfgNicEnable** or **iDRAC.Nic.Enable** is set to **0**, the iDRAC LAN is disabled even if DHCP is enabled.

Configuring IP Filtering

In addition to user authentication, use the following options to provide additional security while accessing iDRAC:

- IP filtering limits the IP address range of the clients accessing iDRAC. It compares the IP address of an incoming login to the specified range and allows iDRAC access only from a management station whose IP address is within the range. All other login requests are denied.
- When repeated login failures occur from a particular IP address, it prevents the address from logging in to iDRAC for a preselected time span. If you unsuccessfully log in up to two times, you are allowed to log in again only after 30 seconds. If you unsuccessfully log in more than two times, you are allowed to log in again only after 60 seconds.

As login failures accumulate from a specific IP address, they are registered by an internal counter. When the user successfully logs in, the failure history is cleared and the internal counter is reset.

NOTE: When login attempts are prevented from the client IP address, few SSH clients may display the message: `ssh exchange identification: Connection closed by remote host`.

NOTE: If you are using Dell Deployment Toolkit (DTK), see the *Dell Deployment Toolkit User's Guide* for the privileges.

Configure IP Filtering Using iDRAC Web Interface

You must have Configure privilege to perform these steps.

To configure IP filtering:

1. In iDRAC Web interface, go to **Overview → iDRAC Settings → Network → Network**.
   The **Network** page is displayed.
2. Click **Advanced Settings**.
   The **Network Security** page is displayed.
3. Specify the IP filtering settings.
   For more information about the options, see *iDRAC Online Help*.
4. Click **Apply** to save the settings.

Configuring IP Filtering Using RACADM

You must have Configure privilege to perform these steps.

To configure IP filtering, use the following RACADM objects:

- With **config** command:

  - cfgRacTuneIpRangeEnable
  - cfgRacTuneIpRangeAddr
  - cfgRacTuneIpRangeMask
- With **set** command, use the objects in the **iDRAC.IPBlocking** group:
  - RangeEnable
  - RangeAddr
  - RangeMask

The **cfgRacTuneIpRangeMask** or the **RangeMask** property is applied to both the incoming IP address and to the **cfgRacTuneIpRangeAddr** or **RangeAddr** property. If the results are identical, the incoming login request is allowed to access iDRAC. Logging in from IP addresses outside this range results in an error.

The login proceeds if the following expression equals zero:

- Using legacy syntax: `cfgRacTuneIpRangeMask & (<incoming-IP-address> ^ cfgRacTuneIpRangeAddr)`
- Using new syntax: `RangeMask & (<incoming-IP-address> ^ RangeAddr)`

where, & is the bitwise AND of the quantities and ^ is the bitwise exclusive-OR.

Examples for IP Filtering

- The following RACADM commands block all IP addresses except 192.168.0.57:
  - Using **config** command:

    ```
    racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
    racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57
    racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
    ```

  - Using **set** command:

    ```
    racadm set iDRAC.IPBlocking.RangeEnable 1
    racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.57
    racadm set iDRAC.IPBlocking.RangeMask 255.255.255.255
    ```

- To restrict logins to a set of four adjacent IP addresses (for example, 192.168.0.212 through 192.168.0.215), select all but the lowest two bits in the mask:
  - Using **set** command:

    ```
    racadm set iDRAC.IPBlocking.RangeEnable 1
    racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.212
    racadm set iDRAC.IPBlocking.RangeMask 255.255.255.252
    ```

    The last byte of the range mask is set to 252, the decimal equivalent of 11111100b.

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/support/manuals**.

Configuring Services

You can configure and enable the following services on iDRAC:

- Local Configuration — Disable access to iDRAC configuration (from the host system) using Local RACADM and iDRAC Settings utility.
- Web Server — Enable access to iDRAC Web interface. If you disable the option, use local RACADM to re-enable the Web Server, since disabling the Web Server also disables remote RACADM.

- SSH — Access iDRAC through firmware RACADM.
- Telnet — Access iDRAC through firmware RACADM
- Remote RACADM — Remotely access iDRAC.
- SNMP Agent — Enables support for SNMP queries (GET, GETNEXT, and GETBULK operations) in iDRAC.
- Automated System Recovery Agent — Enable Last System Crash Screen.
- VNC Server — Enable VNC server with or without SSL encryption.

Configuring Services Using Web Interface

To configure the services using iDRAC Web interface:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network → Services**.
   The **Services** page is displayed.
2. Specify the required information and click **Apply**.
   For information about the various settings, see the *iDRAC Online Help*.

Configuring Services Using RACADM

To enable and configure the various services using RACADM:

- Use the following objects with the **config** command:
  - cfgRacTuneLocalConfigDisable
  - cfgRacTuneCtrlEConfigDisable
  - cfgSerialSshEnable
  - cfgRacTuneSshPort
  - cfgSsnMgtSshIdleTimeout
  - cfgSerialTelnetEnable
  - cfgRacTuneTelnetPort
  - cfgSsnMgtTelnetIdleTimeout
  - cfgRacTuneWebserverEnable
  - cfgSsnMgtWebserverTimeout
  - cfgRacTuneHttpPort
  - cfgRacTuneHttpsPort
  - cfgRacTuneRemoteRacadmEnable
  - cfgSsnMgtRacadmTimeout
  - cfgOobSnmpAgentEnable
  - cfgOobSnmpAgentCommunity
- Use the objects in the following object groups with the **set** command:
  - iDRAC.LocalSecurity
  - iDRAC.LocalSecurity
  - iDRAC.SSH
  - iDRAC.Webserver
  - iDRAC.Telnet

– iDRAC.Racadm
– iDRAC.SNMP

For more information about these objects, see *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Enabling or Disabling HTTPs Redirection

If you do not want automatic redirection from HTTP to HTTPs due to certificate warning issue with default iDRAC certificate or as a temporary setting for debugging purpose, you can configure iDRAC such that redirection from http port (default is 80) to https port (default is 443) is disabled. By default, it is enabled. You have to log out and log in to iDRAC for this setting to take effect. When you disable this feature, a warning message is displayed.

You must have Configure iDRAC privilege to enable or disable HTTPs redirection.

An event is recorded in the Lifecycle Controller log file when this feature is enabled or disabled.

To disable the HTTP to HTTPs redirection:

```
racadm set iDRAC.Webserver.HttpsRedirection Disabled
```

To enable HTTP to HTTPs redirection:

```
racadm set iDRAC.Webserver.HttpsRedirection Enabled
```

To view the status of the HTTP to HTTPs redirection:

```
racadm get iDRAC.Webserver.HttpsRedirection
```

Using VNC Client to Manage Remote Server

You can use a standard open VNC client to manage the remote server using both desktop and mobile devices such as Dell Wyse PocketCloud. When servers in data centers stop functioning, the iDRAC or the operating system sends an alert to the console on the management station. The console sends an email or SMS to a mobile device with required information and launches VNC viewer application on the management station. This VNC viewer can connect to OS/Hypervisor on the server and provide access to keyboard, video and mouse of the host server to perform the necessary remediation. Before launching the VNC client, you must enable the VNC server and configure the VNC server settings in iDRAC such as password, VNC port number, SSL encryption, and the time out value. You can configure these settings using iDRAC Web interface or RACADM.

NOTE: VNC feature is licensed and is available in the iDRAC Enterprise license.

You can choose from many VNC applications or Desktop clients such as the ones from RealVNC or Dell Wyse PocketCloud.

Only one VNC client session can be active at a time.

If a VNC session is active, you can only launch the Virtual Media using Launch Virtual Console and not the Virtual Console Viewer.

If video encryption is disabled, the VNC client starts RFB handshake directly, and a SSL handshake is not required. During VNC client handshake (RFB or SSL), if another VNC session is active or if a Virtual Console session is open, the new VNC client session is rejected. After completion of the initial handshake,

VNC server disables Virtual Console and allows only Virtual Media. After termination of the VNC session, VNC server restores the original state of Virtual Console (enabled or disabled).

NOTE:
- When iDRAC NIC is in shared mode and the host system is power cycled, the network connection is lost for a few seconds. During this time, if you perform any action in the active VNC client, the VNC session may close. You must wait for timeout (value configured for the VNC Server settings in the **Services** page in iDRAC Web interface) and then re-establish the VNC connection.
- If the VNC client window is minimized for more than 60 seconds, the client window closes. You must open a new VNC session. If you maximize the VNC client window within 60 seconds, you can continue to use it.

Configuring VNC Server Using iDRAC Web Interface

To configure the VNC server settings:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network → Services**.
   The **Services** page is displayed.
2. In the **VNC Server** section, enable the VNC server, specify the password, port number, and enable or disable SSL encryption.
   For information about the fields, see the *iDRAC Online Help*.
3. Click **Apply**.
   The VNC server is configured.

Configuring VNC Server Using RACADM

To configure the VNC server, use the `VNCserver` object with the `set` command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Setting Up VNC Viewer With SSL Encryption

While configuring the VNC server settings in iDRAC, if the **SSL Encryption** option was enabled, then the SSL tunnel application must be used along with the VNC Viewer to establish the SSL encrypted connection with iDRAC VNC server.

NOTE: Most of the VNC clients do not have built-in SSL encryption support.

To configure the SSL tunnel application:

1. Configure SSL tunnel to accept connection on `<localhost>:<localport number>`. For example, 127.0.0.1:5930.
2. Configure SSL tunnel to connect to `<iDRAC IP address>:<VNC server port Number>`. For example, 192.168.0.120:5901.
3. Start the tunnel application.
   To establish connection with the iDRAC VNC server over the SSL encrypted channel, connect the VNC viewer to the localhost (link local IP address) and the local port number (127.0.0.1:<local port number>).

Setting Up VNC Viewer Without SSL Encryption

In general, all Remote Frame Buffer (RFB) compliant VNC Viewers connect to the VNC server using the iDRAC IP address and port number that is configured for the VNC server. If the SSL encryption option is

disabled when configuring the VNC server settings in iDRAC, then to connect to the VNC Viewer do the following:

In the **VNC Viewer** dialog box, enter the iDRAC IP address and the VNC port number in the **VNC Server** field.

The format is `<iDRAC IP address:VNC port number>`

For example, if the iDRAC IP address is 192.168.0.120 and VNC port number is 5901, then enter `192.168.0.120:5901`.

Configuring Front Panel Display

You can configure the front panel LCD and LED display for the managed system.

For rack and tower servers, two types of front panels are available:

- LCD front panel and System ID LED
- LED front panel and System ID LED

For blade servers, only the System ID LED is available on the server front panel since the blade chassis has the LCD.

Related Links

Configuring LCD Setting
Configuring System ID LED Setting

Configuring LCD Setting

You can set and display a default string such as iDRAC name, IP, and so on or a user-defined string on the LCD front panel of the managed system.

Configuring LCD Setting Using Web Interface

To configure the server LCD front panel display:

1. In iDRAC Web interface, go to **Overview** → **Hardware** → **Front Panel**.
2. In **LCD Settings** section, from the **Set Home Message** drop-down menu, select any of the following:
   - Service Tag (default)
   - Asset Tag
   - DRAC MAC Address
   - DRAC IPv4 Address
   - DRAC IPv6 Address
   - System Power
   - Ambient Temperature
   - System Model
   - Host Name
   - User Defined
   - None

     If you select **User Defined**, enter the required message in the text box.

If you select **None**, home message is not displayed on the server LCD front panel.

3. Enable Virtual Console indication (optional). If enabled, the Live Front Panel Feed section and the LCD panel on the server displays the `Virtual console session active` message when there is an active Virtual Console session.
4. Click **Apply**.

   The server LCD front panel displays the configured home message.

Configuring LCD Setting Using RACADM

To configure the server LCD front panel display, use the objects in the System.LCD group. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Configuring LCD Setting Using iDRAC Settings Utility

To configure the server LCD front panel display:

1. In the iDRAC Settings utility, go to **Front Panel Security**.

   The **iDRAC Settings.Front Panel Security** page is displayed.
2. Enable or disable the power button.
3. Specify the following:
   - Access to the front panel
   - LCD message string
   - System power units, ambient temperature units, and error display
4. Enable or disable the virtual console indication.

   For information about the options, see the *iDRAC Settings Utility Online Help*.
5. Click **Back**, click **Finish**, and then click **Yes**.

Configuring System ID LED Setting

To identify a server, enable or disable System ID LED blinking on the managed system.

Configuring System ID LED Setting Using Web Interface

To configure the System ID LED display:

1. In iDRAC Web interface, go to **Overview → Hardware → Front Panel**. The **Front Panel** page is displayed.
2. In **System ID LED Settings** section, select any of the following options to enable or disable LED blinking:
   - Blink Off
   - Blink On
   - Blink On 1 Day Timeout
   - Blink On 1 Week Timeout
   - Blink On 1 Month Timeout
3. Click **Apply**.

   The LED blinking on the front panel is configured.

Configuring System ID LED Setting Using RACADM

To configure system ID LED, use the **setled** command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Configuring Time Zone and NTP

You can configure the time zone on iDRAC and synchronize the iDRAC time using Network Time Protocol (NTP) instead of BIOS or host system times.

You must have Configure privilege to configure time zone or NTP settings.

Configuring Time Zone and NTP Using iDRAC Web Interface

To configure time zone and NTP using iDRAC Web interface:

1. Go to **Overview → iDRAC Settings → Properties → Settings**.
   The **Time zone and NTP** page is displayed.
2. To configure the time zone, from the **Time Zone** drop-down menu, select the required time zone, and then click **Apply**.
3. To configure NTP, enable NTP, enter the NTP server addresses, and then click **Apply**.
   For information about the fields, see *iDRAC Online Help*.

Configuring Time Zone and NTP Using RACADM

To configure time zone and NTP using RACADM, use the objects in the **iDRAC.Time** and **iDRAC.NTPConfigGroup** group with the **set** command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Setting First Boot Device

You can set the first boot device for the next boot only or for all subsequent reboots. Based on this selection, you can set the first boot device for the system. The system boots from the selected device on the next and subsequent reboots and remains as the first boot device in the BIOS boot order, until it is changed again either from the iDRAC Web interface or from the BIOS boot sequence. You can set the first boot device to one of the following:

- Normal Boot
- PXE
- BIOS Setup
- Local Floppy/Primary Removable Media
- Local CD/DVD
- Hard Drive
- Virtual Floppy
- Virtual CD/DVD/ISO
- Local SD Card
- vFlash
- Lifecycle Controller

- BIOS Boot Manager

NOTE:

- BIOS Setup (F2), Lifecycle Controller (F10), BIOS Boot Manager (F11) only support boot once enabled.
- Virtual Console does not support permanent boot configuration. It is always boot once.
- The first boot device setting in iDRAC Web Interface overrides the System BIOS boot settings.

Setting First Boot Device Using Web Interface

To set the first boot device using iDRAC Web interface:

1. Go to **Overview** → **Server** → **Setup** → **First Boot Device**.
   The **First Boot Device** page is displayed.
2. Select the required first boot device from the drop-down list, and click **Apply**.
   The system boots from the selected device for subsequent reboots.
3. To boot from the selected device only once on the next boot, select **Boot Once**. Thereafter, the system boots from the first boot device in the BIOS boot order.
   For more information about the options, see the *iDRAC Online Help*.

Setting First Boot Device Using RACADM

- To set the first boot device, use the **cfgServerFirstBootDevice** object.
- To enable boot once for a device, use the **cfgServerBootOnce** object.

For more information about these objects, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Setting First Boot Device Using Virtual Console

You can select the device to boot from as the server is being viewed in the Virtual Console viewer before the server runs through its boot-up sequence. You can perform boot once to all the supported devices listed in Setting First Boot Device.

To set the first boot device using Virtual Console:

1. Launch Virtual Console.
2. In the Virtual Console Viewer, from the **Next Boot** menu, set the required device as the first boot device.

Enabling Last Crash Screen

To troubleshoot the cause of managed system crash, you can capture the system crash image using iDRAC.

To enable the last crash screen:

1. From the *Dell Systems Management Tools and Documentation* DVD, install Server Administrator on the managed system.
   For more information, see the *Dell OpenManage Server Administrator Installation Guide* at **dell.com/support/manuals**.
2. In the **Windows** startup and recovery window, make sure that the automatic reboot option is not selected.

For more information, see Windows documentation.

3. Use Server Administrator to enable the **Auto Recovery** timer, set the Auto Recovery action to **Reset**, **Power Off**, or **Power Cycle**, and set the timer in seconds (a value between 60 - 480).

   For more information, see the *Dell OpenManage Server Administrator Installation Guide* at **dell.com/support/manuals**.

4. Enable the **Auto Shutdown and Recovery** (ASR) option using one of the following:
   - Server Administrator — See *Dell OpenManage Server Administrator User's Guide* at **dell.com/support/manuals**.
   - Local RACADM — Use the command:

     ```
     racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
     ```

5. Enable **Automated System Recovery Agent**. To do this, go to **Overview → iDRAC Settings → Network → Services**, select **Enabled** and click **Apply**.

Enabling or Disabling OS to iDRAC Pass-through

In servers that have Network Daughter Card (NDC) or embedded LAN On Motherboard (LOM) devices, you can enable the OS to iDRAC Pass-through feature that provides a high-speed bi-directional in-band communication between iDRAC and the host operating system through a shared LOM (rack or tower servers), a dedicated NIC (rack, tower, or blade servers), or through the USB NIC. This feature is available for iDRAC Enterprise license.

When enabled through dedicated NIC, you can launch the browser in the host operating system and then access the iDRAC Web interface. The dedicated NIC for the blade servers is through the Chassis Management Controller.

Switching between dedicated NIC or shared LOM does not require a reboot or reset of the host operating system or iDRAC.

You can enable this channel using:

- iDRAC Web interface
- RACADM or WS-MAN (post operating system environment)
- iDRAC Settings utility (pre-operating system environment)

If the network configuration is changed through iDRAC Web interface, you must wait for at least 10 seconds before enabling OS to iDRAC Pass-through.

If you are using the XML configuration file through RACADM or WS-MAN and if the network settings are changed in this file, then you must wait for 15 seconds to either enable OS to iDRAC Pass-through feature or set the OS Host IP address.

Before enabling OS to iDRAC Pass-through, make sure that:

- iDRAC is configured to use dedicated NIC or shared mode (that is, NIC selection is assigned to one of the LOMs).
- Host operating system and iDRAC are in the same subnet and same VLAN.
- Host operating system IP address is configured.
- A card that supports OS to iDRAC pass-through capability is installed.
- You have Configure privilege.

When you enable this feature:

- In shared mode, the host operating system's IP address is used.
- In dedicated mode, you must provide a valid IP address of the host operating system. If more than one LOM is active, enter the first LOM's IP address.

After enabling OS to iDRAC Pass-through feature, if it is not working:

- Check whether the iDRAC's dedicated NIC cable is connected properly.
- Make sure that at least one LOM is active.

Related Links

Supported Cards for OS to iDRAC Pass-through
Supported Operating Systems for USB NIC
Enabling or Disabling OS to iDRAC Pass-through Using Web Interface
Enabling or Disabling OS to iDRAC Pass-through Using RACADM
Enabling or Disabling OS to iDRAC Pass-through Using iDRAC Settings Utility

Supported Cards for OS to iDRAC Pass-through

The following table provides a list of cards that support the OS to iDRAC Pass-through feature using LOM.

Table 7. : OS to iDRAC Pass-through Using LOM — Supported Cards

Category	Manufacturer	Type
NDC	Broadcom	• 5720 QP rNDC 1G BASE-T • 57810S DP bNDC KR • 57800S QP rNDC (10G BASE-T + 1G BASE-T) • 57800S QP rNDC (10G SFP+ + 1G BASE-T) • 57840 4x10G KR • 57840 rNDC
	Intel	• i540 QP rNDC (10G BASE-T + 1G BASE-T) • i350 QP rNDC 1G BASE-T • x520/i350 rNDC 1GB
	Qlogic	QMD8262 Blade NDC

In-built LOM cards also support the OS to iDRAC pass-through feature.

The following cards do not support the OS to iDRAC Pass-through feature:

- Intel 10 GB NDC.
- Intel rNDC with two controllers – 10G controllers does not support.
- Qlogic bNDC
- PCIe, Mezzanine, and Network Interface Cards.

Supported Operating Systems for USB NIC

The operating systems supported for USB NIC are:

- Windows Server 2008 SP2 (64-bit)
- Windows Server 2008 SP2 R2 (64-bit)

- Windows Server 2012 SP1
- SLES 10 SP4 (64-bit)
- SLES 11 SP2 (64-bit)
- RHEL 5.9 (32-bit and 64-bit)
- RHEL 6.4
- vSphere v5.0 U2 ESXi
- vSphere v5.1 U1 ESXi
- vSphere v5.5 ESXi

On servers with Windows 2008 SP2 64-bit operating system, the iDRAC Virtual CD USB Device is not discovered automatically (or enabled). You must enable this manually. For more information, see steps recommended by Microsoft to manually update the Remote Network Driver Interface Specification (RNDIS) driver for this device.

For Linux operating systems, configure the USB NIC as DHCP on the host operating system before enabling USB NIC.

If the host operating system is SUSE Linux Enterprise Server 11, then after enabling the USB NIC in iDRAC, you must manually enable DHCP client on the host operating system. For information to enable DHCP, see the documents for SUSE Linux Enterprise Server 11 operating systems.

For vSphere, you must install the VIB file before enabling USB NIC.

For the following operating systems, if you install the Avahi and nss-mdns packages, then you can use **https://idrac.local** to launch the iDRAC from the host operating system. If these packages are not installed, use **https://169.254.0.1** to launch the iDRAC.

Operating System	Firewall Status	Avahi Package	nss-mdns Package
RHEL 5.9 32–bit	Disable	Install as a separate package (**avahi-0.6.16-10.el5_6.i386.rpm**)	Install as a separate package (**nss-mdns-0.10-4.el5.i386.rpm**)
RHEL 6.4 64–bit	Disable	Install as a separate package (**avahi-0.6.25-12.el6.x86_64.rpm**)	Install as a separate package (**nss-mdns-0.10-8.el6.x86_64.rpm**)
SLES 11 SP3 64–bit	Disable	Avahi package is the part of operating system DVD	nss-mdns is installed while installing Avahi

On the host system, while installing RHEL 5.9 operating system, the USB NIC pass-through mode is in disabled state. If it is enabled after the installation is complete, the network interface corresponding to the USB NIC device is not active automatically. You can do any of the following to make the USB NIC device active:

- Configure the USB NIC interface using Network Manager tool. Navigate to **System → Administrator → Network → Devices → New → Ethernet Connection** and select **Dell computer corp.iDRAC Virtual NIC USB Device**. Click the Activate icon to activate the device. For more information, see the RHEL 5.9 documentation.
- Create corresponding interface's config file as **ifcfg-ethX** in **/etc/sysconfig/network-script/** directory. Add the basic entries DEVICE, BOOTPROTO, HWADDR, ONBOOT. Add TYPE in the **ifcfg-ethX** file and restart the network services using the command `service network restart`.
- Reboot the system.

- Turn off and turn on the system.

On systems with RHEL 5.9 operating system, if the USB NIC was disabled and if you turn off the system or vice-versa, when the system is turned on and if the USB NIC is enabled, the USB NIC device is not active automatically. To make it active, check if any **ifcfg-ethX.bak** file is available in the **/etc/sysconfig/network-script** directory for the USB NIC interface. If it is available, rename it to **ifcfg-ethX** and then use the `ifup ethX` command.

Related Links

Installing VIB File

Installing VIB File

For vSphere operating systems, before enabling the USB NIC, you must install the VIB file.

To install the VIB file:

1. Using Win-SCP, copy the VIB file to **/tmp/** folder of the ESX-i host operating system.
2. Go to the ESXi prompt and run the following command:

   ```
   esxcli software vib install -v /tmp/ iDRAC_USB_NIC-1.0.0-799733X03.vib --no-sig-check
   ```

   The output is:

   ```
   Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: Dell_bootbank_iDRAC_USB_NIC_1.0.0-799733X03
   VIBs Removed:
   VIBs Skipped:
   ```
3. Reboot the server.
4. At the ESXi prompt, run the command: `esxcfg-vmknic -l`.

   The output displays the usb0 entry.

Enabling or Disabling OS to iDRAC Pass-through Using Web Interface

To enable OS to iDRAC Pass-through using Web interface:

1. Go to **Overview → iDRAC Settings → Network → OS to iDRAC Pass-through**.

   The **OS to iDRAC Pass-through** page is displayed.
2. Select any of the following options to enable OS to iDRAC pass-through:
   - **LOM** — The OS to iDRAC pass-through link between the iDRAC and the host operating system is established through the LOM or NDC.
   - **USB NIC** — The OS to iDRAC pass-through link between the iDRAC and the host operating system is established through the internal USB bus.

   To disable this feature, select **Disabled**.
3. If you select **LOM** as the pass-through configuration, and if the server is connected using dedicated mode, enter the IPv4 address of the operating system.

   NOTE: If the server is connected in shared LOM mode, then the **OS IP Address** field is disabled.
4. If you select **USB NIC** as the pass-through configuration, enter the IP address of the USB NIC.

   The default value is 169.254.0.1. It is recommended to use the default IP address. However, if this IP address conflicts with an IP address of other interfaces of the host system or the local network, you must change it.

Do not enter 169.254.0.3 and 169.254.0.4 IPs. These IPs are reserved for the USB NIC port on the front panel when a A/A cable is used.

5. Click **Apply** to apply the settings.
6. Click **Test Network Configuration** to check if the IP is accessible and the link is established between the iDRAC and the host operating system.

Enabling or Disabling OS to iDRAC Pass-through Using RACADM

To enable or disable OS to iDRAC Pass-through using RACADM, use the objects in the iDRAC.OS-BMC group. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Enabling or Disabling OS to iDRAC Pass-through Using iDRAC Settings Utility

To enable or disable OS to iDRAC Pass-through using iDRAC Settings Utility:

1. In the iDRAC Settings utility, go to **Communications Permissions**.
   The **iDRAC Settings.Communications Permissions** page is displayed.
2. Select any of the following options to enable OS to iDRAC pass-through:
   - **LOM** — The OS to iDRAC pass-through link between the iDRAC and the host operating system is established through the LOM or NDC.
   - **USB NIC** — The OS to iDRAC pass-through link between the iDRAC and the host operating system is established through the internal USB bus.

   To disable this feature, select **Disabled**.

   NOTE: The LOM option can be selected only of the card supports OS to iDRAC pass-through capability. Else, this option is grayed-out.
3. If you select **LOM** as the pass-through configuration, and if the server is connected using dedicated mode, enter the IPv4 address of the operating system.

   NOTE: If the server is connected in shared LOM mode, then the **OS IP Address** field is disabled.
4. If you select **USB NIC** as the pass-through configuration, enter the IP address of the USB NIC.
   The default value is 169.254.0.1. However, if this IP address conflicts with an IP address of other interfaces of the host system or the local network, you must change it. Do not enter 169.254.0.3 and 169.254.0.4 IPs. These IPs are reserved for the USB NIC port on the front panel when a A/A cable is used
5. Click **Back**, click **Finish**, and then click **Yes**. The details are saved.

Obtaining Certificates

The following table lists the types of certificates based on the login type.

Table 8. Types of Certificate Based on Login Type

Login Type	Certificate Type	How to Obtain
Single Sign-on using Active Directory	Trusted CA certificate	Generate a CSR and get it signed from a Certificate Authority

Login Type	Certificate Type	How to Obtain
		SHA-2 certificates are also supported.
Smart Card login as a local or Active Directory user	• User certificate • Trusted CA certificate	• User Certificate — Export the smart card user certificate as Base64-encoded file using the card management software provided by the smart card vendor. • Trusted CA certificate — This certificate is issued by a CA. SHA-2 certificates are also supported.
Active Directory user login	Trusted CA certificate	This certificate is issued by a CA. SHA-2 certificates are also supported.
Local User login	SSL Certificate	Generate a CSR and get it signed from a trusted CA **NOTE:** iDRAC ships with a default self-signed SSL server certificate. The iDRAC Web server, Virtual Media, and Virtual Console use this certificate. SHA-2 certificates are also supported.

Related Links

SSL Server Certificates
Generating a New Certificate Signing Request

SSL Server Certificates

iDRAC includes a Web server that is configured to use the industry-standard SSL security protocol to transfer encrypted data over a network. Built upon asymmetric encryption technology, SSL is widely accepted for providing authenticated and encrypted communication between clients and servers to prevent eavesdropping across a network.

An SSL-enabled system can perform the following tasks:

- Authenticate itself to an SSL-enabled client
- Allow the two systems to establish an encrypted connection

The encryption process provides a high level of data protection. iDRAC employs the 128-bit SSL encryption standard, the most secure form of encryption generally available for Internet browsers in North America.

iDRAC Web server has a Dell self-signed unique SSL digital certificate by default. You can replace the default SSL certificate with a certificate signed by a well-known Certificate Authority (CA). A Certificate

Authority is a business entity that is recognized in the Information Technology industry for meeting high standards of reliable screening, identification, and other important security criteria. Examples of CAs include Thawte and VeriSign. To initiate the process of obtaining a CA-signed certificate, use either iDRAC Web interface or RACADM interface to generate a Certificate Signing Request (CSR) with your company's information. Then, submit the generated CSR to a CA such as VeriSign or Thawte. The CA can be a root CA or an intermediate CA. After you receive the CA-signed SSL certificate, upload this to iDRAC.

For each iDRAC to be trusted by the management station, that iDRAC's SSL certificate must be placed in the management station's certificate store. Once the SSL certificate is installed on the management stations, supported browsers can access iDRAC without certificate warnings.

You can also upload a custom signing certificate to sign the SSL certificate, rather than relying on the default signing certificate for this function. By importing one custom signing certificate into all management stations, all the iDRACs using the custom signing certificate are trusted. If a custom signing certificate is uploaded when a custom SSL certificate is already in-use, then the custom SSL certificate is disabled and a one-time auto-generated SSL certificate, signed with the custom signing certificate, is used. You can download the custom signing certificate (without the private key). You can also delete an existing custom signing certificate. After deleting the custom signing certificate, iDRAC resets and auto-generates a new self-signed SSL certificate. If a self-signed certificate is regenerated, then the trust must be re-established between that iDRAC and the management workstation. Auto-generated SSL certificates are self-signed and have an expiration date of seven years and one day and a start date of one day in the past (for different time zone settings on management stations and the iDRAC).

The iDRAC Web server SSL certificate supports the asterisk character (*) as part of the left-most component of the Common Name when generating a Certificate Signing Request (CSR). For example, *.qa.com, or *.company.qa.com. This is called a wildcard certificate. If a wildcard CSR is generated outside of iDRAC, you can have a signed single wildcard SSL certificate that you can upload for multiple iDRACs and all the iDRACs are trusted by the supported browsers. While connecting to iDRAC Web interface using a supported browser that supports a wildcard certificate, the iDRAC is trusted by the browser. While launching viewers, the iDRACs are trusted by the viewer clients.

Related Links

Generating a New Certificate Signing Request
Uploading Server Certificate
Viewing Server Certificate
Uploading Custom Signing Certificate
Downloading Custom SSL Certificate Signing Certificate
Deleting Custom SSL Certificate Signing Certificate

Generating a New Certificate Signing Request

A CSR is a digital request to a Certificate Authority (CA) for a SSL server certificate. SSL server certificates allow clients of the server to trust the identity of the server and to negotiate an encrypted session with the server.

After the CA receives a CSR, they review and verify the information the CSR contains. If the applicant meets the CA's security standards, the CA issues a digitally-signed SSL server certificate that uniquely identifies the applicant's server when it establishes SSL connections with browsers running on management stations.

After the CA approves the CSR and issues the SSL server certificate, it can be uploaded to iDRAC. The information used to generate the CSR, stored on the iDRAC firmware, must match the information contained in the SSL server certificate, that is, the certificate must have been generated using the CSR created by iDRAC.

Related Links

SSL Server Certificates

Generating CSR Using Web Interface

To generate a new CSR:

NOTE: Each new CSR overwrites any previous CSR data stored in the firmware. The information in the CSR must match the information in the SSL server certificate. Else, iDRAC does not accept the certificate.

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network → SSL**, select **Generate Certificate Signing Request (CSR)** and click **Next**.

   The **Generate a New Certificate Signing Request** page is displayed.
2. Enter a value for each CSR attribute.

   For more information, see *iDRAC Online Help*.
3. Click **Generate**.

   A new CSR is generated. Save it to the management station.

Generating CSR Using RACADM

To generate a CSR using RACADM, use the objects in the **cfgRacSecurity** group with the **config** command or use the objects in the **iDRAC.Security** group with the **set** command, and then use the **sslcsrgen** command to generate the CSR. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Uploading Server Certificate

After generating a CSR, you can upload the signed SSL server certificate to the iDRAC firmware. iDRAC must be reset to apply the certificate. iDRAC accepts only X509, Base 64 encoded Web server certificates. SHA-2 certificates are also supported.

CAUTION: During reset, iDRAC is not available for a few minutes.

Related Links

SSL Server Certificates

Uploading Server Certificate Using Web Interface

To upload the SSL server certificate:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network → SSL**, select **Upload Server Certificate** and click **Next**.

   The **Certificate Upload** page is displayed.
2. Under **File Path**, click **Browse** and select the certificate on the management station.
3. Click **Apply**.

   The SSL server certificate is uploaded to iDRAC.
4. A pop-up message is displayed asking you to reset iDRAC immediately or at a later time. Click **Reset iDRAC** or **Reset iDRAC Later** as required.

iDRAC resets and the new certificate is applied. The iDRAC is not available for a few minutes during the reset.

NOTE: You must reset iDRAC to apply the new certificate. Until iDRAC is reset, the existing certificate is active.

Uploading Server Certificate Using RACADM

To upload the SSL server certificate, use the **sslcertupload** command. For more information, see the *RACADM Command Line Reference Guide for iDRAC* available at **dell.com/support/manuals**.

If the CSR is generated outside of iDRAC with a private key available, then to upload the certificate to iDRAC:

1. Send the CSR to a well-known root CA. CA signs the CSR and the CSR becomes a valid certificate.
2. Upload the private key using the remote racadm `sslkeyupload` command.
3. Upload the signed certificate to iDRAC using the remote racadm `sslcertupload` command.

   The new certificate is uploaded iDRAC. A message is displayed asking you to reset iDRAC.
4. Run the racadm **racreset** command to reset iDRAC.

   iDRAC resets and the new certificate is applied. The iDRAC is not available for a few minutes during the reset.

   NOTE: You must reset iDRAC to apply the new certificate. Until iDRAC is reset, the existing certificate is active.

Viewing Server Certificate

You can view the SSL server certificate that is currently being used in iDRAC.

Related Links

SSL Server Certificates

Viewing Server Certificate Using Web Interface

In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network → SSL**. The **SSL** page displays the SSL server certificate that is currently in use at the top of the page.

Viewing Server Certificate Using RACADM

To view the SSL server certificate, use the **sslcertview** command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Uploading Custom Signing Certificate

You can upload a custom signing certificate to sign the SSL certificate. SHA-2 certificates are also supported.

Uploading Custom Signing Certificate Using Web Interface

To upload the custom signing certificate using iDRAC Web interface:

1. Go to **Overview → iDRAC Settings → Network → SSL**.

   The **SSL** page is displayed.
2. Under **Custom SSL Certificate Signing Certificate**, select **Upload Custom SSL Certificate Signing Certificate** and click **Next**.

The **Upload Custom SSL Certificate Signing Certificate** page is displayed.

3. Click **Browse** and select the custom SSL certificate signing certificate file.

   Only Public-Key Cryptography Standards #12 (PKCS #12) compliant certificate is supported.
4. If the certificate is password protected, in the **PKCS#12 Password** field, enter the password.
5. Click **Apply**.

   The certificate is uploaded to iDRAC.
6. A pop-up message is displayed asking you to reset iDRAC immediately or at a later time. Click **Reset iDRAC** or **Reset iDRAC Later** as required.

   After iDRAC resets, the new certificate is applied. The iDRAC is not available for a few minutes during the reset.

   NOTE: You must reset iDRAC to apply the new certificate. Until iDRAC is reset, the existing certificate is active.

Uploading Custom SSL Certificate Signing Certificate Using RACADM

To upload the custom SSL certificate signing certificate using RACADM, use the **sslcertupload** subcommand, and then use the **racreset** command to reset iDRAC. For more information, see the *iDRAC8 2.00.00.00 RACADM Command Line Reference Guide* available at **www.dell.com/esmmanuals**.

Downloading Custom SSL Certificate Signing Certificate

You can download the custom signing certificate using iDRAC Web interface or RACADM.

Downloading Custom Signing Certificate

To download the custom signing certificate using iDRAC Web interface:

1. Go to **Overview → iDRAC Settings → Network → SSL**.

   The **SSL** page is displayed.
2. Under **Custom SSL Certificate Signing Certificate**, select **Download Custom SSL Certificate Signing Certificate** and click **Next**.

   A pop-up message is displayed that allows you to save the custom signing certificate to a location of your choice.

Downloading Custom SSL Certificate Signing Certificate Using RACADM

To download the custom SSL certificate signing certificate, use the **sslcertdownload** subcommand. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Deleting Custom SSL Certificate Signing Certificate

You can also delete an existing custom signing certificate using iDRAC Web interface or RACADM.

Deleting Custom Signing Certificate Using iDRAC Web Interface

To delete the custom signing certificate using iDRAC Web interface:

1. Go to **Overview → iDRAC Settings → Network → SSL**.

   The **SSL** page is displayed.
2. Under **Custom SSL Certificate Signing Certificate**, select **Delete Custom SSL Certificate Signing Certificate** and click **Next**.

3. A pop-up message is displayed asking you to reset iDRAC immediately or at a later time. Click **Reset iDRAC** or **Reset iDRAC Later** as required.

   After iDRAC resets, a new self-signed certificate is generated.

Deleting Custom SSL Certificate Signing Certificate Using RACADM

To delete the custom SSL certificate signing certificate using RACADM, use the **sslcertdelete** subcommand. Then, use the **racreset** command to reset iDRAC. For more information, see the *iDRAC8 2.00.00.00 RACADM Command Line Reference Guide* available at **www.dell.com/esmmanuals**.

Configuring Multiple iDRACs Using RACADM

You can configure one or more iDRACs with identical properties using RACADM. When you query a specific iDRAC using its group ID and object ID, RACADM creates the **.cfg** configuration file from the retrieved information. File name is user specified. Import the file to other iDRACs to identically configure them.

NOTE:

- The configuration file contains information that is applicable for the particular server. The information is organized under various object groups.
- Few configuration files contain unique iDRAC information (such as the static IP address) that you must modify before you export the file to other iDRACs.

You can also use the system configuration XML file to configure multiple iDRACs using RACADM. System configuration XML file contains the component configuration information, and this file is used to apply the configuration for BIOS, iDRAC, RAID, and NIC by importing the file into a target system. For more information, see *XML Configuration Workflow* white paper available at **dell.com/support/manuals** or at Dell Tech Center.

To configure multiple iDRACs using the **.cfg** file:

1. Query the target iDRAC that contains the required configuration using the command: `racadm getconfig -f myfile.cfg`.

   The command requests the iDRAC configuration and generates the **myfile.cfg** file. If required, you can configure the file with another name.

   NOTE: Redirecting the iDRAC configuration to a file using `getconfig -f` is only supported with the local and remote RACADM interfaces.

   NOTE: The generated .cfg file does not contain user passwords.

   The **getconfig** command displays all configuration properties in a group (specified by group name and index) and all configuration properties for a user by user name.
2. Modify the configuration file using a simple text editor (optional).

   NOTE: It is recommended that you edit this file with a simple text editor. The RACADM utility uses an ASCII text parser. Any formatting confuses the parser, which may corrupt the RACADM database.
3. Use the new configuration file to modify the target iDRAC using the command: `racadm config -f myfile.cfg`

   This loads the information into the other iDRAC. You can use **config** subcommand to synchronize the user and password database with Server Administrator.
4. Reset the target iDRAC using the command: `racadm racreset`

Creating an iDRAC Configuration File

The configuration file **.cfg** can be:

- Created
- Obtained from `racadm getconfig -f <filename>.cfg` command or `racadm get -f <filename>.cfg`
- Obtained from `racadm getconfig -f <filename>.cfg` command or `racadm get -f <filename>.cfg`, and then edited

  For information about the **getconfig** and **get** commands, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals** .

The **.cfg** file is first parsed to verify that valid group and object names are present and the basic syntax rules are being followed. Errors are flagged with the line number that detected the error, and a message explains the problem. The entire file is parsed for correctness, and all errors are displayed. Write commands are not transmitted to iDRAC if an error is found in the **.cfg** file. The user must correct all errors before using the file to configure iDRAC. Use the `-c` option in the `config` subcommand, which verifies the syntax and does not perform a write operation to iDRAC.

Use the following guidelines when you create a **.cfg** file:

- If the parser encounters an indexed group, the index of the group is used as the anchor. Any modifications to the objects within the indexed group is also associated with the index value.

  For example:

  – If you have used the **getconfig** command:

  ```
  [cfgUserAdmin]
  # cfgUserAdminIndex=11
  cfgUserAdminUserName=
  # cfgUserAdminPassword=******** (Write-Only)
  cfgUserAdminEnable=0
  cfgUserAdminPrivilege=0x00000000
  cfgUserAdminIpmiLanPrivilege=15
  cfgUserAdminIpmiSerialPrivilege=15
  cfgUserAdminSolEnable=0
  ```

  – If you have used the **get** command:

  ```
  [idrac.users.16]
  Enable=Disabled
  IpmiLanPrivilege=15
  IpmiSerialPrivilege=15
  !!Password=******** (Write-Only)
  Privilege=0x0
  SNMPv3AuthenticationType=SHA
  SNMPv3Enable=Disabled
  SNMPv3PrivacyType=AES
  SolEnable=Disabled
  UserName=
  ```

- The indexes are read-only and cannot be modified. Objects of the indexed group are bound to the index under which they are listed and any valid configuration to the object value is applicable only to that particular index.
- A predefined set of indexes are available for each indexed group. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals** .

- Use the `racresetcfg` subcommand to reset the iDRAC to the default setting, and then run the `racadm config -f <filename>.cfg` or `racadm set -f <filename>.cfg` command. Make sure that the **.cfg** file includes all required objects, users, indexes, and other parameters.

CAUTION: Use the `racresetcfg` subcommand to reset the database and the iDRAC NIC settings to the default settings and remove all users and user configurations. While the root user is available, other user settings are also reset to the default settings.

Parsing Rules

- All lines that start with '#' are treated as comments. A comment line must start in column one. A '#' character in any other column is treated as a '#' character. Some modem parameters may include # characters in its string. An escape character is not required. You may want to generate a **.cfg** from a `racadm getconfig -f <filename> .cfg` command, and then perform a `racadm config -f <filename> .cfg` command to a different iDRAC, without adding escape characters. Example:

  ```
  #

  # This is a comment

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<Modem init # not a comment>
  ```

- All group entries must be surrounded by "`[`" and "`]`" characters. The starting "`[`" character denoting a group name *must* start in column one. This group name *must* be specified before any of the objects in that group. Objects that do not include an associated group name generate an error. The configuration data is organized into groups as defined in the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**. The following example displays a group name, object, and the object's property value.

  ```
  [cfgLanNetworking] -{group name}

  cfgNicIpAddress=143.154.133.121 {object name}
  ```

- All parameters are specified as "object=value" pairs with no white space between the object, =, or value.

  White spaces that are included after the value are ignored. A white space inside a value string remains unmodified. Any character to the right of the '=' is taken as is (for example, a second '=', or a '#', '[', ']', and so forth). These characters are valid modem chat script characters.

  See the example in the previous bullet.

  The `racadm getconfig -f <filename> .cfg` command places a comment in front of index objects, allowing the user to see the included comments.

  To view the contents of an indexed group, use the following command:

  ```
  racadm getconfig -g <groupName> -i <index 1-16>
  ```

- For indexed groups the object anchor must be the first object after the "[ ]" pair. The following are examples of the current indexed groups:

  ```
  [cfgUserAdmin]

  cfgUserAdminIndex=11
  ```

  If you type `racadm getconfig -f <` *myexample* `>.cfg`, the command builds a **.cfg** file for the current iDRAC configuration. This configuration file can be used as an example and as a starting point for your unique . **cfg** file.

Modifying the iDRAC IP Address

When you modify the iDRAC IP address in the configuration file, remove all unnecessary <*variable*>=**value** entries. Only the actual variable group's label with "[" and "]" remains, including the two <*variable*>=**value** entries pertaining to the IP address change.

For example:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

This file is updated as follows:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored

cfgNicGateway=10.35.9.1
```

The command `racadm config -f myfile.cfg` parses the file and identifies any errors by line number. A correct file updates the proper entries. Additionally, you can use the same `getconfig` command from the previous example to confirm the update.

Use this file to download company-wide changes or to configure new systems over the network.

NOTE: "Anchor" is an internal term and do not use it in the file.

Disabling Access to Modify iDRAC Configuration Settings on Host System

You can disable access to modify the iDRAC configuration settings through Local RACADM or iDRAC Settings utility. However, you can view these configuration settings. To do this:

1. In iDRAC Web interface, go to **Overview → iDRAC Settings → Network → Services**.
2. Select one or both of the following:

- **Disable the iDRAC Local Configuration using iDRAC Settings** — Disables access to modify the configuration settings in iDRAC Settings utility.
- **Disable the iDRAC Local Configuration using RACADM** — Disables access to modify the configuration settings in Local RACADM.

3. Click **Apply**.

NOTE: If access is disabled, you cannot use Server Administrator or IPMITool to perform iDRAC configurations. However, you can use IPMI Over LAN.

5

Viewing iDRAC and Managed System Information

You can view iDRAC and managed system's health and properties, hardware and firmware inventory, sensor health, storage devices, network devices, and view and terminate user sessions. For blade servers, you can also view the flex address information.

Related Links

Viewing Managed System Health and Properties
Viewing System Inventory
Viewing Sensor Information
Monitoring Performance Index of CPU, Memory, and I/O Modules
Checking the System for Fresh Air Compliance
Viewing Historical Temperature Data
Inventory and Monitoring Storage Devices
Inventory and Monitoring Network Devices
Inventory and Monitoring FC HBA Devices
Viewing FlexAddress Mezzanine Card Fabric Connections
Viewing or Terminating iDRAC Sessions

Viewing Managed System Health and Properties

When you log in to iDRAC Web interface, the **System Summary** page allows you to view the managed system's health, basic iDRAC information, preview the virtual console, add and view work notes, and quickly launch tasks such as power on or off, power cycle, view logs, update and rollback firmware, switch on or switch off the front panel LED, and reset iDRAC.

To access the **System Summary** page, go to **Overview → Server → Properties → Summary**. The **System Summary** page is displayed. For more information, see the *iDRAC Online Help*.

You can also view the basic system summary information using the iDRAC Settings utility. To do this, in iDRAC Settings utility, go to **System Summary**. The **iDRAC Settings System Summary** page is displayed. For more information, see the *iDRAC Settings Utility Online Help*.

Viewing System Inventory

You can view information about the hardware and firmware components installed on the managed system. To do this, in iDRAC Web interface, go to **Overview → Server → Properties → System Inventory**. For information about the displayed properties, see the *iDRAC Online Help*.

The Hardware Inventory section displays the information for the following components available on the managed system:

- iDRAC

- RAID controller
- Batteries
- CPUs
- DIMMs
- HDDs
- Backplanes
- Network Interface Cards (integrated and embedded)
- Video card
- SD card
- Power Supply Units (PSUs)
- Fans
- Fibre Channel HBAs
- USB

The Firmware Inventory section displays the firmware version for the following components:

- BIOS
- Lifecycle Controller
- iDRAC
- OS driver pack
- 32-bit diagnostics
- System CPLD
- PERC controllers
- Batteries
- Physical disks
- Power supply
- NIC
- Fibre Channel
- Backplane
- Enclosure
- PCIe SSDs

When you replace any hardware component or update the firmware versions, make sure to enable and run the **Collect System Inventory on Reboot** (CSIOR) option to collect the system inventory on reboot. After a few minutes, log in to iDRAC, and navigate to the **System Inventory** page to view the details. It may take up to five minutes for the information to be available depending on the hardware installed on the server.

NOTE: CSIOR option is enabled by default.

Click **Export** to export the hardware inventory in an XML format and save it to a location of your choice.

Viewing Sensor Information

The following sensors help to monitor the health of the managed system:

- **Batteries** — Provides information about the batteries on the system board CMOS and storage RAID On Motherboard (ROMB).

NOTE: The Storage ROMB battery settings are available only if the system has a ROMB with a battery.

- **Fan** (available only for rack and tower servers) — Provides information about the system fans —fan redundancy and fans list that display fan speed and threshold values.
- **CPU** — Indicates the health and state of the CPUs in the managed system. It also reports processor automatic throttling and predictive failure.
- **Memory** — Indicates the health and state of the Dual In-line Memory Modules (DIMMs) present in the managed system.
- **Intrusion**— Provides information about the chassis.
- **Power Supplies** (available only for rack and tower servers) — Provides information about the power supplies and the power supply redundancy status.

  NOTE: If there is only one power supply in the system, the power supply redundancy is set to **Disabled**.
- **Removable Flash Media** — Provides information about the Internal SD Modules—vFlash and Internal Dual SD Module (IDSDM).
  - When IDSDM redundancy is enabled, the following IDSDM sensor status is displayed—IDSDM Redundancy Status, IDSDM SD1, IDSDM SD2. When redundancy is disabled, only IDSDM SD1 is displayed.
  - If IDSDM redundancy is initially disabled when the system is powered on or after an iDRAC reset, the IDSDM SD1 sensor status is displayed only after a card is inserted.
  - If IDSDM redundancy is enabled with two SD cards present in the IDSDM, and the status of one SD card is *online* while the status of the other card is *offline*. A system reboot is required to restore redundancy between the two SD cards in the IDSDM. After the redundancy is restored, the status of both the SD cards in the IDSDM is *online*.
  - During the rebuilding operation to restore redundancy between two SD cards present in the IDSDM, the IDSDM status is not displayed since the IDSDM sensors are powered off.

    NOTE: If the host system is rebooted during IDSDM rebuild operation, the iDRAC does not display the IDSDM information. To resolve this, rebuild IDSDM again or reset the iDRAC.
  - System Event Logs (SEL) for a write-protected or corrupt SD card in the IDSDM module are not repeated until they are cleared by replacing the SD card with a writable or good SD card, respectively.
- **Temperature** — Provides information about the system board inlet temperature and exhaust temperature (only applies to rack servers). The temperature probe indicates whether the status of the probe is within the pre-set warning and critical threshold value.
- **Voltage** — Indicates the status and reading of the voltage sensors on various system components.

The following table provides how to view the sensor information using iDRAC Web interface and RACADM. For information about the properties that are displayed on the Web interface, see the *iDRAC Online Help* for the respective pages.

Table 9. Sensor Information Using Web Interface and RACADM

View Sensor Information For	Using Web Interface	Using RACADM
Batteries	**Overview → Hardware → Batteries**	Use the **getsensorinfo** command. For power supplies, you can also use the **System.Power.Supply** command with the **get** subcommand.

View Sensor Information For	Using Web Interface	Using RACADM
		For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.
Fan	**Overview → Hardware → Fans**	
CPU	**Overview → Hardware → CPU**	
Memory	**Overview → Hardware → Memory**	
Intrusion	**Overview → Server → Intrusion**	
Power Supplies	**Overview → Hardware → Power Supplies**	
Removable Flash Media	**Overview → Hardware → Removable Flash Media**	
Temperature	**Overview → Server → Power/Thermal → Temperatures**	
Voltage	**Overview → Server → Power/Thermal → Voltages**	

Monitoring Performance Index of CPU, Memory, and I/O Modules

In 13th generation Dell PowerEdge servers, Intel ME provides support for Compute Usage Per Second (CUPS) functionality. The CUPS functionality provides real-time monitoring of CPU, memory and I/O utilization and system-level utilization index for the system. Since it is done by Intel ME, it is independent of the OS and does not consume CPU resources. The Intel ME has a system CUPS sensor which provides the Computation, Memory and I/O resource utilization value as CUPS Index. iDRAC monitors this CUPS index for the overall system utilization and also monitors the instantaneous value of CPU, Memory, and I/O utilization index.

Utilization information of system resources is obtained by querying the data from a set of dedicated counters provided by the CPU and chipset. These counters are called Resource Monitoring Counters or RMCs. These counters are aggregated by the node manager to measure the cumulative utilization of each of these system resources that is read from the iDRAC using existing inter-communication mechanisms to provide these vital data through out-of-band management interfaces.

Since Intel sensor representation of performance parameters and index values are for complete physical system, performance data representation on the interfaces is for the complete physical system, even if the system is virtualized and hosting multiple virtual hosts.

To display the performance parameters, the supported sensors must be present in the server.

The four system utilization parameters are:

- **CPU Utilization** - There are individual Resource Monitoring counters (RMCs) for each CPU core which are aggregated to provide cumulative utilization of all the cores in the system. This utilization is based on time spent in active state and time spent in inactive state. Each sample of RMC is taken every six seconds.
- **Memory Utilization** - There are individual counters (RMCs) to measure memory traffic occurring at each memory channel or memory controller instance. These counters are aggregated to measure the cumulative memory traffic across all the memory channels on the system. This is a measure of memory bandwidth consumption and not amount of memory utilization. iDRAC aggregates it for one minute of period, so it may or may not match the memory utilization shown by other OS tools such as TOP in Linux. Memory bandwidth utilization shown by iDRAC is indication of whether workload is memory intensive or not.
- **I/O Utilization** - There are individual Resource Monitoring Counters (RMCs), one per root port in the PCI Express Root Complex to measure PCI Express traffic emanating from or directed to that root port and the lower segment. These counters are then aggregated to measure PCI express traffic for all PCI Express segments emanating from the package. This is measure of IO bandwidth utilization for the system.
- **System Level CUPS Index** - The CUPS index is calculated by aggregating CPU, Memory, and I/O index considering a pre-defined load factor of each system resource. The load factor depends on the nature of the workload run on the system. Thus at any given time, CUPS Index represents the measurement of the compute headroom available on the server. Hence, if the system has a large CUPS Index, then there is limited headroom to place additional workload on that system. As the resource consumption decreases, the system's CUPS Index decreases. A low CUPS Index indicates that there is a large amount of compute headroom and the server is a main target for receiving new workloads or having the workload migrated, and the server being placed into a lower power state in order to reduce power consumption. Such workload monitoring can then be applied throughout the data center to provide a high-level and holistic view of the datacenter's workload, providing a dynamic datacenter solution.

NOTE: The CPU, memory, and I/O utilization indexes are aggregated over one minute. Therefore, if there are any instantaneous spikes in these indexes, they may be suppressed. They are indication of workload patterns not the amount of resource utilization.

The IPMI, SEL, and SNMP traps are generated if the thresholds of the utilization indexes are reached and the sensor events are enabled. The sensor event flags are disabled by default. It can be enabled using the standard IPMI interface.

The required privileges are:

- Login privilege is required to monitor performance data.
- Configure privilege is required for setting warning thresholds and reset historical peaks.
- Login privilege and Enterprise license is required for reading historical statics data.

Monitoring Performance Index for of CPU, Memory, and I/O Modules Using Web Interface

To monitor the performance index of CPU, memory, and I/O modules, in the iDRAC Web interface, go to **Overview → Hardware**. The **Hardware Overview** page displays the following:

- **Hardware** section – Click the required link to view the health of the component.
- **System Performance** section - Displays the current reading and the warning reading for CPU, Memory and I/O utilization index, and system level CUPS index in a graphical view.
- **System Performance Historical Data** section:
  - Provides the statistics for CPU, memory, IO utilization, and the system level CUPS index. If the host system is powered off, then the graph displays the power off line below 0 percent.

  - You can reset the peak utilization for a particular sensor. Click **Reset Historical Peak**. You must have Configure privilege to reset the peak value.
- **Performance Metrics** section:
  - View status and present reading
  - View or specify the warning threshold utilization limit. You must have server configure privilege to set the threshold values.

For information about the displayed properties, see the *iDRAC Online Help*.

Monitoring Performance Index for of CPU, Memory, and I/O Modules Using RACADM

Use the **SystemPerfStatistics** sub command to monitor performance index for CPU, memory, and I/O modules. For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Checking the System for Fresh Air Compliance

Fresh air cooling directly uses outside air to cool systems in the data center. Fresh air compliant systems can operate above its normal ambient operating range (temperatures up to 113 °F (45 °C)).

NOTE: Some servers or certain configurations of a server may not be fresh air compliant. See the specific server manual for details related to fresh air compliance or contact Dell for more details.

To check the system for fresh air compliance:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Power / Thermal** → **Temperatures**.
   The **Temperatures** page is displayed.
2. See the **Fresh Air** section that indicates whether the server is fresh air compliant or not.

Viewing Historical Temperature Data

You can monitor the percentage of time the system has operated at ambient temperature that is greater than the normally supported fresh air temperature threshold. The system board temperature sensor reading is collected over a period of time to monitor the temperature. The data collection starts when the system is first powered on after it is shipped from the factory. The data is collected and displayed for the duration when the system is powered on. You can track and store the monitored temperature for the last seven years.

NOTE: You can track the temperature history even for systems that are not fresh air compliant. However, the threshold limits and fresh air related warnings generated are based on fresh air supported limits. The limits are 42ºC for warning and 47ºC for critical. These values correspond to 40ºC and 45ºC fresh air limits with 2ºC margin for accuracy.

Two fixed temperature bands are tracked that are associated to fresh air limits:

- Warning band — Consists of the duration a system has operated above the temperature sensor warning threshold (42ºC). The system can operate in the warning band for 10% of the time for 12 months.
- Critical band — Consists of the duration a system has operated above the temperature sensor critical threshold (47ºC). The system can operate in the critical band for 1% of the time for 12 months which also increments time in the warning band.

The collected data is represented in a graphical format to track the 10% and 1% levels. The logged temperature data can be cleared only before shipping from the factory.

An event is generated if the system continues to operate above the normally supported temperature threshold for a specified operational time. If the average temperature over the specified operational time is greater than or equal to the warning level (> = 8%) or the critical level (> = 0.8%), an event is logged in the Lifecycle Log and the corresponding SNMP trap is generated. The events are:

- Warning event when the temperature was greater than the warning threshold for duration of 8% or more in the last 12 months.
- Critical event when the temperature was greater than the warning threshold for duration of 10% or more in the last 12 months.
- Warning event when the temperature was greater than the critical threshold for duration of 0.8% or more in the last 12 months.
- Critical event when the temperature was greater than the critical threshold for duration of 1% or more in the last 12 months.

You can also configure iDRAC to generate additional events. For more information, see the Setting Alert Recurrence Event section.

Viewing Historical Temperature Data Using iDRAC Web Interface

To view historical temperature data:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Power / Thermal** → **Temperatures**.
   The **Temperatures** page is displayed.
2. See the **System Board Temperature Historical Data** section that provides a graphical display of the stored temperature (average and peak values) for the last day, last 30 days, and last year.
   For more information, see the *iDRAC Online Help*.

   NOTE: After an iDRAC firmware update or iDRAC reset, some temperature data may not be displayed in the graph.

Viewing Historical Temperature Data Using RACADM

To view historical data using RACADM, use the **inlettemphistory** subcommand. For more information, see the *iDRAC8 RACADM Command Line Reference Guide*.

Configuring Warning Threshold for Inlet Temperature

You can modify the minimum and maximum warning threshold values for the system board inlet temperature sensor. If reset to default action is performed, the temperature thresholds are set to the default values. You must have Configure user privilege to set the warning threshold values for the inlet temperature sensor.

Configuring Warning Threshold for Inlet Temperature Using Web Interface

To configure warning threshold for inlet temperature:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Power/Thermal** → **Temperatures**.
   The **Temperatures** page is displayed.
2. In the **Temperature Probes** section, for the **System Board Inlet Temp**, enter the minimum and maximum values for the **Warning Threshold** in Centigrade or Fahrenheit. If you enter the value in

centigrade, the system automatically calculates and displays the Fahrenheit value. Similarly, if you enter Fahrenheit, the value for Centigrade is displayed.

3. Click **Apply**.

   The values are configured.

   NOTE: Changes to default thresholds are not reflected in the historical data chart since the chart limits are for fresh air limit values only. Warnings for exceeding the custom thresholds are different from warning associated to exceeding fresh air thresholds.

Viewing Network Interfaces Available On Host OS

You can view information about all the network interfaces that are available on the host operating system such as the IP addresses that are assigned to the server. The iDRAC Service Module provides this information to iDRAC. The OS IP address information includes the IPv4 and IPv6 addresses, MAC address, Subnet mask or prefix length, and the FQDD of the network device.

NOTE: This feature is available with iDRAC Express and iDRAC Enterprise licenses.

To view the OS information, make sure that:

- You have Login privilege.
- iDRAC Service Module is installed and running on the host operating system.
- OS Information option is enabled in the **Overview → Server → Service Module** page.

iDRAC can display the IPv4 and IPv6 addresses for all the interfaces configured on the Host OS.

Depending on how the Host OS detects the DHCP server, the corresponding IPv4 or IPv6 DHCP server address may not be displayed. Typically one of IPv4 or IPv6 DHCP address is visible if DHCP is enabled.

Viewing Network Interfaces Available on Host OS Using Web Interface

To view the network interfaces available on the host OS using Web interface:

1. Go to **Overview → Host OS → Network Interfaces**.

   The **Network Interfaces** page displays all the network interfaces that are available on the host operating system.

2. To view the list of network interfaces associated with a network device, from the **Network Device FQDD** drop-down menu, select a network device and click **Apply**.

   The OS IP details are displayed in the **Host OS Network Interfaces** section.

3. From the **Device FQDD** column, click on the network device link.

   The corresponding device page is displayed from the **Hardware → Network Devices**section, where you can view the device details. For information about the properties, see the *iDRAC Online Help*.

4. For each network device, click the + icon to display the additional details.

   Similarly, you can view the host OS network interface information associated with a network device from the **Hardware → Network Devices** page. Click **View Host OS Network Interfaces**.

Viewing Network Interfaces Available on Host OS Using RACADM

Use the gethostnetworkinterfaces command to view the network interfaces available on the host operating systems using RACADM. For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Viewing FlexAddress Mezzanine Card Fabric Connections

In blade servers, FlexAddress allows the use of persistent, chassis-assigned World Wide Names and MAC addresses (WWN/MAC) for each managed server port connection.

You can view the following information for each installed embedded Ethernet and optional mezzanine card port:

- Fabrics to which the cards are connected.
- Type of fabric.
- Server-assigned, chassis-assigned, or remotely assigned MAC addresses.

To view the Flex Address information in iDRAC, configure and enable the Flex Address feature in Chassis Management Controller (CMC). For more information, see the *Dell Chassis Management Controller User Guide* available at **dell.com/support/manuals**. Any existing Virtual Console or Virtual Media session terminates if the FlexAddress setting is enabled or disabled.

NOTE: To avoid errors that may lead to an inability to turn on the managed system, you *must* have the correct type of mezzanine card installed for each port and fabric connection.

The FlexAddress feature replaces the server–assigned MAC addresses with chassis–assigned MAC addresses and is implemented for iDRAC along with blade LOMs, mezzanine cards and I/O modules. The iDRAC FlexAddress feature supports preservation of slot specific MAC address for iDRACs in a chassis. The chassis–assigned MAC address is stored in CMC non–volatile memory and is sent to iDRAC during an iDRAC boot or when CMC FlexAddress is enabled.

If CMC enables chassis–assigned MAC addresses, iDRAC displays the **MAC address** on any of the following pages:

- **Overview → Server → Properties Details → iDRAC Information**.
- **Overview → Server → Properties WWN/MAC**.
- **Overview → iDRAC Settings → Properties iDRAC Information → Current Network Settings**.
- **Overview → iDRAC Settings → Network Network → Network Settings**.

CAUTION: With FlexAddress enabled, if you switch from a server–assigned MAC address to a chassis–assigned MAC address and vice–versa, iDRAC IP address also changes.

Viewing or Terminating iDRAC Sessions

You can view the number of users currently logged in to iDRAC and terminate the user sessions.

Terminating iDRAC Sessions Using Web Interface

The users who do not have administrative privileges must have Configure iDRAC privilege to terminate iDRAC sessions using iDRAC Web interface.

To view and terminate the iDRAC sessions:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Sessions**.

The **Sessions** page displays the session ID, username, IP address, and session type. For more information about these properties, see the *iDRAC Online Help*.

2. To terminate the session, under the **Terminate** column, click the Trashcan icon for a session.

Terminating iDRAC Sessions Using RACADM

You must have administrator privileges to terminate iDRAC sessions using RACADM.

To view the current user sessions, use the **getssninfo** command.

To terminate a user session, use the **closessn** command.

For more information about these commands, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

6

Setting Up iDRAC Communication

You can communicate with iDRAC using any of the following modes:

- iDRAC Web Interface
- Serial connection using DB9 cable (RAC serial or IPMI serial) - For rack and tower servers only
- IPMI Serial Over LAN
- IPMI Over LAN
- Remote RACADM
- Local RACADM
- Remote Services

For an overview of the supported protocols, supported commands, and pre-requisites, see the following table.

Table 10. Communication Modes —Summary

Mode of Communication	Supported Protocol	Supported Commands	Prerequisite
iDRAC Web Interface	Internet Protocol (https)	NA	Web Server
Serial using Null modem DB9 cable	Serial Protocol	RACADM	Part of iDRAC firmware
		SMCLP	RAC Serial or IPMI Serial is enabled.
		IPMI	
IPMI Serial Over LAN	Intelligent Platform Management Bus protocol	IPMI	IPMITool is installed and IPMI Serial Over LAN is enabled.
	SSH		
	Telnet		
IPMI over LAN	Intelligent Platform Management Bus protocol	IPMI	IPMITool is installed and IPMI Settings is enabled.
SMCLP	SSH	SMCLP	SSH or Telnet on iDRAC is enabled.
	Telnet		
Remote RACADM	https	Remote RACADM	Remote RACADM is installed and enabled.

Mode of Communication	Supported Protocol	Supported Commands	Prerequisite
Firmware RACADM	SSH Telnet	Firmware RACADM	Firmware RACADM is installed and enabled
Local RACADM	IPMI	Local RACADM	Local RACADM is installed.
Remote Services [1]	WS-MAN	WinRM (Windows) OpenWSMAN (Linux)	WinRM is installed (Windows) or OpenWSMAN is installed (Linux).

[1] For more information, see the *Lifecycle Controller Remote Services User's Guide* available at **dell.com/support/manuals**.

Related Links

- Communicating With iDRAC Through Serial Connection Using DB9 Cable
- Switching Between RAC Serial and Serial Console While Using DB9 Cable
- Communicating With iDRAC Using IPMI SOL
- Communicating With iDRAC Using IPMI Over LAN
- Enabling or Disabling Remote RACADM
- Disabling Local RACADM
- Enabling IPMI on Managed System
- Configuring Linux for Serial Console During Boot
- Supported SSH Cryptography Schemes

Communicating With iDRAC Through Serial Connection Using DB9 Cable

You can use any of the following communication methods to perform systems management tasks through serial connection to rack and tower servers:

- RAC Serial
- IPMI Serial — Direct Connect Basic mode and Direct Connect Terminal mode

NOTE: In case of blade servers, the serial connection is established through the chassis. For more information, see the *Chassis Management Controller User's Guide* available at **dell.com/support/manuals**.

To establish the serial connection:

1. Configure the BIOS to enable serial connection:
2. Connect the Null Modem DB9 cable from the management station's serial port to the managed system's external serial connector.
3. Make sure that the management station's terminal emulation software is configured for serial connection using any of the following:
   - Linux Minicom in an Xterm

- Hilgraeve's HyperTerminal Private Edition (version 6.3)

Based on where the managed system is in its boot process, you can see either the POST screen or the operating system screen. This is based on the configuration: SAC for Windows and Linux text mode screens for Linux.

4. Enable RAC serial or IPMI serial connections in iDRAC.

Related Links

Configuring BIOS For Serial Connection
Enabling RAC Serial Connection
Enabling IPMI Serial Connection Basic and Terminal Modes

Configuring BIOS For Serial Connection

To configure BIOS for Serial Connection:

NOTE: This is applicable only for iDRAC on rack and tower servers.

1. Turn on or restart the system.
2. Press <F2>.
3. Go to **System BIOS Settings** → **Serial Communication**.
4. Select **External Serial Connector** to **Remote Access device**.
5. Click **Back**, click **Finish**, and then click **Yes**.
6. Press <Esc> to exit **System Setup**.

Enabling RAC Serial Connection

After configuring serial connection in BIOS, enable RAC serial in iDRAC.

NOTE: This is applicable only for iDRAC on rack and tower servers.

Enabling RAC Serial Connection Using Web Interface

To enable RAC serial connection:

1. In the iDRAC Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Serial**.
   The **Serial** page is displayed.
2. Under **RAC Serial**, select **Enabled** and specify the values for the attributes.
3. Click **Apply**.
   The RAC serial settings are configured.

Enabling RAC Serial Connection Using RACADM

To enable RAC serial connection using RACADM, use any of the following:

- Use the objects in the **cfgSerial** group with the **config** command.
- Use the object in the **iDRAC.Serial** group with the **set** command.

Enabling IPMI Serial Connection Basic and Terminal Modes

To enable IPMI serial routing of BIOS to iDRAC, configure IPMI Serial in any of the following modes in iDRAC:

NOTE: This is applicable only for iDRAC on rack and tower servers.

- IPMI basic mode — Supports a binary interface for program access, such as the IPMI shell (ipmish) that is included with the Baseboard Management Utility (BMU). For example, to print the System Event Log using ipmish via IPMI Basic mode, run the following command:

  ```
  ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
  ```

- IPMI terminal mode — Supports ASCII commands that are sent from a serial terminal. This mode supports limited number of commands (including power control) and raw IPMI commands that are typed as hexadecimal ASCII characters. It allows you to view the operating system boot sequences up to BIOS, when you login to iDRAC through SSH or Telnet.

Related Links

Configuring BIOS For Serial Connection
Additional Settings For IPMI Serial Terminal Mode

Enabling Serial Connection Using Web Interface

Make sure to disable the RAC serial interface to enable IPMI Serial.

To configure IPMI Serial settings:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network → Serial**.
2. Under **IPMI Serial**, specify the values for the attributes. For information about the options, see the *iDRAC Online Help*.
3. Click **Apply**.

Enabling Serial Connection IPMI Mode Using RACADM

To configure the IPMI mode, disable the RAC serial interface and then enable the IPMI mode using any of the following:

- Using**config** command:

  ```
  racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
  ```

  ```
  racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode < 0  or  1>
  ```

  where, *0* indicates Terminal mode and *1* indicates Basic mode.

- Using **set** command:

  ```
  racadm set iDRAC.Serial.Enable 0
  ```

  ```
  racadm set iDRAC.IPMISerial.ConnectionMode < 0  or  1>
  ```

  where, *0* indicates Terminal mode and *1* indicates Basic mode.

Enabling Serial Connection IPMI Serial Settings Using RACADM

To configure IPMI Serial settings, you use the **set** or **config** command:

1. Change the IPMI serial connection mode to the appropriate setting using the command:
   - Using **config** command: `racadm config -g cfgSerial -o cfgSerialConsoleEnable 0`
   - Using **set** command: `racadm set iDRAC.Serial.Enable 0`
2. Set the IPMI Serial baud rate:
   - Using **config** command: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <baud_rate>`

- Using **set** command: `racadm set iDRAC.IPMISerial.BaudRate <baud_rate>`

where `<baud_rate>` is 9600, 19200, 57600, or 115200 bps.

3. Enable the IPMI serial hardware flow control:
   - Using **config** command: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1`
   - Using **set** command: `racadm set iDRAC.IPMISerial.FlowControl 1`
4. Set the IPMI serial channel minimum privilege level:
   - Using **config** command: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <level>`
   - Using **set** command: `racadm set iDRAC.IPMISerial.ChanPrivLimit <level>`

   where `<level>` is `2` (User), `3` (Operator), or `4` (Administrator).
5. Make sure that the serial MUX (external serial connector) is set correctly to the remote access device in the BIOS Setup program to configure BIOS for serial connection.

   For more information about these properties, see the IPMI 2.0 specification.

Additional Settings For IPMI Serial Terminal Mode

This section provides additional configuration settings for IPMI serial terminal mode.

Configuring Additional Settings for IPMI Serial Terminal Mode Using Web Interface

To set the Terminal Mode settings:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network → Serial**

   The **Serial** page is displayed.
2. Enable IPMI serial.
3. Click **Terminal Mode Settings.**

   The **Terminal Mode Settings** page is displayed.
4. Specify the following values:
   - Line editing
   - Delete control
   - Echo Control
   - Handshaking control
   - New line sequence
   - Input new line sequences

   For information about the options, see the *iDRAC Online Help*.
5. Click **Apply**.

   The terminal mode settings are configured.
6. Make sure that the serial MUX (external serial connector) is set correctly to the remote access device in the BIOS Setup program to configure BIOS for serial connection.

Configuring Additional Settings for IPMI Serial Terminal Mode Using RACADM

To configure the Terminal Mode settings, run the command:`racadm config cfgIpmiSerial`

Switching Between RAC Serial and Serial Console While Using DB9 Cable

iDRAC supports Escape key sequences that allow switching between RAC Serial Interface communication and Serial Console on rack and tower servers.

Switching From Serial Console to RAC Serial

To switch to RAC Serial Interface communication mode when in Serial Console Mode, use the following key sequence:

```
<Esc> +<Shift> <9>
```

The key sequence directs you to the "iDRAC Login" prompt (if the iDRAC is set to RAC Serial mode) or to the Serial Connection mode where terminal commands can be issued if iDRAC is set to IPMI Serial Direct Connect Terminal Mode.

Switching From RAC Serial to Serial Console

To switch to Serial Console Mode when in RAC Serial Interface Communication Mode, use the following key sequence:

```
<Esc> +<Shift> <q>
```

When in terminal mode, to switch the connection to the Serial Console mode use:

```
<Esc> +<Shift> <q>
```

To go back to the terminal mode use, when connected in Serial Console mode:

```
<Esc> +<Shift> <9>
```

Communicating With iDRAC Using IPMI SOL

IPMI Serial Over LAN (SOL) allows a managed system's text-based console serial data to be redirected over iDRAC's dedicated or shared out-of-band ethernet management network. Using SOL you can:

- Remotely access operating systems with no time-out.
- Diagnose host systems on Emergency Management Services (EMS) or Special Administrator Console (SAC) for Windows or Linux shell.
- View the progress of a servers during POST and reconfigure the BIOS setup program.

To setup the SOL communication mode:

1. Configure BIOS for serial connection.
2. Configure iDRAC to Use SOL.
3. Enable a supported protocol (SSH, Telnet, IPMItool).

Related Links

Configuring BIOS For Serial Connection
Configuring iDRAC to Use SOL

Enabling Supported Protocol

Configuring BIOS For Serial Connection

To configure BIOS for Serial Connection:

NOTE: This is applicable only for iDRAC on rack and tower servers.

1. Turn on or restart the system.
2. Press <F2>.
3. Go to **System BIOS Settings** → **Serial Communication**.
4. Specify the following values:
   - Serial Communication — On With Console Redirection
   - Serial Port Address — COM2.

     NOTE: You can set the **serial communication** field to **On with serial redirection via com1** if **serial device2** in the **serial port address** field is also set to com1.
   - External serial connector — Serial device 2
   - Failsafe Baud Rate — 115200
   - Remote Terminal Type — VT100/VT220
   - Redirection After Boot — Enabled
5. Click **Back** and then click **Finish**.
6. Click **Yes** to save the changes.
7. Press <Esc> to exit **System Setup**.

   NOTE: BIOS sends the screen serial data in 25 x 80 format. The SSH window that is used to invoke the `console com2` command must be set to 25 x 80. Then, the redirected screen appears correctly.

Configuring iDRAC to Use SOL

You can specify the SOL settings in iDRAC using Web interface, RACADM, or iDRAC Settings utility.

Configuring iDRAC to Use SOL Using iDRAC Web Interface

To configure IPMI Serial over LAN (SOL):

1. In the iDRAC Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **Serial Over LAN**.
   The **Serial over LAN** page is displayed.
2. Enable SOL, specify the values, and click **Apply**.
   The IPMI SOL settings are configured.
3. To set the character accumulate interval and the character send threshold, select **Advanced Settings.**
   The **Serial Over LAN Advanced Settings** page is displayed.
4. Specify the values for the attributes and click **Apply**.
   The IPMI SOL advanced settings are configured. These values help to improve the performance.

   For information about the options, see the *iDRAC Online Help*.

Configuring iDRAC to Use SOL Using RACADM

To configure IPMI Serial over LAN (SOL):

1. Enable IPMI Serial over LAN:
   - Using **config** command: `racadm config -g cfgIpmiSol –o cfgIpmiSolEnable 1`
   - Using **set** command: `racadm set iDRAC.IPMISol.Enable 1`
2. Update the IPMI SOL minimum privilege level:
   - Using **config** command: `racadm config -g cfgIpmiSol o cfgIpmiSolMinPrivilege <level>`
   - Using **set** command: `racadm set iDRAC.IPMISol.MinPrivilege 1`

   where `<level>` is 2 (User), 3 (Operator), 4 (Administrator).

   NOTE: The IPMI SOL minimum privilege level determines the minimum privilege to activate IPMI SOL. For more information, see the IPMI 2.0 specification.
3. Update the IPMI SOL baud rate:
   - Using **config** command: `racadm config -g cfgIpmiSol –o cfgIpmiSolBaudRate <baud_rate>`
   - Using **set** command: `racadm set iDRAC.IPMISol.BaudRate <baud_rate>`

   where `<baud_rate>` is 9600, 19200, 57600, or 115200 bps.

   NOTE: To redirect the serial console over LAN, make sure that the SOL baud rate is identical to the managed system's baud rate.
4. Enable SOL for each user:
   - Using **config** command: `racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2`
   - Using **set** command: `racadm set iDRAC.Users.<id>.SolEnable 2`

   where, `<id>` is the user's unique ID.

   NOTE: To redirect the serial console over LAN, make sure that the SOL baud rate is identical to the managed system's baud rate.

Enabling Supported Protocol

The supported protocols are IPMI, SSH, and Telnet.

Enabling Supported Protocol Using Web Interface

To enable SSH or Telnet, go to **Overview → iDRAC Settings → Network → Services** and select **Enabled** for SSH or Telnet, respectively.

To enable IPMI, go to **Overview → iDRAC Settings → Network** and select **Enable IPMI Over LAN**. Make sure that the **Encryption Key** value is all zeroes or press the backspace key to clear and change the value to NULL characters.

Enabling Supported Protocol Using RACADM

To enable the SSH or Telnet, run the command:

- Telnet:

  - Using **config** command: `racadm config -g cfgSerial -o cfgSerialTelnetEnable 1`
  - Using **set** command: `racadm set iDRAC.Telnet.Enable 1`
- SSH:
  - Using **config** command:`racadm config -g cfgSerial -o cfgSerialSshEnable 1`
  - Using **set** command: `racadm set iDRAC.SSH.Enable 1`

  To change the SSH port:
  - Using **config** command:`racadm config -g cfgRacTuning -o cfgRacTuneSshPort <port number>`
  - Using **set** command:`racadm set iDRAC.SSH.Port <port number>`

You can use tools such as:

- IPMItool for using IPMI protocol
- Putty/OpenSSH for using SSH or Telnet protocol

Related Links

SOL Using IPMI Protocol
SOL Using SSH or Telnet Protocol

SOL Using IPMI Protocol

IPMItool <–-> LAN/WAN connection <–-> iDRAC

The IPMI-based SOL utility and IPMItool uses RMCP+ delivered using UDP datagrams to port 623. The RMCP+ provides improved authentication, data integrity checks, encryption, and the ability to carry multiple types of payloads while using IPMI 2.0. For more information, see **http://ipmitool.sourceforge.net/manpage.html**.

The RMCP+ uses an 40-character hexadecimal string (characters 0-9, a-f, and A-F) encryption key for authentication. The default value is a string of 40 zeros.

An RMCP+ connection to iDRAC must be encrypted using the encryption Key (Key Generator (KG)Key). You can configure the encryption key using the iDRAC Web interface or iDRAC Settings utility.

To start SOL session using IPMItool from a management station:

NOTE: If required, you can change the default SOL time-out at **Overview → iDRAC Settings → Network → Services**.

1. Install IPMITool from the *Dell Systems Management Tools and Documentation* DVD.
   For installation instructions, see the *Software Quick Installation Guide*.
2. At the command prompt (Windows or Linux), run the command to start SOL from iDRAC: `ipmitool -H <iDRAC-ip-address> -I lanplus -U <login name> -P <login password> sol activate`
   This connects the management station to the managed system's serial port.
3. To quit a SOL session from IPMItool, press <~> and <.> one after the other. The SOL session closes.

   NOTE: If a SOL session does not terminate, reset iDRAC and allow up to two minutes to complete booting.

SOL Using SSH or Telnet Protocol

Secure Shell (SSH) and Telnet are network protocols used to perform command line communications to iDRAC. You can parse remote RACADM and SMCLP commands through either of these interfaces.

SSH has improved security over Telnet. iDRAC only supports SSH version 2 with password authentication, and is enabled by default. iDRAC supports up to two SSH sessions and two Telnet sessions at a time. It is recommended to use SSH as Telnet is not a secure protocol. You must use Telnet only if you cannot install an SSH client or if your network infrastructure is secure.

Use opensource programs such as PuTTY or OpenSSH that support SSH and Telnet network protocols on a management station to connect to iDRAC.

NOTE: Run `OpenSSH` from a VT100 or ANSI terminal emulator on Windows. Running `OpenSSH` at the Windows command prompt does not result in full functionality (that is, some keys do not respond and no graphics are displayed).

Before using SSH or Telnet to communicate with iDRAC, make sure to:

1. Configure BIOS to enable Serial Console.
2. Configure SOL in iDRAC.
3. Enable SSH or Telnet using iDRAC Web interface or RACADM.

   Telnet (port 23)/ SSH (port 22) client <––> WAN connection <––> iDRAC

   The IPMI-based SOL that uses SSH or Telnet protocol eliminates the need for an additional utility because the serial to network translation happens within iDRAC. The SSH or Telnet console that you use must be able to interpret and respond to the data arriving from the managed systems's serial port. The serial port usually attaches to a shell that emulates an ANSI- or VT100/VT220–terminal. The serial console is automatically redirected to the SSH or Telnet console.

Related Links

Using SOL From Putty On Windows
Using SOL From OpenSSH or Telnet On Linux

Using SOL From Putty On Windows

To start IPMI SOL from PuTTY on a Windows management station:

NOTE: If required, you can change the default SSH or Telnet time-out at **Overview → iDRAC Settings → Network → Services**.

1. Run the command to connect to iDRAC: `putty.exe [-ssh | -telnet] <login name>@<iDRAC-ip-address> <port number>`

   NOTE: The port number is optional. It is required only when the port number is reassigned.
2. Run the command `console com2` or `connect` to start SOL and boot the managed system.

   A SOL session from the management station to the managed system using the SSH or Telnet protocol is opened. To access the iDRAC command line console, follow the ESC key sequence. Putty and SOL connection behavior:

   - While accessing the managed system through putty during POST, if the The Function keys and keypad option on putty is set to:
     - VT100+ — F2 passes, but F12 cannot pass.

  - ESC[n~ — F12 passes, but F2 cannot pass.
- In Windows, if the Emergency Management System (EMS) console is opened immediately after a host reboot, the Special Admin Console (SAC) terminal may get corrupted. Quit the SOL session, close the terminal, open another terminal, and start the SOL session using the same command.

Related Links

Disconnecting SOL Session in iDRAC Command Line Console

Using SOL From OpenSSH or Telnet On Linux

To start SOL from OpenSSH or Telnet on a Linux management station:

NOTE: If required, you can change the default SSH or Telnet session time-out at **Overview → iDRAC Settings → Network → Services**.

1. Start a shell.
2. Connect to iDRAC using the following command:
   - For SSH: ssh *<iDRAC-ip-address>* -l *<login name>*
   - For Telnet: telnet *<iDRAC-ip-address>*

   NOTE: If you have changed the port number for the Telnet service from the default (port 23), add the port number to the end of the Telnet command.
3. Enter one of the following commands at the command prompt to start SOL:
   - `connect`
   - `console com2`

   This connects iDRAC to the managed system's SOL port. Once a SOL session is established, iDRAC command line console is not available. Follow the escape sequence correctly to open the iDRAC command line console. The escape sequence is also printed on the screen as soon as a SOL session is connected. When the managed system is off, it takes sometime to establish the SOL session.

   NOTE: You can use console com1 or console com2 to start SOL. Reboot the server to establish the connection.

   The `console -h com2` command displays the contents of the serial history buffer before waiting for input from the keyboard or new characters from the serial port.

   The default (and maximum) size of the history buffer is 8192 characters. You can set this number to a smaller value using the command:

   ```
   racadm config -g cfgSerial -o cfgSerialHistorySize <number>
   ```
4. Quit the SOL session to close an active SOL session.

Related Links

Using Telnet Virtual Console
Configuring Backspace Key For Your Telnet Session
Disconnecting SOL Session in iDRAC Command Line Console

Using Telnet Virtual Console

Some Telnet clients on the Microsoft operating systems may not display the BIOS setup screen correctly when BIOS Virtual Console is set for VT100/VT220 emulation. If this issue occurs, change the BIOS console to ANSI mode to update the display. To perform this procedure in the BIOS setup menu, select **Virtual Console → Remote Terminal Type → ANSI**.

When you configure the client VT100 emulation window, set the window or application that is displaying the redirected Virtual Console to 25 rows x 80 columns to make sure correct text display. Else, some text screens may be garbled.

To use Telnet virtual console:

1. Enable **Telnet** in **Windows Component Services.**
2. Connect to the iDRAC using the command: `telnet < IP address >:< port number >`, where `IP address` is the IP address for the iDRAC and `port number` is the Telnet port number (if you are using a new port).

Configuring Backspace Key For Your Telnet Session

Depending on the Telnet client, using the <Backspace> key may produce unexpected results. For example, the session may echo `^h`. However, most Microsoft and Linux Telnet clients can be configured to use the <Backspace> key.

To configure a Linux Telnet session to use the <Backspace> key, open a command prompt and type `stty erase ^h`. At the prompt, type `telnet`.

To configure Microsoft Telnet clients to use the <Backspace> key:

1. Open a command prompt window (if required).
2. If you are not running a Telnet session, type `telnet`. If you are running a Telnet session, press `<Ctrl><]>`.
3. At the prompt, type `set bsasdel`.

   The message `Backspace will be sent as delete` is displayed.

Disconnecting SOL Session in iDRAC Command Line Console

The commands to disconnect a SOL session are based on the utility. You can exit the utility only when a SOL session is completely terminated.

To disconnect a SOL session, terminate the SOL session from the iDRAC command line console:

- To quit SOL redirection, press <Enter>, <Esc>, and then <t>. The SOL session closes.
- To quit a SOL session from Telnet on Linux, press and hold <Ctrl>+]. A Telnet prompt is displayed. Enter `quit` to exit Telnet.
- If a SOL session is not terminated completely in the utility, other SOL sessions may not be available. To resolve this, terminate the command line console in the Web interface under **Overview → iDRAC Settings → Sessions**.

Communicating With iDRAC Using IPMI Over LAN

You must configure IPMI over LAN for iDRAC to enable or disable IPMI commands over LAN channels to any external systems. If it is not configuration is not done, then external systems cannot communicate with the iDRAC server using IPMI commands.

Configuring IPMI Over LAN Using Web Interface

To configure IPMI over LAN:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network**.

   The **Network** page is displayed.
2. Under **IPMI Settings**, specify the values for the attributes and click **Apply**.

For information about the options, see the *iDRAC Online Help*.

The IPMI over LAN settings are configured.

Configuring IPMI Over LAN Using iDRAC Settings Utility

To configure IPMI over LAN:

1. In the **iDRAC Settings Utility**, go to **Network**.
   The **iDRAC Settings Network** page is displayed.
2. For **IPMI Settings**, specify the values.
   For information about the options, see the *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
   The IPMI over LAN settings are configured.

Configuring IPMI Over LAN Using RACADM

To configure IPMI over LAN using **set** or **config** command:

1. Enable IPMI over LAN:
   - Using **config** command: `racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1`
   - Using **set** command: `racadm set iDRAC.IPMILan.Enable 1`

   NOTE: This setting determines the IPMI commands that are executed using IPMI over LAN interface. For more information, see the IPMI 2.0 specifications at **intel.com**.
2. Update the IPMI channel privileges:
   - Using **config** command: `racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <level>`
   - Using **set** command: `racadm set iDRAC.IPMILan.PrivLimit <level>`

   where `<level>` is one of the following: 2 (User), `3` (Operator) or `4` (Administrator)
3. Set the IPMI LAN channel encryption key (if required):
   - Using **config** command: `racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <key>`
   - Using **set** command: `racadm set iDRAC.IPMILan.EncryptionKey <key>`

   where `<key>` is a 20-character encryption key in a valid hexadecimal format.

   NOTE: The iDRAC IPMI supports the RMCP+ protocol. For more information, see the IPMI 2.0 specifications at **intel.com**.

Enabling or Disabling Remote RACADM

You can enable or disable remote RACADM using the iDRAC Web interface or RACADM. You can run up to five remote RACADM sessions in parallel.

Enabling or Disabling Remote RACADM Using Web Interface

To enable or disable remote RACADM:

1. In iDRAC Web interface, go to **Overview → iDRAC Settings → Network → Services**.

The **Services** page is displayed.

2. Under **Remote RACADM**, select **Enabled**. Else, select **Disabled**.
3. Click **Apply**.

   The remote RACADM is enabled or disabled based on the selection.

Enabling or Disabling Remote RACADM Using RACADM

The RACADM remote capability is enabled by default. If disabled, type one of the following command:

- Using **config** command: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1`
- Using **set** command: `racadm set iDRAC.Racadm.Enable 1`

To disable the remote capability, type one of the following command:

- Using **config** command: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0`
- Using **set** command: `racadm set iDRAC.Racadm.Enable 0`

NOTE: It is recommended to run these commands on the local system.

Disabling Local RACADM

The local RACADM is enabled by default. To disable, see Disabling Access to Modify iDRAC Configuration Settings on Host System.

Enabling IPMI on Managed System

On a managed system, use the Dell Open Manage Server Administrator to enable or disable IPMI. For more information, see the *Dell Open Manage Server Administrator's User Guide* at **dell.com/support/manuals**.

Configuring Linux for Serial Console During Boot

The following steps are specific to the Linux GRand Unified Bootloader (GRUB). Similar changes are required if a different boot loader is used.

NOTE: When you configure the client VT100 emulation window, set the window or application that is displaying the redirected Virtual Console to 25 rows x 80 columns to make sure the correct text displays. Else, some text screens may be garbled.

Edit the **/etc/grub.conf** file as follows:

1. Locate the General Setting sections in the file and add the following:

   ```
   serial --unit=1 --speed=57600 terminal --timeout=10 serial
   ```

2. Append two options to the kernel line:

   ```
   kernel ............. console=ttyS1,115200n8r console=tty1
   ```

3. Disable GRUB's graphical interface and use the text-based interface. Else, the GRUB screen is not displayed in RAC Virtual Console. To disable the graphical interface, comment-out the line starting with `splashimage`.

The following example provides a sample **/etc/grub.conf** file that shows the changes described in this procedure.

```
# grub.conf generated by anaconda
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You do not have a /boot partition. This means that all
# kernel and initrd paths are relative to /, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sdal
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi
console=ttyS0
console=ttyS1,115200n8r
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

4. To enable multiple GRUB options to start Virtual Console sessions through the RAC serial connection, add the following line to all options:

   ```
   console=ttyS1,115200n8r console=tty1
   ```

   The example shows `console=ttyS1,57600` added to the first option.

Enabling Login to the Virtual Console After Boot

In the file **/etc/inittab**, add a new line to configure `agetty` on the COM2 serial port:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

The following example shows a sample file with the new line.

```
#inittab This file describes how the INIT process should set up
#the system in a certain run-level.
#Author:Miquel van Smoorenburg
#Modified for RHS Linux by Marc Ewing and Donnie Barnes
#Default runlevel. The runlevels used by RHS are:
#0 - halt (Do NOT set initdefault to this)
#1 - Single user mode
#2 - Multiuser, without NFS (The same as 3, if you do not have #networking)
#3 - Full multiuser mode
#4 - unused
#5 - X11
#6 - reboot (Do NOT set initdefault to this)
id:3:initdefault:
#System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
```

```
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
#Things to run in every runlevel.
ud::once:/sbin/update
ud::once:/sbin/update
#Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
#When our UPS tells us power has failed, assume we have a few
#minutes of power left. Schedule a shutdown for 2 minutes from now.
#This does, of course, assume you have power installed and your
#UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
#If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

#Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

#Run xdm in runlevel 5
#xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

In the file **/etc/securetty** add a new line with the name of the serial tty for COM2:

```
ttyS1
```

The following example shows a sample file with the new line.

NOTE: Use the Break Key Sequence (~B) to execute the Linux **Magic SysRq** key commands on serial console using IPMI Tool.

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

Supported SSH Cryptography Schemes

To communicate with iDRAC using SSH protocol, it supports multiple cryptography schemes listed in the following table.

Table 11. SSH Cryptography Schemes

Scheme Type	Scheme
Asymmetric Cryptography	Diffie-Hellman DSA/DSS 512-1024 (random) bits per NIST specification
Symmetric Cryptography	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Message Integrity	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentication	Password
PKA Authentication	Public-private key pairs

Using Public Key Authentication For SSH

iDRAC supports the Public Key Authentication (PKA) over SSH. This is a licensed feature. When the PKA over SSH is set up and used correctly, you need not enter the user name or password while logging into iDRAC. This is useful for setting up automated scripts that perform various functions. The uploaded keys must be in RFC 4716 or openssh format. Else, you must convert the keys into that format.

In any scenario, a pair of private and public key must be generated on the management station. The public key is uploaded to iDRAC local user and private key is used by the SSH client to establish the trust relationship between the management station and iDRAC.

You can generate the public or private key pair using:

- *PuTTY Key Generator* application for clients running Windows
- *ssh-keygen* CLI for clients running Linux.

CAUTION: This privilege is normally reserved for users who are members of the Administrator user group on iDRAC. However, users in the 'Custom' user group can be assigned this privilege. A user with this privilege can modify any user's configuration. This includes creation or deletion of any user, SSH Key management for users, and so on. For these reasons, assign this privilege carefully.

CAUTION: The capability to upload, view, and/ or delete SSH keys is based on the 'Configure Users' user privilege. This privilege allows user(s) to configure another user's SSH key. You should grant this privilege carefully.

Generating Public Keys for Windows

To use the *PuTTY Key Generator* application to create the basic key:

1. Start the application and select either SSH-2 RSA or SSH-2 DSA for the type of key to generate. (SSH-1 is not supported). The supported key generation algorithms are RSA and DSA only.
2. Enter the number of bits for the key. For RSA, it is between 768 and 4096 bits and for DSA, it 1024 bits.
3. Click **Generate** and move the mouse in the window as directed.

   The keys are generated.
4. You can modify the key comment field.
5. Enter a passphrase to secure the key.
6. Save the public and private key.

Generating Public Keys for Linux

To use the *ssh-keygen* application to create the basic key, open a terminal window and at the shell prompt, enter `ssh-keygen –t rsa –b 1024 –C testing`

where:

- `–t` is either *dsa* or *rsa*.
- `–b` specifies the bit encryption size between 768 and 4096.
- `–C` allows modifying the public key comment and is optional.

NOTE: The options are case-sensitive.

Follow the instructions. After the command executes, upload the public file.

CAUTION: Keys generated from the Linux management station using ssh-keygen are in non-4716 format. Convert the keys into the 4716 format using `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. Do not change the permissions of the key file. The conversion must be done using default permissions.

NOTE: iDRAC does not support ssh-agent forward of keys.

Uploading SSH Keys

You can upload up to four public keys *per user* to use over an SSH interface. Before adding the public keys, make sure that you view the keys if they are set up, so that a key is not accidentally overwritten.

When adding new public keys, make sure that the existing keys are not at the index where the new key is added. iDRAC does not perform checks to make sure previous key(s) are deleted before a new key(s) are added. When a new key is added, it is usable if the SSH interface is enabled.

Uploading SSH Keys Using Web Interface

To upload the SSH keys:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → Network → User Authentication → Local Users**.

   The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.

   The **Users Main Menu** page is displayed.
3. Under **SSH Key Configurations**, select **Upload SSH Key(s)** and click **Next**.

   The **Upload SSH Key(s)** page is displayed.
4. Upload the SSH keys in one of the following ways:
   - Upload the key file.
   - Copy the contents of the key file into the text box

   For more information, see iDRAC Online Help.
5. Click **Apply**.

Uploading SSH Keys Using RACADM

To upload the SSH keys, run the following command:

NOTE: You cannot upload and copy a key at the same time.

- For local RACADM: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- From remote RACADM using Telnet or SSH: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

For example, to upload a valid key to iDRAC User ID 2 in the first key space using a file, run the following command:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

NOTE: The `-f` option is not supported on telnet/ssh/serial RACADM.

Viewing SSH Keys

You can view the keys that are uploaded to iDRAC.

Viewing SSH Keys Using Web Interface

To view the SSH keys:

1. In Web interface, go to **Overview → iDRAC Settings → Network → User Authentication → Local Users**.

   The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.

   The **Users Main Menu** page is displayed.
3. Under **SSH Key Configurations**, select **View/Remove SSH Key(s)** and click **Next**.

   The **View/Remove SSH Key(s)** page is displayed with the key details.

Viewing SSH Keys Using RACADM

To view the SSH keys, run the following command:

- Specific key — `racadm sshpkauth -i <2 to 16> -v -k <1 to 4>`
- All keys — `racadm sshpkauth -i <2 to 16> -v -k all`

Deleting SSH Keys

Before deleting the public keys, make sure that you view the keys if they are set up, so that a key is not accidentally deleted.

Deleting SSH Keys Using Web Interface

To delete the SSH key(s):

1. In Web interface, go to **Overview → iDRAC Settings → Network → User Authentication → Local Users**.
   The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.
   The **Users Main Menu** page is displayed.
3. Under **SSH Key Configurations**, select **View/Remove SSH Key(s)** and click **Next**.
   The **View/Remove SSH Key(s)** page displays the key details.
4. Select **Remove for the key(s) you want to delete, and click Apply.**
   The selected key(s) is deleted.

Deleting SSH Keys Using RACADM

To delete the SSH key(s), run the following commands:

- Specific key — `racadm sshpkauth -i <2 to 16> -d -k <1 to 4>`
- All keys — `racadm sshpkauth -i <2 to 16> -d -k all`

7
Configuring User Accounts and Privileges

You can setup user accounts with specific privileges (*role-based authority*) to manage your system using iDRAC and maintain system security. By default iDRAC is configured with a local administrator account. This default user name is *root* and the password is *calvin*. As an administrator, you can setup user accounts to allow other users to access iDRAC.

You can setup local users or use directory services such as Microsoft Active Directory or LDAP to setup user accounts. Using a directory service provides a central location for managing authorized user accounts.

iDRAC supports role-based access to users with a set of associated privileges. The roles are administrator, operator, read only, or none. The role defines the maximum privileges available.

Related Links

Configuring Local Users
Configuring Active Directory Users
Configuring Generic LDAP Users

Configuring Local Users

You can configure up to 16 local users in iDRAC with specific access permissions. Before you create an iDRAC user, verify if any current users exist. You can set user names, passwords, and roles with the privileges for these users. The user names and passwords can be changed using any of the iDRAC secured interfaces (that is, Web interface, RACADM or WS-MAN). You can also enable or disable SNMPv3 authentication for each user.

NOTE: SNMPv3 feature is licensed and is available with iDRAC Enterprise license.

Configuring Local Users Using iDRAC Web Interface

To add and configure local iDRAC users:

NOTE: You must have Configure Users permission to create an iDRAC user.

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → User Authentication → Local Users**.
   The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.

   NOTE: User 1 is reserved for the IPMI anonymous user and you cannot change this configuration.

   The **User Main Menu** page is displayed.
3. Select **Configure User** and click **Next**.

The **User Configuration** page is displayed.

4. Enable the user ID and specify the user name, password, and access privileges for the user. You can also enable SNMPv3 authentication for the user. For more information about the options, see the *iDRAC Online Help*.
5. Click **Apply**. The user is created with the required privileges.

Configuring Local Users Using RACADM

NOTE: You must be logged in as user **root** to execute RACADM commands on a remote Linux system.

You can configure single or multiple iDRAC users using RACADM.

To configure multiple iDRAC users with identical configuration settings, perform one of the following procedures:

- Use the RACADM examples in this section as a guide to create a batch file of RACADM commands and then execute the batch file on each managed system.
- Create the iDRAC configuration file and execute the **racadm config** or **racadm set** subcommand on each managed system using the same configuration file.

If you are configuring a new iDRAC or if you have used the **racadm racresetcfg** command, the only current user is `root` with the password `calvin`. The **racresetcfg** subcommand resets the iDRAC to the default values.

NOTE: Users can be enabled and disabled over time. As a result, a user may have a different index number on each iDRAC.

To verify if a user exists, type the following command at the command prompt:

- Using **config** command: `racadm getconfig -u <username>`

OR

Type the following command once for each index (1–16):

- Using **config** command: `racadm getconfig -g cfgUserAdmin -i <index>`
- Using **get** command: `racadm get iDRAC.Users.<index>.UserName`

NOTE: You can also type `racadm getconfig -f <myfile.cfg>` or `racadm get -f <myfile.cfg>` and view or edit the **myfile.cfg** file, which includes all iDRAC configuration parameters.

Several parameters and object IDs are displayed with their current values. The objects of importance are:

- If you have used **getconfig** command:

  ```
  # cfgUserAdminIndex=XX

  cfgUserAdminUserName=
  ```

- If you have used **get** command:

  ```
  iDRAC.Users.UserName=
  ```

If the **cfgUserAdminUserName** object has no value, that index number, which is indicated by the **cfgUserAdminIndex** object, is available for use. If a name is displayed after the "=", that index is taken by that user name.

When you manually enable or disable a user with the **racadm config** subcommand, you *must* specify the index with the **-i** option.

Observe that the **cfgUserAdminIndex** object displayed in the previous example contains a '#' character. It indicates that it is a read-only object. Also, if you use the **racadm config -f racadm.cfg** command to specify any number of groups/objects to write, the index cannot be specified. This behavior allows more flexibility in configuring multiple iDRAC with the same settings.

To enable SNMP v3 authentication for a user, use **SNMPv3AuthenticationType**, **SNMPv3Enable**, **SNMPv3PrivacyType** objects. For more information, see the *RACADM Command Line Interface Guide* available at **dell.com/esmmanuals**.

If you are using the configuration XML file, then use the **AuthenticationProtocol**, **ProtocolEnable**, and **PrivacyProtocol** attributes to enable SNMPv3 authentication.

Adding iDRAC User Using RACADM

To add a new user to the RAC configuration, perform the following:

1. Set the user name.
2. Set the password.
3. Set the following user privileges:
   - iDRAC
   - LAN
   - Serial Port
   - Serial Over LAN
4. Enable the user.

Example:

The following example describes how to add a new user named "John" with a "123456" password and LOGIN privileges to the RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 3 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 3 123456

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiLanPrivilege 2

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiSerialPrivilege 2

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminEnable 1
```

To verify, use one of the following commands:

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 3
```

For more information on the RACADM commands, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Enabling iDRAC User With Permissions

To enable a user with specific administrative permissions (role-based authority):

NOTE: You can use the **getconfig** and **config** commands or **get** and **set** commands.

1. Locate an available user index using the command syntax:
   - Using **getconfig** command: `racadm getconfig -g cfgUserAdmin -i <index>`
   - Using **get** command: `racadm get iDRAC.Users <index>`

2. Type the following commands with the new user name and password.
   - Using **config** command: `racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <user privilege bitmask value>`
   - Using **set** command: `racadm set iDRAC.Users.<index>.Privilege <user privilege bitmask value>`

   NOTE: For a list of valid bit mask values for specific user privileges, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**. The default privilege value is 0, which indicates the user has no privileges enabled.

Configuring Active Directory Users

If your company uses the Microsoft Active Directory software, you can configure the software to provide access to iDRAC, allowing you to add and control iDRAC user privileges to your existing users in your directory service. This is a licensed feature.

NOTE: Using Active Directory to recognize iDRAC users is supported on the Microsoft Windows 2000, Windows Server 2003, and Windows Server 2008 operating systems.

You can configure user authentication through Active Directory to log in to the iDRAC. You can also provide role-based authority, which enables an administrator to configure specific privileges for each user.

The iDRAC role and privilege names have changed from earlier generation of servers. The role names are:

Table 12. iDRAC Roles

Current Generation	Prior Generation	Privileges
Administrator	Administrator	Login, Configure, Configure Users, Logs, System Control, Access Virtual Console, Access Virtual Media, System Operations, Debug
Operator	Power User	Login, Configure, System Control, Access Virtual Console, Access Virtual Media, System Operations, Debug
Read Only	Guest User	Login
None	None	None

Table 13. iDRAC User Privileges

Current Generation	Prior Generation	Description
Login	Login to iDRAC	Enables the user to log in to iDRAC.
Configure	Configure iDRAC	Enables the user to configure iDRAC.
Configure Users	Configure Users	Enables the user to allow specific users to access the system.
Logs	Clear Logs	Enables the user to clear the System Event Log (SEL).
System Control	Execute Server Control Commands	Allows power cycling the host system.
Access Virtual Console	Access Virtual Console Redirection (for blade servers)	Enables the user to run Virtual Console.
	Access Virtual Console (for rack and tower servers)	
Access Virtual Media	Access Virtual Media	Enables the user to run and use Virtual Media.
System Operations	Test Alerts	Allows user initiated and generated events, and information is sent as an asynchronous notification and logged.
Debug	Execute Diagnostic Commands	Enables the user to run diagnostic commands.

Related Links

Prerequisites for Using Active Directory Authentication for iDRAC
Supported Active Directory Authentication Mechanisms

Prerequisites for Using Active Directory Authentication for iDRAC

To use the Active Directory authentication feature of iDRAC, make sure that you have:

- Deployed an Active Directory infrastructure. See the Microsoft website for more information.
- Integrated PKI into the Active Directory infrastructure. iDRAC uses the standard Public Key Infrastructure (PKI) mechanism to authenticate securely into the Active Directory. See the Microsoft website for more information.
- Enabled the Secure Socket Layer (SSL) on all domain controllers that iDRAC connects to for authenticating to all the domain controllers.

Related Links

Enabling SSL on Domain Controller

Enabling SSL on Domain Controller

When iDRAC authenticates users with an Active Directory domain controller, it starts an SSL session with the domain controller. At this time, the domain controller must publish a certificate signed by the

Certificate Authority (CA)—the root certificate of which is also uploaded into iDRAC. For iDRAC to authenticate to *any* domain controller—whether it is the root or the child domain controller—that domain controller must have an SSL-enabled certificate signed by the domain's CA.

If you are using Microsoft Enterprise Root CA to *automatically* assign all your domain controllers to an SSL certificate, you must:

1. Install the SSL certificate on each domain controller.
2. Export the Domain Controller Root CA Certificate to iDRAC.
3. Import iDRAC Firmware SSL Certificate.

Related Links

Installing SSL Certificate For Each Domain Controller
Exporting Domain Controller Root CA Certificate to iDRAC
Importing iDRAC Firmware SSL Certificate

Installing SSL Certificate For Each Domain Controller

To install the SSL certificate for each controller:

1. Click **Start** → **Administrative Tools** → **Domain Security Policy**.
2. Expand the **Public Key Policies** folder, right-click **Automatic Certificate Request Settings** and click **Automatic Certificate Request**.

   The **Automatic Certificate Request Setup Wizard** is displayed.
3. Click **Next** and select **Domain Controller**.
4. Click **Next** and click **Finish**. The SSL certificate is installed.

Exporting Domain Controller Root CA Certificate to iDRAC

NOTE: If your system is running Windows 2000 or if you are using standalone CA, the following steps may vary.

To export the domain controller root CA certificate to iDRAC:

1. Locate the domain controller that is running the Microsoft Enterprise CA service.
2. Click **Start** → **Run**.
3. Enter `mmc` and click **OK**.
4. In the **Console 1** (MMC) window, click **File (**or **Console** on Windows 2000 systems**)** and select **Add/Remove Snap-in**.
5. In the **Add/Remove Snap-In** window, click **Add**.
6. In the **Standalone Snap-In** window, select **Certificates** and click **Add**.
7. Select **Computer** and click **Next**.
8. Select **Local Computer**, click **Finish**, and click **OK**.
9. In the **Console 1** window, go to **Certificates Personal Certificates** folder.
10. Locate and right-click the root CA certificate, select **All Tasks**, and click **Export...**.
11. In the **Certificate Export Wizard**, click **Next**, and select **No do not export the private key**.
12. Click **Next** and select **Base-64 encoded X.509 (.cer)** as the format.
13. Click **Next** and save the certificate to a directory on your system.
14. Upload the certificate you saved in step 13 to iDRAC.

Importing iDRAC Firmware SSL Certificate

iDRAC SSL certificate is the identical certificate used for iDRAC Web server. All iDRAC controllers are shipped with a default self-signed certificate.

If the Active Directory Server is set to authenticate the client during an SSL session initialization phase, you need to upload iDRAC Server certificate to the Active Directory Domain controller. This additional step is not required if the Active Directory does not perform a client authentication during an SSL session's initialization phase.

NOTE: If your system is running Windows 2000, the following steps may vary.

NOTE: If iDRAC firmware SSL certificate is CA-signed and the certificate of that CA is already in the domain controller's Trusted Root Certificate Authority list, do not perform the steps in this section.

To import iDRAC firmware SSL certificate to all domain controller trusted certificate lists:

1. Download iDRAC SSL certificate using the following RACADM command:
   ```
   racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
   ```
2. On the domain controller, open an **MMC Console** window and select **Certificates** → **Trusted Root Certification Authorities**.
3. Right-click **Certificates**, select **All Tasks** and click **Import**.
4. Click **Next** and browse to the SSL certificate file.
5. Install iDRAC SSL Certificate in each domain controller's **Trusted Root Certification Authority**.
   If you have installed your own certificate, make sure that the CA signing your certificate is in the **Trusted Root Certification Authority** list. If the Authority is not in the list, you must install it on all your domain controllers.
6. Click **Next** and select whether you want Windows to automatically select the certificate store based on the type of certificate, or browse to a store of your choice.
7. Click **Finish** and click **OK**. The iDRAC firmware SSL certificate is imported to all domain controller trusted certificate lists.

Supported Active Directory Authentication Mechanisms

You can use Active Directory to define iDRAC user access using two methods:

- *Standard schema* solution, which uses Microsoft's default Active Directory group objects only.
- *Extended schema* solution, which has customized Active Directory objects. All the access control objects are maintained in Active Directory. It provides maximum flexibility to configure user access on different iDRACs with varying privilege levels.

Related Links

Standard Schema Active Directory Overview
Extended Schema Active Directory Overview

Standard Schema Active Directory Overview

As shown in the following figure, using standard schema for Active Directory integration requires configuration on both Active Directory and iDRAC.

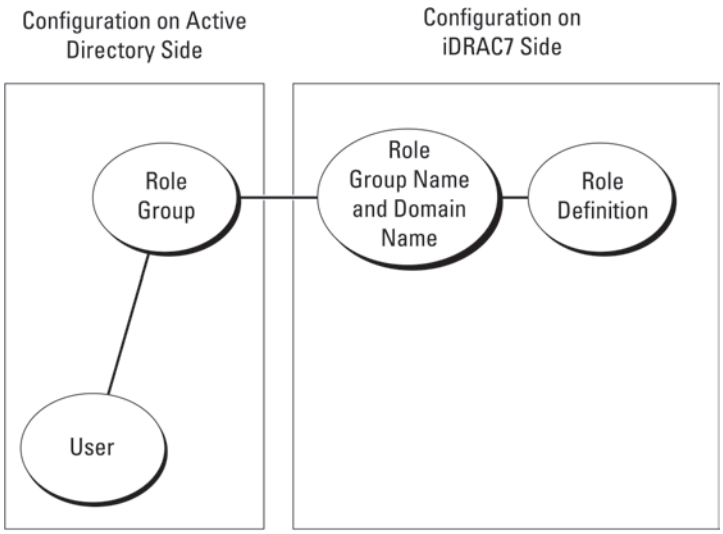


Figure 1. Configuration of iDRAC with Active Directory Standard Schema

In Active Directory, a standard group object is used as a role group. A user who has iDRAC access is a member of the role group. To give this user access to a specific iDRAC, the role group name and its domain name need to be configured on the specific iDRAC. The role and the privilege level is defined on each iDRACand not in the Active Directory. You can configure up to five role groups in each iDRAC. Table reference no shows the default role group privileges.

Table 14. Default Role Group Privileges

Role Groups	Default Privilege Level	Permissions Granted	Bit Mask
Role Group 1	None	Login to iDRAC, Configure iDRAC, Configure Users, Clear Logs, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands	0x000001ff
Role Group 2	None	Login to iDRAC, Configure iDRAC, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands	0x000000f9
Role Group 3	None	Login to iDRAC	0x00000001
Role Group 4	None	No assigned permissions	0x00000000
Role Group 5	None	No assigned permissions	0x00000000

NOTE: The Bit Mask values are used only when setting Standard Schema with the RACADM.

Single Domain Versus Multiple Domain Scenarios

If all the login users and role groups, including the nested groups, are in the same domain, then only the domain controllers' addresses must be configured on iDRAC. In this single domain scenario, any group type is supported.

If all the login users and role groups, or any of the nested groups, are from multiple domains, then Global Catalog server addresses must be configured on iDRAC. In this multiple domain scenario, all the role groups and nested groups, if any, must be a Universal Group type.

Configuring Standard Schema Active Directory

To configure iDRAC for a Active Directory login access:

1. On an Active Directory server (domain controller), open the Active Directory Users and Computers Snap-in.
2. Create a group or select an existing group. Add the Active Directory user as a member of the Active Directory group to access iDRAC.
3. Configure the group name, domain name, and the role privileges on iDRAC using the iDRAC Web interface or RACADM.

Related Links

Configuring Active Directory With Standard Schema Using iDRAC Web Interface
Configuring Active Directory With Standard Schema Using RACADM

Configuring Active Directory With Standard Schema Using iDRAC Web Interface

NOTE: For information about the various fields, see the *iDRAC Online Help*.

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → User Authentication → Directory Services → Microsoft Active Directory**.

   The **Active Directory summary** page is displayed.
2. Click **Configure Active Directory**.

   The **Active Directory Configuration and Management Step 1 of 4** page is displayed.
3. Optionally, enable certificate validation and upload the CA-signed digital certificate used during initiation of SSL connections when communicating with the Active Directory (AD) server. For this, the Domain Controllers and Global Catalog FQDN must be specified. This is done in the next steps. And hence the DNS should be configured properly in the network settings.
4. Click **Next**.

   The **Active Directory Configuration and Management Step 2 of 4** page is displayed.
5. Enable Active Directory and specify the location information about Active Directory servers and user accounts. Also, specify the time iDRAC must wait for responses from Active Directory during iDRAC login.

   NOTE: If certificate validation is enabled, specify the Domain Controller Server addresses and the Global Catalog FQDN. Make sure that DNS is configured correctly under **Overview → iDRAC Settings → Network**.
6. Click **Next**. The **Active Directory Configuration and Management Step 3 of 4** page is displayed.
7. Select **Standard Schema** and click Next.

The **Active Directory Configuration and Management Step 4a of 4** page is displayed.

8. Enter the location of Active Directory global catalog server(s) and specify privilege groups used to authorize users.
9. Click a **Role Group** to configure the control authorization policy for users under the standard schema mode.

   The **Active Directory Configuration and Management Step 4b of 4** page is displayed.
10. Specify the privileges and click **Apply**.

    The settings are applied and the **Active Directory Configuration and Management Step 4a of 4** page is displayed.
11. Click **Finish**. The Active Directory settings for standard schema is configured.

Configuring Active Directory With Standard Schema Using RACADM

To configure iDRAC Active Directory with Standard Schema using the RACADM:

1. At the racadm command prompt, run the following commands:
   - Using **config** command:

     ```
     racadm config -g cfgActiveDirectory -o cfgADEnable 1
     racadm config -g cfgActiveDirectory -o cfgADType 2
     racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupName
     <common name of the role group>
     racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain
     <fully qualified domain name>
     racadm config -g cfgStandardSchema -i <index> -o
     cfgSSADRoleGroupPrivilege <Bit Mask Value for specific RoleGroup
     permissions>
     racadm config -g cfgActiveDirectory -o cfgADDomainController1 <fully
     qualified domain name or IP address of the domain controller>
     racadm config -g cfgActiveDirectory -o cfgADDomainController2 <fully
     qualified domain name or IP address of the domain controller>
     racadm config -g cfgActiveDirectory -o cfgADDomainController3 <fully
     qualified domain name or IP address of the domain controller>
     racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog1 <fully
     qualified domain name or IP address of the domain controller>
     racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog2 <fully
     qualified domain name or IP address of the domain controller>
     racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog3 <fully
     qualified domain name or IP address of the domain controller>
     ```

   - Using **set** command:

     ```
     racadm set iDRAC.ActiveDirectory.Enable 1
     racadm set iDRAC.ActiveDirectory.Schema 2
     racadm set iDRAC.ADGroup.Name <common name of the role group>
     racadm set iDRAC.ADGroup.Domain <fully qualified domain name>
     racadm set iDRAC.ADGroup.Privilege <Bit Mask Value for specific RoleGroup
     permissions>
     racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified
     domain name or IP address of the domain controller>
     racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified
     domain name or IP address of the domain controller>
     racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified
     domain name or IP address of the domain controller>
     racadm set iDRAC.ActiveDirectory.GlobalCatalog1 <fully qualified domain
     name or IP address of the domain controller>
     racadm set iDRAC.ActiveDirectory.GlobalCatalog2 <fully qualified domain
     name or IP address of the domain controller>
     racadm set iDRAC.ActiveDirectory.GlobalCatalog3 <fully qualified domain
     name or IP address of the domain controller>
     ```

For Bit Mask values for specific Role Group permissions, see Default Role Group Privileges.

Enter the FQDN of the domain controller, not the FQDN of the domain. For example, enter `servername.dell.com` instead of `dell.com`.

At least one of the three addresses is required to be configured. iDRAC attempts to connect to each of the configured addresses one-by-one until it makes a successful connection. With Standard Schema, these are the addresses of the domain controllers where the user accounts and the role groups are located.

The Global Catalog server is only required for standard schema when the user accounts and role groups are in different domains. In multiple domain case, only the Universal Group can be used.

The FQDN or IP address that you specify in this field should match the Subject or Subject Alternative Name field of your domain controller certificate if you have certificate validation enabled.

If you want to disable the certificate validation during SSL handshake, enter the following RACADM command:

- Using **config** command: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`
- Using **set** command: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`

In this case, no Certificate Authority (CA) certificate needs to be uploaded.

To enforce the certificate validation during SSL handshake (optional):

- Using **config** command: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`
- Using **set** command: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 1`

In this case, you must upload the CA certificate using the following RACADM command:

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

NOTE: If certificate validation is enabled, specify the Domain Controller Server addresses and the Global Catalog FQDN. Make sure that DNS is configured correctly under **Overview → iDRAC Settings → Network**.

Using the following RACADM command may be optional.

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```

2. If DHCP is enabled on iDRAC and you want to use the DNS provided by the DHCP server, enter the following RACADM commands:
   - Using **config** command: `racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`
   - Using **set** command: `racadm set iDRAC.IPv4.DNSFromDHCP 1`
3. If DHCP is disabled on iDRAC or you want manually input the DNS IP address, enter the following RACADM commands:
   - Using **config** command:

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
     racadm config -g cfgLanNetworking -o cfgDNSServer1 <primary DNS IP
     ```

```
address>
racadm config -g cfgLanNetworking -o cfgDNSServer2 <secondary DNS IP
address>
```

- Using **set** command:

```
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

4. If you want to configure a list of user domains so that you only need to enter the user name when logging in to the Web interface, enter the following command:
   - Using **config** command: `racadm config -g cfgUserDomain -o cfgUserDomainName <fully qualified domain name or IP Address of the domain controller> -i <index>`
   - Using **set** command: `racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the domain controller>`

   You can configure up to 40 user domains with index numbers between 1 and 40.

Extended Schema Active Directory Overview

Using the extended schema solution requires the Active Directory schema extension.

Active Directory Schema Extensions

The Active Directory data is a distributed database of *attributes* and *classes*. The Active Directory schema includes the rules that determine the type of data that can be added or included in the database. The user class is one example of a *class* that is stored in the database. Some example user class attributes can include the user's first name, last name, phone number, and so on. You can extend the Active Directory database by adding your own unique *attributes* and *classes* for specific requirements. Dell has extended the schema to include the necessary changes to support remote management authentication and authorization using Active Directory.

Each *attribute* or *class* that is added to an existing Active Directory Schema must be defined with a unique ID. To maintain unique IDs across the industry, Microsoft maintains a database of Active Directory Object Identifiers (OIDs) so that when companies add extensions to the schema, they can be guaranteed to be unique and not to conflict with each other. To extend the schema in Microsoft's Active Directory, Dell received unique OIDs, unique name extensions, and uniquely linked attribute IDs for the attributes and classes that are added into the directory service:

- Extension is: `dell`
- Base OID is: `1.2.840.113556.1.8000.1280`
- RAC LinkID range is: `12070 to 12079`

Overview of iDRAC Schema Extensions

Dell has extended the schema to include an *Association*, *Device*, and *Privilege* property. The *Association* property is used to link together the users or groups with a specific set of privileges to one or more iDRAC devices. This model provides an administrator maximum flexibility over the different combinations of users, iDRAC privileges, and iDRAC devices on the network without much complexity.

For each physical iDRAC device on the network that you want to integrate with Active Directory for authentication and authorization, create at least one association object and one iDRAC device object. You can create multiple association objects, and each association object can be linked to as many users,

groups of users, or iDRAC device objects as required. The users and iDRAC user groups can be members of any domain in the enterprise.

However, each association object can be linked (or, may link users, groups of users, or iDRAC device objects) to only one privilege object. This example allows an administrator to control each user's privileges on specific iDRAC devices.

iDRAC device object is the link to iDRAC firmware for querying Active Directory for authentication and authorization. When iDRAC is added to the network, the administrator must configure iDRAC and its device object with its Active Directory name so that users can perform authentication and authorization with Active Directory. Additionally, the administrator must add iDRAC to at least one association object for users to authenticate.

The following figure shows that the association object provides the connection that is needed for the authentication and authorization.

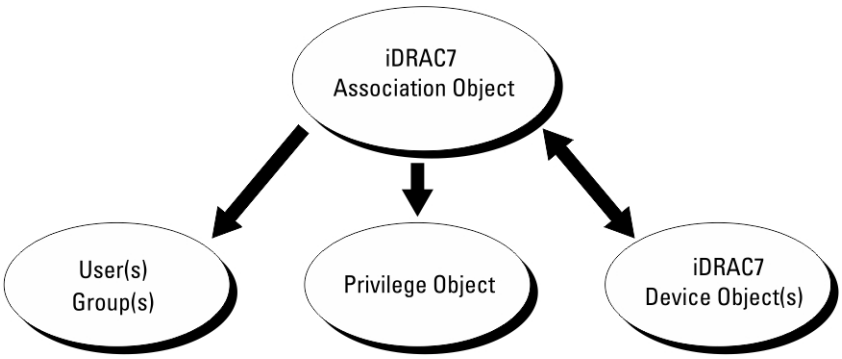


Figure 2. Typical Setup for Active Directory Objects

You can create as many or as few association objects as required. However, you must create at least one Association Object, and you must have one iDRAC Device Object for each iDRAC device on the network that you want to integrate with Active Directory for Authentication and Authorization with iDRAC.

The Association Object allows for as many or as few users and/or groups as well as iDRAC Device Objects. However, the Association Object only includes one Privilege Object per Association Object. The Association Object connects the Users who have Privileges on iDRAC devices.

The Dell extension to the ADUC MMC Snap-in only allows associating the Privilege Object and iDRAC Objects from the same domain with the Association Object. The Dell extension does not allow a group or an iDRAC object from other domains to be added as a product member of the Association Object.

When adding Universal Groups from separate domains, create an Association Object with Universal Scope. The Default Association objects created by the Dell Schema Extender Utility are Domain Local Groups and does not work with Universal Groups from other domains.

Users, user groups, or nested user groups from any domain can be added into the Association Object. Extended Schema solutions support any user group type and any user group nesting across multiple domains allowed by Microsoft Active Directory.

Accumulating Privileges Using Extended Schema

The Extended Schema Authentication mechanism supports Privilege Accumulation from different privilege objects associated with the same user through different Association Objects. In other words, Extended Schema Authentication accumulates privileges to allow the user the super set of all assigned privileges corresponding to the different privilege objects associated with the same user.

The following figure provides an example of accumulating privileges using Extended Schema.

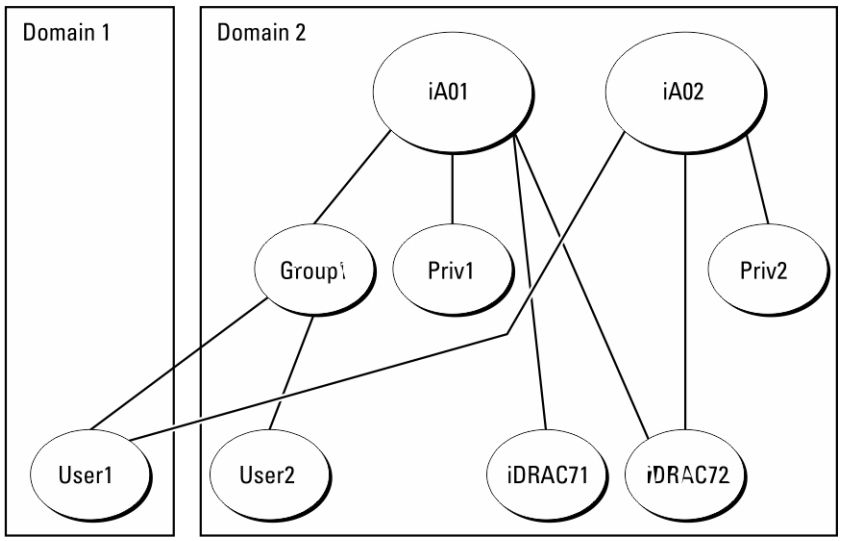


Figure 3. Privilege Accumulation for a User

The figure shows two Association Objects—A01 and A02. User1 is associated to iDRAC2 through both association objects.

Extended Schema Authentication accumulates privileges to allow the user the maximum set of privileges possible considering the assigned privileges of the different privilege objects associated to the same user.

In this example, User1 has both Priv1 and Priv2 privileges on iDRAC2. User1 has Priv1 privileges on iDRAC1 only. User2 has Priv1 privileges on both iDRAC1 and iDRAC2. In addition, this figure shows that User1 can be in a different domain and can be a member of a group.

Configuring Extended Schema Active Directory

To configure Active Directory to access iDRAC:

1. Extend the Active Directory schema.
2. Extend the Active Directory Users and Computers Snap-in.
3. Add iDRAC users and their privileges to Active Directory.
4. Configure iDRAC Active Directory properties using iDRAC Web interface or RACADM.

Related Links

Extended Schema Active Directory Overview
Installing Dell Extension to the Active Directory Users and Computers Snap-In
Adding iDRAC Users and Privileges to Active Directory
Configuring Active Directory With Extended Schema Using iDRAC Web Interface

Configuring Active Directory With Extended Schema Using RACADM

Extending Active Directory Schema

Extending your Active Directory schema adds a Dell organizational unit, schema classes and attributes, and example privileges and association objects to the Active Directory schema. Before you extend the schema, make sure that you have Schema Admin privileges on the Schema Master Flexible Single Master Operation (FSMO) Role Owner of the domain forest.

NOTE: Make sure to use the schema extension for this product is different from the previous generations of RAC products. The earlier schema does not work with this product.

NOTE: Extending the new schema has no impact on previous versions of the product.

You can extend your schema using one of the following methods:

- Dell Schema Extender utility
- LDIF script file

If you use the LDIF script file, the Dell organizational unit is not added to the schema.

The LDIF files and Dell Schema Extender are located on your *Dell Systems Management Tools and Documentation* DVD in the following respective directories:

- DVDdrive**:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools \Remote_Management_Advanced\LDIF_Files**
- <DVDdrive>:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools \Remote_Management_Advanced\Schema Extender**

To use the LDIF files, see the instructions in the readme included in the **LDIF_Files** directory.

You can copy and run the Schema Extender or LDIF files from any location.

Using Dell Schema Extender

CAUTION: The Dell Schema Extender uses the SchemaExtenderOem.ini file. To make sure that the Dell Schema Extender utility functions properly, do not modify the name of this file.

1. In the **Welcome** screen, click **Next.**
2. Read and understand the warning and click **Next**.
3. Select **Use Current Log In Credentials** or enter a user name and password with schema administrator rights.
4. Click **Next** to run the Dell Schema Extender.
5. Click **Finish**.

   The schema is extended. To verify the schema extension, use the MMC and the Active Directory Schema Snap-in to verify that the classes and attributes Classes and Attributes exist. See the Microsoft documentation for details about using the MMC and the Active Directory Schema Snap-in.

Table 15. Class Definitions for Classes Added to the Active Directory Schema

Class Name	Assigned Object Identification Number (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Table 16. dellRacDevice Class

OID	**1.2.840.113556.1.8000.1280.1.7.1.1**
Description	Represents the Dell iDRAC device. iDRAC must be configured as delliDRACDevice in Active Directory. This configuration enables iDRAC to send Lightweight Directory Access Protocol (LDAP) queries to Active Directory.
Class Type	Structural Class
SuperClasses	dellProduct
Attributes	dellSchemaVersion
	dellRacType

Table 17. delliDRACAssociationObject Class

OID	**1.2.840.113556.1.8000.1280.1.7.1.2**
Description	Represents the Dell Association Object. The Association Object provides the connection between the users and the devices.
Class Type	Structural Class
SuperClasses	Group
Attributes	dellProductMembers
	dellPrivilegeMember

Table 18. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Defines the privileges (Authorization Rights) for iDRAC
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellIsLoginUser
	dellIsCardConfigAdmin
	dellIsUserConfigAdmin
	dellIsLogClearAdmin
	dellIsServerResetUser
	dellIsConsoleRedirectUser
	dellIsVirtualMediaUser
	dellIsTestAlertUser
	dellIsDebugCommandAdmin

Table 19. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Description	Used as a container Class for the Dell Privileges (Authorization Rights).
Class Type	Structural Class
SuperClasses	User
Attributes	dellRAC4Privileges

Table 20. dellProduct Class

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Description	The main class from which all Dell products are derived.
Class Type	Structural Class
SuperClasses	Computer
Attributes	dellAssociationMembers

Table 21. List of Attributes Added to the Active Directory Schema

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellPrivilegeMember List of dellPrivilege Objects that belong to this Attribute.	1.2.840.113556.1.8000.1280.1.1.2.1 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers List of dellRacDevice and DelliDRACDevice Objects that belong to this role. This attribute is the forward link to the dellAssociationMembers backward link. Link ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE if the user has Login rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.3 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE if the user has Card Configuration rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.4 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE if the user has User Configuration rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.5 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE if the user has Log Clearing rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE if the user has Server Reset rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE if the user has Virtual Console rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser	1.2.840.113556.1.8000.1280.1.1.2.9 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
TRUE if the user has Virtual Media rights on the device.		
dellIsTestAlertUser TRUE if the user has Test Alert User rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE if the user has Debug Command Admin rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion The Current Schema Version is used to update the schema.	1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType This attribute is the Current RAC Type for the delliDRACDevice object and the backward link to the dellAssociationObjectMembers forward link.	1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers linked attribute. Link ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Installing Dell Extension to the Active Directory Users and Computers Snap-In

When you extend the schema in Active Directory, you must also extend the Active Directory Users and Computers Snap-in so the administrator can manage iDRAC devices, users and user groups, iDRAC associations, and iDRAC privileges.

When you install your systems management software using the *Dell Systems Management Tools and Documentation* DVD, you can extend the Snap-in by selecting the **Active Directory Users and Computers Snap-in** option during the installation procedure. See the Dell OpenManage Software Quick Installation Guide for additional instructions about installing systems management software. For 64-bit Windows Operating Systems, the Snap-in installer is located under:

<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

For more information about the Active Directory Users and Computers Snap-in, see Microsoft documentation.

Adding iDRAC Users and Privileges to Active Directory

Using the Dell-extended Active Directory Users and Computers Snap-in, you can add iDRAC users and privileges by creating device, association, and privilege objects. To add each object, perform the following:

- Create an iDRAC device Object
- Create a Privilege Object
- Create an Association Object
- Add objects to an Association Object

Related Links

Adding Objects to Association Object
Creating iDRAC Device Object
Creating Privilege Object
Creating Association Object

Creating iDRAC Device Object

To create iDRAC device object:

1. In the MMC **Console Root** window, right-click a container.
2. Select **New → Dell Remote Management Object Advanced**.
   The **New Object** window is displayed.
3. Enter a name for the new object. The name must be identical to iDRAC name that you enter while configuring Active Directory properties using iDRAC Web interface.
4. Select iDRAC **Device Object** and click OK.

Creating Privilege Object

To create prvivlege object:

NOTE: You must create a privilege object in the same domain as the related association object.

1. In the **Console Root** (MMC) window, right-click a container.
2. Select **New → Dell Remote Management Object Advanced**.
   The **New Object** window is displayed.
3. Enter a name for the new object.
4. Select **Privilege Object** and click OK.
5. Right-click the privilege object that you created, and select **Properties**.
6. Click the **Remote Management Privileges** tab and assign the privileges for the user or group.

Creating Association Object

To create association object:

NOTE: iDRAC association object is derived from the group and its scope is set to Domain Local.

1. In the **Console Root** (MMC) window, right-click a container.
2. Select **New → Dell Remote Management Object Advanced**.
   This **New Object** window is displayed.
3. Enter a name for the new object and select **Association Object**.
4. Select the scope for the **Association Object** and click OK.
5. Provide access privileges to the authenticated users for accessing the created association objects.

Related Links

Providing User Access Privileges For Association Objects

Providing User Access Privileges For Association Objects

To provide access privileges to the authenticated users for accessing the created association objects:

1. Go to **Administrative Tools → ADSI Edit**. The **ADSI Edit** window is displayed.
2. In the right-pane, navigate to the created association object, right-click and select **Properties**.
3. In the **Security** tab, click **Add**.
4. Type `Authenticated Users`, click **Check Names**, and click **OK**. The authenticated users is added to the list of **Groups and user names**.
5. Click **OK**.

Adding Objects to Association Object

Using the **Association Object Properties** window, you can associate users or user groups, privilege objects, and iDRAC devices or iDRAC device groups.

You can add groups of users and iDRAC devices.

Related Links

Adding Users or User Groups
Adding Privileges
Adding iDRAC Devices or iDRAC Device Groups

Adding Users or User Groups

To add users or user groups:

1. Right-click the **Association Object** and select **Properties**.
2. Select the **Users** tab and click **Add**.
3. Enter the user or user group name and click **OK**.

Adding Privileges

To add privileges:

Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to an iDRAC device. Only one privilege object can be added to an Association Object.

1. Select the **Privileges Object** tab and click **Add**.
2. Enter the privilege object name and click **OK**.

3. Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to an iDRAC device. Only one privilege object can be added to an Association Object.

Adding iDRAC Devices or iDRAC Device Groups

To add iDRAC devices or iDRAC device groups:

1. Select the **Products** tab and click **Add**.
2. Enter iDRAC devices or iDRAC device group name and click **OK**.
3. In the **Properties** window, click **Apply** and click **OK**.
4. Click the **Products** tab to add one iDRAC device connected to the network that is available for the defined users or user groups. You can add multiple iDRAC devices to an Association Object.

Configuring Active Directory With Extended Schema Using iDRAC Web Interface

To configure Active Directory with extended schema using Web interface:

NOTE: For information about the various fields, see the *iDRAC Online Help*.

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → User Authentication → Directory Services → Microsoft Active Directory**.

   The **Active Directory** summary page is displayed.
2. Click **Configure Active Directory**.

   The **Active Directory Configuration and Management Step 1 of 4** page is displayed.
3. Optionally, enable certificate validation and upload the CA-signed digital certificate used during initiation of SSL connections when communicating with the Active Directory (AD) server.
4. Click **Next**.

   The **Active Directory Configuration and Management Step 2 of 4** page is displayed.
5. Specify the location information about Active Directory (AD) servers and user accounts. Also, specify the time iDRAC must wait for responses from AD during login process.

   NOTE:

   - If certificate validation is enabled, specify the Domain Controller Server addresses and the FQDN. Make sure that DNS is configured correctly under **Overview → iDRAC Settings → Network**
   - If the user and iDRAC objects are in different domains, then do not select the **User Domain from Login** option. Instead select **Specify a Domain** option and enter the domain name where the iDRAC object is available.

   .
6. Click **Next**. The **Active Directory Configuration and Management Step 3 of 4** page is displayed.
7. Select **Extended Schema** and click **Next**.

   The **Active Directory Configuration and Management Step 4 of 4** page is displayed.
8. Enter the name and location of the iDRAC device object in Active Directory (AD) and click **Finish**.

   The Active Directory settings for extended schema mode is configured.

Configuring Active Directory With Extended Schema Using RACADM

To configure Active Directory with Extended Schema using the RACADM:

1. Open a command prompt and enter the following RACADM commands:

- Using **config** command:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o cfgADRacName <RAC common name>
racadm config -g cfgActiveDirectory -o cfgADRacDomain <fully qualified
rac domain name>
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <fully
qualified domain name or IP Address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <fully
qualified domain name or IP Address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <fully
qualified domain name or IP Address of the domain controller>
```

- Using **set** command:

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ActiveDirectory.RacName <RAC common name>
racadm set iDRAC.ActiveDirectory.RacDomain <fully qualified rac domain
name>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified
domain name or IP address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified
domain name or IP address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified
domain name or IP address of the domain controller>
```

NOTE: You must configure at least one of the three addresses. iDRAC attempts to connect to each of the configured addresses one-by-one until it makes a successful connection. With Extended Schema, these are the FQDN or IP addresses of the domain controllers where this iDRAC device is located.

To disable the certificate validation during SSL handshake (optional):

- Using **config** command: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`
- Using **set** command: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`

NOTE: In this case, you do not have to upload a CA certificate.

To enforce the certificate validation during SSL handshake (optional):

- Using **config** command: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`
- Using **set** command: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 1`

In this case, you must upload a CA certificate:

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

NOTE: If certificate validation is enabled, specify the Domain Controller Server addresses and the FQDN. Make sure that DNS is configured correctly under **Overview → iDRAC Settings → Network**.

Using the following RACADM command may be optional:

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```

2. If DHCP is enabled on iDRAC and you want to use the DNS provided by the DHCP server, enter the following RACADM command:

- Using **config** command: `racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`
- Using **set** command: `racadm set iDRAC.IPv4.DNSFromDHCP 1`

3. If DHCP is disabled in iDRAC or you want to manually input your DNS IP address, enter the following RACADM commands:
   - Using **config** command:

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
     racadm config -g cfgLanNetworking -o cfgDNSServer1 <primary DNS IP address>
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <secondary DNS IP address>
     ```

   - Using **set** command:

     ```
     racadm set iDRAC.IPv4.DNSFromDHCP 0
     racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
     racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
     ```

4. If you want to configure a list of user domains so that you only need to enter the user name during log in to iDRAC Web interface, enter the following command:
   - Using **config** command: `racadm config -g cfgUserDomain -o cfgUserDomainName <fully qualified domain name or IP Address of the domain controller> -i <index>`
   - Using **set** command: `racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the domain controller>`

   You can configure up to 40 user domains with index numbers between 1 and 40.
5. Press **Enter** to complete the Active Directory configuration with Extended Schema.

Testing Active Directory Settings

You can test the Active Directory settings to verify whether your configuration is correct, or to diagnose the problem with a failed Active Directory log in.

Testing Active Directory Settings Using iDRAC Web Interface

To test the Active Directory settings:

1. In iDRAC Web Interface, go to **Overview → iDRAC Settings → User Authentication → Directory Services → Microsoft Active Directory**.

   The **Active Directory** summary page is displayed.
2. Click **Test Settings**.
3. Enter a test user's name (for example, **username@domain.com**) and password and click **Start Test**. A detailed test results and the test log displays.

   If there is a failure in any step, examine the details in the test log to identify the problem and a possible solution.

   NOTE: When testing Active Directory settings with Enable Certificate Validation checked, iDRAC requires that the Active Directory server be identified by the FQDN and not an IP address. If the Active Directory server is identified by an IP address, certificate validation fails because iDRAC is not able to communicate with the Active Directory server.

Testing Active Directory Settings Using RACADM

To test the Active Directory settings, use the `testfeature` command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Configuring Generic LDAP Users

iDRAC provides a generic solution to support Lightweight Directory Access Protocol (LDAP)-based authentication. This feature does not require any schema extension on your directory services.

To make iDRAC LDAP implementation generic, the commonality between different directory services is utilized to group users and then map the user-group relationship. The directory service specific action is the schema. For example, they may have different attribute names for the group, user, and the link between the user and the group. These actions can be configured in iDRAC.

NOTE: The Smart Card based Two Factor Authentication (TFA) and the Single Sign-On (SSO) logins are not supported for generic LDAP Directory Service.

Related Links

Configuring Generic LDAP Directory Service Using iDRAC Web-Based Interface
Configuring Generic LDAP Directory Service Using RACADM

Configuring Generic LDAP Directory Service Using iDRAC Web-Based Interface

To configure the generic LDAP directory service using Web interface:

NOTE: For information about the various fields, see the *iDRAC Online Help*.

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → User Authentication → Directory Services → Generic LDAP Directory Service**.
   The **Generic LDAP Configuration and Management** page displays the current generic LDAP settings.
2. Click **Configure Generic LDAP**.
3. Optionally, enable certificate validation and upload the digital certificate used during initiation of SSL connections when communicating with a generic LDAP server.

   NOTE: In this release, non-SSL port based LDAP bind is not supported. Only LDAP over SSL is supported.
4. Click **Next**.
   The **Generic LDAP Configuration and Management Step 2 of 3** page is displayed.
5. Enable generic LDAP authentication and specify the location information about generic LDAP servers and user accounts.

   NOTE: If certificate validation is enabled, specify the LDAP Server's FQDN and make sure that DNS is configured correctly under **Overview → iDRAC Settings → Network**.

   NOTE: In this release, nested group is not supported. The firmware searches for the direct member of the group to match the user DN. Also, only single domain is supported. Cross domain is not supported.
6. Click **Next**.
   The **Generic LDAP Configuration and Management Step 3a of 3** page is displayed.

7. Click **Role Group**.

   The **Generic LDAP Configuration and Management Step 3b of 3** page is displayed.
8. Specify the group distinguished name, the privileges associated with the group, and click **Apply**.

   NOTE: If you are using Novell eDirectory and if you have used these characters—#(hash), "(double quotes), ;(semi colon), > (greater than), , (comma), or <(lesser than)—for the Group DN name, they must be escaped.

   The role group settings are saved. The **Generic LDAP Configuration and Management Step 3a of 3** page displays the role group settings.
9. If you want to configure additional role groups, repeat steps 7 and 8.
10. Click **Finish**. The generic LDAP directory service is configured.

Configuring Generic LDAP Directory Service Using RACADM

To configure the LDAP directory service:

- Use the objects in the **cfgLdap** and **cfgLdapRoleGroup** groups with the **config** command.
- Use the objects in the **iDRAC.LDAP** and **iDRAC.LDAPRole** groups with the **set** command.

For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Testing LDAP Directory Service Settings

You can test the LDAP directory service settings to verify whether your configuration is correct, or to diagnose the problem with a failed LDAP log in.

Testing LDAP Directory Service Settings Using iDRAC Web Interface

To test the LDAP directory service settings:

1. In iDRAC Web Interface, go to **Overview → iDRAC Settings → User Authentication → Directory Services → Generic LDAP Directory Service**.

   The **Generic LDAP Configuration and Management** page displays the current generic LDAP settings.
2. Click **Test Settings**.
3. Enter the user name and password of a directory user that is chosen to test the LDAP settings. The format depends on the *Attribute of User Login* is used and the user name entered must match the value of the chosen attribute.

   NOTE: When testing LDAP settings with **Enable Certificate Validation** checked, iDRAC requires that the LDAP server be identified by the FQDN and not an IP address. If the LDAP server is identified by an IP address, certificate validation fails because iDRAC is not able to communicate with the LDAP server.

   NOTE: When generic LDAP is enabled, iDRAC first tries to login the user as a directory user. If it fails, local user lookup is enabled.

   The test results and the test log are displayed.

Testing LDAP Directory Service Settings Using RACADM

To test the LDAP directory service settings, use the `testfeature` command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

8

Configuring iDRAC for Single Sign-On or Smart Card Login

This section provides information to configure iDRAC for Smart Card login (for local users and Active Directory users), and Single Sign-On (SSO) login (for Active Directory users.) SSO and smart card login are licensed features.

iDRAC supports Kerberos based Active Directory authentication to support Smart Card and SSO logins. For information on Kerberos, see the Microsoft website.

Related Links

Configuring iDRAC SSO Login for Active Directory Users
Configuring iDRAC Smart Card Login for Local Users
Configuring iDRAC Smart Card Login for Active Directory Users

Prerequisites for Active Directory Single Sign-On or Smart Card Login

The pre-requisites to Active Directory based SSO or Smart Card logins are:

- Synchronize iDRAC time with the Active Directory domain controller time. If not, kerberos authentication on iDRAC fails. You can use the Time zone and NTP feature to synchronize the time. To do this, see Configuring Time zone and NTP.
- Register iDRAC as a computer in the Active Directory root domain.
- Generate a keytab file using the ktpass tool.
- To enable single sign-on for Extended schema, make sure that the **Trust this user for delegation to any service (Kerberos only)** option is selected on the **Delegation** tab for the keytab user. This tab is available only after creating the keytab file using ktpass utility.
- Configure the browser to enable SSO login.
- Create the Active Directory objects and provide the required privileges.
- For SSO, configure the reverse lookup zone on the DNS servers for the subnet where iDRAC resides.

NOTE: If the host name does not match the reverse DNS lookup, Kerberos authentication fails.

Related Links

Configuring Browser to Enable Active Directory SSO
Registering iDRAC as a Computer in Active Directory Root Domain
Generating Kerberos Keytab File
Creating Active Directory Objects and Providing Privileges

Registering iDRAC as a Computer in Active Directory Root Domain

To register iDRAC in Active Directory root domain:

1. Click **Overview → iDRAC Settings → Network → Network**.
   The **Network** page is displayed.
2. Provide a valid **Preferred/Alternate DNS Server** IP address. This value is a valid DNS server IP address that is part of the root domain.
3. Select **Register iDRAC on DNS**.
4. Provide a valid **DNS Domain Name**.
5. Verify that network DNS configuration matches with the Active Directory DNS information.
   For more information about the options, see the *iDRAC Online Help*.

Generating Kerberos Keytab File

To support the SSO and smart card login authentication, iDRAC supports the configuration to enable itself as a kerberized service on a Windows Kerberos network. The Kerberos configuration on iDRAC involves the same steps as configuring a non–Windows Server Kerberos service as a security principal in Windows Server Active Directory.

The *ktpass* tool (available from Microsoft as part of the server installation CD/DVD) is used to create the Service Principal Name (SPN) bindings to a user account and export the trust information into a MIT–style Kerberos *keytab* file, which enables a trust relation between an external user or system and the Key Distribution Centre (KDC). The keytab file contains a cryptographic key, which is used to encrypt the information between the server and the KDC. The ktpass tool allows UNIX–based services that support Kerberos authentication to use the interoperability features provided by a Windows Server Kerberos KDC service. For more information on the **ktpass** utility, see the Microsoft website at: **technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

Before generating a keytab file, you must create an Active Directory user account for use with the **-mapuser** option of the `ktpass` command. Also, you must have the same name as iDRAC DNS name to which you upload the generated keytab file.

To generate a keytab file using the ktpass tool:

1. Run the *ktpass* utility on the domain controller (Active Directory server) where you want to map iDRAC to a user account in Active Directory.
2. Use the following ktpass command to create the Kerberos keytab file:

   ```
   C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -
   mapuser DOMAINNAME\username -mapOp set -crypto AES256-SHA1 -ptype
   KRB5_NT_PRINCIPAL -pass [password] -out c:\krbkeytab
   ```

   The encryption type is AES256-SHA1. The principal type is KRB5_NT_PRINCIPAL. The properties of the user account to which the Service Principal Name is mapped to must have **Use AES 256 encryption types for this account** property enabled.

   NOTE: Use lowercase letters for the **iDRACname** and **Service Principal Name**. Use uppercase letters for the domain name as shown in the example.
3. Run the following command:

   ```
   C:\>setspn -a HTTP/iDRACname.domainname.com username
   ```

A keytab file is generated.

NOTE: If you find any issues with iDRAC user for which the keytab file is created, create a new user and a new keytab file. If the same keytab file which was initially created is again executed, it does not configure correctly.

Creating Active Directory Objects and Providing Privileges

Perform the following steps for Active Directory Extended schema based SSO login:

1. Create the device object, privilege object, and association object in the Active Directory server.
2. Set access privileges to the created privilege object. It is recommended not to provide administrator privileges as this could bypass some security checks.
3. Associate the device object and privilege object using the association object.
4. Add the preceding SSO user (login user) to the device object.
5. Provide access privilege to *Authenticated Users* for accessing the created association object.

Related Links

Adding iDRAC Users and Privileges to Active Directory

Configuring Browser to Enable Active Directory SSO

This section provides the browser settings for Internet Explorer and Firefox to enable Active Directory SSO.

NOTE: Google Chrome and Safari do not support Active Directory for SSO login.

Configuring Internet Explorer to Enable Active Directory SSO

To configure the browser settings for Internet Explorer:

1. In Internet Explorer, navigate to **Local Intranet** and click **Sites**.
2. Select the following options only:
   - Include all local (intranet) sites not listed on other zones.
   - Include all sites that bypass the proxy server.
3. Click **Advanced**.
4. Add all relative domain names that will be used for iDRAC instances that is part of the SSO configuration (for example, **myhost.example.com**.)
5. Click **Close** and click **OK** twice.

Configuring Firefox to Enable Active Directory SSO

To configure the browser settings for Firefox:

1. In Firefox address bar, enter `about:config`.
2. In **Filter**, enter `network.negotiate`.
3. Add the iDRAC name to network.negotiate-auth.trusted-uris (using comma separated list.)
4. Add the iDRAC name to network.negotiate-auth.delegation-uris (using comma separated list.)

Configuring iDRAC SSO Login for Active Directory Users

Before configuring iDRAC for Active Directory SSO login, make sure that you have completed all the prerequisites.

You can configure iDRAC for Active Directory SSO when you setup an user account based on Active Directory.

Related Links

Prerequisites for Active Directory Single Sign-On or Smart Card Login
Configuring Active Directory With Standard Schema Using iDRAC Web Interface
Configuring Active Directory With Standard Schema Using RACADM
Configuring Active Directory With Extended Schema Using iDRAC Web Interface
Configuring Active Directory With Extended Schema Using RACADM

Configuring iDRAC SSO Login for Active Directory Users Using Web Interface

To configure iDRAC for Active Directory SSO login:

NOTE: For information about the options, see the *iDRAC Online Help*.

1. Verify whether the iDRAC DNS name matches the iDRAC Fully Qualified Domain Name. To do this, in iDRAC Web interface, go to **Overview → iDRAC Settings → Network → Network** and see the **DNS Domain Name** property.
2. While configuring Active Directory to setup a user account based on standard schema or extended schema, perform the following two additional steps to configure SSO:
   - Upload the keytab file on the **Active Directory Configuration and Management Step 1 of 4** page.
   - Select **Enable Single Sign-On** option on the **Active Directory Configuration and Management Step 2 of 4** page.

Configuring iDRAC SSO Login for Active Directory Users Using RACADM

In addition to the steps performed while configuring Active Directory, to enable SSO, run any of the following command:

- Using **config** command:
  ```
  racadm config -g cfgActiveDirectory -o cfgADSSOEnable 1
  ```
- Using **set** command:
  ```
  racadm set iDRAC.ActiveDirectory.SSOEnable 1
  ```

Configuring iDRAC Smart Card Login for Local Users

To configure iDRAC local user for smart card login:

1. Upload the smart card user certificate and trusted CA certificate to iDRAC.
2. Enable smart card login.

Related Links

Obtaining Certificates
Uploading Smart Card User Certificate

Enabling or Disabling Smart Card Login

Uploading Smart Card User Certificate

Before you upload the user certificate, make sure that the user certificate from the smart card vendor is exported in Base64 format. SHA-2 certificates are also supported.

Related Links

Obtaining Certificates

Uploading Smart Card User Certificate Using Web Interface

To upload smart card user certificate:

1. In iDRAC Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **User Authentication** → **Local Users**.
   The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.
   The **Users Main Menu** page is displayed.
3. Under **Smart Card Configurations**, select **Upload User Certificate** and click **Next**.
   The **User Certificate Upload** page is displayed.
4. Browse and select the Base64 user certificate, and click **Apply**.

Uploading Smart Card User Certificate Using RACADM

To upload smart card user certificate, use the **usercertupload** object. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Uploading Trusted CA Certificate For Smart Card

Before you upload the CA certificate, make sure that you have a CA-signed certificate.

Related Links

Obtaining Certificates

Uploading Trusted CA Certificate For Smart Card Using Web Interface

To upload trusted CA certificate for smart card login:

1. In iDRAC Web interface, go to **Overview** → **iDRAC Settings** → **Network** → **User Authentication** → **Local Users**.
   The **Users** page is displayed.
2. In the **User ID** column, click a user ID number.
   The **Users Main Menu** page is displayed.
3. Under **Smart Card Configurations**, select **Upload Trusted CA Certificate** and click **Next**.
   The **Trusted CA Certificate Upload** page is displayed.
4. Browse and select the trusted CA certificate, and click **Apply**.

Uploading Trusted CA Certificate For Smart Card Using RACADM

To upload trusted CA certificate for smart card login, use the **usercertupload** object. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Configuring iDRAC Smart Card Login for Active Directory Users

Before configuring iDRAC Smart Card login for Active Directory users, make sure that you have completed the required prerequisites.

To configure iDRAC for smart card login:

1. In iDRAC Web interface, while configuring Active Directory to set up an user account based on standard schema or extended schema, on the **Active Directory Configuration and Management Step 1 of 4** page:
   - Enable certificate validation.
   - Upload a trusted CA-signed certificate.
   - Upload the keytab file.
2. Enable smart card login. For information about the options, see the *iDRAC Online Help*.

Related Links

Enabling or Disabling Smart Card Login
Obtaining Certificates
Generating Kerberos Keytab File
Configuring Active Directory With Standard Schema Using iDRAC Web Interface
Configuring Active Directory With Standard Schema Using RACADM
Configuring Active Directory With Extended Schema Using iDRAC Web Interface
Configuring Active Directory With Extended Schema Using RACADM

Enabling or Disabling Smart Card Login

Before enabling or disabling smart card login for iDRAC, make sure that:

- You have configure iDRAC permissions.
- iDRAC local user configuration or Active Directory user configuration with the appropriate certificates is complete.

NOTE: If smart card login is enabled, then SSH, Telnet, IPMI Over LAN, Serial Over LAN, and remote RACADM are disabled. Again, if you disable smart card login, the interfaces are not enabled automatically.

Related Links

Obtaining Certificates
Configuring iDRAC Smart Card Login for Active Directory Users
Configuring iDRAC Smart Card Login for Local Users

Enabling or Disabling Smart Card Login Using Web Interface

To enable or disable the Smart Card logon feature:

1. In the iDRAC Web interface, go to **Overview → iDRAC Settings → User Authentication → Smart Card** .

   The **Smart Card** page is displayed.
2. From the **Configure Smart Card Logon** drop-down menu, select **Enabled** to enable smart card logon or select **Enabled With Remote RACADM**. Else, select **Disabled**.

   For more information about the options, see the *iDRAC Online Help*.
3. Click **Apply** to apply the settings.

   You are prompted for a Smart Card login during any subsequent logon attempts using the iDRAC Web interface.

Enabling or Disabling Smart Card Login Using RACADM

To enable smart card login, use one of the following:

- Use the objects in the **cfgSmartCard** group with the **config** command.
- Use the objects in the **iDRAC.SmartCard** group with the **set** command.

For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide*available at **dell.com/support/manuals**.

Enabling or Disabling Smart Card Login Using iDRAC Settings Utility

To enable or disable the Smart Card logon feature:

1. In the iDRAC Settings utility, go to **Smart Card**.

   The **iDRAC Settings Smart Card** page is displayed.
2. Select **Enabled** to enable smart card logon. Else, select **Disabled**. For more information about the options, see *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.

   The smart card logon feature is enabled or disabled based on the selection.

9

Configuring iDRAC to Send Alerts

You can set alerts and actions for certain events that occur on the managed system. An event occurs when the status of a system component is greater than the pre-defined condition. If an event matches an event filter and you have configured this filter to generate an alert (e-mail, SNMP trap, IPMI alert, remote system logs, or WS events), then an alert is sent to one or more configured destinations. If the same event filter is also configured to perform an action (such as reboot, power cycle, or power off the system), the action is performed. You can set only one action for each event.

To configure iDRAC to send alerts:

1. Enable alerts.
2. Optionally, you can filter the alerts based on category or severity.
3. Configure the e-mail alert, IPMI alert, SNMP trap, remote system log, operating system log, and/or WS-event settings.
4. Enable event alerts and actions such as:
   - Send an email alert, IPMI alert, SNMP traps, remote system logs, operating system log, or WS events to configured destinations.
   - Perform a reboot, power off, or power cycle the managed system.

Related Links

Enabling or Disabling Alerts
Filtering Alerts
Setting Event Alerts
Setting Alert Recurrence Event
Configuring Email Alert, SNMP Trap, or IPMI Trap Settings
Configuring Remote System Logging
Configuring WS Eventing
Alerts Message IDs

Enabling or Disabling Alerts

For sending an alert to configured destinations or to perform an event action, you must enable the global alerting option. This property overrides individual alerting or event actions that is set.

Related Links

Filtering Alerts
Configuring Email Alert, SNMP Trap, or IPMI Trap Settings

Enabling or Disabling Alerts Using Web Interface

To enable or disable generating alerts:

1. In iDRAC Web interface, go to **Overview** → **Server** → **Alerts**. The **Alerts** page is displayed.
2. Under **Alerts** section:
   - Select **Enable** to enable alert generation or perform an event action.
   - Select **Disable** to disable alert generation or disable an event action.
3. Click **Apply** to save the setting.

Enabling or Disabling Alerts Using RACADM

To enable or disable generating alerts or event actions using **config** command:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

To enable or disable generating alerts or event actions using **set** command:

```
racadm set iDRAC.IPMILan.AlertEnable 1
```

Enabling or Disabling Alerts Using iDRAC Settings Utility

To enable or disable generating alerts or event actions:

1. In the iDRAC Settings utility, go to **Alerts**.
   The **iDRAC Settings Alerts** page is displayed.
2. Under **Platform Events**, select **Enabled** to enable alert generation or event action. Else, select **Disabled**. For more information about the options, see *iDRAC Settings Utility Online Help.*
3. Click **Back**, click **Finish**, and then click **Yes**.
   The alert settings are configured.

Filtering Alerts

You can filter alerts based on category and severity.

Related Links

Enabling or Disabling Alerts
Configuring Email Alert, SNMP Trap, or IPMI Trap Settings

Filtering Alerts Using iDRAC Web Interface

To filter the alerts based on category and severity:

NOTE: Even if you are a user with read-only privileges, you can filter the alerts.

1. In iDRAC Web interface, go to **Overview** → **Server** → **Alerts**. The **Alerts** page is displayed.
2. Under **Alerts Filter** section, select one or more of the following categories:
   - System Health
   - Storage
   - Configuration
   - Audit

- Updates
- Work Notes

3. Select one or more of the following severity levels:
   - Informational
   - Warning
   - Critical
4. Click **Apply**.

   The **Alert Results** section displays the results based on the selected category and severity.

Filtering Alerts Using RACADM

To filter the alerts, use the **eventfilters** command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Setting Event Alerts

You can set event alerts such as e-mail alerts, IPMI alerts, SNMP traps, remote system logs, operating system logs, and WS events to be sent to configured destinations.

Related Links

Enabling or Disabling Alerts
Configuring Email Alert, SNMP Trap, or IPMI Trap Settings
Filtering Alerts
Configuring Remote System Logging
Configuring WS Eventing

Setting Event Alerts Using Web Interface

To set an event alert using the Web interface:

1. Make sure that you have configured the e-mail alert, IPMI alert, SNMP trap settings, and/or remote system log settings.
2. Go to **Overview** → **Server** → **Alerts**.

   The **Alerts** page is displayed.
3. Under **Alerts Results**, select one or all of the following alerts for the required events:
   - Email Alert
   - SNMP Trap
   - IPMI Alert
   - Remote System Log
   - OS Log
   - WS Eventing
4. Click **Apply**.

   The setting is saved.
5. Under **Alerts** section, select the **Enable** option to send alerts to configured destinations.
6. Optionally, you can send a test event. In the **Message ID to Test Event** field, enter the message ID to test if the alert is generated and click **Test**. For the list of message IDs, see the *Event Messages Guide* available at **dell.com/support/manuals**.

Setting Event Alerts Using RACADM

To set an event alert, use the **eventfilters** command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Setting Alert Recurrence Event

You can configure iDRAC to generate additional events at specific intervals if the system continues to operate at a temperature which is greater than the inlet temperature threshold limit. The default interval is 30 days. The valid range is 0 to 366 days. A value of '0' indicates no event recurrence.

NOTE: You must have Configure iDRAC privilege to set the alert recurrence value.

Setting Alert Recurrence Events Using iDRAC Web Interface

To set the alert recurrence value:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Alerts** → **Alert Recurrence**.
   The **Alert Recurrence** page is displayed.
2. In the **Recurrence** column, enter the alert frequency value for the required category, alert, and severity type(s).
   For more information, see the *iDRAC Online help*.
3. Click **Apply**.
   The alert recurrence settings are saved.

Setting Alert Recurrence Events Using RACADM

To set the alert recurrence event using RACADM, use the **eventfilters** subcommand. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide*.

Setting Event Actions

You can set event actions such as perform a reboot, power cycle, power off, or perform no action on the system.

Related Links

Filtering Alerts
Enabling or Disabling Alerts

Setting Event Actions Using Web Interface

To set an event action:

1. In iDRAC Web interface, go to **Overview** → **Server** → **Alerts**. The **Alerts** page is displayed.
2. Under **Alerts Results**, from the **Actions** drop-down menu, for each event select an action:
   - Reboot
   - Power Cycle
   - Power Off

- No Action

3. Click **Apply**.
   The setting is saved.

Setting Event Actions Using RACADM

To configure an event action, use one of the following:

- **eventfilters** command.
- **cfgIpmiPefAction** object with **config** command.

For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Configuring Email Alert, SNMP Trap, or IPMI Trap Settings

The management station uses Simple Network Management Protocol (SNMP) and Intelligent Platform Management Interface (IPMI) traps to receive data from iDRAC. For systems with large number of nodes, it may not be efficient for a management station to poll each iDRAC for every condition that may occur. For example, event traps can help a management station with load balancing between nodes or by issuing an alert if an authentication failure occurs. SNMP v1, v2, and v3 formats are supported.

You can configure the IPv4 and IPv6 alert destinations, email settings, and SMTP server settings, and test these settings. You can also specify the SNMP v3 user to whom you want to send the SNMP traps.

Before configuring the email, SNMP, or IPMI trap settings, make sure that:

- You have Configure RAC permission.
- You have configured the event filters.

Related Links

Configuring IP Alert Destinations
Configuring Email Alert Settings

Configuring IP Alert Destinations

You can configure the IPv6 or IPv4 addresses to receive the IPMI alerts or SNMP traps. For information about the iDRAC MIBs required to monitor the servers using SNMP, see the *SNMP Reference Guide for iDRAC8* available at **dell.com/support/manuals**.

Configuring IP Alert Destinations Using Web Interface

To configure alert destination settings using Web interface:

1. Go to **Overview → Server → Alerts → SNMP and E-mail Settings**.
2. Select the **State** option to enable an alert destination (IPv4 address, IPv6 address, or Fully Qualified Domain Name (FQDN)) to receive the traps.
   You can specify up to eight destination addresses. For more information about the options, see the *iDRAC Online Help*.
3. Select the SNMP v3 user to whom you want to send the SNMP trap.
4. Enter the iDRAC SNMP community string (applicable only for SNMPv1 and v2) and the SNMP alert port number.

For more information about the options, see the *iDRAC Online Help*.

NOTE: The Community String value indicates the community string to use in a Simple Network Management Protocol (SNMP) alert trap sent from iDRAC. Make sure that the destination community string is the same as the iDRAC community string. The default value is Public.

5. To test whether the IP address is receiving the IPMI or SNMP traps, click **Send** under **Test IPMI Trap** and **Test SNMP Trap** respectively.
6. Click **Apply**.

   The alert destinations are configured.
7. In the **SNMP Trap Format** section, select the protocol version to be used to send the traps on the trap destination(s) — **SNMP v1**, **SNMP v2**, or **SNMP v3** and click **Apply**.

   NOTE: The **SNMP Trap Format** option applies only for SNMP Traps and not for IPMI Traps. IPMI Traps are always sent in SNMP v1 format and is not based on the configured **SNMP Trap Format** option.

   The SNMP trap format is configured.

Configuring IP Alert Destinations Using RACADM

To configure the trap alert settings:

1. To enable traps:
   - For IPv4 address:

     ```
     racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i (index) (0|1)
     ```
   - For IPv6 address:

     ```
     racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertEnable -i (index)
     (0|1)
     ```

     where, (index) is the destination index and 0 or 1 disables or enables the trap, respectively.

     For example, to enable trap with index 4, enter the following command:

     ```
     racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
     ```
2. To configure the trap destination address:

   ```
   racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertDestIPAddr -i
   [index] [IP-address]
   ```

   where `[index]` is the trap destination index and `[IP-address]` is the destination IP address of the system that receives the platform event alerts.
3. Configure the SNMP community name string:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName [name]
   ```

   where `[name]` is the SNMP Community Name.
4. To configure SNMP destination:
   - To set the SNMP trap destination for SNMPv3:

     ```
     racadm set idrac.SNMP.Alert.[index].DestAddr [Ip address]
     ```

     For example,

     ```
     racadm set idrac.SNMP.Alert.1.DestAddr 1.2.3.4
     ```
   - To set SNMPv3 users for trap destinations:

     ```
     racadm set idrac.SNMP.Alert.1.SNMPv3Username root
     ```

- To enable SNMPv3 for a user:

  ```
  racadm set idrac.users.2.SNMPv3Enable Enabled
  ```

5. To test the trap, if required:

   ```
   racadm testtrap -i [index]
   ```

   where `[index]` is the trap destination index to test.

   For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Configuring IP Alert Destinations Using iDRAC Settings Utility

You can configure alert destinations (IPv4, IPv6, or FQDN) using the iDRAC Settings utility. To do this:

1. In the **iDRAC Settings utility**, go to **Alerts**.

   The **iDRAC Settings Alerts** page is displayed.
2. Under **Trap Settings**, enable the IP address(es) to receive the traps and enter the IPv4, IPv6, or FQDN destination address(es). You can specify up to eight addresses.
3. Enter the community string name.

   For information about the options, see the *iDRAC Settings Utility Online Help*.
4. Click **Back**, click **Finish**, and then click **Yes**.

   The alert destinations are configured.

Configuring Email Alert Settings

You can configure the email address to receive the email alerts. Also, configure the SMTP server address settings.

NOTE: If your mail server is Microsoft Exchange Server 2007, make sure that iDRAC domain name is configured for the mail server to receive the email alerts from iDRAC.

NOTE: Email alerts support both IPv4 and IPv6 addresses. The DRAC DNS Domain Name must be specified when using IPv6.

Related Links

Configuring SMTP Email Server Address Settings

Configuring Email Alert Settings Using Web Interface

To configure the email alert settings using Web interface:

1. Go to **Overview → Server → Alerts → SNMP and Email Settings** .
2. Select the **State** option to enable the email address to receive the alerts and type a valid email address. For more information about the options, see the *iDRAC Online Help*.
3. Click **Send** under **Test Email** to test the configured email alert settings.
4. Click **Apply**.

Configuring Email Alert Settings Using RACADM

To configure the email alert settings:

1. To enable email alert:

- Using **config** command:

  ```
  racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i [index] [0|1]
  ```

  where `[index]` is the email destination index. 0 disables the email alert and 1 enables the alert.

  The email destination index can be a value from 1 through 4. For example, to enable email with index 4, enter the following command:

  ```
  racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
  ```

- Using **set** command:

  ```
  racadm set iDRAC.EmailAlert.Enable.[index] 1
  ```

  where `[index]` is the email destination index. 0 disables the email alert and 1 enables the alert.

  The email destination index can be a value from 1 through 4. For example, to enable email with index 4, enter the following command:

  ```
  racadm set iDRAC.EmailAlert.Enable.4 1
  ```

2. To configure email settings:
   - Using **config** command:

     ```
     racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 [email-address]
     ```

     where 1 is the email destination index and `[email-address]` is the destination email address that receives the platform event alerts.
   - Using **set** command:

     ```
     racadm set iDRAC.EmailAlert.Address.1 [email-address]
     ```

     where 1 is the email destination index and `[email-address]` is the destination email address that receives the platform event alerts.
3. To configure a custom message:
   - Using **config** command:

     ```
     racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i [index] [custom-message]
     ```

     where `[index]` is the email destination index and `[custom-message]` is the custom message.
   - Using **set** command:

     ```
     racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
     ```

     where `[index]` is the email destination index and `[custom-message]` is the custom message.
4. To test the configured email alert, if required:

   ```
   racadm testemail -i [index]
   ```

   where `[index]` is the email destination index to test.

   For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Configuring SMTP Email Server Address Settings

You must configure the SMTP server address for email alerts to be sent to specified destinations.

Configuring SMTP Email Server Address Settings Using iDRAC Web Interface

To configure the SMTP server address:

1. In iDRAC Web interface, go to **Overview → Server → Alerts → SNMP and E-mail Settings**.
2. Enter the valid IP address or fully qualified domain name (FQDN) of the SMTP server to be used in the configuration.

3. Select the **Enable Authentication** option and then provide the user name and password (of a user who has access to SMTP server).
4. Enter the SMTP port number.
   For more information about the fields, see the *iDRAC Online Help*.
5. Click **Apply**.
   The SMTP settings are configured.

Configuring SMTP Email Server Address Settings Using RACADM

To configure the SMTP email server, use one of the following:

- Using **set** command:
  ```
  racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP Address>
  ```
- Using **config** command:
  ```
  racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr <SMTP E-mail Server IP Address>
  ```

Configuring WS Eventing

The WS Eventing protocol is used for a client service (subscriber) to register interest (subscription) with a server (event source) for receiving messages containing the server events (notifications or event messages). Clients interested in receiving the WS Eventing messages can subscribe with iDRAC and receive Lifecycle Controller job related events.

The steps required to configure WS eventing feature to receive WS Eventing messages for changes related to Lifecycle Controller jobs are described in the Web service Eventing Support for iDRAC 1.30.30 specification document. In addition to this specification, see the DSP0226 (DMTF WS Management Specification), Section 10 Notifications (Eventing) document for the complete information on the WS Eventing protocol. The Lifecycle Controller related jobs are described in the DCIM Job Control Profile document.

Alerts Message IDs

The following table provides the list of message IDs that are displayed for the alerts.

Table 22. Alert Message IDs

Message ID	Description
AMP	Amperage
ASR	Auto Sys Reset
BAR	Backup/Restore
BAT	Battery Event
BIOS	BIOS Management
BOOT	BOOT Control

Message ID	Description
CBL	Cable
CPU	Processor
CPUA	Proc Absent
CTL	Storage Contr
DH	Cert Mgmt
DIS	Auto-Discovery
ENC	Storage Enclosr
FAN	Fan Event
FSD	Debug
HWC	Hardware Config
IPA	DRAC IP Change
ITR	Intrusion
JCP	Job Control
LC	Lifecycle Contr
LIC	Licensing
LNK	Link Status
LOG	Log event
MEM	Memory
NDR	NIC OS Driver
NIC	NIC Config
OSD	OS Deployment
OSE	OS Event
PCI	PCI Device
PDR	Physical Disk
PR	Part Exchange

Message ID	Description
PST	BIOS POST
PSU	Power Supply
PSUA	PSU Absent
PWR	Power Usage
RAC	RAC Event
RDU	Redundancy
RED	FW Download
RFL	IDSDM Media
RFLA	IDSDM Absent
RFM	FlexAddress SD
RRDU	IDSDM Redundancy
RSI	Remote Service
SEC	Security Event
SEL	Sys Event Log
SRD	Software RAID
SSD	PCIe SSD
STOR	Storage
SUP	FW Update Job
SWC	Software Config
SWU	Software Change
SYS	System Info
TMP	Temperature
TST	Test Alert
UEFI	UEFI Event
USR	User Tracking

Message ID	Description
VDR	Virtual Disk
VF	vFlash SD card
VFL	vFlash Event
VFLA	vFlash Absent
VLT	Voltage
VME	Virtual Media
VRM	Virtual Console
WRK	Work Note

10

Managing Logs

iDRAC provides Lifecycle log that contains events related to system, storage devices, network devices, firmware updates, configuration changes, license messages, and so on. However, the system events are also available as a separate log called System Event Log (SEL). The lifecycle log is accessible through iDRAC Web interface, RACADM, and WS-MAN interface.

When the size of the lifecycle log reaches 800 KB, the logs are compressed and archived. You can only view the non-archived log entries, and apply filters and comments to non-archived logs. To view the archived logs, you must export the entire lifecycle log to a location on your system.

Related Links

Viewing System Event Log
Viewing Lifecycle Log
Exporting Lifecycle Controller Logs
Adding Work Notes
Configuring Remote System Logging

Viewing System Event Log

When a system event occurs on a managed system, it is recorded in the System Event Log (SEL). The same SEL entry is also available in the LC log.

Viewing System Event Log Using Web Interface

To view the SEL, in iDRAC Web interface, go to **Overview → Server → Logs**.

The **System Event Log** page displays a system health indicator, a time stamp, and a description for each event logged. For more information, see the *iDRAC Online Help*.

Click **Save As** to save the **SEL** to a location of your choice.

NOTE: If you are using Internet Explorer and if there is a problem when saving, download the Cumulative Security Update for Internet Explorer. You can download it from the Microsoft Support website at **support.microsoft.com**.

To clear the logs, click **Clear Log**.

NOTE: Clear Log only appears if you have Clear Logs permission.

After the SEL is cleared, an entry is logged in the Lifecycle Controller log. The log entry includes the user name and the IP address from where the SEL was cleared.

Viewing System Event Log Using RACADM

To view the SEL:

```
racadm getsel <options>
```

If no arguments are specified, the entire log is displayed.

To display the number of SEL entries: `racadm getsel -i`

To clear the SEL entries: `racadm clrsel`

For more information, see *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Viewing System Event Log Using iDRAC Settings Utility

You can view the total number of records in the System Event Log (SEL) using the iDRAC Settings Utility and clear the logs. To do this:

1. In the iDRAC Settings Utililty, go to **System Event Log**.
   The **iDRAC Settings.System Event Log** displays the **Total Number of Records**.
2. To clear the records, select **Yes**. Else, select **No**.
3. To view the system events, click **Display System Event Log**.
4. Click **Back**, click **Finish**, and then click **Yes**.

Viewing Lifecycle Log

Lifecycle Controller logs provide the history of changes related to components installed on a managed system. It provides logs about events related to:

- Storage Devices
- System events
- Network Devices
- Configuration
- Audit
- Updates
- Work notes

When you log in or log out of iDRAC using any of the following interfaces, the log in, log out, or log in failure events are recorded in the Lifecycle logs:

- Telnet
- SSH
- Web interface
- RACADM
- SM-CLP
- IPMI Over LAN
- Serial
- Virtual Console
- Virtual Media

You can filter logs based on the category and severity level, view, export, and add a work note to a log event.

Related Links

Filtering Lifecycle Logs
Exporting Lifecycle Controller Logs Using Web Interface
Adding Comments to Lifecycle Logs

Viewing Lifecycle Log Using Web Interface

To view the Lifecycle Logs, click **Overview** → **Server** → **Logs** → **Lifecycle Log**.The **Lifecycle Log** page is displayed. For more information about the options, see the *iDRAC Online Help*.

Filtering Lifecycle Logs

You can filter logs based on category, severity, keyword, or date range.

To filter the lifecycle logs:

1. In the **Lifecycle Log** page, under the **Log Filter** section, do any or all of the following:
   - Select the **Log Type** from the drop-down list.
   - Select the severity level from the **Severity** drop-down list.
   - Enter a keyword.
   - Specify the date range.
2. Click **Apply**.
   The filtered log entries are displayed in **Log Results**.

Adding Comments to Lifecycle Logs

To add comments to the lifecycle logs:

1. In the **Lifecycle Log** page, click the + icon for the required log entry.
   The Message ID details are displayed.
2. Enter the comments for the log entry in the **Comment** box.
   The comments are displayed in the **Comment** box.

Viewing Lifecycle Log Using RACADM

To view Lifecycle logs, use the `lclog` command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Exporting Lifecycle Controller Logs

You can export the entire Lifecycle Controller log (active and archived entries) in a single zipped XML file to a network share or to the local system. The zipped XML file extension is **.xml.gz**. The file entries are ordered sequentially based on their sequence numbers, ordered from the lowest sequence number to the highest.

Exporting Lifecycle Controller Logs Using Web Interface

To export the Lifecycle Controller logs using the Web interface:

1. In the **Lifecycle Log** page, click **Export**.
2. Select any of the following options:
   - **Network** — Export the Lifecycle Controller logs to a shared location on the network.
   - **Local** — Export the Lifecycle Controller logs to a location on the local system.

   NOTE: While specifying the network share settings, it is recommended to avoid special characters for user name and password or percent encode the special characters.

   For information about the fields, see the *iDRAC Online Help*.
3. Click **Export** to export the log to the specified location.

Exporting Lifecycle Controller Logs Using RACADM

To export the Lifecycle Controller logs using RACADM, use the `lclog export` command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals** or **dell.com/esmmanuals**.

Adding Work Notes

Each user who logs in to iDRAC can add work notes and this is stored in the lifecycle log as an event. You must have iDRAC logs privilege to add work notes. A maximum of 255 characters are supported for each new work note.

NOTE: You cannot delete a work note.

To add a work note:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Properties** → **Summary**.
   The **System Summary** page is displayed.
2. Under **Work Notes**, enter the text in the blank text box.

   NOTE: It is recommended not to use too many special characters.
3. Click **Add**.
   The work note is added to the log. For more information, see the *iDRAC Online Help*.

Configuring Remote System Logging

You can send lifecycle logs to a remote system. Before doing this, make sure that:

- There is network connectivity between iDRAC and the remote system.
- The remote system and iDRAC is on the same network.

Configuring Remote System Logging Using Web Interface

To configure the remote syslog server settings:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Logs** → **Settings**.

The **Remote Syslog Settings** page is displayed

2. Enable remote syslog, specify the server address, and the port number. For information about the options, see the *iDRAC Online Help*.
3. Click **Apply**.

   The settings are saved. All logs written to the lifecycle log are also simultaneously written to configured remote server(s).

Configuring Remote System Logging Using RACADM

To configure the remote syslog server settings, use one of the following:

- Objects in the **cfgRemoteHosts** group with the **config** command.
- Objects in the **iDRAC.SysLog** group with the **set** command.

For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

11

Monitoring and Managing Power

You can use iDRAC to monitor and manage the power requirements of the managed system. This helps to protect the system from power outages by appropriately distributing and regulating the power consumption on the system.

The key features are:

- **Power Monitoring** — View the power status, history of power measurements, the current averages, peaks, and so on for the managed system.
- **Power Capping** — View and set the power cap for the managed system, including displaying the minimum and maximum potential power consumption. This is a licensed feature.
- **Power Control** — Enables you to remotely perform power control operations (such as, power on, power off, system reset, power cycle, and graceful shutdown) on the managed system.
- **Power Supply Options** — Configure the power supply options such as redundancy policy, hot spare, and power factor correction.

Related Links

Monitoring Power
Executing Power Control Operations
Power Capping
Configuring Power Supply Options
Enabling or Disabling Power Button
Setting Warning Threshold for Power Consumption

Monitoring Power

iDRAC monitors the power consumption in the system continuously and displays the following power values:

- Power consumption warning and critical thresholds.
- Cumulative power, peak power, and peak amperage values.
- Power consumption over the last hour, last day or last week.
- Average, minimum, and maximum power consumption.
- Historical peak values and peak timestamps.
- Peak headroom and instantaneous headroom values (for rack and tower servers).

Monitoring Power Using Web Interface

To view the power monitoring information, in iDRAC Web interface, go to **Overview → Server → Power/Thermal → Power Monitoring**. The **Power Monitoring page** is displayed. For more information, see the *iDRAC Online Help*.

Monitoring Power Using RACADM

To view the power monitoring information, use the **System.Power** group objects with the **get** command or the **cfgServerPower** object with the **getconfig** command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Setting Warning Threshold for Power Consumption

You can set the warning threshold value for the power consumption sensor in the rack and tower systems. The warning/critical power threshold for rack and tower systems may change on system power cycle based on PSU capacity and redundancy policy. However, the warning threshold must not exceed the critical threshold even if Power Supply Unit capacity of the redundancy policy is changed.

The warning power threshold for blade systems is set to CMC power allocation.

If reset to default action is performed, the power thresholds will be set to default.

You must have Configure user privilege to set the warning threshold value for power consumption sensor.

Setting Warning Threshold for Power Consumption Using Web Interface

1. In the iDRAC Web interface, go to **Overview → Server → Power/Thermal → Power Monitoring**.
   The **Power Monitoring** page is displayed.
2. In the **Present Power Reading and Thresholds** section, in the **Warning Threshold** column, enter the value in **Watts** or **BTU/hr**.
   The values must be lower than the **Failure Threshold** values. The values are rounded off to the nearest value that is divisible by 14. If you enter **Watts**, the system automatically calculates and displays the **BTU/hr** value. Similarly, if you enter BTU/hr, the value for **Watts** is displayed.
3. Click **Apply**. The values are configured.

Executing Power Control Operations

iDRAC enables you to remotely perform a power-on, power off, reset, graceful shutdown, Non-Masking Interrupt (NMI), or power cycle using the Web interface or RACADM.

You can also perform these operations using Lifecycle Controller Remote Services or WS-Management. For more information, see the *Lifecycle Controller Remote Services Quick Start Guide* available at **dell.com/support/manuals** and the *Dell Power State Management* profile document available at **delltechcenter.com**.

Executing Power Control Operations Using Web Interface

To perform power control operations:

1. In iDRAC Web interface, go to **Overview → Server → Power/Thermal → Power Configuration → Power Control**. The **Power Control** page is displayed.
2. Select the required power operation:
   - Power On System

- Power Off System
- NMI (Non-Masking Interrupt)
- Graceful Shutdown
- Reset System (warm boot)
- Power Cycle System (cold boot)

3. Click **Apply**. For more information, see the *iDRAC Online Help*.

Executing Power Control Operations Using RACADM

To perform power actions, use the **serveraction** command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Power Capping

You can view the power threshold limits that covers the range of AC and DC power consumption that a system under heavy workload presents to the datacenter. This is a licensed feature.

Power Capping in Blade Servers

Before a blade server powers up, iDRAC provides CMC with its power requirements. It is higher than the actual power that the blade can consume and is calculated based on limited hardware inventory information. It may request a smaller power range after the server is powered up based on the actual power consumed by the server. If the power consumption increases over time and if the server is consuming power near its maximum allocation, iDRAC may request an increase of the maximum potential power consumption thus increasing the power envelope. iDRAC only increases its maximum potential power consumption request to CMC. It does not request for a lesser minimum potential power if the consumption decreases. iDRAC continues to request for more power if the power consumption exceeds the power allocated by CMC.

After, the system is powered on and initialized, iDRAC calculates a new power requirement based on the actual blade configuration. The blade stays powered on even if the CMC fails to allocate new power request.

CMC reclaims any unused power from lower priority servers and subsequently allocates the reclaimed power to a higher priority infrastructure module or a server.

If there is not enough power allocated, the blade server does not power on. If the blade has been allocated enough power, the iDRAC turns on the system power.

Viewing and Configuring Power Cap Policy

When power cap policy is enabled, it enforces user-defined power limits for the system. If not, it uses the hardware power protection policy that is implemented by default. This power protection policy is independent of the user defined policy. The system performance is dynamically adjusted to maintain power consumption close to the specified threshold.

Actual power consumption may be less for light workloads and momentarily may exceed the threshold until performance adjustments are completed. For example, for a given system configuration, the Maximum Potential Power Consumption is 700W and the Minimum Potential Power Consumption is 500W. You can specify and enable a Power Budget Threshold to reduce consumption from its current

650W to 525W. From that point onwards, the system's performance is dynamically adjusted to maintain power consumption so as to not exceed the user-specified threshold of 525W.

If the power cap value is set to be lower than the minimum recommended threshold, iDRAC may not be able maintain the requested power cap.

You can specify the value in Watts, BTU/hr, or as a percentage (%) of the recommended maximum power limit.

When setting the power cap threshold in BTU/hr, the conversion to Watts is rounded to the nearest integer. When reading the power cap threshold back, the Watts to BTU/hr conversion is again rounded in this manner. As a result, the value written could be nominally different than the value read; for example, a threshold set to 600 BTU/hr will be read back as 601 BTU/hr.

Configuring Power Cap Policy Using Web Interface

To view and configure the power policies:

1. In iDRAC Web interface, go to **Overview → Server → Power/Thermal → Power Configuration → Power Configuration**. The **Power Configuration** page is displayed.

   The **Power Configuration** page is displayed. The current power policy limit is displayed under the **Currently Active Power Cap Policy** section.
2. Select **Enable** under **iDRAC Power Cap Policy**.
3. Under **User-Defined Limits** section, enter the maximum power limit in Watts and BTU/hr or the maximum % of recommended system limit.
4. Click **Apply** to apply the values.

Configuring Power Cap Policy Using RACADM

To view and configure the current power cap values:

- Use the following objects with the **config** subcommand:
  - cfgServerPowerCapWatts
  - cfgServerPowerCapBTUhr
  - cfgServerPowerCapPercent
  - cfgServerPowerCapEnable
- Using the following objects with the **set** subcommand:
  - System.Power.Cap.Enable
  - System.Power.Cap.Watts
  - System.Power.Cap.Btuhr
  - System.Power.Cap.Percent

For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Configuring Power Cap Policy Using iDRAC Settings Utility

To view and configure power policies:

1. In iDRAC Settings utility, go to **Power Configuration**.

NOTE: The **Power Configuration** link is available only if the server power supply unit supports power monitoring.

The **iDRAC Settings Power Configuration** page is displayed.

2. Select **Enabled** to enable the **Power Cap Policy** Else, select **Disabled**.
3. Use the recommended settings, or under **User Defined Power Cap Policy**, enter the required limits. For more information about the options, see the *iDRAC Settings Utility Online Help*.
4. Click **Back**, click **Finish**, and then click **Yes**.
   The power cap values are configured.

Configuring Power Supply Options

You can configure the power supply options such as redundancy policy, hot spare, and power factor correction.

Hot spare is a power supply feature that configures redundant Power Supply Units (PSUs) to turn off depending on the server load. This allows the remaining PSUs to operate at a higher load and efficiency. This requires PSUs that support this feature, so that it quickly powers ON when needed.

In a two PSU system, either PSU1 or PSU2 can be configured as the primary PSU. In a four PSU system, you must set the pair of PSUs (1+1 or 2+2) as the primary PSU.

After Hot Spare is enabled, PSUs can become active or go to sleep based on load. If Hot Spare is enabled, asymmetric electrical current sharing between the two PSUs is enabled. One PSU is *awake* and provides the majority of the current; the other PSU is in sleep mode and provides a small amount of the current. This is often called 1 + 0 with two PSUs and hot spare enabled. If all PSU-1s are on Circuit-A and all PSU-2s are on Circuit-B, then with hot spare enabled (default hot spare factory configuration), Circuit-B has much less load and triggers the warnings. If hot spare is disabled, the electrical current sharing is 50-50 between the two PSUs, the Circuit-A and Circuit-B normally has the same load.

Power factor is the ratio of real power consumed to the apparent power. When power factor correction is enabled, the server consumes a small amount of power when the host is OFF. By default, power factor correction is enabled when the server is shipped from the factory.

Configuring Power Supply Options Using Web Interface

To configure the power supply options:

1. In iDRAC Web interface, go to **Overview → Server → Power/Thermal → Power Configuration → Power Configuration**. The **Power Configuration** page is displayed.
2. Under **Power Supply Options**, select the required options. For more information, see *iDRAC Online Help*.
3. Click **Apply**. The power supply options are configured.

Configuring Power Supply Options Using RACADM

To configure the power supply options, use the following objects with the **set** subcommand:

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU

- System.Power.PFC.Enable

For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Configuring Power Supply Options Using iDRAC Settings Utility

To configure the power supply options:

1. In iDRAC Settings utility, go to **Power Configuration**.

   NOTE: The **Power Configuration** link is available only if the server power supply unit supports power monitoring.

   The **iDRAC Settings Power Configuration** page is displayed.
2. Under **Power Supply Options**:
   - Enable or disable power supply redundancy.
   - Enable or disable hot spare.
   - Set the primary power supply unit.
   - Enable or disable power factor correction. For more information about the options, see the *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
   The power supply options are configured.

Enabling or Disabling Power Button

To enable or disable the power button on the managed system:

1. In iDRAC Settings utility, go to **Front Panel Security**.
   The **iDRAC Settings Front Panel Security** page is displayed.
2. Select **Enabled** to enable the power button. Else, select **Disabled**.
3. Click **Back**, click **Finish**, and then click **Yes**. The settings are saved.

12

Inventory, Monitoring, and Configuring Network Devices

You can inventory, monitor, and configure the following network devices:

- Network Interface Cards (NICs)
- Converged Network Adapters (CNAs)
- LAN On Motherboards (LOMs)
- Network Daughter Cards (NDCs)
- Mezzanine cards (only for blade servers)

Related Links

Inventory and Monitoring FC HBA Devices
Dynamic Configuration of Virtual Addresses, Initiator, and Storage Target Settings

Inventory and Monitoring Network Devices

You can remotely monitor the health and view the inventory of the network devices in the managed system.

For each device, you can view the following information of the ports and supported partitions:

- Link Status
- Properties
- Settings and Capabilities
- Receive and Transmit Statistics

Related Links

Inventory, Monitoring, and Configuring Network Devices
Dynamic Configuration of Virtual Addresses, Initiator, and Storage Target Settings

Monitoring Network Devices Using Web Interface

To view the network device information using Web interface, go to **Overview → Hardware → Network Devices**. The **Network Devices** page is displayed. For more information about the displayed properties, see *iDRAC Online Help*.

NOTE: If the **OS Driver State** displays the state as Operational, it indicates the operating system driver state or the UEFI driver state.

Monitoring Network Devices Using RACADM

To view the network device information, use the **hwinventory** and **nicstatistics** commands. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Additional properties may be displayed when using RACADM or WS-MAN in addition to the properties displayed in the iDRAC Web interface.

Inventory and Monitoring FC HBA Devices

You can remotely monitor the health and view the inventory of the Fibre Channel Host Bus Adapters (FC HBA) devices in the managed system. The Emulex and QLogic (except FC8) FC HBAs are supported. For each FC HBA device, you can view the following information for the ports:

- Link Status and Information
- Port Properties
- Receive and Transmit Statistics

Related Links

Inventory, Monitoring, and Configuring Network Devices

Monitoring FC HBA Devices Using Web Interface

To view the FC HBA device information using Web interface, go to **Overview → Hardware → Fibre Channel**. The FC page is displayed. For more information about the displayed properties, see *iDRAC Online Help*.

The page name also displays the slot number where the FC HBA device is available and the type of FC HBA device.

Monitoring FC HBA Devices Using RACADM

To view the FC HBA device information using racadm, use the **hwinventory** subcommand. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Dynamic Configuration of Virtual Addresses, Initiator, and Storage Target Settings

You can dynamically view and configure the virtual address, initiator and storage target settings, and apply a persistence policy. It allows the application to apply the settings based on power state changes (that is, operating system restart, warm reset, cold reset, or AC cycle) and also based on persistence policy setting for that power state. This provides more flexibility in deployments that need rapid re-configuration of system workloads to another system.

The virtual addresses are:

- Virtual MAC Address
- Virtual iSCSI MAC Address
- Virtual FIP MAC Address
- Virtual WWN
- Virtual WWPN

NOTE: When you clear the persistence policy, all the virtual addresses are reset to the default permanent address set at the factory.

Using the IO Identity feature, you can:

- View and configure the virtual addresses for network devices (for example, NIC, CNA, FC HBA)
- Configure the initiator (for iSCSI and FCoE) and storage target settings (for iSCSI, FCoE, and FC)
- Specify persistence or clearance of the configured values over a system AC power loss, cold, and warm system resets.

The values configured for virtual addresses, initiator and storage targets may change based on the way the main power is handled during system reset and whether the NIC, CNA, or FC HBA device has auxiliary power. The persistence of IO identity settings can be achieved based on the policy setting made using iDRAC.

Only if the I/O identity feature is enabled, the persistence policies take effect. Each time the system resets or powers on, the values are persisted or cleared based on the policy settings.

Related Links

Inventory, Monitoring, and Configuring Network Devices
Supported Cards for I/O Identity Optimization
Supported BIOS Version for I/O Identity Optimization
Supported NIC Firmware Versions for I/O Identity Optimization
Enabling or Disabling I/O Identity Optimization
Configuring Persistence Policy Settings

Supported Cards for I/O Identity Optimization

The following table provides the cards that support the I/O Identity Optimization feature.

Manufacturer	Type
Broadcom	• 5720 PCIe 1 GB • 5719 PCIe 1 GB • 57810 PCIe 10 GB • 57810 bNDC 10 GB • 57800 rNDC 10 GB + 1 GB • 57840 rNDC 10 GB • 57840 bNDC 10 GB • 5720 rNDC 1 GB • 5719 Mezz 1 GB • 57810 Mezz 10 GB • 5720 bNDC 1 GB
Intel	• i350 Mezz 1Gb • x520+i350 rNDC 10Gb+1Gb • I350 bNDC 1Gb • x540 PCIe 10Gb • x520 PCIe 10Gb • i350 PCIe 1Gb • x540+i350 rNDC 10Gb+1Gb • i350 rNDC 1Gb • x520 bNDC 10Gb
Qlogic	• QME2662 Mezz FC16 • QLE2660 PCIe FC16

Manufacturer	Type
Emulex	• QLE2662 PCIe FC16 • LPM16002 Mezz FC16 • LPe16000 PCIe FC16 • LPe16002 PCIe FC16 • LPM16002 Mezz FC16 • OCm14104-UX-D rNDC 10Gb • OCm14102-U2-D bNDC 10Gb • OCm14102-U3-D Mezz 10Gb • Ce14102-UX-D PCIe 10Gb

NOTE: I/O Identity Optimization is not supported on the following cards:

- Intel x520 Mezz 10 GB
- Mellanox cards

Supported BIOS Version for I/O Identity Optimization

In 13th generation Dell PowerEdge servers, the required BIOS version is available by default.

The following table provides the minimum BIOS version supported on the 12th generation PowerEdge servers.

Dell PowerEdge 12th Generation Server	Minimum Supported BIOS Version
R720, R720xd, R620, T620, and M620	2.1.0
R820	2.0.15
R520, R320, R420, T420, T320, M520, and M420	2.0.19
M820	1.7.0

Supported NIC Firmware Versions for I/O Identity Optimization

In 13th generation Dell PowerEdge servers, the required NIC firmware is available by default.

The following table provides the NIC firmware versions for the I/O identity optimization feature.

Manufacturer	Supported NIC Firmware Version
Broadcom cards	7.8.x
Intel cards	15.0.x
QLogic 82xx (CNA)	1.13.x / 6.0.0.x

System Behavior for FlexAddress and IO Identity

	FlexAddress Feature State in CMC	IO Identity Feature State in iDRAC	Remote Agent VA Available for this Reboot Cycle?	VA Programming Source	Reboot Cycle VA Persistence Behavior
Server with FA-equivalent Persistence	Enabled	Disabled		FlexAddress from CMC	Per FlexAddress spec
	N/A, Enabled, or Disabled	Enabled	Yes - New or Persisted	Remote Agent Virtual Address	Per FlexAddress spec
			No	Virtual Address Cleared	
	Disabled	Disabled			
Server with VAM Persistence Policy Feature	Enabled	Disabled		FlexAddress from CMC	Per FlexAddress spec
	Enabled	Enabled	Yes - New or Persisted	Remote Agent Virtual Address	Per Remote Agent Policy Setting
			No	FlexAddress from CMC	Per FlexAddress spec
	Disabled	Enabled	Yes - New or Persisted	Remote Agent Virtual Address	Per Remote Agent Policy Setting
			No	Virtual Address Cleared	
	Disabled	Disabled			

Enabling or Disabling I/O Identity Optimization

Normally, after the system boots, the devices are configured and then after a reboot the devices are initialized. You can enable the I/O Identity Optimization feature to achieve boot optimization. If it is enabled, it sets the virtual address, initiator, and storage target attributes after the device is reset and before it is initialized, thus eliminating a second BIOS restart. The device configuration and boot operation occur in a single system start and is optimized for boot time performance.

Before enabling I/O identity optimization, make sure that:

- You have the Login, Configure, and System Control privileges.
- BIOS, iDRAC, and network cards are updated to the latest firmware. For information on the supported versions, see Supported BIOS Version For I/O Identity Optimization and Supported NIC Firmware Version for I/O Identity Optimization.

After enabling I/O Identity Optimization feature, export the XML configuration file from iDRAC, modify the required I/O Identity attributes in the XML configuration file, and import the file back to iDRAC.

For the list of I/O Identity Optimization attributes that you can modify in the XML configuration file, see the *NIC Profile* document available at **delltechcenter.com/idrac**.

NOTE: Do not modify non I/O Identity Optimization attributes.

Enabling or Disabling I/O Identity Optimization Using Web Interface

To enable or disable I/O Identity Optimization:

1. In the iDRAC Web interface, go to **Overview → Hardware → Network Devices**.
   The **Network Devices** page is displayed.
2. Click the **I/O Identity Optimization** tab, select the **I/O Identity Optimization** option to enable this feature. To disable, clear this option.
3. Click **Apply** to apply the setting.

Enabling or Disabling I/O Identity Optimization Using RACADM

To enable I/O Identity Optimization, use the command:

```
racadm set idrac.ioidopt.IOIDOptEnable Enabled
```

After enabling this feature, you must restart the system for the settings to take effect.

To disable I/O Identity Optimization, use the command:

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

To view the I/O Identity Optimization setting, use the command:

```
racadm get iDRAC.IOIDOpt
```

Configuring Persistence Policy Settings

Using IO identity, you can configure policies specifying the system reset and power cycle behaviors that determine the persistence or clearance of the virtual address, initiator, and storage target settings. Each individual persistence policy attribute applies to all ports and partitions of all applicable devices in the system. The device behavior changes between auxillary powered devices and non-auxillary powered devices.

You can configure the following persistence policies:

- Virtual Address: Auxiliary powered devices
- Virtual Address: Non-Auxiliary powered devices
- Initiator
- Storage target

Before applying the persistence policy, make sure to:

- Inventory the network hardware at least once, that is, enabled Collect System Inventory On Restart.
- Enable I/O Identity Optimization.

Events are logged to the Lifecycle Controller log when:

- I/O Identity Optimization is enabled or disabled.
- Persistence policy is changed.
- Virtual address, initiator and target values are set based on the policy. A single log entry is logged for the configured devices and the values that are set for those devices when the policy is applied.

Event actions are enabled for SNMP, email, or WS-eventing notifications. Logs are also included in the remote syslogs.

Default Values for Persistence Policy

Persistence Policy	AC Power Loss	Cold Boot	Warm Boot
Virtual Address: Auxiliary Powered Devices	Not selected	Selected	Selected
Virtual Address: Non-Auxiliary Powered Devices	Not selected	Not selected	Selected
Initiator	Selected	Selected	Selected
Storage Target	Selected	Selected	Selected

Related Links

Enabling or Disabling I/O Identity Optimization

Configuring Persistence Policy Settings Using iDRAC Web Interface

To configure the persistence policy:

1. In the iDRAC Web interface, go to **Overview → Hardware → Network Devices**.
   The **Network Devices** page is displayed.
2. Click **I/O Identity Optimization** tab.
3. In the **Persistence Policy** section, select one or more of the following for each persistence policy:
   - **A/C Power Loss** - The virtual address or target settings persist when AC power loss conditions occur.
   - **Cold Boot** - The virtual address or target settings persist when cold reset conditions occur.
   - **Warm Boot** - The virtual address or target settings persist when warm reset condition occurs.
4. Click **Apply**.
   The persistence policies are configured.

Configuring Persistence Policy Settings Using RACADM

To set persistence policy, use the following racadm object with the **set** sub command:

- For virtual addresses, use **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwrd** and **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwrd** objects
- For initiator, use **iDRAC.IOIDOPT.InitiatorPersistencePolicy** object
- For storage targets, use **iDRAC.IOIDOpt.StorageTargetPersistencePolicy** object

For more information, see the *iDRAC RACADM Command Line Interface Reference Guide* available at **dell.com/esmmanuals**.

iSCSI Initiator and Storage Target Default Values

The following tables provide the list of default values for iSCSI initiator and storage targets when the persistence policies are cleared.

Table 23. iSCSI Initiator —Default Values

iSCSI Initiator	Default Values in IPv4 mode	Default Values in IPv6 mode
IscsiInitiatorIpAddr	0.0.0.0	::
IscsiInitiatorIpv4Addr	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Addr	::	::
IscsiInitiatorSubnet	0.0.0.0	0.0.0.0
IscsiInitiatorSubnetPrefix	0	0
IscsiInitiatorGateway	0.0.0.0	::
IscsiInitiatorIpv4Gateway	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Gateway	::	::
IscsiInitiatorPrimDns	0.0.0.0	::
IscsiInitiatorIpv4PrimDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
IscsiInitiatorName	Value Cleared	Value Cleared
IscsiInitiatorChapId	Value Cleared	Value Cleared
IscsiInitiatorChapPwd	Value Cleared	Value Cleared
IPVer	Ipv4	

Table 24. iSCSI Storage Target Attributes — Default Values

iSCSI Storage Target Attributes	Default Values in IPv4 mode	Default Values in IPv6 mode
ConnectFirstTgt	Disabled	Disabled
FirstTgtIpAddress	0.0.0.0	::
FirstTgtTcpPort	3260	3260
FirstTgtBootLun	0	0
FirstTgtIscsiName	Value Cleared	Value Cleared

iSCSI Storage Target Attributes	Default Values in IPv4 mode	Default Values in IPv6 mode
FirstTgtChapId	Value Cleared	Value Cleared
FirstTgtChapPwd	Value Cleared	Value Cleared
FirstTgtIpVer	Ipv4	
ConnectSecondTgt	Disabled	Disabled
SecondTgtIpAddress	0.0.0.0	::
SecondTgtTcpPort	3260	3260
SecondTgtBootLun	0	0
SecondTgtIscsiName	Value Cleared	Value Cleared
SecondTgtChapId	Value Cleared	Value Cleared
SecondTgtChapPwd	Value Cleared	Value Cleared
SecondTgtIpVer	Ipv4	

13

Managing Storage Devices

In the iDRAC 2.00.00.00 release, iDRAC expands its agent-free management to include direct configuration of the new PERC9 controllers. It enables you to remotely configure the storage components attached to your system at run-time. These components include RAID and non-RAID controllers and the channels, ports, enclosures, and disks attached to them.

The complete storage subsystem discovery, topology, health monitoring and configuration are accomplished in the Comprehensive Embedded Management (CEM) framework by interfacing with the internal and external PERC controllers through the MCTP protocol over I2C interface. For real-time configuration, CEM supports PERC9 controllers. The firmware version for PERC9 controllers must be 9.1 or later.

Using iDRAC, you can perform most of the functions that are available in OpenManage Storage Management including real-time (no reboot) configuration commands (for example, create virtual disk). You can completely configure RAID before installing the operating system.

You can configure and manage the controller functions without accessing the BIOS. These functions include configuring virtual disks and applying RAID levels and hot spares for data protection. You can initiate many other controller functions such as rebuilds and troubleshooting. You can protect your data by configuring data-redundancy or assigning hot spares.

The storage devices are:

- Controllers — Most operating systems do not read and write data directly from the disks, but instead send read and write instructions to a controller. The controller is the hardware in your system that interacts directly with the disks to write and retrieve data. A controller has connectors (channels or ports) which are attached to one or more physical disks or an enclosure containing physical disks. RAID controllers can span the boundaries of the disks to create an extended amount of storage space — or a virtual disk — using the capacity of more than one disk. Controllers also perform other tasks, such as initiating rebuilds, initializing disks, and more. To complete their tasks, controllers require special software known as firmware and drivers. In order to function properly, the controller must have the minimum required version of the firmware and drivers installed. Different controllers have different characteristics in the way they read and write data and execute tasks. It is helpful to understand these features to most efficiently manage the storage.
- Physical disks or physical devices — Reside within an enclosure or are attached to the controller. On a RAID controller, physical disks or devices are used to create virtual disks.
- Virtual disk — It is storage created by a RAID controller from one or more physical disks. Although a virtual disk may be created from several physical disks, it is viewed by the operating system as a single disk. Depending on the RAID level used, the virtual disk may retain redundant data if there is a disk failure or have particular performance attributes. Virtual disks can only be created on a RAID controller.
- Enclosure — It is attached to the system externally while the backplane and its physical disks are internal.
- Backplane — It is similar to an enclosure. In a Backplane, the controller connector and physical disks are attached to the enclosure, but it does not have the management features (temperature probes,

alarms, and so on) associated with external enclosures. Physical disks can be contained in an enclosure or attached to the backplane of a system.

In addition to managing the physical disks contained in the enclosure, you can monitor the status of the fans, power supply, and temperature probes in an enclosure. You can hot plug enclosures. Hot plugging is defined as adding of a component to a system while the operating system is still running.

The physical devices connected to the controller must have the latest firmware. For the latest supported firmware, contact your service provider.

Storage events from PERC are mapped to SNMP traps and WSMAN events as applicable. Any changes to the storage configurations are logged in the Lifecycle Log.

PERC Capability	CEM configuration Capable Controller (PERC 9.1 or later)	CEM configuration Non-capable Controller (PERC 9.0 and lower)
Real-time	If there is no existing pending or scheduled jobs for the controller, then configuration is applied. If there are pending or scheduled jobs for that controller, then the jobs have to be cleared or you must wait for the jobs to be completed before applying the configuration at run-time. Run-time or real-time means, a reboot is not required.	Configuration is applied. An error message is displayed. Job creation is not successful and you cannot create real-time jobs using Web interface.
Staged	If all the set operations are staged, the configuration is staged and applied after reboot or it is applied at real-time.	Configuration is applied after reboot

Related Links

Understanding RAID Concepts
Inventory and Monitoring Storage Devices
Viewing Storage Device Topology
Managing Controllers
Managing Physical Disks
Managing Enclosures or Backplanes
Managing PCIe SSDs
Managing Virtual Disks
Blinking or Unblinking Component LEDs
Supported Controllers
Supported Enclosures
Summary of Supported Features for Storage Devices

Understanding RAID Concepts

Storage Management uses the Redundant Array of Independent Disks (RAID) technology to provide Storage Management capability. Understanding Storage Management requires an understanding of RAID

concepts, as well as some familiarity with how the RAID controllers and operating system view disk space on your system.

What Is RAID?

RAID is a technology for managing the storage of data on the physical disks that reside or are attached to the system. A key aspect of RAID is the ability to span physical disks so that the combined storage capacity of multiple physical disks can be treated as a single, extended disk space. Another key aspect of RAID is the ability to maintain redundant data which can be used to restore data in the event of a disk failure. RAID uses different techniques, such as striping, mirroring, and parity, to store and reconstruct data. There are different RAID levels that use different methods for storing and reconstructing data. The RAID levels have different characteristics in terms of read/write performance, data protection, and storage capacity. Not all RAID levels maintain redundant data, which means for some RAID levels lost data cannot be restored. The RAID level you choose depends on whether your priority is performance, protection, or storage capacity.

NOTE: The RAID Advisory Board (RAB) defines the specifications used to implement RAID. Although RAB defines the RAID levels, commercial implementation of RAID levels by different vendors may vary from the actual RAID specifications. An implementation of a particular vendor may affect the read and write performance and the degree of data redundancy.

Hardware And Software RAID

RAID can be implemented with either hardware or software. A system using hardware RAID has a RAID controller that implements the RAID levels and processes data reads and writes to the physical disks. When using software RAID provided by the operating system, the operating system implements the RAID levels. For this reason, using software RAID by itself can slow the system performance. You can, however, use software RAID along with hardware RAID volumes to provide better performance and variety in the configuration of RAID volumes. For example, you can mirror a pair of hardware RAID 5 volumes across two RAID controllers to provide RAID controller redundancy.

RAID Concepts

RAID uses particular techniques for writing data to disks. These techniques enable RAID to provide data redundancy or better performance. These techniques include:

- Mirroring — Duplicating data from one physical disk to another physical disk. Mirroring provides data redundancy by maintaining two copies of the same data on different physical disks. If one of the disks in the mirror fails, the system can continue to operate using the unaffected disk. Both sides of the mirror contain the same data always. Either side of the mirror can act as the operational side. A mirrored RAID disk group is comparable in performance to a RAID 5 disk group in read operations but faster in write operations.
- Striping — Disk striping writes data across all physical disks in a virtual disk. Each stripe consists of consecutive virtual disk data addresses that are mapped in fixed-size units to each physical disk in the virtual disk using a sequential pattern. For example, if the virtual disk includes five physical disks, the stripe writes data to physical disks one through five without repeating any of the physical disks. The amount of space consumed by a stripe is the same on each physical disk. The portion of a stripe that resides on a physical disk is a stripe element. Striping by itself does not provide data redundancy. Striping in combination with parity does provide data redundancy.
- Stripe size — The total disk space consumed by a stripe not including a parity disk. For example, consider a stripe that contains 64KB of disk space and has 16KB of data residing on each disk in the stripe. In this case, the stripe size is 64KB and the stripe element size is 16KB.
- Stripe element — A stripe element is the portion of a stripe that resides on a single physical disk.

- Stripe element size — The amount of disk space consumed by a stripe element. For example, consider a stripe that contains 64KB of disk space and has 16KB of data residing on each disk in the stripe. In this case, the stripe element size is 16KB and the stripe size is 64KB.
- Parity — Parity refers to redundant data that is maintained using an algorithm in combination with striping. When one of the striped disks fails, the data can be reconstructed from the parity information using the algorithm.
- Span — A span is a RAID technique used to combine storage space from groups of physical disks into a RAID 10, 50, or 60 virtual disk.

RAID Levels

Each RAID level uses some combination of mirroring, striping, and parity to provide data redundancy or improved read and write performance. For specific information on each RAID level, see Choosing RAID Levels.

Organizing Data Storage For Availability And Performance

RAID provides different methods or RAID levels for organizing the disk storage. Some RAID levels maintain redundant data so that you can restore data after a disk failure. Different RAID levels also entail an increase or decrease in the I/O (read and write) performance of a system.

Maintaining redundant data requires the use of additional physical disks. The possibility of a disk failure increases with an increase in the number of disks. Since the differences in I/O performance and redundancy, one RAID level may be more appropriate than another based on the applications in the operating environment and the nature of the data being stored.

When choosing a RAID level, the following performance and cost considerations apply:

- Availability or fault-tolerance — Availability or fault-tolerance refers to the ability of a system to maintain operations and provide access to data even when one of its components has failed. In RAID volumes, availability or fault-tolerance is achieved by maintaining redundant data. Redundant data includes mirrors (duplicate data) and parity information (reconstructing data using an algorithm).
- Performance — Read and write performance can be increased or decreased depending on the RAID level you choose. Some RAID levels may be more appropriate for particular applications.
- Cost efficiency — Maintaining the redundant data or parity information associated with RAID volumes requires additional disk space. In situations where the data is temporary, easily reproduced, or non-essential, the increased cost of data redundancy may not be justified.
- Mean Time Between Failure (MTBF) — Using additional disks to maintain data redundancy also increases the chance of disk failure at any given moment. Although this option cannot be avoided in situations where redundant data is a requirement, it does have implications on the workload of the system support staff within your organization.
- Volume — Volume refers to a single disk non-RAID virtual disk. You can create volumes using external utilities like the O-ROM <Ctrl> <r>. Storage Management does not support the creation of volumes. However, you can view volumes and use drives from these volumes for creation of new virtual disks or Online Capacity Expansion (OCE) of existing virtual disks, provided free space is available. Storage Management allows Rename and Delete operations on such volumes.

Choosing RAID Levels

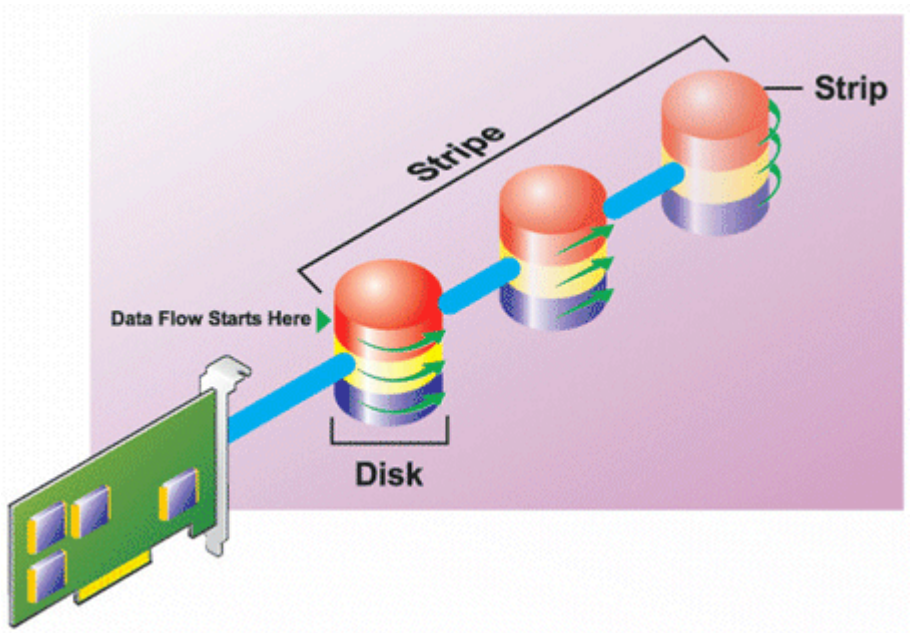
You can use RAID to control data storage on multiple disks. Each RAID level or concatenation has different performance and data protection characteristics.

The following topics provide specific information on how each RAID level store data as well as their performance and protection characteristics:

- RAID Level 0 (Striping)
- RAID Level 1 (Mirroring)
- RAID Level 5 (Striping With Distributed Parity)
- RAID Level 6 (Striping With Additional Distributed Parity)
- RAID Level 50 (Striping Over RAID 5 Sets)
- RAID Level 60 (Striping Over RAID 6 Sets)
- RAID Level 10 (Striping Over Mirror Sets)

RAID Level 0 (Striping)

RAID 0 uses data striping, which is writing data in equal-sized segments across the physical disks. RAID 0 does not provide data redundancy.

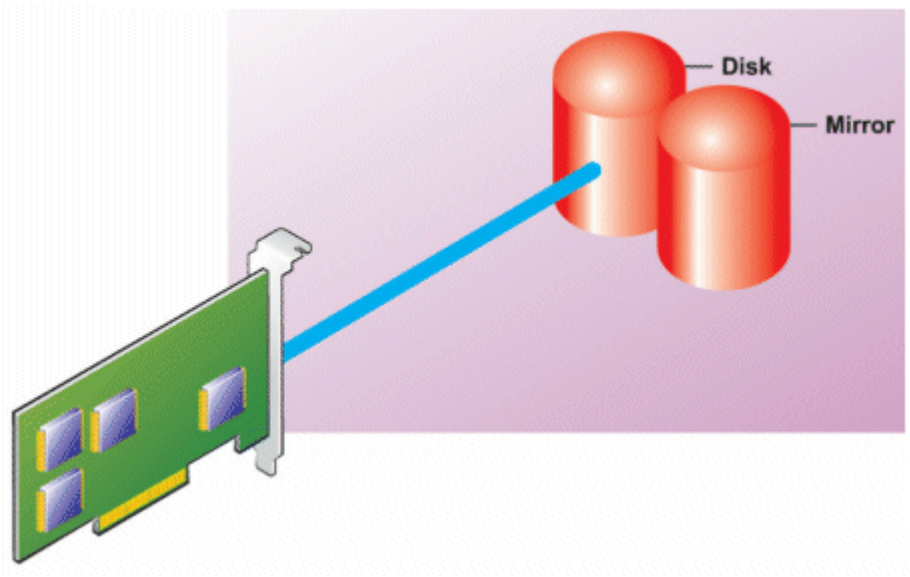


RAID 0 characteristics:

- Groups *n* disks as one large virtual disk with a capacity of (smallest disk size) **n* disks.
- Data is stored to the disks alternately.
- No redundant data is stored. When a disk fails, the large virtual disk fails with no means of rebuilding the data.
- Better read and write performance.

RAID Level 1 (Mirroring)

RAID 1 is the simplest form of maintaining redundant data. In RAID 1, data is mirrored or duplicated on one or more physical disks. If a physical disk fails, data can be rebuilt using the data from the other side of the mirror.

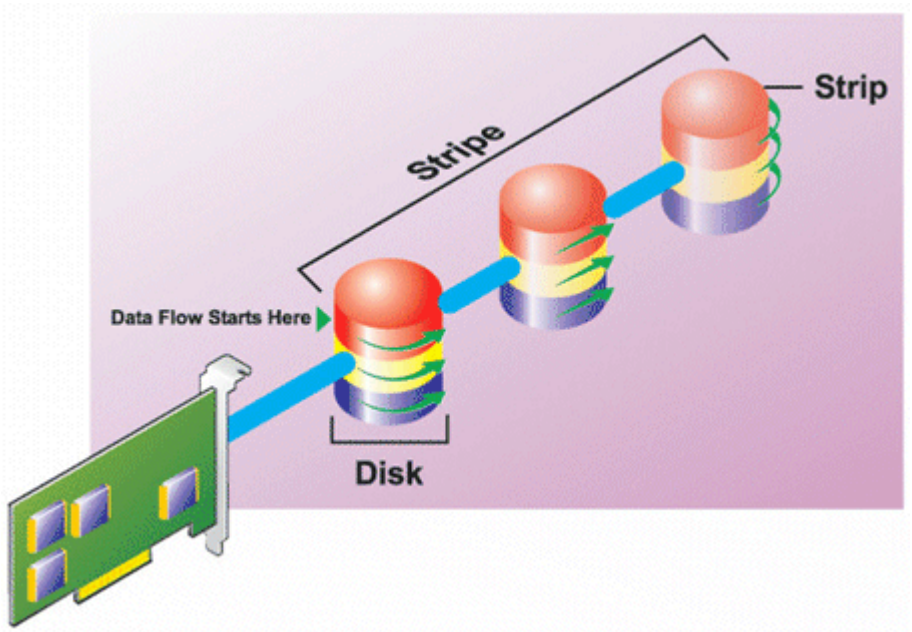


RAID 1 characteristics:

- Groups *n* + *n* disks as one virtual disk with the capacity of *n* disks. The controllers currently supported by Storage Management allow the selection of two disks when creating a RAID 1. Because these disks are mirrored, the total storage capacity is equal to one disk.
- Data is replicated on both the disks.
- When a disk fails, the virtual disk still works. The data is read from the mirror of the failed disk.
- Better read performance, but slightly slower write performance.
- Redundancy for protection of data.
- RAID 1 is more expensive in terms of disk space since twice the number of disks are used than required to store the data without redundancy.

RAID Level 5 (Striping With Distributed Parity)

RAID 5 provides data redundancy by using data striping in combination with parity information. Rather than dedicating a physical disk to parity, the parity information is striped across all physical disks in the disk group.

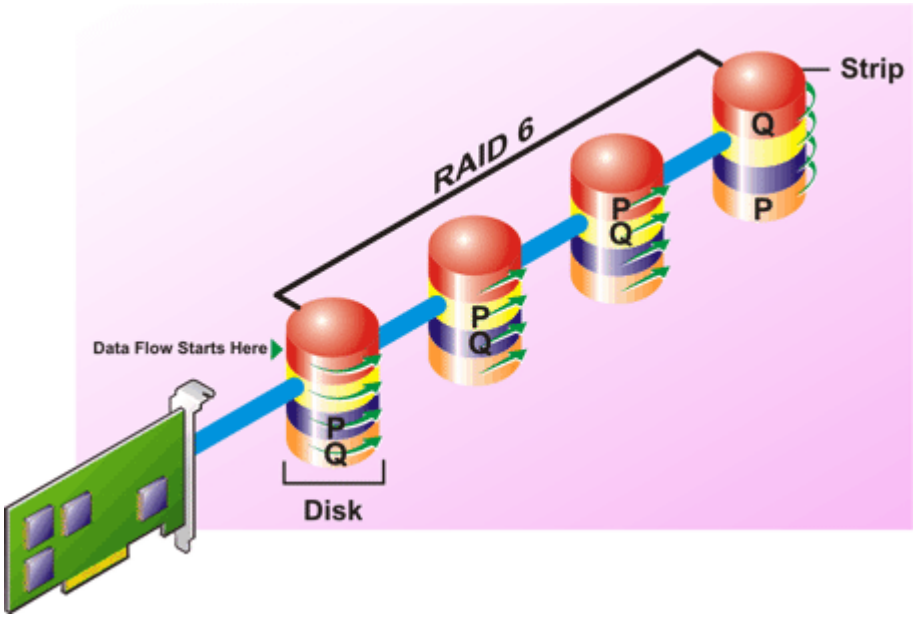


RAID 5 characteristics:

- Groups *n* disks as one large virtual disk with a capacity of (*n*-1) disks.
- Redundant information (parity) is alternately stored on all disks.
- When a disk fails, the virtual disk still works, but it is operating in a degraded state. The data is reconstructed from the surviving disks.
- Better read performance, but slower write performance.
- Redundancy for protection of data.

RAID Level 6 (Striping With Additional Distributed Parity)

RAID 6 provides data redundancy by using data striping in combination with parity information. Similar to RAID 5, the parity is distributed within each stripe. RAID 6, however, uses an additional physical disk to maintain parity, such that each stripe in the disk group maintains two disk blocks with parity information. The additional parity provides data protection in the event of two disk failures. In the following image, the two sets of parity information are identified as **P** and **Q**.



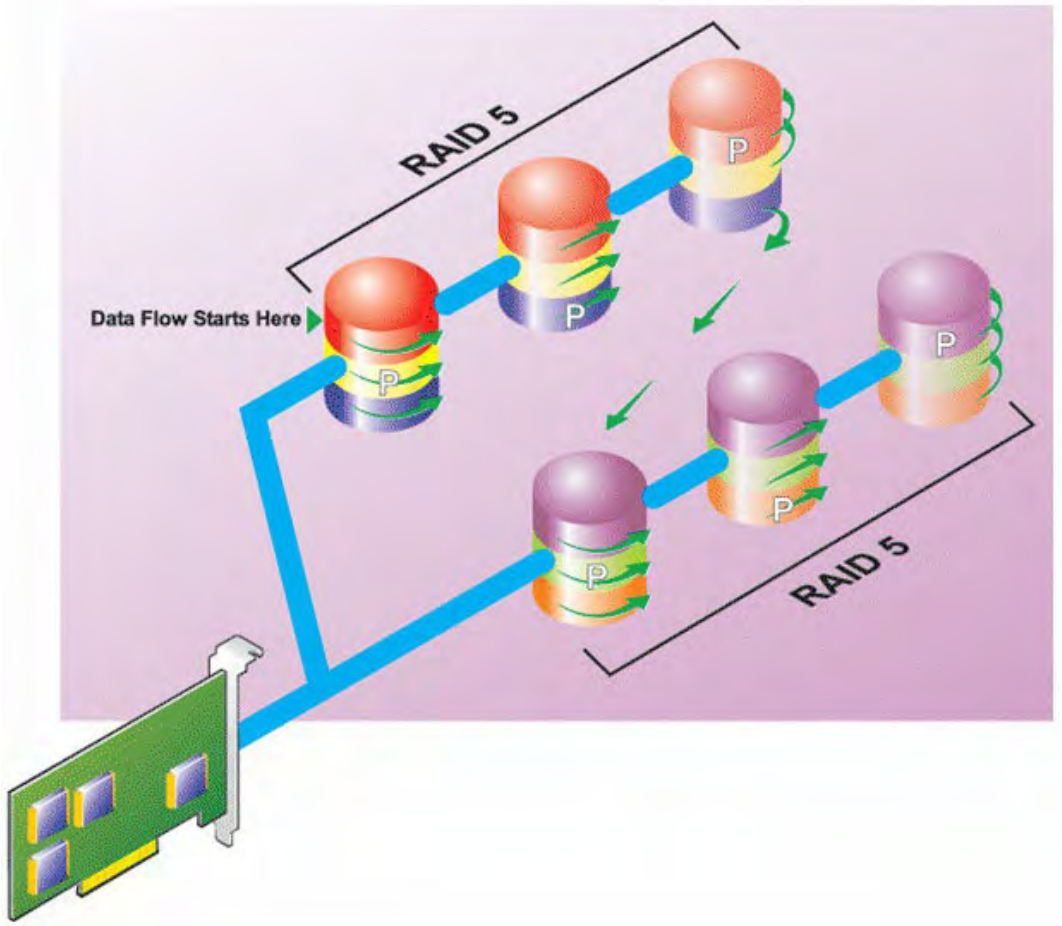
RAID 6 characteristics:

- Groups *n* disks as one large virtual disk with a capacity of (*n*-2) disks.
- Redundant information (parity) is alternately stored on all disks.
- The virtual disk remains functional with up to two disk failures. The data is reconstructed from the surviving disks.
- Better read performance, but slower write performance.
- Increased redundancy for protection of data.
- Two disks per span are required for parity. RAID 6 is more expensive in terms of disk space.

RAID Level 50 (Striping Over RAID 5 Sets)

RAID 50 is striping over more than one span of physical disks. For example, a RAID 5 disk group that is implemented with three physical disks and then continues on with a disk group of three more physical disks would be a RAID 50.

It is possible to implement RAID 50 even when the hardware does not directly support it. In this case, you can implement more than one RAID 5 virtual disks and then convert the RAID 5 disks to dynamic disks. You can then create a dynamic volume that is spanned across all RAID 5 virtual disks.

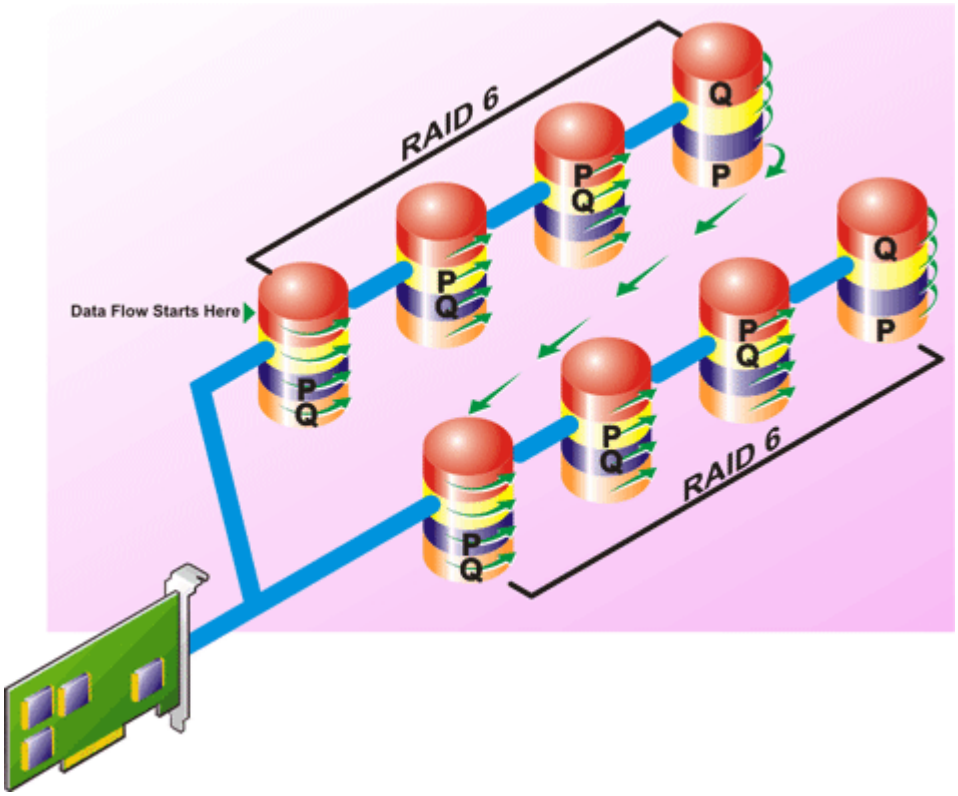


RAID 50 characteristics:

- Groups *n***s* disks as one large virtual disk with a capacity of *s**(*n*-1) disks, where *s* is the number of spans and *n* is the number of disks within each span.
- Redundant information (parity) is alternately stored on all disks of each RAID 5 span.
- Better read performance, but slower write performance.
- Requires as much parity information as standard RAID 5.
- Data is striped across all spans. RAID 50 is more expensive in terms of disk space.

RAID Level 60 (Striping Over RAID 6 Sets)

RAID 60 is striping over more than one span of physical disks that are configured as a RAID 6. For example, a RAID 6 disk group that is implemented with four physical disks and then continues on with a disk group of four more physical disks would be a RAID 60.

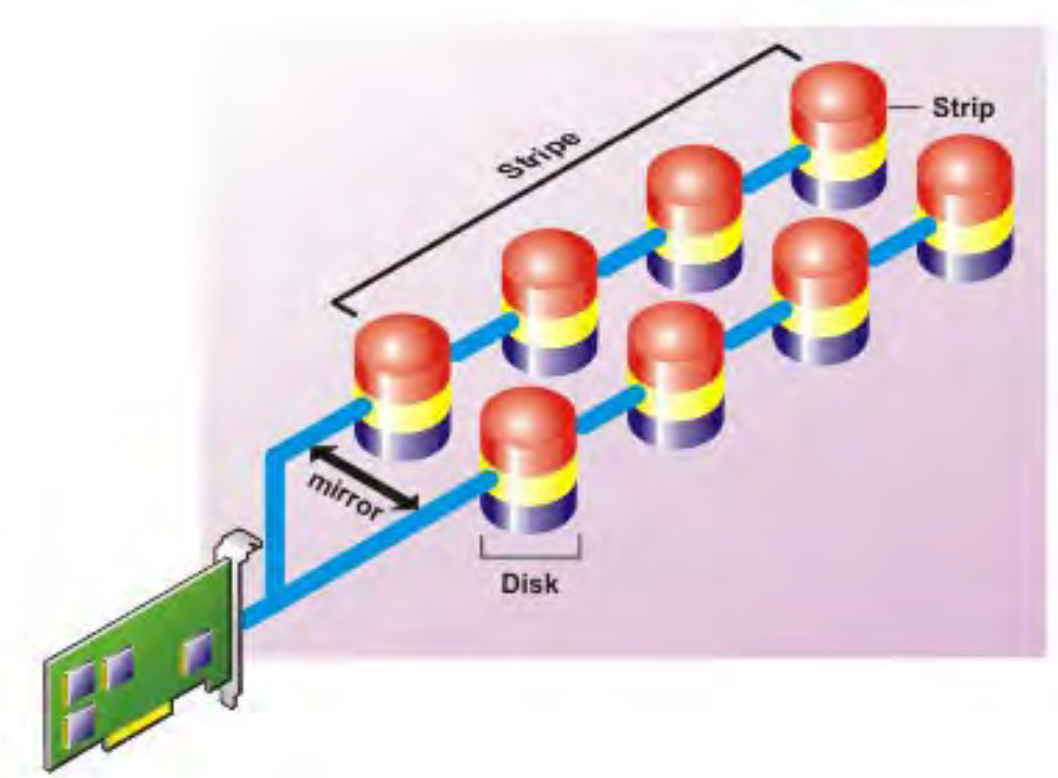


RAID 60 characteristics:

- Groups *n***s* disks as one large virtual disk with a capacity of *s**(*n*-2) disks, where *s* is the number of spans and *n* is the number of disks within each span.
- Redundant information (parity) is alternately stored on all disks of each RAID 6 span.
- Better read performance, but slower write performance.
- Increased redundancy provides greater data protection than a RAID 50.
- Requires proportionally as much parity information as RAID 6.
- Two disks per span are required for parity. RAID 60 is more expensive in terms of disk space.

RAID Level 10 (Striped-Mirrors)

The RAB considers RAID level 10 to be an implementation of RAID level 1. RAID 10 combines mirrored physical disks (RAID 1) with data striping (RAID 0). With RAID 10, data is striped across multiple physical disks. The striped disk group is then mirrored onto another set of physical disks. RAID 10 can be considered a *mirror of stripes*.



RAID 10 characteristics:

- Groups *n* disks as one large virtual disk with a capacity of (*n*/2) disks, where *n* is an even integer.
- Mirror images of the data are striped across sets of physical disks. This level provides redundancy through mirroring.
- When a disk fails, the virtual disk still works. The data is read from the surviving mirrored disk.
- Improved read performance and write performance.
- Redundancy for protection of data.

Comparing RAID Level Performance

The following table compares the performance characteristics associated with the more common RAID levels. This table provides general guidelines for choosing a RAID level. Evaluate your specific environment requirements before choosing a RAID level.

Table 25. RAID Level Performance Comparison

RAID Level	Data Availability	Read Performance	Write Performance	Rebuild Performance	Minimum Disks Required	Suggested Uses
RAID 0	None	Very Good	Very Good	N/A	N	Noncritical data.
RAID 1	Excellent	Very Good	Good	Good	2N (N = 1)	Small databases, database

RAID Level	Data Availability	Read Performance	Write Performance	Rebuild Performance	Minimum Disks Required	Suggested Uses
						logs, and critical information.
RAID 5	Good	Sequential reads: good. Transactional reads: Very good	Fair, unless using writeback cache	Fair	N + 1 (N = at least two disks)	Databases and other read intensive transactional uses.
RAID 10	Excellent	Very Good	Fair	Good	2N x X	Data intensive environments (large records).
RAID 50	Good	Very Good	Fair	Fair	N + 2 (N = at least 4)	Medium sized transactional or data intensive uses.
RAID 6	Excellent	Sequential reads: good. Transactional reads: Very good	Fair, unless using writeback cache	Poor	N + 2 (N = at least two disks)	Critical information. Databases and other read intensive transactional uses.
RAID 60	Excellent	Very Good	Fair	Poor	X x (N + 2) (N = at least 2)	Critical information. Medium sized transactional or data intensive uses.
N = Number of physical disks X = Number of RAID sets						

Supported Controllers

Supported RAID Controllers

The iDRAC interfaces support the following PERC9 controllers:

- PERC H830
- PERC H730P
- PERC H730
- PERC H330

The iDRAC interfaces support the following PERC8 controllers:

- PERC H810
- PERC H710P
- PERC H710
- PERC H310

Supported Non-RAID Controllers

The iDRAC interfaces supports 12Gbps SAS HBA External Adapter.

NOTE: iDRAC does not support software RAID. For information about software RAID, see *Lifecycle Controller GUI User's Guide* available at **dell.com/support/manuals**.

Supported Enclosures

iDRAC supports MD1400 and MD1420 enclosures.

Summary of Supported Features for Storage Devices

The following table provides the features supported by the storage devices through iDRAC.

Feature Name	PERC 9 Controllers				PERC 8 Controllers				PCIe SSD
	H830	H730P	H730	H330	H810	H710P	H710	H310	
Assign or unassign physical disk as a global hot spare	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Create virtual disks	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Edit virtual disks cache policies	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable

Feature Name	PERC 9 Controllers				PERC 8 Controllers				PCIe SSD
	H830	H730P	H730	H330	H810	H710P	H710	H310	
Check virtual disk consistency	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Cancel check consistency	Real-time	Real-time	Real-time	Real-time	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Initialize virtual disks	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Cancel initialization	Real-time	Real-time	Real-time	Real-time	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Encrypt virtual disks	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Assign or unassign dedicated hot spare	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Delete virtual disks	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Set Patrol Read Mode	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Patrol Read Unconfigured Areas	Real-time (only in Web interface)	Real-time (only in Web interface)	Real-time (only in Web interface)	Real-time (only in Web interface)	Staged (only in Web interface)	Staged (only in Web interface)	Staged (only in Web interface)	Staged (only in Web interface)	Not applicable
Check Consistency Mode	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Copyback Mode	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Load Balance Mode	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable

Feature Name	PERC 9 Controllers				PERC 8 Controllers				PCIe SSD
	H830	H730P	H730	H330	H810	H710P	H710	H310	
Check Consistency Rate	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Rebuild Rate	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
BGI Rate	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Reconstruct Rate	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Import foreign configuration	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Auto-import foreign configuration	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Clear foreign configuration	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Reset controller configuration	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Create or change security keys	Real-time	Real-time	Real-time	Real-time	Staged	Staged	Staged	Staged	Not applicable
Inventory and remotely monitor the health of PCIe SSD devices	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Real-time
Prepare the PCIe SSD to be removed	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Real-time
Securely erase the data	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Staged

Feature Name	PERC 9 Controllers				PERC 8 Controllers				PCIe SSD
	H830	H730P	H730	H330	H810	H710P	H710	H310	
Configure Backplane mode	Real-time	Real-time	Real-time	Real-time	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Blink or unblink component LEDs	Real-time	Real-time	Real-time	Real-time	Real-time	Real-time	Real-time	Real-time	Real-time

Inventory and Monitoring Storage Devices

You can remotely monitor the health and view the inventory of the following Comprehensive Embedded Management (CEM) enabled storage devices in the managed system using iDRAC Web interface:

- RAID controllers, non-RAID controllers, and PCIe extenders
- Enclosures that includes Enclosure Management Modules (EMMs), power supply, fan probe, and temperature probe
- Physical disks
- Virtual disks
- Batteries

However, RACADM and WS-MAN display information for most of the storage devices in the system.

iDRAC inventories and monitors the PERC 8 series of RAID controllers that include H310, H710, H710P, and H810. The controllers that do not support Comprehensive Embedded Management are Internal Tape Adapters (ITAs), SAS 6 Gbps HBA, and SAS 12 Gbps HBA.

The recent storage events and topology of storage devices are also displayed.

Alerts and SNMP traps are generated for storage events. The events are logged in the Lifecycle Log.

Monitoring Storage Device Using Web Interface

To view the storage device information using Web interface:

- Go to **Overview → Storage → Summary** to view the summary of the storage components and the recently logged events. This page is automatically refreshed every 30 seconds.
- Go to **Overview → Storage → Topology** to view the hierarchical physical containment view of the key storage components.
- Go to **Overview → Storage → Physical Disks → Properties** to view physical disk information. The **Physical Disks Properties** page is displayed.
- Go to **Overview → Storage → Virtual Disks → Properties** to view virtual disks information. The **Virtual Disks Properties** page is displayed.
- Go to **Overview → Storage → Controllers → Properties** to view the RAID controller information. The **Controllers Properties** page is displayed.
- Go to **Overview → Storage → Enclosures → Properties** to view the enclosure information. The **Enclosures Properties** page is displayed.

You can also use filters to view specific device information.

For more information on the displayed properties and to use the filter options, see *iDRAC Online Help*.

Monitoring Storage Device Using RACADM

To view the storage device information, use the **raid** or **storage** subcommand. For more information, see the *iDRAC RACADM Command Line Reference Guide*available at **dell.com/support/manuals**.

Monitoring Backplane Using iDRAC Settings Utility

In the iDRAC Settings utility, go to **System Summary**. The **iDRAC Settings.System Summary** page is displayed. The **Backplane Inventory** section displays the backplane information. For information about the fields, see the *iDRAC Settings Utility Online Help*.

Viewing Storage Device Topology

You can view the hierarchical physical containment view of the key storage components, that is, a list of controllers, enclosures connected to the controller and a link to the physical disk contained in each enclosure. The physical disks attached directly to the controller are also displayed.

To view the storage device topology, go to **Overview** → **Storage** → **Topology**. The **Topology** page displays the hierarchical representation of the storage components in the system.

Click the links to view the respective component details.

Managing Physical Disks

You can perform the following for physical disks:

- View physical disk properties
- Assign or unassign physical disk as a global hotspare
- Convert to RAID capable disk (supported only in RACADM and is a staged operation)
- Convert to non-RAID disk (supported only in RACADM and is a staged operation)
- Blink or unblink the LED

Related Links

Inventory and Monitoring Storage Devices
Assigning or Unassigning Physical Disk as Global Hot spare

Assigning or Unassigning Physical Disk as Global Hot spare

A global hot spare is an unused backup disk that is part of the disk group. Hot spares remain in standby mode. When a physical disk that is used in a virtual disk fails, the assigned hot spare is activated to replace the failed physical disk without interrupting the system or requiring your intervention. When a hot spare is activated, it rebuilds the data for all redundant virtual disks that were using the failed physical disk.

You can change the hot spare assignment by unassigning a disk and choosing another disk as needed. You can also assign more than one physical disk as a global hot spare.

Global hot spares must be assigned and unassigned manually. They are not assigned to specific virtual disks. If you want to assign a hot spare to a virtual disk (it replaces any physical disk that fails in the virtual disk), then see Assigning or Unassigning Dedicated Hot Spares.

When deleting virtual disks, all assigned global hot spares may be automatically unassigned when the last virtual disk associated with the controller is deleted.

If you reset the configuration, the virtual disks are deleted and all the hot spares are unassigned.

You must be familiar with the size requirements and other considerations associated with hot spares.

Before assigning a physical disk as a global hot spare:

- Make sure that Lifecycle Controller is enabled.
- If there are no disk drives available in ready state, insert additional disk drives and make sure the drives are in ready state.
- If no virtual disks are present, create at least one virtual disk.
- If physical disks are in non-RAID mode convert them to RAID mode using racadm command or <CTRL+R>.

If you have assigned a physical disk as a global hot spare in Add to Pending Operation mode, the pending operation is created but a job is not created. Then, if you try to unassign the same disk as global hot spare, the assign global hot spare pending operation is cleared.

If you have unassigned a physical disk as a global hot spare in Add to Pending Operation mode, the pending operation is created but a job is not created. Then, if you try to assign the same disk as a global hot spare, the unassign global hot spare pending operation is cleared.

Assigning or Unassigning Global Hot spare Using Web Interface

To assign or unassign a global hotspare for a physical disk drive:

1. In the iDRAC Web interface, go to **Overview** → **Storage** → **Physical Disks** → .
   The **Setup** page is displayed.
2. From the **Controller** drop-down menu, select the controller to view the associated physical disks.
3. To assign as a global hotspare, from the drop-down menus in the **Action-Assign to All** column, select**Global Hotspare** for one or more physical disks.
4. To unassign a hotspare, from the drop-down menus in the **Action-Assign to All** column, select **Unassign Hotspare** for one or more physical disks.
5. From the **Apply Operation Mode** drop-down menu, select when you want to apply the settings.
6. Click **Apply**.
   Based on the selected operation mode, the settings are applied.

Related Links

Choosing Operation Mode Using Web Interface

Assigning or Unassigning Global Hot spare Using RACADM

Use the storage **subcommand** and specify the type as global hot spare. For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Related Links

Choosing Operation Mode Using RACADM

Convert To RAID Capable Disk

This task enables a disk for all RAID operations.

If the physical disk drive(s) are in non-RAID mode, to convert them to RAID mode:

1. Press <Ctrl+R> while restarting the server, and then select the required controller.
2. Press <F2> and select the **Convert to RAID capable** option, and then complete the operation.

NOTE:

- This task is not supported on PERC hardware controllers running in **HBA** mode.
- This task is only supported as a staged operation.

Convert To Non-RAID Disk

This task converts a disk to a Non-RAID disk. After converting a disk to non- RAID, the disk is exposed to the operating system unlike unconfigured good disks and it enables usage of disk in direct pass-through mode.

This task is supported on H310 and H330 controllers.

NOTE: This task is not supported on PERC hardware controllers running in **HBA** mode.

Managing Virtual Disks

You can perform the following operations for the virtual disks:

- Create
- Delete
- Edit policies
- Initialize
- Check consistency
- Cancel check consistency
- Encrypt virtual disks
- Assign or unassign dedicated hot spares
- Blink and unblink virtual disks

Related Links

Creating Virtual Disks
Editing Virtual Disk Cache Policies
Deleting Virtual Disks
Checking Virtual Disk Consistency
Initializing Virtual Disks
Encrypting Virtual Disks
Assigning or Unassigning Dedicated Hot Spares
Managing Virtual Disks Using Web Interface
Managing Virtual Disks Using RACADM

Creating Virtual Disks

To implement RAID functions, you must create a virtual disk. A virtual disk refers to storage created by a RAID controller from one or more physical disks. Although a virtual disk may be created from several physical disks, it is seen by the operating system as a single disk.

Before creating a virtual disk, you should be familiar with the information in Considerations Before Creating Virtual Disks.

You can create a Virtual Disk using the Physical Disks attached to the PERC controller. To create a Virtual Disk, you must have the Server Control user privilege. You can create a maximum of 64 virtual drives and a maximum of 16 virtual drives in the same drive group.

You cannot create a virtual disk if:

- Physical disk drives are not available for virtual disk creation. Install additional physical disk drives.
- Maximum number of virtual disks that can be created on the controller has been reached. You must delete at least one virtual disk and then create a new virtual disk.
- Maximum number of virtual disks supported by a drive group has been created. You must delete one virtual disk from the selected group and then create a new virtual disk.
- A job is currently running or scheduled on the selected controller. You must wait for this job to complete or you can delete the job before attempting a new operation. You can view and manage the status of the scheduled job in the Job Queue page.
- Physical disk is in non-RAID mode. You must convert to RAID mode using the racadm command or <CTRL+R>.

NOTE: If you create a virtual disk in Add to Pending Operation mode and a job is not created, and then if you delete the Virtual disk, then the create pending operation for the virtual disk is cleared.

Considerations Before Creating Virtual Disks

Before creating virtual disks, consider the following:

- Virtual disk names not stored on controller—The names of the virtual disks that you create are not stored on the controller. This means that if you reboot using a different operating system, the new operating system may rename the virtual disk using its own naming conventions.
- Disk grouping is a logical grouping of disks attached to a RAID controller on which one or more virtual disks are created, such that all virtual disks in the disk group use all of the physical disks in the disk group. The current implementation supports the blocking of mixed disk groups during the creation of logical devices.
- Physical disks are bound to disk groups. Therefore, there is no RAID level mixing on one disk group.
- There are limitations on the number of physical disks that can be included in the virtual disk. These limitations depend on the controller. When creating a virtual disk, controllers support a certain number of stripes and spans (methods for combining the storage on physical disks). Because the number of total stripes and spans is limited, the number of physical disks that can be used is also limited. The limitations on stripes and spans affect the RAID levels as follows:
  - Maximum number of spans affects RAID 10, RAID 50, and RAID 60.
  - Maximum number of stripes affects RAID 0, RAID 5, RAID 50, RAID 6, and RAID 60.
  - Number of physical disks in a mirror is always 2. This affects RAID 1 and RAID 10.
- Cannot create virtual disks on PCIe SSDs.

Creating Virtual Disks Using Web interface

To create virtual disk:

1. In the iDRAC Web interface, go to **Overview** → **Storage** → **Virtual Disks** → **Create**.
   The **Create Virtual Disk** page is displayed.
2. In the **Settings** section, do the following:
   a. Enter the name for the virtual disk.

b. From the **Controller** drop-down menu, select the controller for which you want to create the virtual disk.
c. From the **Layout** drop-down menu, select the RAID level for the Virtual Disk.

   Only those RAID levels supported by the controller appear in the drop-down menu and it is based on the RAID levels are available based on the total number of physical disks available.
d. Select the **Media Type**, **Stripe Size**, **Read Policy**, **Write Policy**, **Disk Cache Policy**, **T10 PI Capability**.

   Only those values supported by the controller appear in the drop-down menus for these properties.
e. In the **Capacity** field, enter the size of the virtual disk.

   The maximum size is displayed and then updated as disks are selected.
f. The **Span Count** field is displayed based on the selected physical disks (step 3). You cannot set this value. It is automatically calculated after selecting disks for multi-raid level. If you have selected RAID 10 and if the controller supports uneven RAID 10, then the span count value is not displayed. The controller automatically sets the appropriate value.

3. In the **Select Physical Disks** section, select the number of physical disks.

   For more information about the fields, see the *iDRAC Online Help*
4. From the **Apply Operation Mode** drop-down menu, select when you want to apply the settings.
5. Click **Create Virtual Disk**.

   Based on the selected **Apply Operation Mode**, the settings are applied.

Creating Virtual Disks Using RACADM

Use `racadm storage createvd` command. For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Editing Virtual Disk Cache Policies

You can change the read, write, or disk cache policy of a virtual disk.

NOTE: Some of the controllers do not support all read or write policies. Therefore, when a policy is applied, an error message is displayed.

The read policies indicate whether the controller must read sequential sectors of the virtual disk searching for data:

- **Adaptive Read Ahead** — The controller initiates read ahead only if the two most recent read requests accessed sequential sectors of the disk. If subsequent read requests access random sectors of the disk, the controller reverts to no read ahead policy. The controller continues to evaluate whether read requests are accessing sequential sectors of the disk, and initiates read ahead if necessary.
- **Read Ahead** — The controller reads sequential sectors of the virtual disk when seeking data. Read ahead policy may improve system performance if the data is written to the sequential sectors of the virtual disk.
- **No Read Ahead** — Selecting no read ahead policy indicates that the controller should not use read ahead policy.

The write policies specify if the controller sends a write-request completion signal as soon as the data is in the cache or after it has been written to the disk.

- **Write Through** — The controller sends a write-request completion signal only after the data is written to the disk. Write-through caching provides better data security than write-back caching, since the system assumes the data is available only after it has been safely written to the disk.
- **Write Back** — The controller sends a write-request completion signal as soon as the data is in the controller cache but has not yet been written to disk. Write back caching may provide improved

performance since subsequent read requests can retrieve data quickly from the cache then from the disk. However, data loss may occur in the event of a system failure which prevents that data from being written on a disk. Other applications may also experience problems when actions assume that the data is available on the disk.

- **Force Write Back** — The write cache is enabled regardless of whether the controller has a battery. If the controller does not have a battery and force write back caching is used, data loss may occur in the event of a power failure.

The Disk Cache policy apply to readings on a specific virtual disk. These settings do not affect the read-ahead policy.

NOTE:

- Controller non-volatile cache and battery backup of controller cache affects the read-policy or the write policy that a controller can support. All PERCs do not have battery and cache.
- Read ahead and write back requires cache. Therefore, if the controller does not have cache, it does not allow you to set the policy value.

  Similarly, if the PERC has cache but not battery and the policy is set that requires accessing cache, then data loss may occur if base of power off. So few PERCs may not allow that policy.

  Therefore, depending upon the PERC, the policy value is set.

Deleting Virtual Disks

Deleting a virtual disk destroys all information including file systems and volumes residing on the virtual disk and removes the virtual disk from the controller's configuration. When deleting virtual disks, all assigned global hot spares may be automatically unassigned when the last virtual disk associated with the controller is deleted. When deleting the last virtual disk of a disk group, all assigned dedicated hot spares automatically become global hot spares.

You must have the Login and Server Control privilege to perform delete virtual disks.

When this operation is allowed, you can delete a boot virtual drive. It is done from sideband and the independent of the operating system. Hence, a warning message appears before you delete the virtual drive.

If you delete a virtual disk and immediately create a new virtual disk with all the same characteristics as the one that was deleted, the controller recognizes the data as if the first virtual disk were never deleted. In this situation, if you do not want the old data after recreating a new virtual disk, re-initialize the virtual disk.

Checking Virtual Disk Consistency

This operation verifies the accuracy of the redundant (parity) information. This task only applies to redundant virtual disks. When necessary, the check consistency task rebuilds the redundant data. If the virtual drive has a degraded status, running a check consistency may be able to return the virtual drive to ready status. You can also cancel the check consistency operation.

The cancel check consistency is a real-time operation.

You must have Login and Server Control privilege to check consistency of virtual disks.

Initializing Virtual Disks

Initializing virtual disks erases the all the data on the disk but does not change the virtual disk configuration. You must initialize a virtual disk that is configured before it is used.

NOTE: Do not initialize virtual disks when attempting to recreate an existing configuration.

You can perform a fast initialization, a full Initialization, or cancel the initialization operation.

NOTE: The cancel initialization is a real-time operation. You can cancel the initialization using only the iDRAC Web interface and not RACADM.

Fast Initialization

The fast initialize operation initializes all physical disks included in the virtual disk. It updates the metadata on the physical disks so that all disk space is available for future write operations. The initialize task can be completed quickly because the existing information on the physical disks is not erased, although future write operations overwrite any information that remains on the physical disks.

Fast initialization only deletes the boot sector and stripe information. Perform a fast initialize only if you are constrained for time or the hard drives are new or unused. Fast Initialization takes less time to complete (usually 30-60 seconds).

CAUTION: Performing a fast initialize causes existing data to be inaccessible.

The fast initialize task does not write zeroes to the disk blocks on the physical disks. It is because the Fast Initialize task does not perform a write operation, it causes less degradation to the disk.

A fast initialization on a virtual disk overwrites the first and last 8 MB of the virtual disk, clearing any boot records or partition information. The operation takes only 2-3 seconds to complete and is recommended when you are recreating virtual disks.

A background initialization starts five minutes after the Fast Initialization is completed.

Full or Slow Initialization

The full initialization (also called slow initialize) operation initializes all physical disks included in the virtual disk. It updates the metadata on the physical disks and erases all existing data and file systems. You can perform a full initialization after creating the virtual disk. In comparison with the fast initialize operation, you may want to use the full initialize if you have trouble with a physical disk or suspect that it has bad disk blocks. The full initialize operation remaps bad blocks and writes zeroes to all disk blocks.

If full initialization of a virtual disk is performed, background initialization is not required. During full initialization, the host is not able to access the virtual disk. If the system reboots during a full initialization, the operation terminates and a background initialization process starts on the virtual disk.

It is always recommended to do a full initialization on drives that previously contained data. Full initialization can take up to 1-2 minutes per GB. The speed of initialization depends on the controller model, speed of hard drives, and the firmware version.

The full initialize task initializes one physical disk at a time.

NOTE: Full initialize is supported only in real-time. Only few controllers support full initialization.

Encrypting Virtual Disks

When encryption is disabled on a controller (that is, the security key is deleted), manually enable encryption for virtual disks created using SED drives. If the virtual disk is created after encryption is enabled on a controller, the virtual disk is automatically encrypted. It is automatically configured as an encrypted virtual disk unless the enabled encryption option is disabled during the virtual disk creation.

NOTE: This task can only be staged and real-time is not supported.

You must have Login and Server Control privilege to manage the encryption keys.

Assigning or Unassigning Dedicated Hot Spares

A dedicated hot spare is an unused backup disk that is assigned to a virtual disk. When a physical disk in the virtual disk fails, the hot spare is activated to replace the failed physical disk without interrupting the system or requiring your intervention.

You must have Login and Server Control privilege to run this operation.

Only T10 PI (DIF) capable physical disks can be assigned as a hot spare to T10 PI (DIF) enabled virtual disks. Any non T10 PI (DIF) drives that are assigned as dedicated hot spare will not be a hot spare if T10 PI (DIF) is enabled on a virtual disk later on.

You can assign only 4K drives as hot spare to 4K virtual disks.

If you have assigned a virtual disk as a dedicated hot spare in Add to Pending Operation mode, the pending operation is created but a job is not created. Then, if you try to unassign the dedicated hot spare, the assign dedicated hot spare pending operation is cleared.

If you have unassigned a virtual disk as a dedicated hot spare in Add to Pending Operation mode, the pending operation is created but a job is not created. Then, if you try to assign the dedicated hot spare, the unassign dedicated hot spare pending operation is cleared.

Managing Virtual Disks Using Web Interface

1. In the iDRAC Web interface, go to **Overview → Storage → Virtual Disks → Manage**.
   The **Manage Virtual Disks** page is displayed.
2. From the **Controller** drop-down menu, select the controller for which you want to manage the virtual disks.
3. For one or more Virtual Disks, from each **Action** drop-down menu, select an action.
   You can specify more than one action for a virtual drive. When you select an action, an additional **Action** drop-down menu is displayed. Select another action from this drop-down menu. The action that is already selected does not appear in the additional **Action** drop-down menus. Also, the **Remove** link is displayed next to the selected action. Click this link to remove the selected action.
   - **Delete**
   - **Edit Policy: Read Cache** — Change the read cache policy to one of the following options:
     - **Adaptive Read Ahead**

  - **No Read Ahead**
  - **Read Ahead**
- **Edit Policy: Write Cache** — Change the write cache policy to one of the following options:
  - **Write Through**
  - **Write Back**
  - **Force Write Back**
- **Edit Policy: Disk Cache** — Change the disk cache policy to one of the following options:
  - **Default**
  - **Enabled**
  - **Disabled**
- **Initialize: Fast** — Updates the metadata on the physical disks so that all the disk space is available for future write operations. The initialize can be completed quickly because existing information on the physical disks is not erased, although future write operations overwrites any information that remains on the physical disks.
- **Initialize: Full** — All existing data and file systems are erased.
- **Check Consistency**
- **Encrypt Virtual Disk** — Encrypts the virtual disk drive. If the controller is encryption capable, you can create, change or delete the security keys.
- **Manage Dedicated Hotspares** — Assign or unassign a physical disk as a dedicated hotspare. Only the valid dedicated hotspares are displayed. If there are no valid dedicated hotspares, then this section does not appear in the drop-down menu.

For more information about these options, see the *iDRAC Online Help*.

4. From the **Apply Operation Mode** drop-down menu, select when you want to apply the settings.
5. Click **Apply**.

   Based on the selected operation mode, the settings are applied.

Managing Virtual Disks Using RACADM

Use the following RACADM commands to manage virtual disks:

- To delete virtual disk: `racadm storage deletevd:<VD FQDD>`
- To initialize virtual disk: `racadm storage init:<VD FQDD> -speed {fast|full}`
- To check consistency of virtual disks: `racadm storage ccheck:<vdisk fqdd>`
- To encrypt virtual disks: `racadm storage encryptvd:<VD FQDD>`
- To assign or unassign dedicated hot spares: `racadm storage hotspare:<Physical Disk FQDD> -assign yes -type dhs -vdkey: <FQDD of VD>`
- To cancel the check consistency: `racadm storage cancelcheck: <vdisks fqdd>`

Managing Controllers

You can perform the following for Controllers:

- Configure controller properties
- Import or auto import foreign configuration
- Clear foreign configuration
- Reset controller configuration

- Create, change, or delete security keys

Related Links

Configuring Controller Properties
Importing or Auto Importing Foreign Configuration
Clearing Foreign Configuration
Resetting Controller Configuration
Supported Controllers
Summary of Supported Features for Storage Devices
Convert To RAID Capable Disk
Convert To Non-RAID Disk

Configuring Controller Properties

You can configure the following properties for the controller:

- Patrol read mode (auto or manual)
- Start or stop patrol read if patrol read mode is manual
- Patrol read unconfigured areas
- Check consistency mode
- Copyback mode
- Load balance mode
- Check consistency rate
- Rebuild rate
- BGI rate
- Reconstruct rate
- Enhanced auto import foreign configuration
- Create or change security keys

NOTE: You can configure the Patrol Read Unconfigured Areas property using the iDRAC Web interface and not RACADM.

You must have Login and Server Control privilege to configure the controller properties.

Patrol Read Mode Considerations

Patrol read identifies disk errors to avoid disk failures, data loss, or corruption.

The Patrol Read does not run on a physical disk in the following circumstances:

- The physical disk is not included in a virtual disk or assigned as a hot spare.
- The physical disk is included in a virtual disk that is currently undergoing one of the following:
  - A rebuild
  - A re-configuration or reconstruction
  - A background initialization
  - A check consistency

In addition, the Patrol Read operation suspends during heavy I/O activity and resumes when the I/O is complete.

NOTE: For more information on how often the Patrol Read operation runs when in auto mode, see the respective controller documentation.

Load Balance

The Load Balance property provides the ability to automatically use both controller ports or connectors connected to the same enclosure to route I/O requests. This property is available only on SAS controllers.

BGI Rate

On PERC controllers, background initialization of a redundant virtual disk begins automatically within 0 to 5 minutes after the virtual disk is created. The background initialization of a redundant virtual disk prepares the virtual disk to maintain redundant data and improves write performance. For example, after the background initialization of a RAID 5 virtual disk completes, the parity information has been initialized. After the background initialization of a RAID 1 virtual disk completes, the physical disks are mirrored.

The background initialization process helps the controller identify and correct problems that may occur with the redundant data at a later time. In this regard, the background initialization process is similar to a check consistency. The background initialization should be allowed to run to completion. If cancelled, the background initialization automatically restarts within 0 to 5 minutes. Some processes such as read and write operations are possible while the background initialization is running. Other processes, such as creating a virtual disk, cannot be run concurrently with a background initialization. These processes cause the background initialization to cancel.

The background initialization rate, configurable between 0% and 100%, represents the percentage of the system resources dedicated to running the background initialization task. At 0%, the background initialization has the lowest priority for the controller, takes the most time to complete, and is the setting with the least impact to system performance. A background initialization rate of 0% does not mean that the background initialization is stopped or paused. At 100%, the background initialization is the highest priority for the controller. The background initialization time is minimized and is the setting with the most impact to system performance.

Check Consistency

The Check Consistency task verifies the accuracy of the redundant (parity) information. This task only applies to redundant virtual disks. When necessary, the Check Consistency task rebuilds the redundant data. If the virtual disk is in a Failed Redundancy state, running a check consistency may be able to return the virtual disk to a Ready state.

The check consistency rate, configurable between 0% and 100%, represents the percentage of the system resources dedicated to running the check consistency task. At 0%, the check consistency has the lowest priority for the controller, takes the most time to complete, and is the setting with the least impact to system performance. A check consistency rate of 0% does not mean that the check consistency is stopped or paused. At 100%, the check consistency is the highest priority for the controller. The check consistency time is minimized and is the setting with the most impact to system performance.

Create or Change Security Keys

When configuring the controller properties, you can create or change the security keys. The controller uses the encryption key to lock or unlock access to SED. You can create only one encryption key for

each encryption-capable controller. The security key is managed using the Local Key Management (LKM) feature. LKM is used to generate the key ID and the password or key required to secure the virtual disk. If you are using LKM, you must create the encryption key by providing the Security Key Identifier and the Passphrase.

This task is not supported on PERC hardware controllers running in HBA mode.

If you create the security key in Add to Pending Operation mode and a job is not created, and then if you delete the security key, the create security key pending operation is cleared.

Configuring Controller Properties Using Web Interface

1. In the iDRAC Web interface, go to **Overview → Storage → Controllers → Setup**.
   The **Setup Controllers** page is displayed.
2. In the **Configure Controller Properties** section, from the **Controller** drop-down menu, select the controller that you want to configure.
3. Specify the required information for the various properties.
   The **Current Value** column displays the existing values for each property. You can modify this value by selecting the option from the **Action** drop-down menu for each property.
   For information about the fields, see the *iDRAC Online Help*.
4. From the **Apply Operation Mode** drop-down menu, select when you want to apply the settings.
5. Click **Apply**.
   Based on the selected operation mode, the settings are applied.

Configuring Controller Properties Using RACADM

- To set Patrol Read Mode:
  ```
  racadm set storage.controller.<index>.PatrolReadMode  {Automatic | Manual | Disabled}
  ```
- If Patrol read mode is set to manual, use the following commands to start and stop Patrol read Mode:
  ```
  racadm storage patrolread:<Controller FQDD> -state {start|stop}
  ```
- To specify the Check Consistency Mode, use **Storage.Controller.CheckConsistencyMode** object.
- To enable or disable the Copyback Mode, use **Storage.Controller.CopybackMode** object.
- To enable or disable the Load Balance Mode, use **Storage.Controller.PossibleloadBalancedMode** object.
- To specify the percentage of the system's resources dedicated to perform a check consistency on a redundant virtual disk, use **Storage.Controller.CheckConsistencyRate** object.
- To specify the percentage of the controller's resources dedicated to rebuild a failed disk, use **Storage.Controller.RebuildRate** object
- To specify the percentage of the controller's resources dedicated to perform the background initialization (BGI) of a virtual disk after it is created, use**Storage.Controller.BackgroundInitializationRate** object
- To specify the percentage of the controller's resources dedicated to reconstruct a disk group after adding a physical disk or changing the RAID level of a virtual disk residing on the disk group, use **Storage.Controller.ReconstructRate** object
- To enable or disable the enhanced auto import of foreign configuration for the controller, use **Storage.Controller.EnhancedAutoImportForeignConfig** object

- To create, modify, or delete security key to encrypt virtual drives:

```
racadm storage createsecuritykey:<Controller FQDD> -key <Key id> -passwd
<passphrase>

racadm storage modifysecuritykey:<Controller FQDD> -key <key id> -oldpasswd
<old passphrase> -newpasswd <new passphrase>

racadm storage deletesecuritykey:<Controller FQDD>
```

Importing or Auto Importing Foreign Configuration

A foreign configuration is data residing on physical disks that have been moved from one controller to another. Virtual disks residing on physical disks that have been moved are considered to be a foreign configuration.

You can import foreign configurations so that virtual disks are not lost after moving Physical Disks. A foreign configuration can be imported only if it contains a virtual disk that is in either Ready or Degraded state or a hotspare that is dedicated to a virtual disk which can be imported or is already present.

All of the virtual disk data must be present, but if the virtual disk is using a redundant RAID level, the additional redundant data is not required.

For example, if the foreign configuration contains only one side of a mirror in a RAID 1 virtual disk, then the virtual disk is in a Degraded state and can be imported. If the foreign configuration contains only one physical disk that was originally configured as a RAID 5 using three physical disks, then the RAID 5 virtual disk is in a Failed state and cannot be imported.

In addition to virtual disks, a foreign configuration may consist of a physical disk that was assigned as a hot spare on one controller and then moved to another controller. The Import Foreign Configuration task imports the new physical disk as a hot spare. If the physical disk was set as a dedicated hot spare on the previous controller, but the virtual disk to which the hot spare was assigned is no longer present in the foreign configuration, then the physical disk is imported as a global hot spare.

If any foreign configurations locked using Local Key manager (LKM) are Detected, then import foreign configuration operation is not possible in iDRAC in this release. You must unlock the drives through CTRL-R and then continue to import foreign configuration from iDRAC.

The Import Foreign Configuration task is only displayed when the controller has detected a foreign configuration. You can also identify whether a physical disk contains a foreign configuration (virtual disk or hot spare) by checking the physical disk state. If the physical disk state is Foreign, then the physical disk contains all or some portion of a virtual disk or has a hot spare assignment.

NOTE: The task of importing foreign configuration imports all virtual disks residing on physical disks that have been added to the controller. If more than one foreign virtual disk is present, all the configurations are imported.

PERC9 controller provides support for auto import of foreign configuration without requiring user interactions. The auto import can be enabled or disabled. If enabled, the PERC controller can auto import any foreign configuration detected without manual intervention. If disabled the PERC does not auto import any foreign configuration.

You must have Login and Server Control privilege to import foreign configurations.

This task is not supported on PERC hardware controllers running in HBA mode.

NOTE: It is not recommended to remove an external enclosure cable while the operating system is running on the system. Removing the cable could result in a foreign configuration when the connection is re-established.

You can manage foreign configurations in the following cases:

- All the physical disks in a configuration are removed and re-inserted.
- Some of the physical disks in a configuration are removed and re-inserted.
- All the physical disks in a virtual disk are removed, but at different times, and then re-inserted.
- The physical disks in a non-redundant virtual disk are removed.

The following constraints apply to the physical disks that are considered for import:

- The drive state of a physical disk can change from the time the foreign configuration is scanned to when the actual import occurs. The foreign import occurs only on drives that are in the Unconfigured Good state.
- Drives in the failed or offline state cannot be imported.
- The firmware does not allow you to import more than eight foreign configurations.

Importing Foreign Configuration Using Web Interface

To import foreign configuration:

1. In the iDRAC Web interface, go to **Overview → Storage → Controllers → Setup**.
   The **Setup Controllers** page is displayed.
2. In the **Foreign Configuration** section, from the **Controller** drop-down menu, select the controller that you want to configure.
3. From the **Apply Operation Mode** drop-down menu, select when you want to import.
4. Click **Import Foreign Configuration**.
   Based on the selected operation mode, the configuration is imported.

   To automatically import foreign configurations, in the **Configure Controller Properties** section, enable the **Enhanced Auto Import Foreign Config** option, select the **Apply Operation Mode** and click **Apply**.

   NOTE: You must reboot the system after enabling **Enhanced Auto Import Foreign Config** option for the foreign configurations to be imported.

Importing Foreign Configuration Using RACADM

To import foreign configuration, use the following command:

```
racadm storage importconfig:<Controller FQDD>
```

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Clearing Foreign Configuration

After moving a physical disk from one controller to another, you may find that the physical disk contains all or some portion of a virtual disk (foreign configuration). You can identify whether a previously used

physical disk contains a foreign configuration (virtual disk) by checking the physical disk state. If the physical disk state is Foreign, then the physical disk contains all or some portion of a virtual disk. You can clear or erase the virtual disk information from the newly attached physical disks.

The Clear Foreign Configuration operation permanently erases all data residing on the physical disks that are added to the controller. If more than one foreign virtual disk is present, all the configurations are erased. You may prefer to import the virtual disk rather than destroy the data. An initialization must be performed to remove foreign data. If you have an incomplete foreign configuration which cannot be imported, you can use the Clearing Foreign Configuration option to erase the foreign data on the physical disks.

Clearing Foreign Configuration Using Web Interface

To clear the foreign configuration:

1. In the iDRAC Web interface, go to **Overview → Storage → Controllers → Setup**.
   The **Setup Controllers** page is displayed.
2. In the **Foreign Configuration** section, from the **Controller** drop-down menu, select the controller for which you want to clear the foreign configuration.
3. From the **Apply Operation Mode** drop-down menu, select when you want to clear the data.
4. Click **Clear**.
   Based on the selected operation mode, the virtual disks residing on the physical disk is erased.

Clearing Foreign Configuration Using RACADM

To clear foreign configuration, use the following command:

```
racadm storage clearconfig:<Controller FQDD>
```

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Resetting Controller Configuration

You can reset the configuration for a controller. This operation deletes virtual disk drives and unassigns all hot spares on the controller. It does not erase any data other than removing the disks from the configuration. Reset configuration also does not remove any foreign configurations. The real-time support of this feature is available only in PERC 9.1 firmware. Reset configuration does not erase any data. You may recreate the exact same configuration without an initialize operation which may result in the data being recovered. You must have server control privilege.

NOTE: Resetting the controller configuration does not remove a foreign configuration. To remove a foreign configuration, perform clear configuration operation.

Resetting Controller Configuration Using Web Interface

To reset the controller configuration:

1. In the iDRAC Web interface, go to **Overview → Storage → Controllers → Troubleshooting**.
   The **Controllers Troubleshooting** page is displayed.
2. From the **Actions** drop-down menu, select **Reset Configuration** for one or more controllers.
3. For each controller, from the **Apply Operation Mode** drop-down menu, select when you want to apply the settings.
4. Click **Apply**.

Based on the selected operation mode, the settings are applied.

Resetting Controller Configuration Using RACADM

To reset the controller configuration, use the following command:

```
racadm storage resetconfig:<Controller FQDD>
```

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

12Gbps SAS HBA Adapter Operations

The non-RAID controllers are the HBAs that do not have few RAID capabilities. They do not support virtual disks.

iDRAC interface supports only 12 Gbps SAS HBA controller in this release.

You can perform the following for non-RAID controllers:

- View controller, physical disks, and enclosure properties as applicable for the non-RAID controller. Also, view EMM, fan , power supply unit, and temperature probe properties associated with the enclosure. The properties are displayed based on the type of controller.
- View software and hardware inventory information.
- Update firmware for enclosures behind the 12 GBps SAS HBA controller (staged)
- Monitor the polling or polling frequency for physical disk SMART trip status when there is change detected
- Monitor the physical disks hot plug or hot removal status
- Blink or unblink LEDs

NOTE:

- You must perform Collect System Inventory On Reboot (CSIOR) operation before inventorying or monitoring the non-RAID controllers.
- Reboot the system after performing a firmware update.
- Real-time monitoring for SMART enabled drives and SES enclosure sensors is only done for the 12 GBps SAS HBA controllers.

Related Links

Inventory and Monitoring Storage Devices
Viewing System Inventory
Updating Device Firmware
Monitoring Predictive Failure Analysis On Drives
Blinking or Unblinking Component LEDs

Monitoring Predictive Failure Analysis On Drives

Storage management supports Self Monitoring Analysis and Reporting Technology (SMART) on physical disks that are SMART-enabled.

SMART performs predictive failure analysis on each disk and sends alerts if a disk failure is predicted. The controllers check physical disks for failure predictions and, if found, pass this information to iDRAC. iDRAC immediately logs an alert.

Controller Operations in Non-RAID (HBA) Mode

If the controller is in non-RAID mode (HBA mode), then:

- Virtual disks or hot spares are not available.
- Security state of the controller is disabled.
- All physical disks are in non-RAID mode.

You can perform the following operations if the controller is in non-RAID mode:

- Blink/unblink the physical disk.
- Configure the following properties:
  - Load balanced mode
  - Check consistency mode
  - Patrol read mode
  - Copyback mode
  - Controller boot mode
  - Enhanced auto import foreign configuration
  - Rebuild rate
  - Check consistency rate
  - Reconstruct rate
  - BGI rate
  - Enclosure or backplane mode
- View all properties that are applicable to a RAID controller expect for virtual disks.
- Clear foreign configuration

NOTE: If an operation is not supported in non-RAID mode, an error message is displayed.

You cannot monitor the enclosure temperature probes, fans, and power supplies when the controller is in non-RAID mode.

Running RAID Configuration Jobs On Multiple Storage Controllers

While performing operations on more than two storage controllers from any supported iDRAC interface, make sure to:

- Run the jobs on each controller individually. Wait for each job to complete before starting the configuration and job creation on the next controller.
- Schedule multiple jobs to run at a later time using the scheduling options.

Managing PCIe SSDs

Peripheral Component Interconnect Express (PCIe) solid-state device (SSD) is a high-performance storage device designed for solutions requiring low latency, high Input Output Operations per Second (IOPS), and enterprise class storage reliability and serviceability. The PCIe SSD is designed based on Single

Level Cell (SLC) and Multi-Level Cell (MLC) NAND flash technology with a high-speed PCIe 2.0 or PCIe 3.0 compliant interface.

Using iDRAC interfaces, you can view and configure NVMe PCIe SSDs.

The key features of PCIe SSD are:

- Hot plug capability
- High-performance device

The PCIe SSD subsystem consists of the Backplane, PCIe Extender card which is attached to the backplane of the system and provides PCIe connectivity for up to four or eight PCIe SSDs at the front of the chassis and the PCIe SSDs.

You can perform the following operations for PCIe SSDs:

- Inventory and remotely monitor the health of PCIe SSDs in the server
- Prepare the PCIe SSD to be removed
- Securely erase the data
- Blink or unblink the device LED

Related Links

Inventory and Monitoring PCIe SSDs
Preparing to Remove PCIe SSD
Erasing PCIe SSD Device Data

Inventory and Monitoring PCIe SSDs

In staged or real-time, the following inventory and monitoring information is available for PCIe SSDs:

- Hardware information:
  - PCIe SSD Extender card
  - PCIe SSD Backplane
- Software inventory includes only the firmware version for the PCIe SSD.

Inventory and Monitoring PCIe SSDs Using Web Interface

To inventory and monitor PCIe SSD devices, in the iDRAC Web interface, go to **Overview → Storage → Physical Disks** . The **Properties** page is displayed. For PCIe SSDs, the **Name** column displays **PCIe SSD**. Expand to view the properties.

Inventory and Monitoring PCIe SSDs Using RACADM

Use the `racadm storage get controllers:<PcieSSD controller FQDD>` command to inventory and monitor PCIe SSDs.

To view all PCIe SSD drives:

```
racadm storage get pdisks
```

To view PCIe extender cards:

```
racadm storage get controllers
```

To view PCIe SSD backplane information:

```
racadm storage get enclosures
```

NOTE: For all the mentioned commands, PERC devices are also displayed.

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Preparing to Remove PCIe SSD

PCIe SSDs support orderly hot swap allowing you to add or remove a device without halting or rebooting the system in which the devices are installed. To prevent data loss, it is mandatory that you use the Prepare to Remove operation before physically removing a device.

NOTE:

- Orderly hot swap is only supported when PCIe SSDs are installed in a supported system running a supported operating system. To make sure that you have the correct configuration for your PCIe SSD, see the system-specific Owner's Manual.
- The Prepare to Remove task is not supported for PCIe SSDs on VMware vSphere (ESXi) systems.
- The Prepare to Remove task can only be staged and real-time is not supported.

The Prepare to Remove operation stops any background activity and any ongoing I/O activity so that device can be removed safely. It causes the status LEDs on the device to blink. You can safely remove the device from the system under the following conditions after you initiate the Prepare to Remove operation:

- The PCIe SSD is blinking the safe to remove LED pattern.
- The PCIe SSD is no longer accessible by the system.

Before preparing the PCIe SSD for removal, make sure that:

- iDRAC Service Module is installed.
- Lifecycle Controller is enabled.
- You have Server Control and Login privileges

Preparing to Remove PCIe SSD Using Web Interface

To prepare the PCIe SSD for removal:

1. In the iDRAC Web interface, go to **Overview** → **Storage** → **Physical Disks** → **Setup**.
   The **Setup Physical Disk** page is displayed.
2. From the **Controller** drop-down menu, select the extender to view the associated PCIe SSDs.
3. From the drop-down menus, select **Prepare to Remove** for one or more PCIe SSDs.
   If you have selected **Prepare to Remove** and you want to view the other options in the drop-down menu, then select **Action** and then click the drop-down menu to view the other options.
4. From the **Apply Operation Mode** drop-down menu, select **Apply Now** to apply the actions immediately.
   If there are jobs to be completed, then this option is grayed-out.

   NOTE: For PCIe SSD devices, only the **Apply Now** option is available. This operation is not supported in staged mode.
5. Click **Apply**.

If the job is not created, a message indicating that the job creation was not successful is displayed. Also, the message ID and the recommended response action is displayed.

If the job is created successfully, a message indicating that the job ID is created for the selected controller is displayed. Click **Job Queue** to view the progress of the job in the **Job Queue** page.

If pending operation is not created, an error message is displayed. If pending operation is successful and job creation is not successful, then an error message is displayed.

Preparing to Remove PCIe SSD Using RACADM

To prepare the PCIeSSD drive for removal, run the following command:

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

To create the target job after executing **preparetoremove** command, run the following command:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

To query the job ID returned, run the following command:

```
racadm jobqueue view -i <job ID>
```

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Erasing PCIe SSD Device Data

Secure Erase permanently erases all data present on the disk. Performing a Cryptographic Erase on an PCIe SSD overwrites all blocks and results in permanent loss of all data on the PCIe SSD. During Cryptographic Erase, the host is unable to access the PCIe SSD. The changes are applied after system reboot.

If the system reboots or experiences a power loss during cryptographic erase, the operation is canceled. You must reboot the system and restart the process.

Before erasing PCIe SSD device data, make sure that:

- Lifecycle Controller is enabled.
- You have Server Control and Login privileges

NOTE:

- After the drive is erased, it displays in the operating system as online but it is not initialized. You must re-initialize and re-format the drive before using it again.
- After you hot-plug a PCIe SSD, it may take several seconds to be displayed on the Web interface.

Erasing PCIe SSD Device Data Using Web Interface

To erase the data on the PCIe SSD device:

1. In the iDRAC Web interface, go to **Overview → Storage → Physical Disks → Setup**.
   The **Setup Physical Disk** page is displayed.
2. From the **Controller** drop-down menu, select the controller to view the associated PCIe SSDs.
3. From the drop-down menus, select **Secure Erase** for one or more PCIe SSDs.
   If you have selected **Secure Erase** and you want to view the other options in the drop-down menu, then select **Action** and then click the drop-down menu to view the other options.

4. From the **Apply Operation Mode** drop-down menu, select one of the following options:
   - **At Next Reboot** — Select this option to apply the actions during the next system reboot. This is the default option for PERC 8 controllers.
   - **At Scheduled Time** — Select this option to apply the actions at a scheduled day and time:
     - **Start Time** and **End Time** — Click the calendar icons and select the days. From the drop-down menus, select the time. The action is applied between the start time and end time.
     - From the drop-down menu, select the type of reboot:
       * No Reboot (Manually Reboot System)
       * Graceful Shutdown
       * Force Shutdown
       * Power Cycle System (cold boot)

       NOTE: For PERC 8 or earlier controllers, **Graceful Shutdown** is the default option. For PERC 9 controllers, **No Reboot (Manually Reboot System)** is the default option.
5. Click **Apply**.

   If the job is not created, a message indicating that the job creation was not successful is displayed. Also, the message ID and the recommended response action is displayed.

   If the job is created successfully, a message indicating that the job ID is created for the selected controller is displayed. Click **Job Queue** to view the progress of the job in the Job Queue page.

   If pending operation is not created, an error message is displayed. If pending operation is successful and job creation is not successful, then an error message is displayed.

Erasing PCIe SSD Device Data Using RACADM

To perform a secure erase on PCIeSSD device, run the following command:

```
racadm storage secureerase:<PCIeSSD FQDD>
```

To create the target job after executing **secureerase** command, run the following command:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

To query the job ID returned, run the following command:

```
racadm jobqueue view -i <job ID>
```

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Managing Enclosures or Backplanes

You can perform the following for enclosures or backplanes:

- View properties
- Configure universal mode or split mode
- View slot information (universal or shared)
- Set SGPIO mode

Related Links

Summary of Supported Features for Storage Devices
Supported Enclosures
Configuring Backplane Mode

Viewing Universal Slots
Setting SGPIO Mode

Configuring Backplane Mode

The 13th generation Dell PowerEdge servers supports a new internal storage topology, where two storage controllers (PERCs) can be connected to a set of internal drives through a single expander. This configuration is used for high performance mode with no failover or High Availability (HA) functionality. The expander splits the internal drive array between the two storage controllers. In this mode, virtual disk creation only displays the drives connected to a particular controller. There are no licensing requirements for this feature. This feature is supported only on a few systems.

Backplane supports two modes:

- Unified mode — The primary PERC controller has access to all the drives connected to the backplane even if a second PERC controller is installed.
- Split mode — One controller has access to the first 12 drives and the second controller has access to the last 12 drives. This splitting is not configurable. The drives connected to the first controller are numbered 0-11 while the drives connected to the second controller are numbered 12-23.

By default, it is in unified mode.

iDRAC allows the split mode setting if the expander has the capability to support the configuration. You may want to enable this mode prior to installing the second controller. iDRAC performs a check for expander capability prior to allowing this mode to be configured and does not check whether the second PERC controller is present.

To modify the setting, you must have Server Control privilege.

If any other RAID operations are in pending state or any RAID job is scheduled, you cannot change the backplane mode. Similarly, if this setting is pending, you cannot schedule other RAID jobs.

NOTE:

- Warning messages are displayed when the setting is being changed as there is a possibility of data loss.
- LC Wipe or iDRAC reset operation does not change the expander setting for this mode.
- This operation is supported only in real-time and not staged.

Any change in this setting only takes effect after a system power reset. If you change from Split mode to Unified, an error message is displayed on the next boot as the second controller does not see any drives. Also, the first controller will see a foreign configuration. If you ignore the error, the existing virtual disks are lost.

Configuring Backplane Mode Using Web Interface

To configure backplane mode using iDRAC Web interface:

1. In the iDRAC Web interface, go to **Overview** → **Storage** → **Enclosures** → **Setup**
   The **Enclosure Setup** page is displayed.
2. From the **Controller** drop-down menu, select the controller to configure its associated enclosures.
3. In the **Value** column, select the required mode for the required backplane or enclosure:
   - Unified

- Split

4. From the **Apply Operation Mode** drop-down menu, select **Apply Now** to apply the actions immediately, and then click **Apply**.

   A job ID is created.
5. Go to the **Job Queue** page and verify that it displays the status as Completed for the job.
6. Power cycle the system for the setting to take affect.

Configuring Enclosure Using RACADM

To configure the enclosure or backplane, use the `BackplaneMode` object with the `set` subcommand.

For example, to set the BackplaneMode attribute to split mode:

1. At the RACADM command prompt, run the following command to view the current backplane mode:

   ```
   get storage.enclosure.1.backplanecurrentmode
   ```

   The output is:

   ```
   BackplaneCurrentMode=UnifiedMode
   ```
2. Run the following command to view the requested mode:

   ```
   get storage.enclosure.1.backplanerequestedmode
   ```

   The output is:

   ```
   BackplaneRequestedMode=None
   ```
3. Run the following command to set the requested backplane mode to split mode:

   ```
   set storage.enclosure.1.backplanerequestedmode "splitmode"
   ```

   The successful message is displayed.
4. Run the following command to verify if the `backplanerequestedmode` attribute is set to split mode:

   ```
   get storage.enclosure.1.backplanerequestedmode
   ```

   The output is:

   ```
   BackplaneRequestedMode=None (Pending=SplitMode)
   ```
5. Run `storage get controllers` command and note down the controller instance ID.
6. Run the following command to create a job:

   ```
   jobqueue create <controller instance ID> -s TIME_NOW --realtime
   ```

   A job ID is returned.
7. Run the following command to query the job status:

   ```
   jobqueue view -i JID_xxxxxxxx
   ```

   where, `JID_xxxxxxxx` is the job ID from step 6.

   The status is displayed as Pending.

   Continue to query the job ID until you view the Completed status (this process may take up to three minutes).
8. Run the following command to view the `backplanerequestedmode` attribute value:

   ```
   get storage.enclosure.1.backplanerequestedmode
   ```

The output is:

```
BackplaneRequestedMode=SplitMode
```

9. Run the following command to cold reboot the server:

```
serveraction powercycle
```

10. After the system completes POST and CSIOR, type the following command to verify the `backplanerequestedmode`:

```
get storage.enclosure.1.backplanerequestedmode
```

The output is:

```
BackplaneRequestedMode=None
```

11. Run the following to verify is the backplane mode is set to split mode:

```
get storage.enclosure.1.backplanecurrentmode
```

The output is:

```
BackplaneCurrentMode=SplitMode
```

12. Run the following command and verify that only 0–11 drives are displayed:

```
storage get pdisks
```

For more information about the racadm command, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**

Viewing Universal Slots

Some of the 13th generation PowerEdge server backplanes supports both SAS/SATA and PCIe SSD drives in the same slot. These slots are wired to the primary storage controller (PERC) and a PCIe extender card. These slots are called “universal” slots. Backplane firmware provides information on the slots that support this feature. The backplane supports SAS/SATA disks or PCIe SSDs. Typically the four higher number slots are universal. For, example, in a universal backplane supporting 24 slots, slots 0-19 support only SAS/SATA disks while slots 20-23 support either SAS/SATA or PCIe SSD.

The roll-up health status for the enclosure provides the combined health status for all the drives in the enclosure. The enclosure link on the **Topology** page display the entire enclosure information, irrespective of which controller it is associated with. As two storage controllers (PERC and PCIe extender) can be connected to the same backplane, only the backplane associated with the PERC controller is displayed in **System Inventory** page.

In the **Storage** → **Enclosures** → **Properties** page, the **Physical Disks Overview** section displays the following:

- If a slot is empty, **Slot Empty** is displayed for the slot.
- If there are no PCIe capable slots, then the **PCIe Capable** column is not displayed.
- If it is a universal backplane with PCIe SSD in one of the slots, then the **Bus Protocol** column displays **PCIe**.
- The **Hotspare** column is not applicable for PCIe SSD.

NOTE: Hot swapping is supported for universal slots. If you want to remove a PCIe SSD drive and swap it with a SAS/SATA drive, make sure to first complete the PrepareToRemove task for the PCIe SSD drive. If you do not perform this task, the host operating system may have issues such as a blue screen, kernel panic, and so on.

Setting SGPIO Mode

The storage controller can connect to the backplane in I2C mode (default setting for Dell backplanes) or Serial General Purpose Input/Output (SGPIO) mode. This connection is required for blinking LEDs on the drives. Dell PERC controllers and backplane support both these modes. To support certain channel adapters, the backplane mode must be changed SGPIO mode.

The SGPIO mode is only supported for passive backplanes. It is not supported for expander-based backplanes or passive backplanes in downstream mode. Backplane firmware provides information on capability, current state, and requested state.

After LC wipe operation or iDRAC reset to default, the SGPIO mode is reset to disabled state. It compares the iDRAC setting with the backplane setting. If the backplane is set to SGPIO mode, iDRAC changes its setting to match the backplane setting.

Server power cycle is required for any change in setting to take effect.

You must have Server Control privilege to modify this setting.

NOTE: You cannot set the SGPIO mode using iDRAC Web interface.

Setting SGPIO Mode Using RACADM

To configure the SGPIO mode, use the **SGPIOMode** object with the **set** sub command. If it is set to disabled, it is I2C mode. If enabled, it is set to SGPIO mode. For more information, see the *iDRAC RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Choosing Operation Mode to Apply Settings

While creating and managing virtual disks, setting up physical disks, controllers, and enclosures or resetting controllers, before you apply the various settings, you must select the operation mode. That is, specify when you want to apply the settings:

- Immediately
- During the next system reboot
- At a scheduled time
- As a pending operation to be applied as a batch as part of a single job.

Choosing Operation Mode Using Web Interface

To select the operation mode to apply the settings:

1. You can select the operation mode on when you are on any of the following pages:
   - **Overview → Storage → Physical Disks → Setup**.
   - **Overview → Storage → Virtual Disks → Create**
   - **Overview → Storage → Virtual Disks → Manage**
   - **Overview → Storage → Controllers → Setup**
   - **Overview → Storage → Controllers → Troubleshooting**
   - **Overview → Storage → Enclosures → Setup**

- **Overview → Storage → Pending Operations**

2. Select one of the following from the **Apply Operation Mode** drop-down menu:
   - **Apply Now** — Select this option to apply the settings immediately. This option is available for PERC 9 controllers only. If there are jobs to be completed, then this option is grayed-out. This job take at least 2 minutes to complete.
   - **At Next Reboot** — Select this option to apply the settings during the next system reboot. This is the default option for PERC 8 controllers.
   - **At Scheduled Time** — Select this option to apply the settings at a scheduled day and time:
     - **Start Time** and **End Time** — Click the calendar icons and select the days. From the drop-down menus, select the time. The settings are applied between the start time and end time.
     - From the drop-down menu, select the type of reboot:
       * No Reboot (Manually Reboot System)
       * Graceful Shutdown
       * Force Shutdown
       * Power Cycle System (cold boot)

       NOTE: For PERC 8 or earlier controllers, **Graceful Shutdown** is the default option. For PERC 9 controllers, **No Reboot (Manually Reboot System)** is the default option.
   - **Add to Pending Operations** — Select this option to create a pending operation to apply the settings. You can view all pending operations for a controller in the **Overview → Storage → Pending Operations** page.

   NOTE:
   - The **Add to Pending Operations** option in not applicable for the **Pending Operations** page and for PCIe SSDs in the **Physical Disks → Setup** page.
   - Only the **Apply Now** option is available on the **Enclosure Setup** page.

3. Click **Apply**.

   Based on the operation mode selected, the settings are applied.

Choosing Operation Mode Using RACADM

Use the `jobqueue` subcommand to select the operation mode. For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Viewing and Applying Pending Operations

You can view and commit all pending operations for the storage controller. All the settings are either applied at once, during the next reboot, or at a scheduled time based on the selected options. You can delete all the pending operations for a controller. You cannot delete individual pending operations.

Pending Operations are created on the selected components (controllers, enclosures, physical disks, and virtual disks).

Configuration jobs are created only on controller. In case of PCIe SSD, job is created on PCIe SSD disk and not on the PCIe Extender.

Viewing, Applying, or Deleting Pending Operations Using Web Interface

1. In the iDRAC Web interface, go to **Overview → Storage → Pending Operations**.

The **Pending Operations** page is displayed.

2. From the **Component** drop-down menu, select the controller for which you want to view, commit, or delete the pending operations.

   The list of pending operations is displayed for the selected controller.

   NOTE:
   - Pending operations are created for import foreign configuration, clear foreign configuration, security key operations, and encrypt virtual disks. But, they are not displayed in the **Pending Operations** page and in the Pending Operations pop-up message.
   - Jobs for PCIe SSD cannot be created from the **Pending Operations** page

3. To delete the pending operations for the selected controller, click **Delete All Pending Operations**.
4. From the drop-down menu, select one of the following and click **Apply** to commit the pending operations:
   - **Apply Now** — Select this option to commit all the operations immediately. This option is available for PERC 9 controllers with the latest firmware versions.
   - **At Next Reboot** — Select this option to commit all the operations during the next system reboot. This is the default option for PERC 8 controllers. This option is applicable for PERC 8 and later versions.
   - **At Scheduled Time** — Select this option to commit the operations at a scheduled day and time. This option is applicable for PERC 8 and later versions.
     - **Start Time** and **End Time** — Click the calendar icons and select the days. From the drop-down menus, select the time. The action is applied between the start time and end time.
     - From the drop-down menu, select the type of reboot:
       * No Reboot (Manually Reboot System)
       * Graceful Shutdown
       * Force Shutdown
       * Power Cycle System (cold boot)

       NOTE: For PERC 8 or earlier controllers, **Graceful Shutdown** is the default option. For PERC 9 controllers, **No Reboot (Manually Reboot System)** is the default option.
5. If the commit job is not created, a message indicating that the job creation was not successful is displayed. Also, the message ID and the recommended response action is displayed.
6. If the commit job is created successfully, a message indicating that the job ID is created for the selected controller is displayed. Click **Job Queue** to view the progress of the job in the **Job Queue** page.

   If the clear foreign configuration, import foreign configuration, security key operations, or encrypt virtual disk operations are in pending state, and if these are the only operations pending, then you cannot create a job from the**Pending Operations** page. You must perform any other storage configuration operation or use RACADM or WSMAN to create the required configuration job on the required controller.

   You cannot view or clear pending operations for PCIe SSDs in the **Pending Operations** page. Use the racadm command to clear the pending operations for PCIe SSDs.

Viewing and Applying Pending Operations Using RACADM

Use **jobqueue** subcommand to apply pending operations.For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Storage Devices — Apply Operation Scenarios

Case 1: Selected an Apply Operation (Apply Now, At Next Reboot, or At Scheduled Time) and there are no existing pending operations

If you have selected **Apply Now**, **At Next Reboot**, or **At Scheduled Time** and then clicked **Apply**, first the pending operation is created for the selected storage configuration operation.

- If the pending operation is successful and there are no prior existing pending operations, then the job is created. If the job is created successfully, a message indicating that the job ID is created for the selected device is displayed. Click **Job Queue** to view the progress of the job in the **Job Queue** page. If the job is not created, a message indicating that the job creation was not successful is displayed. Also, the message ID and the recommended response action are displayed.
- If the pending operation creation is unsuccessful and there are no prior existing pending operations, an error message with ID and recommended response action is displayed.

Case 2: Selected an Apply Operation (Apply Now, At Next Reboot, or At Scheduled Time) and there are existing pending operations

If you have selected **Apply Now**, **At Next Reboot**, or **At Scheduled Time** and then clicked **Apply**, first the pending operation is created for the selected storage configuration operation.

- If the pending operation is created successfully and if there are existing pending operations, then a message is displayed.
  - Click the **View Pending Operations** link to view the pending operations for the device.
  - Click **Create Job** to create job for the selected device. If the job is created successfully, a message indicating that the job ID is created for the selected device is displayed. Click **Job Queue** to view the progress of the job in the **Job Queue** page. If the job is not created, a message indicating that the job creation was not successful is displayed. Also, the message ID and the recommended response action is displayed.
  - Click **Cancel** to not create the job and remain on the page to perform more storage configuration operations.
- If the pending operation is not created successfully and if there are existing pending operations, then an error message is displayed.
  - Click **Pending Operations** to view the pending operations for the device.
  - Click **Create Job For Successful Operations** to create the job for the existing pending operations. If the job is created successfully, a message indicating that the job ID is created for the selected device is displayed. Click **Job Queue** to view the progress of the job in the **Job Queue** page. If the job is not created, a message indicating that the job creation was not successful is displayed. Also, the message ID and the recommended response action are displayed.
  - Click **Cancel** to not create the job and remain on the page to perform more storage configuration operations.

Case 3: Selected Add to Pending Operations and there are no existing pending operations

If you have selected **Add to Pending Operations** and then clicked **Apply**, first the pending operation is created for the selected storage configuration operation.

- If the pending operation is created successfully and if there are no existing pending operations, then an information message is displayed:

- Click **OK** to remain on the page to perform more storage configuration operations.
- Click **Pending Operations** to view the pending operations for the device. Until the job is created on the selected controller, these pending operations are not applied.

- If the pending operation is not created successfully and if there are no existing pending operations, then an error message is displayed.

Case 4: Selected Add to Pending Operations and there are prior existing pending operations

If you have selected **Add to Pending Operations** and then clicked **Apply**, first the pending operation is created for the selected storage configuration operation.

- If the pending operation is created successfully and if there are existing pending operations, then an information message is displayed:
  - Click **OK** to remain on the page to perform more storage configuration operations.
  - Click **Pending Operations** to view the pending operations for the device.
- If the pending operation is not created successfully and if there are existing pending operations, then an error message is displayed.
  - Click **OK** to remain on the page to perform more storage configuration operations.
  - Click **Pending Operations** to view the pending operations for the device.

NOTE:

- At any time, if you do not see the option to create a job on the storage configuration pages, go to **Storage Overview → Pending Operations** page to view the existing pending operations and to create the job on the required controller.
- Only cases 1 and 2 are applicable for PCIe SSD. You cannot view the pending operations for PCIe SSDs and hence **Add to Pending Operations** option is not available. Use racadm command to clear the pending operations for PCIe SSDs.

Blinking or Unblinking Component LEDs

You can locate a physical disk, virtual disk drive and PCIe SSDs within an enclosure by blinking one of the Light Emitting Diodes (LEDs) on the disk.

You must have Login privilege to blink or unblink an LED.

The controller must be real-time configuration capable. The real-time support of this feature is available only in PERC 9.1 firmware and later.

NOTE: Blink or unblink is not supported for servers without backplane.

Blinking or Unblinking Component LEDs Using Web Interface

To blink or unblink a component LED:

1. In the iDRAC Web interface, go to any of the following pages as per your requirement:
   - **Overview → Storage → Identify** - Displays the **Identify Component LEDs** page where you can blink or unblink the physical disks, virtual disks, and PCIe SSDs.
   - **Overview → Storage → Physical Disks → Identify**– Displays the **Identify Physical Disks** page where you can blink or unblink the physical disks and PCIe SSDs.

- **Overview → Storage → Virtual Disks → Identify**- Displays the **Identify Virtual Disks** page where you can blink or unblink the virtual disks.

2. If you are on the **Identify Component LED** page:
   - Select or deselect all component LEDs — Select the **Select/Deselect All** option and click **Blink** to start blinking the component LEDs. Similarly, click **Unblink** to stop blinking the component LEDs.
   - Select or deselect individual component LEDs — Select one or more component(s) and click **Blink** to start blinking the selected component LED(s). Similarly, click **Unblink** to stop blinking the component LEDs.
3. If you are on the **Identify Physical Disks** page:
   - Select or deselect all physical disk drives or PCIe SSDs — Select the **Select/Deselect All** option and click **Blink** to start blinking all the physical disk drives and the PCIe SSDs. Similarly, click **Unblink** to stop blinking the LEDs.
   - Select or deselect individual physical disk drives or PCIe SSDs — Select one or more physical disk drives and click **Blink** to start blinking the LEDs for the physical disk drives or the PCIe SSDs. Similarly, click **Unblink** to stop blinking the LEDs.
4. If you are on the **Identify Virtual Disk** page:
   - Select or deselect all virtual disks — Select the **Select/Deselect All** option and click **Blink** to start blinking the LEDs for all the virtual disks. Similarly, click **Unblink** to stop blinking the LEDs.
   - Select or deselect individual virtual disks — Select one or more virtual disks and click **Blink** to start blinking the LEDs for the virtual disks. Similarly, click **Unblink** to stop blinking the LEDs.

   If the blink or unblink operation is not successful, error messages are displayed.

Blinking or Unblinking Component LEDs Using RACADM

To blink or unblink component LEDs, use the following commands:

```
racadm storage blink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

```
racadm storage unblink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

14

Configuring and Using Virtual Console

You can use the virtual console to manage a remote system using the keyboard, video, and mouse on your management station to control the corresponding devices on a managed server. This is a licensed feature for rack and tower servers. It is available by default in blade servers.

The key features are:

- A maximum of six simultaneous Virtual Console sessions are supported. All the sessions view the same managed server console simultaneously.
- You can launch virtual console in a supported Web browser using Java or ActiveX plug-in. You must use the Java viewer if the management station runs on an operating system other than Windows.
- When you open a Virtual Console session, the managed server does not indicate that the console has been redirected.
- You can open multiple Virtual Console sessions from a single management station to one or more managed systems simultaneously.
- You cannot open two virtual console sessions from the management station to the managed server using the same plug-in.
- If a second user requests a Virtual Console session, the first user is notified and is given the option to refuse access, allow read-only access, or allow full shared access. The second user is notified that another user has control. The first user must respond within thirty seconds, or else access is granted to the second user based on the default setting. When two sessions are concurrently active, the first user sees a message in the upper-right corner of the screen that the second user has an active session. If neither the first or second user has administrator privileges, terminating the first user's session automatically terminates the second user's session.

Related Links

Configuring Web Browsers to Use Virtual Console
Configuring Virtual Console
Launching Virtual Console

Supported Screen Resolutions and Refresh Rates

The following table lists the supported screen resolutions and corresponding refresh rates for a Virtual Console session running on the managed server.

Table 26. Supported Screen Resolutions and Refresh Rates

Screen Resolution	Refresh Rate (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85

Screen Resolution	Refresh Rate (Hz)
1024x768	60, 70, 72, 75, 85
1280x1024	60

It is recommended that you configure your monitor display resolution to 1280x1024 pixels or higher.

NOTE: If you have an active Virtual Console session and a lower resolution monitor is connected to the Virtual Console, the server console resolution may reset if the server is selected on the local console. If the system is running a Linux operating system, an X11 console may not be viewable on the local monitor. Press <Ctrl><Alt><F1> at the iDRAC Virtual Console to switch Linux to a text console.

Configuring Web Browsers to Use Virtual Console

To use Virtual Console on your management station:

1. Make sure that a supported version of the browser (Internet Explorer (Windows), or Mozilla Firefox (Windows or Linux), Google Chrome, Safari) is installed.

   For more information about the supported browser versions, see the *Readme* available at **dell.com/support/manuals**.
2. To use Internet Explorer, set IE to **Run As Administrator**.
3. Configure the Web browser to use ActiveX or Java plug-in.

   ActiveX viewer is supported only with Internet Explorer. A Java viewer is supported on any browser.
4. Import the root certificates on the managed system to avoid the pop-ups that prompt you to verify the certificates.
5. Install the **compat-libstdc++-33-3.2.3-61** related package.

   NOTE: On Windows, the "compat-libstdc++-33-3.2.3-61" related package may be included in the .NET framework package or the operating system package.
6. If you are using MAC operating system, select the **Enable access for assistive devices** option in the **Universal Access** window.

   For more information, see the MAC operating system documentation.

Related Links

Configuring Web Browser to Use Java Plug-in
Configuring IE to Use ActiveX Plug-in
Importing CA Certificates to Management Station

Configuring Web Browser to Use Java Plug-in

Install a Java Runtime Environment (JRE) if you are using Firefox or IE and want to use the Java Viewer.

NOTE: Install a 32-bit or 64-bit JRE version on a 64-bit operating system or a 32-bit JRE version on a 32-bit operating system.

To configure IE to use Java plug-in:

- Disable automatic prompting for file downloads in Internet Explorer.
- Disable *Enhanced Security Mode* in Internet Explorer.

Related Links

Configuring Virtual Console

Configuring IE to Use ActiveX Plug-in

You must configure the IE browser settings before you launch and run ActiveX based Virtual Console and Virtual Media applications. The ActiveX applications are delivered as signed CAB files from the iDRAC server. If the plug-in type is set to Native-ActiveX type in Virtual console, when you try to launch the Virtual Console, the CAB file is downloaded to the client system and ActiveX based Virtual Console is launched. Internet Explorer requires some configurations to download, install, and run these ActiveX based applications.

Internet explorer is available in both 32–bit and 64–bit versions on 64–bit browsers. You can use any version, but if you install the plug-in in the 64–bit browser, and then try to run the viewer in a 32–bit browser you have to install the plug-in again.

NOTE: You can use ActiveX plug-in only with Internet Explorer.

For ActiveX applications in Windows 2003, Windows XP, Windows Vista, Windows 7, and Windows 2008, configure the following IE settings to use the ActiveX plug-in:

1. Clear the browser's cache.
2. Add iDRAC IP or hostname to the **Trusted Sites** list.
3. Reset the custom settings to **Medium-low** or change the settings to allow installation of signed ActiveX plug-ins.
4. Enable the browser to download encrypted content and to enable third-party browser extensions. To do this, go to **Tools** → **Internet Options** → **Advanced**, clear the **Do not save encrypted pages to disk** option, and select the **Enable third-party browser extensions** option.

   NOTE: Restart Internet Explorer for the Enable third-party browser extension setting to take effect.
5. Go to **Tools** → **Internet Options** → **Security** and select the zone you want to run the application.
6. Click **Custom level**. In the **Security Settings** window, do the following:
   - Select **Enable** for **Automatic prompting for ActiveX controls**.
   - Select **Prompt** for **Download signed ActiveX controls**.
   - Select **Enable** or **Prompt** for **Run ActiveX controls and plugins**.
   - Select **Enable** or **Prompt** for **Script ActiveX controls marked safe for scripting**.
7. Click **OK** to close the **Security Settings** window.
8. Click **OK** to close the **Internet Options** window.

   NOTE:
   - The varying versions of Internet Explorer share the same **Internet Options**. Therefore, after you add the server to the list of *trusted sites* for one browser the other browser uses the same setting.
   - Before installing the ActiveX control, Internet Explorer may display a security warning. To complete the ActiveX control installation procedure, accept the ActiveX control when Internet Explorer prompts you with a security warning.

Related Links

Clearing Browser Cache

Additional Settings for Windows Vista or Newer Microsoft Operating Systems

Additional Settings for Windows Vista or Newer Microsoft Operating Systems

The Internet Explorer browsers in Windows Vista or newer operating systems have an additional security feature called *Protected Mode*.

To launch and run ActiveX applications in Internet Explorer browsers with *Protected Mode*:

1. Run IE as an administrator.
2. Go to **Tools** → **Internet Options** → **Security** → **Trusted Sites**.
3. Make sure that the **Enable Protected Mode** option is not selected for Trusted Sites zone. Alternatively, you can add the iDRAC address to sites in the Intranet zone. By default, protected mode is turned off for sites in Intranet Zone and Trusted Sites zone.
4. Click **Sites**.
5. In the **Add this website to the zone** field, add the address of your iDRAC and click **Add**.
6. Click **Close** and then click **OK**.
7. Close and restart the browser for the settings to take effect.

Clearing Browser Cache

If you have issues when operating the Virtual Console, (out of range errors, synchronization issues, and so on) clear the browser's cache to remove or delete any old versions of the viewer that may be stored on the system and try again.

NOTE: You must have administrator privilege to clear the browser's cache.

Clearing Earlier ActiveX Versions in IE7

To clear earlier versions of Active-X viewer for IE7, do the following:

1. Close the Video Viewer and Internet Explorer browser.
2. Open the Internet Explorer browser again and go to **Internet Explorer** → **Tools** → **Manage Add-ons** and click **Enable or Disable Add-ons**. The **Manage Add-ons** window is displayed.
3. Select **Add-ons that have been used by Internet Explorer** from the **Show** drop-down menu.
4. Delete the *Video Viewer* add-on.

Clearing Earlier ActiveX Versions in IE8

To clear earlier versions of Active-X viewer for IE8, do the following:

1. Close the Video Viewer and Internet Explorer browser.
2. Open the Internet Explorer browser again and go to **Internet Explorer** → **Tools** → **Manage Add-ons** and click **Enable or Disable Add-ons**. The **Manage Add-ons** window is displayed.
3. Select **All Add-ons** from the **Show** drop-down menu.
4. Select the *Video Viewer* add-on and click the **More Information** link.
5. Select **Remove** from the **More Information** window.
6. Close the **More Information** and the **Manage Add-ons** windows.

Clearing Earlier Java Versions

To clear older versions of Java viewer in Windows or Linux, do the following:

1. At the command prompt, run `javaws-viewer` or `javaws-uninstall`.

The **Java Cache** viewer is displayed.

2. Delete the items titled *iDRAC Virtual Console Client*.

Importing CA Certificates to Management Station

When you launch Virtual Console or Virtual Media, prompts are displayed to verify the certificates. If you have custom Web server certificates, you can avoid these prompts by importing the CA certificates to the Java or ActiveX trusted certificate store.

Related Links

Importing CA certificate to Java Trusted Certificate Store
Importing CA Certificate to ActiveX Trusted Certificate Store

Importing CA certificate to Java Trusted Certificate Store

To import the CA certificate to the Java trusted certificate store:

1. Launch the **Java Control Panel**.
2. Click **Security** tab and then click **Certificates**.
   The **Certificates** dialog box is displayed.
3. From the Certificate type drop-down menu, select **Trusted Certificates**.
4. Click **Import**, browse, select the CA certificate (in Base64 encoded format), and click **Open**.
   The selected certificate is imported to the Web start trusted certificate store.
5. Click **Close** and then click **OK**. The **Java Control Panel** window closes.

Importing CA Certificate to ActiveX Trusted Certificate Store

You must use the OpenSSL command line tool to create the certificate Hash using Secure Hash Algorithm (SHA). It is recommended to use OpenSSL tool 1.0.x and later since it uses SHA by default. The CA certificate must be in Base64 encoded PEM format. This is one-time process to import each CA certificate.

To import the CA certificate to the ActiveX trusted certificate store:

1. Open the OpenSSL command prompt.
2. Run a 8 byte hash on the CA certificate that is currently in-use on the management station using the command: `openssl x509 -in (name of CA cert) -noout -hash`
   An output file is generated. For example, if the CA certificate file name is **cacert.pem**, the command is:
   ```
   openssl x509 –in cacert.pem –noout –hash
   ```
   The output similar to “431db322” is generated.
3. Rename the CA file to the output file name and include a “.0" extension. For example, 431db322.0.
4. Copy the renamed CA certificate to your home directory. For example, **C:\Documents and Settings \<user> directory**.

Configuring Virtual Console

Before configuring the Virtual Console, make sure that the management station is configured.

You can configure the virtual console using iDRAC Web interface or RACADM command line interface.

Related Links

Configuring Web Browsers to Use Virtual Console
Launching Virtual Console

Configuring Virtual Console Using Web Interface

To configure Virtual Console using iDRAC Web interface:

1. Go to **Overview** → **Server** → **Virtual Console**. The **Virtual Console** page is displayed.
2. Enable virtual console and specify the required values. For information about the options, see the *iDRAC Online Help*.
3. Click **Apply**. The virtual console is configured.

Configuring Virtual Console Using RACADM

To configure the Virtual Console, use one of the following:

- Use the objects in the **iDRAC.VirtualConsole** group with the **set** command.
- Use the following objects with the **config** command:
  - cfgRACTuneConRedirEnable
  - cfgRACTuneConRedirPort
  - cfgRACTuneConRedirEncryptEnable
  - cfgRacTunePluginType
  - cfgRacTuneVirtualConsoleAuthorizeMultipleSessions

For more information on these objects, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Previewing Virtual Console

Before launching the Virtual Console, you can preview the state of the Virtual Console on the **System** → **Properties** → **System Summary** page. The **Virtual Console Preview** section displays an image showing the state of the Virtual Console. The image is refreshed every 30 seconds. This is a licensed feature.

NOTE: The Virtual Console image is available only if you have enabled Virtual Console.

Launching Virtual Console

You can launch the virtual console using the iDRAC Web Interface or a URL.

NOTE: Do not launch a Virtual Console session from a Web browser on the managed system.

Before launching the Virtual Console, make sure that:

- You have administrator privileges.
- Web browser is configured to use Java or ActiveX plug-ins.
- Minimum network bandwidth of one MB/sec is available.

NOTE: If the embedded video controller is disabled in BIOS and if you launch the Virtual Console, the Virtual Console Viewer is blank.

While launching Virtual Console using 32-bit or 64-bit IE browsers, the required plug-in (Java or ActiveX) is available in the respective browser. The Internet Options settings are common for both the browsers.

While launching the Virtual Console using Java plug-in, occasionally you may see a Java compilation error. To resolve this, go to **Java control panel → General → Network Settings** and select **Direct Connection**.

If the Virtual Console is configured to use ActiveX plug-in, it may not launch the first time. This is because of the slow network connection and the temporary credentials (that Virtual Console uses to connect) timeout is two minutes. The ActiveX client plug-in download time may exceed this time. After the plug-in is successfully downloaded, you can launch the Virtual Console normally.

When you launch Virtual Console for the first time using IE8 with ActiveX plug-in, a "`Certificate Error: Navigation Blocked`" message may be displayed. Click **Continue to this website** and then click **Install** to install ActiveX controls on the **Security Warning** window. The Virtual Console session is launched.

Related Links

Launching Virtual Console Using URL
Configuring Web Browser to Use Java Plug-in
Configuring IE to Use ActiveX Plug-in
Launching Virtual Console Using Web Interface
Disabling Warning Messages While Launching Virtual Console Or Virtual Media Using Java or ActiveX Plug-in
Synchronizing Mouse Pointers

Launching Virtual Console Using Web Interface

You can launch the virtual console in the following ways:

- Go to **Overview → Server → Virtual Console**. The **Virtual Console** page is displayed. Click **Launch Virtual Console**. The **Virtual Console Viewer** is launched.
- Go to **Overview → Server → Properties**. The **System Summary** page is displayed. Under **Virtual Console Preview** section, click **Launch**. The **Virtual Console Viewer** is launched.

The **Virtual Console Viewer** displays the remote system's desktop. Using this viewer, you can control the remote system's mouse and keyboard functions from your management station.

Multiple message boxes may appear after you launch the application. To prevent unauthorized access to the application, navigate through these message boxes within three minutes. Otherwise, you are prompted to relaunch the application.

If one or more Security Alert windows appear while launching the viewer, click Yes to continue.

Two mouse pointers may appear in the viewer window: one for the managed server and another for your management station. To synchronize the cursors, see Synchronizing Mouse Pointers.

Virtual Console launch from a Windows Vista management station may lead to Virtual Console restart messages. To avoid this, set the appropriate time out values in the following locations:

- **Control Panel → Power Options → Power Saver → Advanced Settings → Hard Disk → Turnoff Hard Disk After <time_out>**

- **Control Panel → Power Options → High−Performance → Advanced Settings → Hard Disk → Turnoff Hard Disk After <time_out>**

Launching Virtual Console Using URL

To launch the Virtual Console using the URL:

1. Open a supported Web browser and in the address box, type the following URL in lower case: **https://iDRAC_ip/console**
2. Based on the login configuration, the corresponding **Login** page is displayed:
   - If Single Sign On is disabled and Local, Active Directory, LDAP, or Smart Card login is enabled, the corresponding **Login** page is displayed.
   - If Single-Sign On is enabled, the **Virtual Console Viewer** is launched and the **Virtual Console** page is displayed in the background.

   NOTE: Internet Explorer supports Local, Active Directory, LDAP, Smart Card (SC) and Single Sign-On (SSO) logins. Firefox supports Local, AD, and SSO logins on Windows-based operating system and Local, Active Directory, and LDAP logins on Linux-based operating systems.

   NOTE: If you do not have Access Virtual Console privilege but have Access Virtual Media privilege, then using this URL launches the Virtual Media instead of the Virtual Console.

Disabling Warning Messages While Launching Virtual Console Or Virtual Media Using Java or ActiveX Plug-in

You can disable the warning messages while launching the Virtual Console or Virtual Media using Java plug-in.

1. Initially, when you launch Virtual Console or Virtual Media using Java plug-in, the prompt to verify the publisher is displayed. Click **Yes**.

   A certificate warning message is displayed indicating that a trusted certificate is not found.

   NOTE: If the certificate is found in the operating system's certificate store or if it is found in a previously specified user location, then this warning message is not displayed.
2. Click **Continue**.

   The Virtual Console Viewer or Virtual Media Viewer is launched.

   NOTE: The Virtual Media viewer is launched if Virtual Console is disabled.
3. From the **Tools** menu, click **Session Options** and then **Certificate** tab.
4. Click **Browse Path**, specify the location to store the user's certificate, click **Apply**, click **OK**, and exit from the viewer.
5. Launch Virtual Console again.
6. In the certificate warning message, select the **Always trust this certificate** option, and then click **Continue**.
7. Exit from the viewer.
8. When you re-launch Virtual Console, the warning message is not displayed.

Using Virtual Console Viewer

The Virtual Console Viewer provides various controls such as mouse synchronization, virtual console scaling, chat options, keyboard macros, power actions, next boot devices, and access to Virtual Media. For information to use these features, see the *iDRAC Online Help*.

NOTE: If the remote server is powered off, the message 'No Signal' is displayed.

The Virtual Console Viewer title bar displays the DNS name or the IP address of the iDRAC you are connected to from the management station. If iDRAC does not have a DNS name, then the IP address is displayed. The format is:

- For rack and tower servers:
  `<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>`
- For blade servers:
  `<DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>`

Sometimes the Virtual Console Viewer may display low quality video. This is due to slow network connectivity that leads to loss of one or two video frames when you start the Virtual Console session. To transmit all the video frames and improve the subsequent video quality, do any of the following:

- In the **System Summary** page, under **Virtual Console Preview** section, click **Refresh**.
- In the **Virtual Console Viewer**, under **Performance** tab, set the slider to **Maximum Video Quality**.

Synchronizing Mouse Pointers

When you connect to a managed system through the Virtual Console, the mouse acceleration speed on the managed system may not synchronize with the mouse pointer on the management station and displays two mouse pointers in the Viewer window.

When using Red Hat Enterprise Linux or Novell SUSE Linux, configure the mouse mode for Linux before you launch the Virtual Console viewer. The operating system's default mouse settings are used to control the mouse arrow in the Virtual Console viewer.

When two mouse cursors are seen on the client Virtual Console viewer, it indicates that the server's operating system supports Relative Positioning. This is typical for Linux operating systems or Lifecycle Controller and causes two mouse cursors if the server's mouse acceleration settings are different from the mouse acceleration settings on the Virtual Console client. To resolve this, switch to single cursor or match the mouse acceleration on the managed system and the management station:

- To switch to single cursor, from the **Tools** menu, select **Single Cursor**.
- To set the mouse acceleration, go to **Tools → Session Options → Mouse**. Under **Mouse Acceleration** tab, select **Windows** or **Linux** based on the operating system.

To exit single cursor mode, press <F9> or the configured termination key.

NOTE: This is not applicable for managed systems running Windows operating system since they support Absolute Positioning.

When using the Virtual Console to connect to a managed system with a recent Linux distribution operating system installed, you may experience mouse synchronization problems. This may be due to the Predictable Pointer Acceleration feature of the GNOME desktop. For correct mouse synchronization in the iDRAC Virtual Console, this feature must be disabled. To disable Predictable Pointer Acceleration, in the mouse section of the **/etc/X11/xorg.conf** file, add:

```
Option "AccelerationScheme" "lightweight".
```

If synchronization problems continue, do the following additional change in the **<user_home>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml** file:

Change the values for `motion_threshold` and `motion_acceleration` to `-1`.

If you turn off mouse acceleration in GNOME desktop, in the Virtual Console viewer, go to **Tools** → **Session Options** → **Mouse**. Under **Mouse Acceleration** tab, select **None**.

For exclusive access to the managed server console, you must disable the local console and re-configure the **Max Sessions** to `1` on the **Virtual Console page**.

Passing All Keystrokes Through Virtual Console

You can enable the **Pass all keystrokes to server** option and send all keystrokes and key combinations from the management station to the managed system through the Virtual Console Viewer. If it is disabled, it directs all the key combinations to the management station where the Virtual Console session is running. To pass all keystrokes to the server, in the Virtual Console Viewer, go to **Tools** → **Session Options** → **General** tab and select the **Pass all keystrokes to server** option to pass the management station's keystrokes to the managed system.

The behavior of the Pass all keystrokes to server feature depends on the:

- Plug-in type (Java or ActiveX) based on which Virtual Console session is launched.
  For the Java client, the native library must be loaded for Pass all keystrokes to server and Single Cursor mode to function. If the native libraries are not loaded, the **Pass all keystrokes to server** and **Single Cursor** options are deselected. If you attempt to select either of these options, an error message is displayed indicating that the selected options are not supported.

  For the ActiveX client, the native library must be loaded for Pass all keystrokes to server function to work. If the native libraries are not loaded, the **Pass all keystrokes to server** option is deselected. If you attempt to select this option, an error message is displayed indicating that the feature is not supported

  For MAC operating systems, enable the **Enable access of assistive device** option in **Universal Access** for the Pass all keystrokes to server feature to work.
- Operating system running on the management station and managed system. The key combinations that are meaningful to the operating system on the management station are not passed to the managed system.
- Virtual Console Viewer mode—Windowed or Full Screen.
  In Full Screen mode, **Pass all keystrokes to server** is enabled by default.

  In Windowed mode, the keys passed only when the Virtual Console Viewer is visible and is active.

  When changed from Full Screen mode to Windowed mode, the previous state of Pass all keys is resumed.

Related Links

Java-based Virtual Console Session running on Windows Operating System
Java Based Virtual Console Session Running on Linux Operating System
ActiveX Based Virtual Console Session Running on Windows Operating System

Java-based Virtual Console Session running on Windows Operating System

- Ctrl+Alt+Del key is not sent to the managed system, but always interpreted by the management station.
- When Pass All Keystrokes to Server is enabled, the following keys are not sent to the managed system:
  - Browser Back Key
  - Browser Forward Key
  - Browser Refresh key
  - Browser Stop Key
  - Browser Search Key
  - Browser Favorites key
  - Browser Start and Home key
  - Volume mute key
  - Volume down key
  - Volume up key
  - Next track key
  - Previous track key
  - Stop Media key
  - Play/Pause media key
  - Start mail key
  - Select media key
  - Start Application 1 key
  - Start Application 2 key
- All the individual keys (not a combination of different keys, but a single key stroke) are always sent to the managed system. This includes all the Function keys, Shift, Alt, Ctrl key and Menu keys. Some of these keys affect both management station and managed system.

  For example, if the management station and the managed system is running Windows operating system, and Pass All Keys is disabled, when you press the Windows key to open the **Start** Menu, the **Start** menu opens on both management station and managed system. However, if Pass All Keys is enabled, then the **Start** menu is opened only on the managed system and not on the management station.
- When Pass All Keys is disabled, the behavior depends on the key combinations pressed and the special combinations interpreted by the operating system on the management station.

Java Based Virtual Console Session Running on Linux Operating System

The behavior mentioned for Windows operating system is also applicable for Linux operating system with the following exceptions:

- When Pass all keystrokes to server is enabled, <Ctrl+Alt+Del> is passed to the operating system on the managed system.
- Magic SysRq keys are key combinations interpreted by the Linux Kernel. It is useful if the operating system on the management station or the managed system freezes and you need to recover the system. You can enable the magic SysRq keys on the Linux operating system using one of the following methods:
  - Add an entry to **/etc/sysctl.conf**

- echo "1" > /proc/sys/kernel/sysrq

- When Pass all keystrokes to server is enabled, the magic SysRq keys are sent to the operating system on the managed system. The key sequence behavior to reset the operating system, that is reboot without un-mounting or sync, depends on whether the magic SysRq is enabled or disabled on the management station:
  - If SysRq is enabled on the management station, then <Ctrl+Alt+SysRq+b> or <Alt+SysRq+b> resets the management station irrespective of the system's state.
  - If SysRq is disabled on the management station, then the <Ctrl+Alt+SysRq+b> or <Alt+SysRq +b>keys resets the operating system on the managed system.
  - Other SysRq key combinations (example, <Alt+SysRq+k>, <Ctrl+Alt+SysRq+m>, and so on) are passed to the managed system irrespective of the SysRq keys enabled or not on the management station.

Using SysRq Magic Keys Through Remote Console

You can enable SysRq magic keys through the remote console using any of the following:

- Opensoure IPMI tool
- Using SSH/Telnet or External Serial Connector

Using Opensource IPMI Tool

Make sure that BIOS/iDRAC settings supports console redirection using SOL.

1. At the command prompt, run the SOL activate command:

   ```
   Ipmitool –I lanplus –H <ipaddr> -U <username> -P <passwd> sol activate
   ```

   The SOL session is activated.
2. After the server boots to the operating system, the `localhost.localdomain` login prompt appears. Log in using the operating system user name and password.
3. If SysRq is not enabled, enable using `echo 1 >/proc/sys/kernel/sysrq`.
4. Run break sequence `~B`.
5. Use the SysRq magic key to enable the SysRq function. For example, the following command displays the memory information on the console:

   ```
   echo m > /proc/sysrq-trigger displays
   ```

Using SSH/Telnet or External Serial Connector (Directly Connecting Through Serial Cable)

1. For telnet/SSH sessions, after logging in using the iDRAC username and password, at the `/admin>` prompt, run the command `console com2`. The `localhost.localdomain` prompt appears.
2. For console redirection using external serial connector directly connected to the system through a serial cable, the `localhost.localdomain` login prompt appears after the server boots to the operating system.
3. Log in using the operating system user name and password.
4. If SysRq is not enabled, enable using `echo 1 >/proc/sys/kernel/sysrq`.
5. Use the magic key to enable the SysRq function. For example, the following command reboots the server:

   ```
   echo b > /proc/sysrq-trigger
   ```

   NOTE: You do not have to run break sequence before using the magic SysRq keys.

ActiveX Based Virtual Console Session Running on Windows Operating System

The behavior of the pass all keystrokes to server feature in ActiveX based Virtual Console session running on Windows operating system is similar to the behavior explained for Java based Virtual Console session running on the Windows management station with the following exceptions:

- When Pass All Keys is disabled, pressing F1 launches the application Help on both management station and managed system, and the following message is displayed:

  ```
  Click Help on the Virtual Console page to view the online Help
  ```

- The media keys may not be blocked explicitly.
- <Alt + Space>, <Ctrl + Alt + +>, <Ctrl + Alt + -> are not sent to the managed system and is interpreted by the operating system on the management station.

15

Managing Virtual Media

Virtual media allows the managed server to access media devices on the management station or ISO CD/DVD images on a network share as if they were devices on the managed server.

Using the Virtual Media feature, you can:

- Remotely access media connected to a remote system over the network
- Install applications
- Update drivers
- Install an operating system on the managed system

This is a licensed feature for rack and tower servers. It is available by default for blade servers.

The key features are:

- Virtual Media supports virtual optical drives (CD/DVD), floppy drives (including USB-based drives), and USB flash drives.
- You can attach only one floppy, USB flash drive, image, or key and one optical drive on the management station to a managed system. Supported floppy drives include a floppy image or one available floppy drive. Supported optical drives include a maximum of one available optical drive or one ISO image file.

  The following figure shows a typical Virtual Media setup.
- Virtual floppy media of iDRAC is not accessible from virtual machines.
- Any connected Virtual Media emulates a physical device on the managed system.
- On Windows-based managed systems, the Virtual Media drives are auto-mounted if they are attached and configured with a drive letter.
- On Linux-based managed systems with some configurations, the Virtual Media drives are not auto-mounted. To manually mount the drives, use the mount command.
- All the virtual drive access requests from the managed system are directed to the management station across the network.
- Virtual devices appear as two drives on the managed system without the media being installed in the drives.
- You can share the management station CD/DVD drive (read only), but not a USB media, between two managed systems.
- Virtual media requires a minimum available network bandwidth of 128 Kbps.
- If LOM or NIC failover occurs, then the Virtual Media session may be disconnected.

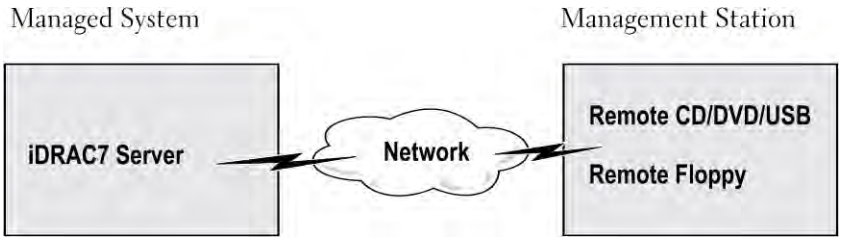


Figure 4. Virtual Media Setup

Supported Drives and Devices

The following table lists the drives supported through virtual media.

Table 27. Supported Drives and Devices

Drive	Supported Storage Media
Virtual Optical Drives	• Legacy 1.44 floppy drive with a 1.44 floppy diskette • CD-ROM • DVD • CD-RW • Combination drive with CD-ROM media
Virtual floppy drives	• CD-ROM/DVD image file in the ISO9660 format • Floppy image file in the ISO9660 format
USB flash drives	• USB CD-ROM drive with CD-ROM media • USB Key image in the ISO9660 format

Configuring Virtual Media

Before you configure the Virtual Media settings, make sure that you have configured your Web browser to use Java or ActiveX plug-in.

Related Links

Configuring Web Browsers to Use Virtual Console

Configuring Virtual Media Using iDRAC Web Interface

To configure virtual media settings:

CAUTION: Do not reset iDRAC when running a Virtual Media session. Otherwise, undesirable results may occur, including data loss.

1. In the iDRAC Web interface, go to **Overview → Server → Attached Media**.
2. Specify the required settings. For more information, see the *iDRAC Online Help*.
3. Click **Apply** to save the settings.

Configuring Virtual Media Using RACADM

To configure the virtual media,

- Use the objects in the **iDRAC.VirtualMedia** group with the **set** command.
- Use the objects in the **cfgRacVirtual** group with the **config** command.

For more information, see the *RACADM Command Line Reference Guide for iDRAC* available at **dell.com/support/manuals**.

Configuring Virtual Media Using iDRAC Settings Utility

You can attach, detach, or auto-attach virtual media using the iDRAC Settings utility. To do this:

1. In the iDRAC Settings utility, go to **Media and USB Port Settings**.
   The**iDRAC Settings . Media and USB Port Settings** page is displayed.
2. In the **Virtual Media** section, select **Detach**, **Attach**, or **Auto attach** based on the requirement. For more information about the options, see *iDRAC Settings Utility Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
   The Virtual Media settings are configured.

Attached Media State and System Response

The following table describes the system response based on the Attached Media setting.

Table 28. Attached Media State and System Response

Attached Media State	System Response
Detach	Cannot map an image to the system.
Attach	Media is mapped even when **Client View** is closed.
Auto-attach	Media is mapped when **Client View** is opened and unmapped when **Client View** is closed.

Server Settings For Viewing Virtual Devices in Virtual Media

You must configure the following settings in the management station to allow visibility of empty drives. To do this, in Windows Explorer, from the **Organize** menu, click **Folder and search options**. On the **View** tab, deselect **Hide empty drives in the Computer folder** option and click **OK**.

Accessing Virtual Media

You can access Virtual Media with or without using the Virtual Console. Before you access Virtual Media, make sure to configure your Web browser(s).

Virtual Media and RFS are mutually exclusive. If the RFS connection is active and you attempt to launch the Virtual Media client, the following error message is displayed: *Virtual Media is currently unavailable. A Virtual Media or Remote File Share session is in use.*

If the RFS connection is not active and you attempt to launch the Virtual Media client, the client launches successfully. You can then use the Virtual Media client to map devices and files to the Virtual Media virtual drives.

Related Links

Configuring Web Browsers to Use Virtual Console
Configuring Virtual Media

Launching Virtual Media Using Virtual Console

Before you launch Virtual Media through the Virtual Console, make sure that:

- Virtual Console is enabled.
- System is configured to not hide empty drives — In Windows Explorer, navigate to **Folder Options**, clear the **Hide empty drives in the Computer folder** option, and click **OK**.

To access Virtual Media using Virtual Console:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Virtual Console**.
   The **Virtual Console** page is displayed.
2. Click **Launch Virtual Console**.
   The **Virtual Console Viewer** is launched.

   NOTE: On Linux, Java is the default plug-in type for accessing the Virtual Console. On Windows, open the.**jnlp** file to launch the Virtual Console using Java.
3. Click **Virtual Media** → **Connect Virtual Media**.
   The Virtual Media session is established and the **Virtual Media** menu displays the list of devices available for mapping.

   NOTE: The **Virtual Console Viewer** window must remain active while you access the Virtual Media.

   .

Related Links

Configuring Web Browsers to Use Virtual Console
Configuring Virtual Media
Disabling Warning Messages While Launching Virtual Console Or Virtual Media Using Java or ActiveX Plug-in

Launching Virtual Media Without Using Virtual Console

Before you launch Virtual Media when the **Virtual Console** is disabled, make sure that

- Virtual Media is in *Attach* state.
- System is configured to unhide empty drives. To do this, in Windows Explorer, navigate to **Folder Options**, clear the **Hide empty drives in the Computer folder** option, and click **OK**.

To launch Virtual Media when Virtual Console is disabled:

1. In the iDRAC Web Interface, go to **Overview** → **Server** → **Virtual Console**.
   The **Virtual Console** page is displayed.
2. Click **Launch Virtual Console**.

The following message is displayed:

```
Virtual Console has been disabled. Do you want to continue using Virtual
Media redirection?
```

3. Click **OK** .

   The **Virtual Media** window is displayed.

4. From the **Virtual Media** menu, click **Map CD/DVD** or **Map Removable Disk**.

   For more information, see Mapping Virtual Drive.

   NOTE: The virtual device drive letters on the managed system do not coincide with the physical drive letters on the management station.

   NOTE: The Virtual Media may not function correctly on Windows operating system clients that are configured with Internet Explorer Enhanced Security. To resolve this issue, see the Microsoft operating system documentation or contact the system administrator.

Related Links

Configuring Virtual Media

Disabling Warning Messages While Launching Virtual Console Or Virtual Media Using Java or ActiveX Plug-in

Adding Virtual Media Images

You can create a media image of the remote folder and mount it as a USB attached device to the server's operating system. To add Virtual Media images:

1. Click **Virtual Media** → **Create Image...**.
2. In the **Source Folder** field, click **Browse** and browse to the folder or directory to be used as the source for the image file. The image file is on the management station or the C: drive of the managed system.
3. In the **Image File Name** field, the default path to store the created image files (typically the desktop directory) appears. To change this location, click **Browse** and navigate to a location.
4. Click **Create Image**.

   The image creation process starts. If the image file location is within the source folder, a warning message is displayed indicating that the image creation cannot proceed as the image file location within the source folder causes an infinite loop. If the image file location is not within the source folder, then the image creation proceeds.

   After the image is created, a success message is displayed.

5. Click **Finish**.

   The image is created.

   When a folder is added as an image, a **.img** file is created on the Desktop of the management station from which this feature is used. If this **.img** file is moved or deleted, then the corresponding entry for this folder in the **Virtual Media** menu does not work. Therefore, it is recommended not to move or delete the **.img** file while the *image* is being used. However, the **.img** file can be removed after the relevant entry is first deselected and then removed using **Remove Image** to remove the entry.

Viewing Virtual Device Details

To view the virtual device details, in the Virtual Console Viewer, click **Tools** → **Stats**. In the **Stats** window, the **Virtual Media** section displays the mapped virtual devices and the read/write activity for each device.

If Virtual Media is connected, this information is displayed. If Virtual Media is not connected, the "Virtual Media is not connected" message is displayed.

If the Virtual Media is launched without using the Virtual Console, then the **Virtual Media** section is displayed as a dialog box. It provides information about the mapped devices.

Resetting USB

To reset the USB device:

1. In the Virtual Console viewer, click **Tools** → **Stats**.

   The **Stats** window is displayed.
2. Under **Virtual Media**, click **USB Reset**.

   A message is displayed warning the user that resetting the USB connection can affect all the input to the target device including Virtual Media, keyboard, and mouse.
3. Click **Yes**.

   The USB is reset.

   NOTE: iDRAC Virtual Media does not terminate even after you log out of iDRAC Web interface session.

Mapping Virtual Drive

To map the virtual drive:

NOTE: While using ActiveX-based Virtual Media, you must have administrative privileges to map an operating system DVD or a USB flash drive (that is connected to the management station.) To map the drives, launch IE as an administrator or add the iDRAC IP address to the list of trusted sites.

1. To establish a Virtual Media session, from the **Virtual Media** menu, click **Connect Virtual Media**.

   For each device available for mapping from the host server, a menu item appears under the **Virtual Media** menu. The menu item is named according to the device type such as:

   - Map CD/DVD
   - Map Removable Disk
   - Map Floppy Disk

   NOTE: The **Map Floppy Disk** menu item appears on the list if the **Floppy Emulation** option is enabled on the **Attached Media** page. When **Floppy Emulation** is enabled, **Map Removable Disk** is replaced with **Map Floppy Disk**.

   The **Map DVD/CD** option can be used for ISO files and the **Map Removable Disk** option can be used for images.
2. Click the device type that you want to map.

   NOTE: The active session displays if a Virtual Media session is currently active from the current Web interface session, from another Web interface session, or from VMCLI.
3. In the **Drive/Image File** field, select the device from the drop-down list.

   The list contains all the available (unmapped) devices that you can map (CD/DVD, Removable Disk, Floppy Drive) and image file types that you can map (ISO or IMG). The image files are located in the default image file directory (typically the user's desktop). If the device is not available in the drop-down list, click **Browse** to specify the device.

   The correct file type for CD/DVD is ISO and for removable disk and floppy disk it is IMG.

If the image is created in the default path (Desktop), when you select **Map Removable Disk**, the created image is available for selection in the drop-down menu.

If image is created in a different location, when you select **Map Removable Disk**, the created image is not available for selection in the drop-down menu. Click **Browse** to specify the image.

4. Select **Read-only** to map writable devices as read-only.
   For CD/DVD devices, this option is enabled by default and you cannot disable it.
5. Click **Map Device** to map the device to the host server.
   After the device/file is mapped, the name of its **Virtual Media** menu item changes to indicate the device name. For example, if the CD/DVD device is mapped to an image file named **foo.iso**, then the CD/DVD menu item on the Virtual Media menu is named **foo.iso mapped to CD/DVD**. A check mark for that menu item indicates that it is mapped.

Related Links

Displaying Correct Virtual Drives For Mapping
Adding Virtual Media Images

Displaying Correct Virtual Drives For Mapping

On a Linux-based management station, the Virtual Media **Client** window may display removable disks and floppy disks that are not part of the management station. To make sure that the correct virtual drives are available to map, you must enable the port setting for the connected SATA hard drive. To do this:

1. Reboot the operating system on the management station. During POST, press <F2> to enter **System Setup**.
2. Go to **SATA settings**. The port details are displayed.
3. Enable the ports that are actually present and connected to the hard drive.
4. Access the Virtual Media **Client** window. It displays the correct drives that can be mapped.

Related Links

Mapping Virtual Drive

Unmapping Virtual Drive

To ummap the virtual drive:

1. From the **Virtual Media** menu, do any of the following:
   - Click the device that you want to unmap.
   - Click **Disconnect Virtual Media**.

   A message appears asking for confirmation.
2. Click **Yes**.
   The check mark for that menu item does not appear indicating that it is not mapped to the host server.

Setting Boot Order Through BIOS

Using the System BIOS Settings utility, you can set the managed system to boot from virtual optical drives or virtual floppy drives.

NOTE: Changing Virtual Media while connected may stop the system boot sequence.

To enable the managed system to boot:

1. Boot the managed system.
2. Press <F2> to enter the **System Setup** page.
3. Go to **System BIOS Settings** → **Boot Settings** → **BIOS Boot Settings** → **Boot Sequence**.

   In the pop-up window, the virtual optical drives and virtual floppy drives are listed with the standard boot devices.
4. Make sure that the virtual drive is enabled and listed as the first device with bootable media. If required, follow the on-screen instructions to modify the boot order.
5. Click **OK**, navigate back to **System BIOS Settings** page, and click **Finish**.
6. Click **Yes** to save the changes and exit.

   The managed system reboots.

   The managed system attempts to boot from a bootable device based on the boot order. If the virtual device is connected and a bootable media is present, the system boots to the virtual device. Otherwise, the system overlooks the device—similar to a physical device without bootable media.

Enabling Boot Once for Virtual Media

You can change the boot order only once when you boot after attaching remote Virtual Media device.

Before you enable the boot once option, make sure that:

- You have *Configure User* privilege.
- Map the local or virtual drives (CD/DVD, Floppy, or USB flash device) with the bootable media or image using the Virtual Media options
- Virtual Media is in *Attached* state for the virtual drives to appear in the boot sequence.

To enable the boot once option and boot the managed system from the Virtual Media:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Attached Media**.
2. Under **Virtual Media**, select the **Enable Boot Once** and click **Apply**.
3. Turn on the managed system and press **<F2>** during boot.
4. Change the boot sequence to boot from the remote Virtual Media device.
5. Reboot the server.

   The managed system boots once from the Virtual Media.

Related Links

Mapping Virtual Drive

Configuring Virtual Media

16

Installing and Using VMCLI Utility

The Virtual Media Command Line Interface (VMCLI) utility is an interface that provides virtual media features from the management station to iDRAC on the managed system. Using this utility you can access virtual media features, including image files and physical drives, to deploy an operating system on multiple remote systems in a network.

NOTE: You can run the VMCLI utility only on the management station that is installed with 32–bit operating system.

The VMCLI utility supports the following features:

- Manage removable devices or images that are accessible through virtual media.
- Automatically terminate the session when the iDRAC firmware **Boot Once** option is enabled.
- Secure communications to iDRAC using Secure Sockets Layer (SSL).
- Execute VMCLI commands until:
  - The connections automatically terminate.
  - An operating system terminates the process.

  NOTE: To terminate the process in Windows, use the Task Manager.

Installing VMCLI

The VMCLI utility is included in the *Dell Systems Management Tools and Documentation* DVD.

To install the VMCLI utility:

1. Insert the *Dell Systems Management Tools and Documentation* DVD into the management station's DVD drive.
2. Follow the on-screen instructions to install DRAC tools.
3. After successful install, check **install\Dell\SysMgt\rac5** folder to make sure **vmcli.exe** exists. Similarly, check the respective path for UNIX.

   The VMCLI utility is installed on the system.

Running VMCLI Utility

- If the operating system requires specific privileges or group membership, you require similar privileges to run the VMCLI commands.
- On Windows systems, non-administrators must have **Power User** privileges to run the VMCLI utility.
- On Linux systems, to access iDRAC, run VMCLI utility, and log user commands, non-administrators must prefix `sudo` to the VMCLI commands. However, to add or edit users in the VMCLI administrators group, use the `visudo` command.

VMCLI Syntax

The VMCLI interface is identical on both Windows and Linux systems. The VMCLI syntax is:

```
VMCLI [parameter] [operating_system_shell_options]
```

For example, `vmcli -r iDRAC-IP-address:iDRAC-SSL-port`

The *parameter* enables VMCLI to connect to the specified server, access iDRAC, and map to the specified virtual media.

NOTE: VMCLI syntax is case-sensitive.

To ensure security, it is recommended to use the following VMCLI parameters:

- `vmcli -i` — Enables an interactive method of starting VMCLI. It ensures that the user name and password are not visible when processes are examined by other users.
- vmcli `-r <iDRAC-IP-address[:iDRAC-SSL-port]> -S -u <iDRAC-user-name> -p <iDRAC-user-password> -c {< device-name > | < image-file >}` — Indicates whether the iDRAC CA certificate is valid. If the certificate is not valid, a warning message is displayed when you run this command. However, the command is executed successfully and a VMCLI session is established. For more information on VMCLI parameters, see the *VMCLI Help* or the *VMCLI Man pages*.

Related Links

VMCLI Commands to Access Virtual Media
VMCLI Operating System Shell Options

VMCLI Commands to Access Virtual Media

The following table provides the VMCLI commands required for accessing different virtual media.

Table 29. VMCLI Commands

Virtual Media	Command
Floppy drive	`vmcli -r [RAC IP or hostname] -u [iDRAC user name] -p [iDRAC user password] -f [device name]`
Bootable floppy or USB key image	`vmcli -r [iDRAC IP address] [iDRAC user name] -p [iDRAC password] -f [floppy.img]`
CD drive using -f option	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -f [device name]| [image file]-f [cdrom - dev ]`
Bootable CD/DVD image	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -c [DVD.img]`

If the file is not write-protected, Virtual Media may write to the image file. To make sure that Virtual Media does not write to the media:

- Configure the operating system to write-protect a floppy image file that must not be overwritten.
- Use the write-protection feature of the device.

When virtualizing read-only image files, multiple sessions can use the same image media simultaneously.

When virtualizing physical drives, only one session can access a given physical drive at a time.

VMCLI Operating System Shell Options

VMCLI uses shell options to enable the following operating system features:

- stderr/stdout redirection — Redirects any printed utility output to a file.

  For example, using the greater-than character (>) followed by a filename overwrites the specified file with the printed output of the VMCLI utility.

  NOTE: The VMCLI utility does not read from standard input (stdin). Hence, stdin redirection is not required.
- Background execution — By default, the VMCLI utility runs in the foreground. Use the operating system's command shell features for the utility to run in the background.

  For example, under a Linux operating system, the ampersand character (&) following the command causes the program to be spawned as a new background process. This technique is useful in script programs, as it allows the script to proceed after a new process is started for the VMCLI command (otherwise, the script blocks until the VMCLI program is terminated).

  When multiple VMCLI sessions are started, use the operating system-specific facilities for listing and terminating processes.

17

Managing vFlash SD Card

The vFlash SD card is a Secure Digital (SD) card that plugs into the vFlash SD card slot in the system. You can use a card with a maximum of 16 GB capacity. After you insert the card, you must enable vFlash functionality to create and manage partitions. vFlash is a licensed feature.

If the card is not available in the system's vFlash SD card slot, the following error message is displayed in the iDRAC Web interface at **Overview → Server → vFlash**:

```
SD card not detected. Please insert an SD card of size 256MB or greater.
```

NOTE: Make sure that you only insert a vFlash compatible SD card in the iDRAC vFlash card slot. If you insert a non-compatible SD card, the following error message is displayed when you initialize the card: *An error has occurred while initializing SD card.*

The key features are:

- Provides storage space and emulates USB device (s).
- Create up to 16 partitions. These partitions, when attached, are exposed to the system as a Floppy drive, Hard Disk drive, or a CD/DVD drive depending on the selected emulation mode.
- Create partitions from supported file system types. Supports .**img** format for floppy, **.iso** format for CD/DVD, and both **.iso** and **.img** formats for Hard Disk emulation types.
- Create bootable USB device(s).
- Boot once to an emulated USB device.

NOTE: It is possible that a vFlash license may expire during a vFlash operation. If it happens, the on-going vFlash operations complete normally.

Configuring vFlash SD Card

Before configuring vFlash, make sure that the vFlash SD card is installed on the system. For information on how to install and remove the card from your system, see the system's *Hardware Owner's Manual* at **dell.com/support/manuals**.

NOTE: You must have Access Virtual Media privilege to enable or disable vFlash functionality, and initialize the card.

Related Links

Viewing vFlash SD Card Properties
Enabling or Disabling vFlash Functionality
Initializing vFlash SD Card

Viewing vFlash SD Card Properties

After vFlash functionality is enabled, you can view the SD card properties using iDRAC Web interface or RACADM.

Viewing vFlash SD Card Properties Using Web Interface

To view the vFlash SD card properties, in the iDRAC Web interface, go to **Overview → Server → vFlash**. The **SD Card Properties** page is displayed. For information about the displayed properties, see the *iDRAC Online Help*.

Viewing vFlash SD Card Properties Using RACADM

To view the vFlash SD card properties using RACADM, use one of the following:

- Use the `cfgvFlashSD` object with the `getconfig` command. The following read-only properties are displayed:
  - cfgVFlashSDSize
  - cfgVFlashSDLicensed
  - cfgVFlashSDAvailableSize
  - cfgVFlashSDHealth
  - cfgVFlashSDEnable
  - cfgVFlashSDWriteProtect
  - cfgVFlashSDInitialized
- Use the following objects with the `get` command:
  - iDRAC.vflashsd.AvailableSize
  - iDRAC.vflashsd.Health
  - iDRAC.vflashsd.Licensed
  - iDRAC.vflashsd.Size
  - iDRAC.vflashsd.WriteProtect

For more information about these objects, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals** or **dell.com/esmamanuals**.

Viewing vFlash SD Card Properties Using iDRAC Settings Utility

To view the vFlash SD card properties, in the **iDRAC Settings Utility**, go to **Media and USB Port Settings**. The **iDRAC Settings . Media and USB Port Settings** page displays the properties. For information about the displayed properties, see the *iDRAC Settings Utility Online Help*.

Enabling or Disabling vFlash Functionality

You must enable the vFlash functionality to perform partition management.

Enabling or Disbaling vFlash Functionality Using Web Interface

To enable or disable the vFlash functionality:

1. In the iDRAC Web interface, go to **Overview → Server → vFlash**.

The **SD Card Properties** page is displayed.

2. Select or clear the **vFLASH Enabled** option to enable or disable the vFlash functionality. If any vFlash partition is attached, you cannot disable vFlash and an error message is displayed.

   NOTE: If vFlash functionality is disabled, SD card properties are not displayed.

3. Click **Apply**. The vFlash functionality is enabled or disabled based on the selection.

Enabling or Disabling vFlash Functionality Using RACADM

To enable or disable the vFlash functionality using RACADM, use one of the following:

- Using `config` command:
  - To enable vFlash:
    ```
    racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
    ```
  - To disable vFlash:
    ```
    racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
    ```
- Using `set` command:
  - To enable vFlash:
    ```
    racadm set iDRAC.vflashsd.Enable 1
    ```
  - To disable vFlash:
    ```
    racadm set iDRAC.vflashsd.Enable 0
    ```

NOTE: The RACADM command functions only if a vFlash SD card is present. If a card is not present, the following message is displayed: *ERROR: SD Card not present*.

Enabling or Disabling vFlash Functionality Using iDRAC Settings Utility

To enable or disable the vFlash functionality:

1. In the iDRAC Settings utility, go to **Media and USB Port Settings**.
   The **iDRAC Settings . Media and USB Port Settings** page is displayed.
2. In the **vFlash Media** section, select **Enabled** to enable vFlash functionality or select **Disabled** to disable the vFlash functionality.
3. Click **Back**, click **Finish**, and then click **Yes**.
   The vFlash functionality is enabled or disabled based on the selection.

Initializing vFlash SD Card

The initialize operation reformats the SD card and configures the initial vFlash system information on the card.

NOTE: If the SD card is write-protected, then the Initialize option is disabled.

Initializing vFlash SD Card Using Web Interface

To initialize the vFlash SD card:

1. In the iDRAC Web interface, go to **Overview → Server → vFlash**.
   The **SD Card Properties** page is displayed.
2. Enable **vFLASH** and click **Initialize**.

All existing contents are removed and the card is reformatted with the new vFlash system information.

If any vFlash partition is attached, the initialize operation fails and an error message is displayed.

Initializing vFlash SD Card Using RACADM

To initialize the vFlash SD card using RACADM, use one of the following:

- Using `vFlashSD` command:
  `racadm vflashsd initialize`
- Using `set` command:
  `racadm set iDRAC.vflashsd.Initialized 1`

All existing partitions are deleted and the card is reformatted.

For more information about these commands, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals** and **dell.com/esmmanuals**.

Initializing vFlash SD Card Using iDRAC Settings Utility

To initialize the vFlash SD card using iDRAC Settings utility:

1. In the iDRAC Settings utility, go to **Media and USB Port Settings**.
   The **iDRAC Settings . Media and USB Port Settings** page is displayed.
2. Click **Initialize vFlash**.
3. Click **Yes**. The initialization operation starts.
4. Click **Back** and navigate to the same **iDRAC Settings . Media and USB Port Settings** page to view the successful message.
   All existing contents are removed and the card is reformatted with the new vFlash system information.

Getting the Last Status Using RACADM

To get the status of the last initialize command sent to the vFlash SD card:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the command: `racadm vFlashsd status`
   The status of commands sent to the SD card is displayed.
3. To get the last status of all the vflash partitions, use the command:`racadm vflashpartition status -a`
4. To get the last status of a particular partition, use command:`racadm vflashpartition status -i (index)`

   NOTE: If iDRAC is reset, the status of the last partition operation is lost.

Managing vFlash Partitions

You can perform the following using the iDRAC Web interface or RACADM:

NOTE: An administrator can perform all operations on the vFlash partitions. Else, you must have **Access Virtual Media** privilege to create, delete, format, attach, detach, or copy the contents for the partition.

- Creating an Empty Partition
- Creating a Partition Using an Image File
- Formatting a Partition
- Viewing Available Partitions
- Modifying a Partition
- Attaching or Detaching Partitions
- Deleting Existing Partitions
- Downloading Partition Contents
- Booting to a Partition

NOTE: If you click any option on the vFlash pages when an application such as WS-MAN, iDRAC Settings utility, or RACADM is using vFlash, or if you navigate to some other page in the GUI, iDRAC may display the message: `vFlash is currently in use by another process. Try again after some time.`

vFlash is capable of performing fast partition creation when there is no other on-going vFlash operation such as formatting, attaching partitions, and so on. Therefore, it is recommended to first create all partitions before performing other individual partition operations.

Creating an Empty Partition

An empty partition, when attached to the system, is similar to an empty USB flash drive. You can create empty partitions on a vFlash SD card. You can create partitions of type *Floppy* or *Hard Disk*. The partition type CD is supported only while creating partitions using images.

Before creating an empty partition, make sure that:

- You have **Access Virtual Media** privilege.
- The card is initialized.
- The card is not write-protected.
- An initialize operation is not being performed on the card.

Creating an Empty Partition Using the Web Interface

To create an empty vFlash partition:

1. In iDRAC Web interface, go to **Overview → Server → vFlash → Create Empty Partition**.
   The **Create Empty Partition** page is displayed.
2. Specify the required information and click **Apply**. For information about the options, see the *iDRAC Online Help*.
   A new unformatted empty partition is created that is read-only by default. A page indicating the progress percentage is displayed. An error message is displayed if:
   - The card is write-protected.
   - The label name matches the label of an existing partition.
   - A non-integer value is entered for the partition size, the value exceeds the available space on the card, or the partition size is greater than 4 GB.

- An initialize operation is being performed on the card.

Creating an Empty Partition Using RACADM

To create a 20 MB empty partition:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the command: `racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20`

   A 20 MB empty partition in FAT16 format is created. By default, an empty partition is created as read-write.

Creating a Partition Using an Image File

You can create a new partition on the vFlash SD card using an image file (available in the **.img** or **.iso** format.) The partitions are of emulation types: Floppy (**.img**), Hard Disk (**.img**), or CD (**.iso**). The created partition size is equal to the image file size.

Before creating a partition from an image file, make sure that:

- You have Access Virtual Media privilege.
- The card is initialized.
- The card is not write-protected.
- An initialize operation is not being performed on the card.
- The image type and the emulation type match.

  NOTE: The uploaded image and the emulation type must match. There are issues when iDRAC emulates a device with incorrect image type. For example, if the partition is created using an ISO image and the emulation type is specified as Hard Disk, then the BIOS cannot boot from this image.
- Image file size is less than or equal to the available space on the card.
- Image file size is less than or equal to 4 GB as the maximum partition size supported is 4 GB. However, while creating a partition using a Web browser, the image file size must be less than 2 GB.

NOTE: The vFlash partition is an image file on a FAT32 file system. Thus, the image file has the 4 GB limitation.

Creating a Partition Using an Image File Using Web Interface

To create a vFlash partition from an image file:

1. In iDRAC Web interface, go to **Overview → Server → vFlash → Create From Image**.

   The **Create Partition from Image File** page is displayed.
2. Enter the required information and click **Apply**. For information about the options, see the *iDRAC Online Help*.

   A new partition is created. For CD emulation type, a read-only partition is created. For Floppy or Hard Disk emulation type, a read-write partition is created. An error message is displayed if:

   - The card is write-protected
   - The label name matches the label of an existing partition.
   - The size of the image file is greater than 4 GB or exceeds the available space on the card.
   - The image file does not exist or the image file extension is neither .img nor .iso.

- An initialize operation is already being performed on the card.

Creating a Partition From an Image File Using RACADM

To create a partition from an image file using RACADM:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the command: `racadm vflashpartition create –i 1 –o drive1 –e HDD –t image –l //myserver/sharedfolder/foo.iso –u root –p mypassword`

   A new partition is created. By default, the created partition is read-only. This command is case sensitive for the image file name extension. If the file name extension is in upper case, for example FOO.ISO instead of FOO.iso, then the command returns a syntax error.

   NOTE: This feature is not supported in local RACADM.

   NOTE: Creating vFlash partition from an image file located on the CFS or NFS IPv6 enabled network share is not supported.

Formatting a Partition

You can format an existing partition on the vFlash SD card based on the type of file system. The supported file system types are EXT2, EXT3, FAT16, and FAT32. You can only format partitions of type Hard Disk or Floppy, and not CD. You cannot format read-only partitions.

Before creating an partition from an image file, make sure that:

- You have **Access Virtual Media** privilege.
- The card is initialized.
- The card is not write-protected.
- An initialize operation is not being performed on the card.

To format vFlash partition:

1. In iDRAC Web interface, go to **Overview → Server → vFlash → Format**.

   The **Format Partition** page is displayed.
2. Enter the required information and click **Apply**.

   For information about the options, see the *iDRAC Online Help*.

   A warning message indicating that all the data on the partition will be erased is displayed.
3. Click **OK**.

   The selected partition is formatted to the specified file system type. An error message is displayed if:
   - The card is write-protected.
   - An initialize operation is already being performed on the card.

Viewing Available Partitions

Make sure that the vFlash functionality is enabled to view the list of available partitions.

Viewing Available Partitions Using Web Interface

To view the available vFlash partitions, in the iDRAC Web interface, go to **Overview → Server → vFlash → Manage**. The **Manage Partitions** page is displayed listing the available partitions and related information for each partition. For information on the partitions, see the *iDRAC Online Help*.

Viewing Available Partitions Using RACADM

To view the available partitions and their properties using RACADM:

1. Open a Telnet, SSH, or Serial console to the system and log in.
2. Enter the following commands:
   - To list all existing partitions and its properties:
     `racadm vflashpartition list`
   - To get the status of operation on partition 1:
     `racadm vflashpartition status -i 1`
   - To get the status of all existing partitions:
     `racadm vflashpartition status -a`

   NOTE: The -a option is valid only with the status action.

Modifying a Partition

You can change a read-only partition to read-write or vice-versa. Before modifying the partition, make sure that:

- The vFlash functionality is enabled.
- You have **Access Virtual Media** privileges.

NOTE: By default, a read-only partition is created.

Modifying a Partition Using Web Interface

To modify a partition:

1. In the iDRAC Web interface, go to **Overview → Server → vFlash → Manage**.
   The **Manage Partitions** page is displayed.
2. In the **Read-Only** column:
   - Select the checkbox for the partition(s) and click **Apply** to change to read-only.
   - Clear the checkbox for the partition(s) and click **Apply** to change to read-write.
     The partitions are changed to read-only or read-write, based on the selections.

   NOTE: If the partition is of type CD, the state is read-only. You cannot change the state to read-write. If the partition is attached, the check box is grayed-out.

Modifying a Partition Using RACADM

To view the available partitions and their properties on the card:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Use any one of the following:
   - Using `config` command to change the read-write state of the partition:
     - To change a read-only partition to read-write:
       `racadm config –g cfgvflashpartition –i 1 –o cfgvflashPartitionAccessType 1`

  - To change a read-write partition to read-only:
    ```
    racadm config –g cfgvflashpartition –i 1 –o
    cfgvflashPartitionAccessType 0
    ```
- Using `set` command to change the read-write state of the partition:
  - To change a read-only partition to read-write:
    ```
    racadm set iDRAC.vflashpartition.<index>.AccessType 1
    ```
  - To change a read-write partition to read-only:
    ```
    racadm set iDRAC.vflashpartition.<index>.AccessType 0
    ```
- Using `set` command to specify the Emulation type:
  ```
  racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or
  CD-DVD>
  ```

Attaching or Detaching Partitions

When you attach one or more partitions, they are visible to the operating system and BIOS as USB mass storage devices. When you attach multiple partitions, based on the assigned index, they are listed in an ascending order in the operating system and the BIOS boot order menu.

If you detach a partition, it is not visible in the operating system and the BIOS boot order menu.

When you attach or detach a partition, the USB bus in the managed system is reset. This affects applications that are using vFlash and disconnects the iDRAC Virtual Media sessions.

Before attaching or detaching a partition, make sure that:

- The vFlash functionality is enabled.
- An initialize operation is not already being performed on the card.
- You have **Access Virtual Media** privileges.

Attaching or Detaching Partitions Using Web Interface

To attach or detach partitions:

1. In the iDRAC Web interface, go to **Overview → Server → vFlash → Manage**.
   The **Manage Partitions** page is displayed.
2. In the **Attached** column:
   - Select the checkbox for the partition(s) and click **Apply** to attach the partition(s).
   - Clear the checkbox for the partition(s) and click **Apply** to detach the partition(s).
     The partitions are attached or detached, based on the selections.

Attaching or Detaching Partitions Using RACADM

To attach or detach partitions:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Use any one of the following:
   - Using `config` command:
     - To attach a partition:

```
racadm config –g cfgvflashpartition –i 1 –o
cfgvflashPartitionAttachState 1
```

– To detach a partition:

```
racadm config –g cfgvflashpartition –i 1 –o
cfgvflashPartitionAttachState 0
```

- Using `set` command:
  - To attach a partition:

    ```
    racadm set iDRAC.vflashpartition.<index>.AttachState 1
    ```

  - To detach a partition:

    ```
    racadm set iDRAC.vflashpartition.<index>.AttachState 0
    ```

Operating System Behavior for Attached Partitions

For Windows and Linux operating systems:

- The operating system controls and assigns the drive letters to the attached partitions.
- Read-only partitions are read-only drives in the operating system.
- The operating system must support the file system of an attached partition. Else, you cannot read or modify the contents of the partition from the operating system. For example, in a Windows environment the operating system cannot read the partition type EXT2 which is native to Linux. Also, in a Linux environment the operating system cannot read the partition type NTFS which is native to Windows.
- The vFlash partition label is different from the volume name of the file system on the emulated USB device. You can change the volume name of the emulated USB device from the operating system. However, it does not change the partition label name stored in iDRAC.

Deleting Existing Partitions

Before deleting existing partition(s), make sure that:

- The vFlash functionality is enabled.
- The card is not write-protected.
- The partition is not attached.
- An initialize operation is not being performed on the card.

Deleting Existing Partitions Using Web Interface

To delete an existing partition:

1. In the iDRAC Web interface, go to **Overview → Server → vFlash → Manage**.
   The **Manage Partitions** page is displayed.
2. In the **Delete** column, click the delete icon for the partition that you want to delete.
   A message is displayed indicating that this action permanently deletes the partition.
3. Click **OK**.
   The partition is deleted.

Deleting Existing Partitions Using RACADM

To delete partitions:

1. Open a telnet, SSH, or Serial console to the system and log in.
2. Enter the following commands:
   - To delete a partition:
     ```
     racadm vflashpartition delete -i 1
     ```
   - To delete all partitions, re-initialize the vFlash SD card.

Downloading Partition Contents

You can download the contents of a vFlash partition in the **.img** or **.iso** format to the:

- Managed system (where iDRAC is operated from)
- Network location mapped to a management station.

Before downloading the partition contents, make sure that:

- You have Access Virtual Media privileges.
- The vFlash functionality is enabled.
- An initialize operation is not being performed on the card.
- For a read-write partition, it must not be attached.

To download the contents of the vFlash partition:

1. In the iDRAC Web interface, go to **Overview → Server → vFlash → Download**.
   The **Download Partition** page is displayed.
2. From the **Label** drop-down menu, select a partition that you want to download and click **Download**.

   NOTE: All existing partitions (except attached partitions) are displayed in the list. The first partition is selected by default.
3. Specify the location to save the file.
   The contents of the selected partition are downloaded to the specified location.

   NOTE: If only the folder location is specified, then the partition label is used as the file name, along with the extension **.iso** for CD and Hard Disk type partitions, and **.img** for Floppy and Hard Disk type partitions.

Booting to a Partition

You can set an attached vFlash partition as the boot device for the next boot operation.

Before booting a partition, make sure that:

- The vFlash partition contains a bootable image (in the **.img** or **.iso** format) to boot from the device.
- The vFlash functionality is enabled.
- You have Access Virtual Media privileges.

Booting to a Partition Using Web Interface

To set the vFlash partition as a first boot device, see Setting First Boot Device.

NOTE: If the attached vFlash partition(s) are not listed in the **First Boot Device** drop-down menu, make sure that the BIOS is updated to the latest version.

Booting to a Partition Using RACADM

To set a vFlash partition as the first boot device, use `cfgServerInfo`. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

NOTE: When you run this command, the vFlash partition label is automatically set to boot once—`cfgserverBootOnce` is set to `1`. Boot once boots the device to the partition only once and does not keep it persistently first in the boot order.

18

Using SMCLP

The Server Management Command Line Protocol (SMCLP) specification enables CLI-based systems management. It defines a protocol for management commands transmitted over standard character oriented streams. This protocol accesses a Common Information Model Object Manager (CIMOM) using a human-oriented command set. The SMCLP is a sub-component of the Distributed Management Task Force (DMTF) SMASH initiative to streamline systems management across multiple platforms. The SMCLP specification, along with the Managed Element Addressing Specification and numerous profiles to SMCLP mapping specifications, describes the standard verbs and targets for various management task executions.

NOTE: It is assumed that you are familiar with the Systems Management Architecture for Server Hardware (SMASH) Initiative and the Server Management Working Group (SMWG) SMCLP specifications.

The SM-CLP is a subcomponent of the Distributed Management Task Force (DMTF) SMASH initiative to streamline server management across multiple platforms. The SM-CLP specification, along with the Managed Element Addressing Specification and numerous profiles to SM-CLP mapping specifications, describes the standard verbs and targets for various management task executions.

The SMCLP is hosted from the iDRAC controller firmware and supports Telnet, SSH, and serial-based interfaces. The iDRAC SMCLP interface is based on the SMCLP Specification Version 1.0 provided by the DMTF organization.

NOTE: Information about the profiles, extensions, and MOFs are available at **delltechcenter.com** and all DMTF information is available at **dmtf.org/standards/profiles/**.

SM-CLP commands implement a subset of the local RACADM commands. The commands are useful for scripting since you can execute these commands from a management station command line. You can retrieve the output of commands in well-defined formats, including XML, facilitating scripting and integration with existing reporting and management tools.

System Management Capabilities Using SMCLP

iDRAC SMCLP enables you to:

- Manage Server Power — Turn on, shut down, or reboot the system
- Manage System Event Log (SEL) — Display or clear the SEL records
- Manage iDRAC user account
- View system properties

Running SMCLP Commands

You can run the SMCLP commands using SSH or Telnet interface. Open a SSH or Telnet interface and log in to iDRAC as an administrator. The SMCLP prompt (admin ->)is displayed.

SMCLP prompts:

- yx1x blade servers use `-$`.
- yx1x rack and tower servers use `admin->`.
- yx2x blade, rack, and tower servers use `admin->`.

where, y is a alpha-numeric character such as M (for blade servers), R (for rack servers), and T (for tower servers) and x is a number. This indicates the generation of Dell PowerEdge servers.

NOTE: Scripts using `-$` can use these for yx1x systems, but starting with yx2x systems one script with `admin->` can be used for blade, rack, and tower servers.

iDRAC SMCLP Syntax

The iDRAC SMCLP uses the concept of verbs and targets to provide systems management capabilities through the CLI. The verb indicates the operation to perform, and the target determines the entity (or object) that runs the operation.

The SMCLP command line syntax:

```
<verb> [<options>] [<target>] [<properties>]
```

The following table provides the verbs and its definitions.

Table 30. SMCLP Verbs

Verb	Definition
cd	Navigates through the MAP using the shell
set	Sets a property to a specific value
help	Displays help for a specific target
reset	Resets the target
show	Displays the target properties, verbs, and subtargets
start	Turns on a target
stop	Shuts down a target
exit	Exits from the SMCLP shell session
version	Displays the version attributes of a target

Verb	Definition
load	Moves a binary image to a specified target address from a URL

The following table provides a list of targets.

Table 31. SMCLP Targets

Target	Definitions
admin1	admin domain
admin1/profiles1	Registered profiles in iDRAC
admin1/hdwr1	Hardware
admin1/system1	Managed system target
admin1/system1/capabilities1	Managed system SMASH collection capabilities
admin1/system1/capabilities1/pwrcap1	Managed system power utilization capabilities
admin1/system1/capabilities1/elecap1	Managed system target capabilities
admin1/system1/logs1	Record Log collections target
admin1/system1/logs1/log1	System Event Log (SEL) record entry
admin1/system1/logs1/log1/record*	An individual SEL record instance on the managed system
admin1/system1/settings1	Managed system SMASH collection settings
admin1/system1/capacities1	Managed system capacities SMASH collection
admin1/system1/consoles1	Managed system consoles SMASH collection
admin1/system1/sp1	Service Processor
admin1/system1/sp1/timesvc1	Service Processor time service
admin1/system1/sp1/capabilities1	Service processor capabilities SMASH collection
admin1/system1/sp1/capabilities1/clpcap1	CLP service capabilities
admin1/system1/sp1/capabilities1/pwrmgtcap1	Power state management service capabilities on the system
admin1/system1/sp1/capabilities1/acctmgtcap*	Account management service capabilities

Target	Definitions
admin1/system1/sp1/capabilities1/ rolemgtcap*	Local Role Based Management capabilities
admin1/system1/sp1/capabilities/ PwrutilmgtCap1	Power utilization management capabilities
admin1/system1/sp1/capabilities1/ elecap1	Authentication capabilities
admin1/system1/sp1/settings1	Service Processor settings collection
admin1/system1/sp1/settings1/ clpsetting1	CLP service settings data
admin1/system1/sp1/clpsvc1	CLP service protocol service
admin1/system1/sp1/clpsvc1/clpendpt*	CLP service protocol endpoint
admin1/system1/sp1/clpsvc1/tcpendpt*	CLP service protocol TCP endpoint
admin1/system1/sp1/jobq1	CLP service protocol job queue
admin1/system1/sp1/jobq1/job*	CLP service protocol job
admin1/system1/sp1/pwrmgtsvc1	Power state management service
admin1/system1/sp1/account1-16	Local user account
admin1/sysetm1/sp1/account1-16/ identity1	Local user identity account
admin1/sysetm1/sp1/account1-16/ identity2	IPMI identity (LAN) account
admin1/sysetm1/sp1/account1-16/ identity3	IPMI identity (Serial) account
admin1/sysetm1/sp1/account1-16/ identity4	CLP identity account
admin1/system1/sp1/acctsvc1	Local user account management service
admin1/system1/sp1/acctsvc2	IPMI account management service
admin1/system1/sp1/acctsvc3	CLP account management service
admin1/system1/sp1/rolesvc1	Local Role Base Authorization (RBA) service
admin1/system1/sp1/rolesvc1/Role1-16	Local role
admin1/system1/sp1/rolesvc1/Role1-16/ privilege1	Local role privilege
admin1/system1/sp1/rolesvc2	IPMI RBA service

Target	Definitions
admin1/system1/sp1/rolesvc2/Role1-3	IPMI role
admin1/system1/sp1/rolesvc2/Role4	IPMI Serial Over LAN (SOL) role
admin1/system1/sp1/rolesvc3	CLP RBA Service
admin1/system1/sp1/rolesvc3/Role1-3	CLP role
admin1/system1/sp1/rolesvc3/Role1-3/privilege1	CLP role privilege

Related Links

Running SMCLP Commands
Usage Examples

Navigating the MAP Address Space

Objects that can be managed with SM-CLP are represented by targets arranged in a hierarchical space called the Manageability Access Point (MAP) address space. An address path specifies the path from the root of the address space to an object in the address space.

The root target is represented by a slash (/) or a backslash (\). It is the default starting point when you log in to iDRAC. Navigate down from the root using the `cd` verb.

NOTE: The slash (/) and backslash (\) are interchangeable in SM-CLP address paths. However, a backslash at the end of a command line continues the command on the next line and is ignored when the command is parsed.

For example to navigate to the third record in the System Event Log (SEL), enter the following command:

```
->cd /admin1/system1/logs1/log1/record3
```

Enter the `cd` verb with no target to find your current location in the address space. The `..` and `.` abbreviations work as they do in Windows and Linux: `..` refers to the parent level and `.` refers to the current level.

Using Show Verb

To learn more about a target use the `show` verb. This verb displays the target's properties, sub-targets, associations, and a list of the SM-CLP verbs that are allowed at that location.

Using the -display Option

The `show -display` option allows you to limit the output of the command to one or more of properties, targets, associations, and verbs. For example, to display just the properties and targets at the current location, use the following command:

```
show -display properties,targets
```

To list only certain properties, qualify them, as in the following command:

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

If you only want to show one property, you can omit the parentheses.

Using the -level Option

The `show -level` option executes `show` over additional levels beneath the specified target. To see all targets and properties in the address space, use the `-l all` option.

Using the -output Option

The `-output` option specifies one of four formats for the output of SM-CLP verbs: **text**, **clpcsv**, **keyword**, and **clpxml**.

The default format is **text**, and is the most readable output. The **clpcsv** format is a comma-separated values format suitable for loading into a spreadsheet program. The **keyword** format outputs information as a list of keyword=value pairs one per line. The **clpxml** format is an XML document containing a **response** XML element. The DMTF has specified the **clpcsv** and **clpxml** formats and their specifications can be found on the DMTF website at **dmtf.org**.

The following example shows how to output the contents of the SEL in XML:

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Usage Examples

This section provides use case scenarios for SMCLP:

- Server Power Management
- SEL Management
- MAP Target Navigation

Server Power Management

The following examples show how to use SMCLP to perform power management operations on a managed system.

Type the following commands at the SMCLP command prompt:

- To switch off the server:
  ```
  stop /system1
  ```
  The following message is displayed:
  ```
  system1 has been stopped successfully
  ```
- To switch on the server:
  ```
  start /system1
  ```
  The following message is displayed:
  ```
  system1 has been started successfully
  ```

- To reboot the server:
  ```
  reset /system1
  ```

  The following message is displayed:

  ```
  system1 has been reset successfully
  ```

SEL Management

The following examples show how to use the SMCLP to perform SEL-related operations on the managed system. Type the following commands at the SMCLP command prompt:

- To view the SEL:
  ```
  show/system1/logs1/log1
  ```

  The following output is displayed:

  ```
  /system1/logs1/log1

  Targets:

  Record1

  Record2

  Record3

  Record4

  Record5

  Properties:

  InstanceID = IPMI:BMC1 SEL Log

  MaxNumberOfRecords = 512

  CurrentNumberOfRecords = 5

  Name = IPMI SEL

  EnabledState = 2

  OperationalState = 2

  HealthState = 2

  Caption = IPMI SEL

  Description = IPMI SEL

  ElementName = IPMI SEL
  ```

```
Commands:

cd

show

help

exit

version
```

- To view the SEL record:
  `show/system1/logs1/log1`

  The following output is displayed:

```
/system1/logs1/log1/record4


Properties:

LogCreationClassName= CIM_RecordLog

CreationClassName= CIM_LogRecord

LogName= IPMI SEL

RecordID= 1

MessageTimeStamp= 20050620100512.000000-000

Description= FAN 7 RPM: fan sensor, detected a failure

ElementName= IPMI SEL Record


Commands:

cd

show

help

exit

version
```

- To clear the SEL:
  `delete /system1/logs1/log1/record*`

  The following output is displayed:

```
All records deleted successfully
```

MAP Target Navigation

The following examples show how to use the cd verb to navigate the MAP. In all examples, the initial default target is assumed to be /.

Type the following commands at the SMCLP command prompt:

- To navigate to the system target and reboot:
  cd system1 reset The current default target is /.
- To navigate to the SEL target and display the log records:
  ```
  cd system1

  cd logs1/log1

  show
  ```
- To display current target:
  type `cd .`
- To move up one level:
  type `cd ..`
- To exit:
  `exit`

19

Using iDRAC Service Module

The iDRAC Service Module is a software application that is recommended to be installed on the server (it is not installed by default). It complements iDRAC with monitoring information from the operating system. It does not have an interface but, complements iDRAC by providing additional data to work with iDRAC interfaces such as the Web interface, RACADM, and WSMAN. You can configure the features monitored by the iDRAC Service Module to control the CPU and memory consumed on the server's operating system.

NOTE: You can use the iDRAC Service Module only if you have installed iDRAC Express or iDRAC Enterprise license.

Before using iDRAC Service Module, make sure that:

- You have Login, Configure, and Server Control privileges in iDRAC to enable or disable the iDRAC Service Module features.
- OS to iDRAC pass-through feature is enabled through the internal USB bus in iDRAC.

  NOTE:

  – When iDRAC Service Module runs for the first time, by default it enables the OS to iDRAC pass-through channel in iDRAC. If you disable this feature after installing the iDRAC Service Module, then you must enable it manually in iDRAC.

  – If the OS to iDRAC pass-through channel is enabled through LOM in iDRAC, then you cannot use the iDRAC Service Module.

Installing iDRAC Service Module

You can download and install the iDRAC Service Module from **dell.com/support**. You must have administrator privilege on the sever's operating system to install the iDRAC Service Module. For information on installation, see the *iDRAC Service Module Installation Guide* available at **dell.com/support/manuals**.

NOTE: This feature is not applicable for Dell Precision PR7910 systems.

Supported Operating Systems for iDRAC Service Module

For the list of operating systems supported by the iDRAC Service Module, see the *iDRAC Service Module Installation Guide* available at **dell.com/openmanagemanuals.com**.

iDRAC Service Module Monitoring Features

The iDRAC Service Module provides the following monitoring features:

- View Operating System (OS) information
- Replicate Lifecycle Controller logs to operating system logs
- Perform automatic system recovery options
- Populate Windows Management Instrumentation (WMI) Management Providers
- Integrate with Technical Support Report. This is applicable only if iDRAC Service Module Version 2.0 or later is installed. For more information, see Generating Tech Support Report.
- Prepare to Remove NVMe PCIe SSD. For more information, see iDRACUG_Preparing to Remove NVMe PCIe SSD.

NOTE: The features such as Windows Management Instrumentation Providers, Prepare to Remove NVMe PCIe SDD through iDRAC, Automating Technical Support Report OS collection are supported only on 13th generation Dell PowerEdge servers with minimum firmware version 2.00.00.00 or later.

Operating System Information

The OpenManage Server Administrator currently shares operating system information and host name with iDRAC. The iDRAC Service Module provides similar information such as OS name, OS version, and Fully Qualified Domain Name (FQDN) with iDRAC. By default, this monitoring feature is enabled. It is not disabled if OpenManage Server Administrator is installed on the host OS.

iDRAC Service Module 2.0 has amended the operating system information feature with the OS network interface Monitoring. When iDRAC Service Module version 2.0 is used with iDRAC 2.00.00.00, it starts monitoring the operating system network interfaces. You can view this information using iDRAC Web interface, RACADM, or WSMAN. For more information, see Viewing Network Interfaces Available On Host OS.

When iDRAC Service Module version 2.0 is used with iDRAC version lower than 2.00.00.00, the OS information feature does not provide OS network interface monitoring.

Replicate Lifecycle Logs to OS Log

You can replicate the Lifecycle Controller Logs to the OS logs from the time when the feature is enabled in iDRAC. This is similar to the System Event Log (SEL) replication performed by OpenManage Server Administrator. All events that have the **OS Log** option selected as the target (in the **Alerts** page, or in the equivalent RACADM or WSMAN interfaces) are replicated in the OS log using the iDRAC Service Module. The default set of logs to be included in the OS logs is the same as configured for SNMP alerts or traps.

iDRAC Service Module also logs the events that have occurred when the operating system is not functioning. The OS logging performed by iDRAC Service Module follows the IETF syslog standards for Linux based operating systems.

If OpenManage Server Administrator is installed, this monitoring feature is disabled to avoid duplicate SEL entries in the OS log.

Automatic System Recovery Options

The ASR feature is a hardware-based timer. If a hardware failure occurs, the Health Monitor may not be called, but the server is reset as if the power switch was activated. ASR is implemented using a "heartbeat" timer that continuously counts down. The Health Monitor frequently reloads the counter to prevent it from counting down to zero. If the ASR counts down to zero, it is assumed that the operating system has locked up and the system automatically attempts to reboot.

You can perform automatic system recovery operations such as reboot, power cycle, or power off the server after a specified time interval. This feature is enabled only if the operating system watchdog timer is disabled. If OpenManage Server Administrator is installed, this monitoring feature is disabled to avoid duplicate watchdog timers.

Windows Management Instrumentation Providers

WMI is a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification. WMI is Microsoft's implementation of the Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards from the Distributed Management Task Force (DMTF) to manage Server hardware, operating systems and applications. WMI Providers helps to integrate with Systems Management Consoles such as Microsoft System Center and enables scripting to manage Microsoft Windows Servers.

You can enable or disable the WMI option in iDRAC. iDRAC exposes the WMI classes through the iDRAC Service Module providing the server's health information. By default, WMI information feature is enabled. The iDRAC Service Module exposes the WSMAN monitored classes in iDRAC through WMI. The classes are exposed in the root/cimv2/dcim namespace.

The classes can be accessed using any of the standard WMI client interfaces. For more information, see the profile documents.

The following example is using the DCIM_account class to illustrate the capability that WMI information feature provides in iDRAC Service Module. For the details of the supported classes and profiles, see the WSMAN profiles documentation available at Dell Tech Center.

CIM Interface	WinRM	WMIC	PowerShell
Enumerate instances of a class	`winrm e wmi/root/cimv2/dcim/dcim_account`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account`	`Get-WmiObject dcim_account -namespace root/cimv2/dcim`
Get a specific instance of a class	`winrm g wmi/root/cimv2/dcim/DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.2+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name="iDRAC.Embedded.1#Users.16"`	`Get-WmiObject -Namespace root\cimv2\dcim -Class dcim_account -filter "Name='iDRAC.Embedded.1#Users.16'"`
Get associated instances of an instance	`winrm e wmi/root/cimv2/dcim/* -dialect:association -filter:{object=DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name='iDRAC.Embedded.1#Users.2' ASSOC`	`Get-Wmiobject -Query "ASSOCIATORS OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPC`

CIM Interface	WinRM	WMIC	PowerShell
	1+SystemCreationClassName=DCIM_SPComputerSystem +SystemName=systemmc}		omputerSystem',SystemName='systemmc' }" -namespace root/cimv2/dcim
Get references of an instance	winrm e wmi/root/cimv2/dcim/* -dialect:association –associations -filter: {object=DCIM_Account? CreationClassName=DCIM_Account +Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem +SystemName=systemmc}	Not applicable	Get-Wmiobject -Query "REFERENCES OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc' }" -namespace root/cimv2/dcim

Co-existence of OpenManage Server Administrator and iDRAC Service Module

In a system, both OpenManage Server Administrator and the iDRAC Service Module can co-exist and continue to function correctly and independently.

If you have enabled the monitoring features during the iDRAC Service Module installation, then after the installation is complete if the iDRAC Service Module detects the presence of OpenManage Server Administrator, it disables the set of monitoring features that overlap. If OpenManage Server Administrator is running, the iDRAC Service Module disables the overlapping monitoring features after logging to the OS and iDRAC.

When you re-enable these monitoring features through the iDRAC interfaces at a later time, the same checks are performed and the features are enabled depending on whether OpenManage Server Administrator is running or not.

Using iDRAC Service Module From iDRAC Web Interface

To use the iDRAC Service Module from the iDRAC Web interface:

1. Go to **Overview → Server → Service Module**.
   The **iDRAC Service Module Setup** page is displayed.
2. You can view the following:
   - Installed iDRAC Service Module version on the host operating system
   - Connection status of the iDRAC Service Module with iDRAC.
3. To perform out-of-band monitoring functions, select one or more of the following options:
   - **OS Information** — View the operating system information.
   - **Replicate Lifecycle Log in OS Log** — Include Lifecycle Controller logs to operating system logs. This option is disabled if OpenManage Server Administrator is installed on the system.

- **WMI Information** — Include WMI information.
- **Auto System Recovery Action** — Perform auto recovery operations on the system after a specified time (in seconds):
  - **Reboot**
  - **Power Off System**
  - **Power Cycle System**

  This option is disabled if OpenManage Server Administrator is installed on the system.

Using iDRAC Service Module From RACADM

To use the iDRAC Service Module from RACADM, use the objects in the **ServiceModule** group. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

20

Using USB Port for Server Management

In Dell PowerEdge 12th generation servers, all USB ports are dedicated to the server. With the 13th generation of servers, one of the front panel USB port is used by iDRAC for management purposes such as pre-provisioning and troubleshooting. The port has an icon to indicate that it is a management port. All 13th generation servers with LCD panel support this feature. This port is not available in a few of the 200-500 model variations without the LCD panel. In such cases, you may prefer to use these ports for the server operating system.

When the USB port is used by iDRAC:

- The USB network interface enables use of existing out-of-band remote management tools from a portable device such as laptop by using a USB type A/A cable connected to iDRAC. The iDRAC is assigned the IP address (169.254.0.3) and the laptop is assigned the IP 169.254.0.4.
- You can store a server configuration profile in the USB device and update the server configuration from the USB device.

NOTE: This feature is supported on:

- USB devices having FAT file system and has single partition.
- All Dell Windows 8 and Windows RT tablets, including the XPS 10 and The Venue Pro 8. For those devices that have USB-mini port such as the XPS 10 and the Venue Pro 8, you must use the On-The-Go (OTG) dongle and a Type-A/A cable together for it to work.

Related Links

Configuring iDRAC Using Server Configuration Profile on USB Device
Accessing iDRAC Interface over Direct USB Connection

Accessing iDRAC Interface over Direct USB Connection

In 13th generation servers, the new iDRAC direct feature allows you to directly connect your laptop or PC USB port to the iDRAC USB port. This allows you to interact directly with iDRAC interfaces (such as Web interface, RACADM, and WSMAN) for advanced server management and servicing.

You must use a Type A/A cable to connect the laptop (a USB Host Controller) to the iDRAC in the server (a USB device).

When iDRAC behaves as a USB device and the management port mode is set to Automatic, the USB port is always used by iDRAC. The port does not switch automatically to OS.

To access the iDRAC interface over the USB port:

1. Turn off any wireless networks and disconnect from any other hard wired network.
2. Make sure that the USB port is enabled. For more information, see Configuring USB Management Port Settings.
3. Connect a Type A/A cable from the laptop to iDRAC's USB port.

Management LED (if present) turns green and remains ON for two seconds.

4. Wait for the IP address to be assigned to the laptop (169.254.0.4) and iDRAC (169.254.0.3). This may take several seconds.
5. Start using iDRAC network interfaces such as Web interface, RACADM, or WS-Man.
6. When iDRAC is using the USB port, LED blinks indicating activity. Blink frequency is four per second.
7. After using, disconnect the cable.

   The LED turns off.

Configuring iDRAC Using Server Configuration Profile on USB Device

With the new iDRAC Direct feature, you can configure iDRAC at-the-server. First configure the USB Management port settings in iDRAC, insert the USB device that has the server configuration profile, and then import the server configuration profile from the USB device to iDRAC.

NOTE: PowerEdge systems that do not have the LCD and the LED panel does not support the USB key.

Related Links

Configuring USB Management Port Settings
Importing Server Configuration Profile From USB Device

Configuring USB Management Port Settings

You can configure the USB port in iDRAC:

- Enable or disable a server's USB port using BIOS setup. When you set it to either **All Ports off** or **Front ports off**, iDRAC also disables the managed USB port. You can view the port status using in the iDRAC interfaces. If the status is disabled:
  - iDRAC does not process a USB device or host connected to the managed USB port.
  - You can modify the managed USB configuration, but the settings do not have effect until the front panel USB ports are enabled in BIOS.
- Set the USB Management Port Mode that determines whether the USB port is used by iDRAC or the server OS:
  - Automatic (Default): If a USB device is not supported by iDRAC or if the server configuration profile is not present on the device, the USB port is detached from iDRAC and attached to the server. When a device is removed from the server, the port configuration is reset and is for use by iDRAC.
  - Standard OS Use: USB device is always used by the operating system.
  - iDRAC Direct Only: USB device is always used by iDRAC.

You must have Server Control privilege to configure the USB management port.

When a USB device is connected, the System Inventory page displays the USB device information under the Hardware Inventory section.

An event is logged in the Lifecycle Controller logs when:

- The device is in Automatic or iDRAC mode and USB device is inserted or removed.
- USB Management Port Mode is modified.

- Device is automatically switched from iDRAC to OS.
- Device is ejected from iDRAC or OS

When a device exceeds its power requirements as allowed by USB specification, the device is detached and an over-current event is generated with the following properties:

- Category : System Health
- Type: USB device
- Severity: Warning
- Allowed notifications: Email, SNMP trap, remote syslog and WS-Eventing.
- Actions: None.

An error message is displayed and logged to Lifecycle Controller log when:

- You try to configure the USB management port without the Server Control user privilege.
- A USB device is in use by iDRAC and you attempt to modify the USB Management Port Mode.
- A USB device is in use by iDRAC and you remove the device.

Configuring USB Management Port Using Web interface

To configure the USB port:

1. In the iDRAC Web interface, go to **Overview → Hardware → USB Management Port**.
   The **Configure USB Management Port** page is displayed.
2. From the **USB Management Port Mode** drop-down menu, select any of the following options:
   - **Automatic** — USB Port is used by iDRAC or the server's operating system.
   - **Standard OS Use** — USB port is used by the server OS.
   - **iDRAC Direct only** — USB pot is used by iDRAC.
3. From the iDRAC Managed: USB XML Configuration drop-down menu, select options to configure a server by importing XML configuration files stored on a USB drive:
   - **Disabled**
   - **Enabled only when server has default credential settings**
   - **Enabled**

   For information about the fields, see the *iDRAC Online Help*.
4. Click **Apply** to apply the settings.

Configuring USB Management Port Using RACADM

To configure the USB management port, use the following RACADM sub commands and objects:

- To view the USB port status:
  `racadm get iDRAC.USB.ManagementPortStatus`
- To view the USB port configuration:
  `racadm get iDRAC.USB.ManagementPortMode`
- To modify the USB port configuration:
  `racadm set iDRAC.USB.ManagementPortMode <Automatic|OS|iDRAC|>`
- To view USB device inventory:
  `racadm hwinventory`
- To set up over current alert configuration:
  `racadm eventfilters`

For more information, see the *iDRAC RACADM Command Line Interface Reference Guide* available at **dell.com/esmmanuals.com**.

Configuring USB Management Port Using iDRAC Settings Utility

To configure the USB port:

1. In the iDRAC Settings Utility, go to **Media and USB Port Settings**.
   The **iDRAC Settings Media and USB Port Settings** page is displayed.
2. From the **USB Management Port Mode** drop-down menu, do the following:
   - **Automatic** — USB Port is used by iDRAC or the server's operating system.
   - **Standard OS Use** — USB port is used by the server OS.
   - **iDRAC Direct only** — USB pot is used by iDRAC.
3. From the **iDRAC Direct: USB Configuration XML** drop-down menu, select options to configure a server by importing server configuration profile stored on a USB drive:
   - **Disabled**
   - **Enabled while server has default credential settings only**
   - **Enabled**

   For information about the fields, see the *iDRAC Settings Utility Online Help*.
4. Click **Back**, click **Finish** and then click **Yes** to apply the settings.

Importing Server Configuration Profile From USB Device

Make sure to create a directory in root of the USB device called **System_Configuration_XML** which contains both the **config.xml** and **control.xml** files.:

- Server Configuration Profile is in the **System_Configuration_XML** sub-directory under the USB device root directory. This file includes all the attribute-value pairs of the server. This includes attributes of iDRAC, PERC, RAID, and BIOS. You can edit this file to configure any attribute on the server. The file name can be **<servicetag>-config.xml**, **<modelnumber>-config.xml**, or **config.xml**.
- Control XML file – Includes parameters to control the import operation and does not have attributes of iDRAC or any other component in the system. The control file contain three parameters:
  - ShutdownType – Graceful, Forced, No Reboot.
  - TimeToWait (in secs) – 300 minimum and 3600 maximum.
  - EndHostPowerState – on/off.

Example of **control.xml** file:

```
<InstructionTable>       <InstructionRow>
<InstructionType>Configuration XML import Host control Instruction</
InstructionType>                  <Instruction>ShutdownType</
Instruction>                 <Value>NoReboot</Value>
<ValuePossibilities>Graceful,Forced,NoReboot</ValuePossibilities>       </
InstructionRow>       <InstructionRow>
<InstructionType>Configuration XML import Host control Instruction</
InstructionType>                  <Instruction>TimeToWait</
Instruction>                 <Value>300</Value>
<ValuePossibilities>Minimum value is 300 -Maximum value is 3600 seconds.</
ValuePossibilities>       </InstructionRow>
<InstructionRow>                  <InstructionType>Configuration XML import
Host control Instruction</InstructionType>
<Instruction>EndHostPowerState</Instruction>                <Value>On</
```

```
Value>                  <ValuePossibilities>On,Off</ValuePossibilities>       </
InstructionRow></InstructionTable>
```

You must have Server Control privilege to perform this operation.

To import the server configuration profile from the USB device to iDRAC:

1. Configure the USB management port:
   - Set **USB Management Port Mode** to **Automatic** or **iDRAC**.
   - Set **iDRAC Managed: USB XML Configuration** to **Enabled with default credentials** or **Enabled**.
2. Insert the USB key (that has the **configuration.xml** and the **control.xml** file) to the iDRAC USB port.
3. The server configuration profile is discovered on the USB device in the **System_Configuration_XML** sub-directory under the USB device root directory. It is discovered in the following sequence:
   - **<servicetag>-config.xml**
   - **<modelnum>-config.xml**
   - **config.xml**
4. A server configuration profile import job starts.

   If the profile is not discovered, then the operation stops.

   If **iDRAC Managed: USB XML Configuration** was set to **Enabled with default credentials** and the BIOS setup password is not null or if one of the iDRAC user accounts have been modified, an error message is displayed and the operation stops.
5. LCD panel and LED (if present) displays the status that an import job has started.
6. If there is a configuration that needs to be staged and the **Shut Down Type** is specified as **No Reboot** is specified in the control file, then you must reboot the server for the settings to be configured. Else, server is rebooted and the configuration is applied. Only when the server was already powered down, then the staged configuration is applied even if the **No Reboot** option is specified.
7. After the import job is complete, the LCD/LED indicates that the job is complete. If a reboot is required, LCD displays the job status as “Paused waiting on reboot”.
8. If the USB device is left inserted on the server, the result of the import operation is recorded in the **results.xml** file in the USB device.

LCD Messages

If the LCD panel is available, it displays the following messages in a sequence:

1. Importing – When the server configuration profile is being copied from the USB device.
2. Applying — When the job is in-progress.
3. Completed — When the job has completed successfully.
4. Completed with errors — When the job has completed with errors.
5. Failed — When the job has failed.

For more details, see the results file on the USB device.

LED Blinking Behavior

If the USB LED is present, it indicates the following:

- Solid green – When the server configuration profile is being copied from the USB device.
- Blinking green – When the job is in-progress.

- Solid green – When the job has completed successfully.

Logs and Results File

The following information is logged for the import operation:

- Automatic import from USB is logged in the Lifecycle Controller log file.
- If the USB device is left inserted, the job results are recorded in the Results file located in the USB key.

A Result file named **Results.xml** is updated or created in the subdirectory with the following information:

- Service tag – Data is recorded after the import operation has either returned a job ID or returned an error.
- Job ID – Data is recorded after the import operation has returned a job ID.
- Start Date and Time of Job - Data is recorded after the import operation has returned a job ID.
- Status – Data is recorded when the import operation returns an error or when the job results are available.

21

Using iDRAC Quick Sync

A few 13th generation Dell PowerEdge servers have the Quick Sync bezel that supports the Quick Sync feature. This feature enables at-the-server management with a mobile device. This allows you to view inventory and monitoring information and configure basic iDRAC settings (such as root credential setup and configuration of the first boot device) using the mobile device.

You can configure iDRAC Quick Sync access for your mobile device (example, OpenManage Mobile) in iDRAC. You must install the OpenManage Mobile application on the mobile device to manage server using iDRAC Quick Sync interface.

NOTE: This feature is currently supported on mobile devices with Android operating system.

In the current release, this feature is available only with Dell PowerEdge R730, R730xd, and R630 rack servers. For these servers, you can optionally purchase a bezel. Therefore, it is a hardware up-sell and the feature capabilities are not dependent on iDRAC software licensing.

The iDRAC Quick Sync hardware includes the following:

- Activation button – You must press this button to activate the Quick Sync interface. In a closely stacked rack infrastructure, this helps to identify and enable the server that is the target for communication. The Quick Sync feature is inactive after being idle for a configurable amount of time (default is 30 seconds) or when pressed to de-activate.
- Activity LED – If Quick Sync is disabled, the LED blinks a few times and then turns off. Also, if the configurable inactivity timer is triggered, the LED turns off and deactivates the interface.

After configuring iDRAC Quick Sync settings in iDRAC, hold the mobile device close to the server, that is, less than two centimeters away and read pertinent information about the server and perform iDRAC configuration settings.

Using OpenManage Mobile, you can:

- View inventory information:
- View monitoring information:
- Configure the basic iDRAC network settings

For more information about OpenManage Mobile, see the *OpenManage Mobile User's Guide* at **dell.com/support/manuals**.

Related Links

Configuring iDRAC Quick Sync
Using Mobile Device to View iDRAC Information

Configuring iDRAC Quick Sync

Using iDRAC Web interface or RACADM, you can configure iDRAC Quick Sync feature to allow access to the mobile device:

- Access — You can specify any of the following options to configure the access state of iDRAC Quick Sync feature:
  - Read-Write — Default status.
  - Read-write access – Allows you to configure the basic iDRAC settings.
  - Read-only access – Allows you to view inventory and monitoring information.
  - Disabled access – Does not allow you to view information and configure settings.
- Time-out — You can enable or disable iDRAC Quick Sync inactivity timer:
  - If enabled, you can specify a time after which the Quick Sync mode is turned off. To turn on, press the activation button again.
  - If disabled, the timer does not allow you to enter a time-out period.
- Time-out Limit — Allows you specify the time after which the Quick Sync mode is disabled. The default value is 30 seconds.

You must have Server Control privilege to configure the settings. A server reboot is not required for the settings to take effect.

An entry is logged to the Lifecycle Controller log when the configuration is modified.

Configuring iDRAC Quick Sync Settings Using Web Interface

To configure iDRAC Quick Sync:

1. In the iDRAC Web interface, go to **Overview → Hardware → Front Panel**.
2. In the **iDRAC Quick Sync** section, from the **Access** drop-down menu, select one of the following to provide access to the Andriod mobile device:
   - Read-write
   - Read-only
   - Disabled
3. Enable the Timer.
4. Specify the Timeout value.
   For more information about the fields, see the *iDRAC Online Help*.
5. Click **Apply** to apply the settings.

Configuring iDRAC Quick Sync Settings Using RACADM

To configure the iDRAC Quick Sync feature, use the racadm objects in the **System.QuickSync** group. For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Configuring iDRAC Quick Sync Settings Using iDRAC Settings Utility

To configure iDRAC Quick Sync:

1. In the iDRAC Settings Utility, go to **Front Panel Security**.
   The **iDRAC Settings Front Panel Security** page is displayed.
2. In the **iDRAC Quick Sync** section:
   - Specify the access level.
   - Enable Timeout.
   - Specify the User Defined Timeout Limit (15 seconds to 3600 seconds).

   For more information about the fields, see the *iDRAC Online Help*.
3. Click **Back**, click **Finish**, and then click **Yes**.
   The settings are applied.

Using Mobile Device to View iDRAC Information

To view iDRAC information from the mobile device, see the *OpenManage Mobile User's Guide* available at **dell.com/support/manuals** for the steps.

22

Deploying Operating Systems

You can use any of the following utilities to deploy operating systems to managed systems:

- Virtual Media Command Line Interface (CLI)
- Virtual Media Console
- Remote File Share

Related Links

Deploying Operating System Using VMCLI
Deploying Operating System Using Remote File Share
Deploying Operating System Using Virtual Media

Deploying Operating System Using VMCLI

Before you deploy the operating system using the vmdeploy script, make sure that:

- VMCLI utility is installed on the management station.
- **Configure User** and **Access Virtual Media** privileges for iDRAC are enabled for the user.
- IPMItool is installed on the management station.

  NOTE: IPMItool does not work if IPv6 is configured either on the managed system or the management station.
- iDRAC is configured on the target remote systems.
- System is able to boot from the image file.
- IPMI Over LAN is enabled in iDRAC.
- Network share contains drivers and operating system bootable image file, in an industry standard format such as **.img** or **.iso**.

  NOTE: While creating the image file, follow standard network-based installation procedures, and mark the deployment image as read-only to make sure that each target system boots and executes the same deployment procedure.
- Virtual Media status is in attach state.
- **vmdeploy** script is installed on the management station. Review this sample vmdeploy script included with VMCLI. The script describes how to deploy the operating system to remote systems in the network. It internally uses VMCLI and IPMItool.

  NOTE: The **vmdeploy** script is dependent on some support files in the directory during installation. To use the script from another directory, copy all the files with it. If the IPMItool utility is not installed, copy the utility along with the other files.

To deploy the operating system on target remote systems:

1. List the iDRAC IPv4 addresses of the target remote systems, in the **ip.txt** text file. List one IPv4 address per line.
2. Insert a bootable operating system, CD or DVD, into the management station drive.

3. Open a command prompt with administrator privileges and run the **vmdeploy** script:

```
vmdeploy.bat -r <iDRAC-IPAddress or file> -u <iDRAC-user> -p <iDRAC-user-passwd> [ -f {<floppy-image> | < device-name>} | -c { <device-name>|<image-file>} ] [-i <DeviceID>]
```

NOTE: vmdeploy does not support IPv6, since IPv6 does not support the IPMI tool.

NOTE: The vmdeploy script processes the `-r` option slightly differently than the `vmcli -r` option. If the argument to the `-r` option is the name of an existing file, the script reads iDRAC IPv4 or IPv6 addresses from the specified file and runs the utility once for each line. If the argument to the `-r` option is not a filename, then it should a single iDRAC address. In this case, the **-r** works as described for the VMCLI utility.

The following table describes the vmdeploy command parameters.

Table 32. vmdeploy Command Parameters

Parameter	Description
`<iDRAC-user>`	iDRAC user name. It must have the following attributes: • Valid user name • iDRAC Virtual Media User permission If iDRAC authentication fails, an error message is displayed and the command is terminated.
`<iDRAC-ip | file>`	iDRAC IP address or the file containing the iDRAC IP address.
`<iDRAC-user-password>` or `<iDRAC-passwd>`	Password for the iDRAC user. If iDRAC authentication fails, an error message is displayed and the command is terminated.
`-c {<device-name> | <image-file>}`	Path to an ISO9660 image of the operating system installation CD or DVD.
`<floppy-device>`	Path to the device containing the operating system installation CD, DVD, or Floppy.
`<floppy-image>`	Path to a valid floppy image.
`<Device ID>`	ID of the device to boot once.

Related Links

Configuring Virtual Media

Configuring iDRAC

Deploying Operating System Using Remote File Share

Before you deploy the operating system using Remote File Share (RFS), make sure that:

- **Configure User** and **Access Virtual Media** privileges for iDRAC are enabled for the user.

- Network share contains drivers and operating system bootable image file, in an industry standard format such as **.img** or **.iso**.

  NOTE: While creating the image file, follow standard network-based installation procedures, and mark the deployment image as read-only to make sure that each target system boots and executes the same deployment procedure.

To deploy an operating system using RFS:

1. Using Remote File Share (RFS), mount the ISO or IMG image file to the managed system through NFS or CIFS.
2. Go to **Overview → Setup → First Boot Device**.
3. Set the boot order in the **First Boot Device** drop-down list to **Remote File Share**.
4. Select the **Boot Once** option to enable the managed system to reboot using the image file for the next instance only.
5. Click **Apply**.
6. Reboot the managed system and follow the on-screen instructions to complete the deployment.

Related Links

Managing Remote File Share
Setting First Boot Device

Managing Remote File Share

Using Remote File Share (RFS) feature, you can set an ISO or IMG image file on a network share and make it available to the managed server's operating system as a virtual drive by mounting it as a CD or DVD using NFS or CIFS. RFS is a licensed feature.

NOTE: IPv4 address is supported for both CIFS and NFS. IPv6 address is supported only for CIFS.

Remote file share supports only **.img** and **.iso** image file formats. A **.img** file is redirected as a virtual floppy and a **.iso** file is redirected as a virtual CDROM.

You must have Virtual Media privileges to perform an RFS mounting.

NOTE: If ESXi is running on the managed system and if you mount a floppy image (**.img**) using RFS, the connected floppy image is not available to the ESXi operating system.

RFS and Virtual Media features are mutually exclusive.

- If the Virtual Media client is not active, and you attempt to establish an RFS connection, the connection is established and the remote image is available to the host operating system.
- If the Virtual Media client is active, and you attempt to establish an RFS connection, the following error message is displayed:

  Virtual Media is detached or redirected for the selected virtual drive.

The connection status for RFS is available in iDRAC log. Once connected, an RFS-mounted virtual drive does not disconnect even if you log out from iDRAC. The RFS connection is closed if iDRAC is reset or the network connection is dropped. The Web interface and command-line options are also available in CMC and iDRAC to close the RFS connection. The RFS connection from CMC always overrides an existing RFS mount in iDRAC.

NOTE: iDRAC vFlash feature and RFS are not related.

If you update the iDRAC firmware from version 1.30.30 to 1.50.50 firmware while there is an active RFS connection and the Virtual Media Attach Mode is set to **Attach** or **Auto Attach**, the iDRAC attempts to re-establish the RFS connection after the firmware upgrade is completed and the iDRAC reboots.

If you update the iDRAC firmware from version 1.30.30 to 1.50.50 firmware while there is an active RFS connection and the Virtual Media Attach Mode is set to **Detach**, the iDRAC does not attempt to re-establish the RFS connection after the firmware upgrade is completed and the iDRAC reboots.

Configuring Remote File Share Using Web Interface

To enable remote file sharing:

1. In iDRAC Web interface, go to **Overview** → **Server** → **Attached Media**.
   The **Attached Media** page is displayed.
2. Under **Attached Media**, select **Attach** or **Auto Attach**.
3. Under **Remote File Share**, specify the image file path, domain name, user name, and password. For information about the fields, see the *iDRAC Online Help*.
   Example for image file path:
   - CIFS — //<IP to connect for CIFS file system>/<file path>/<image name>
   - NFS —< IP to connect for NFS file system>/<file path>/<image name>

   NOTE: Both '/' or '\' characters can be used for the file path.

   CIFS supports both IPv4 and IPv6 addresses but NFS supports only IPv4 address.

   If you are using NFS share, make sure that you provide the exact <file path> and <image name> as it is case-sensitive.

   The following characters are supported for image file path, user name and password:
   - Uppercase characters
   - Lowercase characters
   - Digits from 0–9
   - _, -, ?, <, >, /, \, :, *, |, @
   - Whitespace

   NOTE: While specifying the network share settings, it is recommended to avoid special characters for user name and password or percent encode the special characters.
4. Click **Apply** and then click **Connect**.
   After the connection is established, the **Connection Status** displays **Connected**.

   NOTE: Even if you have configured remote file sharing, the Web interface does not display user credential information due to security reasons.

   For Linux distributions, this feature may require a manual mount command when operating at runlevel init 3. The syntax for the command is:

   ```
   mount /dev/OS_specific_device / user_defined_mount_point
   ```

   where, `user_defined_mount_point` is any directory you choose to use for the mount similar to any mount command.

For RHEL, the CD device (**.iso** virtual device) is `/dev/scd0` and floppy device (**.img** virtual device) is `/dev/sdc`.

For SLES, the CD device is `/dev/sr0` and the floppy device is /dev/sdc. To make sure that the correct device is used (for either SLES or RHEL), when you connect the virtual device, on the Linux OS you must immediately run the command:

```
tail /var/log/messages | grep SCSI
```

This displays the text that identifies the device (example, SCSI device sdc). This procedure also applies to Virtual Media when you are using Linux distributions in runlevel init 3. By default, the virtual media is not auto-mounted in init 3.

Configuring Remote File Share Using RACADM

To configure remote file share using RACADM, use:

```
racadm remoteimage

racadm remoteimage <options>
```

Options are:

`-c` : connect image

`-d` : disconnect image

`-u` <username>: username to access the network share

`-p` <password>: password to access the network share

`-l` <image_location>: image location on the network share; use double quotes around the location. See examples for image file path in Configuring Remote File Share Using Web Interface section

`-s` : display current status

NOTE: All characters including alphanumeric and special characters are allowed as part of user name, password, and image_location except the following characters: ' (single quote), "(double quote), ,(comma), < (less than), and > (greater than).

Deploying Operating System Using Virtual Media

Before you deploy the operating system using Virtual Media, make sure that:

- Virtual Media is in *Attached* state for the virtual drives to appear in the boot sequence.
- If Virtual Media is in *Auto Attached* mode, the Virtual Media application must be launched before booting the system.
- Network share contains drivers and operating system bootable image file, in an industry standard format such as **.img** or **.iso**.

To deploy an operating system using Virtual Media:

1. Do one of the following:
   - Insert the operating system installation CD or DVD into the management station CD or DVD drive.

- Attach the operating system image.

2. Select the drive on the management station with the required image to map it.
3. Use one of the following methods to boot to the required device:
   - Set the boot order to boot once from **Virtual Floppy** or **Virtual CD/DVD/ISO** using the iDRAC Web interface.
   - Set the boot order through **System Setup** → **System BIOS Settings** by pressing <F2> during boot.
4. Reboot the managed system and follow the on-screen instructions to complete the deployment.

Related Links

Configuring Virtual Media
Setting First Boot Device
Configuring iDRAC

Installing Operating System From Multiple Disks

1. Unmap the existing CD/DVD.
2. Insert the next CD/DVD into the remote optical drive.
3. Remap the CD/DVD drive.

Deploying Embedded Operating System On SD Card

To install an embedded hypervisor on an SD card:

1. Insert the two SD cards in the Internal Dual SD Module (IDSDM) slots on the system.
2. Enable SD module and redundancy (if required) in BIOS.
3. Verify if the SD card is available on one of the drives when you <F11> during boot.
4. Deploy the embedded operating system and follow the operating system installation instructions.

Related Links

About IDSDM
Enabling SD Module and Redundancy in BIOS

Enabling SD Module and Redundancy in BIOS

To enable SD module and redundancy in BIOS:

1. Press <F2> during boot.
2. Go to **System Setup** → **System BIOS Settings** → **Integrated Devices**.
3. Set the **Internal USB Port** to **On**. If it is set to **Off**, the IDSDM is not available as a boot device.
4. If redundancy is not required (single SD card), set **Internal SD Card Port** to **On** and **Internal SD Card Redundancy** to **Disabled**.
5. If redundancy is required (two SD cards), set **Internal SD Card Port** to **On** and **Internal SD Card Redundancy** to **Mirror**.
6. Click **Back** and click **Finish**.
7. Click **Yes** to save the settings and press <Esc> to exit **System Setup**.

About IDSDM

Internal Dual SD Module (IDSDM) is available only on applicable platforms. IDSDM provides redundancy on the hypervisor SD card by using another SD card that mirrors the first SD card's content.

Either of the two SD cards can be the master. For example, if two new SD cards are installed in the IDSDM, SD1 is active (master) card and SD2 is the standby card. The data is written on both the cards, but the data is read from SD1. At any time if SD1 fails or is removed, SD2 automatically become the active (master) card.

You can view the status, health, and the availability of IDSDM using iDRAC Web Interface or RACADM. The SD card redundancy status and failure events are logged to SEL, displayed on the front panel, and PET alerts are generated if alerts are enabled.

Related Links

Viewing Sensor Information

23

Troubleshooting Managed System Using iDRAC

You can diagnose and troubleshoot a remote managed system using:

- Diagnostic console
- Post code
- Boot and crash capture videos
- Last system crash screen
- System event logs
- Lifecycle logs
- Front panel status
- Trouble indicators
- System health

Related Links

Using Diagnostic Console
Scheduling Remote Automated Diagnostics
Viewing Post Codes
Viewing Boot and Crash Capture Videos
Viewing Logs
Viewing Last System Crash Screen
Viewing Front Panel Status
Hardware Trouble Indicators
Viewing System Health
Generating Technical Support Report

Using Diagnostic Console

iDRAC provides a standard set of network diagnostic tools that are similar to the tools included with Microsoft Windows or Linux-based systems. Using iDRAC Web interface, you can access the network debugging tools.

To access Diagnostics Console:

1. In the iDRAC Web interface, go to **Overview** → **Server** → **Troubleshooting** → **Diagnostics**.
2. In the **Command** text box, enter a command and click **Submit**. For information about the commands, see the *iDRAC Online Help*.

   The results are displayed on the same page.

Scheduling Remote Automated Diagnostics

You can remotely invoke automated offline diagnostics on a server as a one-time event and return the results. If the diagnostics require a reboot, you can reboot immediately or stage it for a subsequent reboot or maintenance cycle (similar to updates). When diagnostics are run, the results are collected and stored in the internal iDRAC storage. You can then export the results to an NFS or CIFS network share using the `diagnostics export` racadm command. You can also run diagnostics using the appropriate WSMAN command(s). For more information, see the WSMAN documentation.

You must have iDRAC Express license to use remote automated diagnostics.

You can perform the diagnostics immediately or schedule it on a particular day and time, specify the type of diagnostics, and the type of reboot.

For the schedule, you can specify the following:

- Start time – Run the diagnostic at a future day and time. If you specify TIME NOW, the diagnostic is run on the next reboot.
- End time - Run the diagnostic until a date and time after the Start time. If it is not started by End time, it is marked as failed with End time expired. If you specify TIME NA, then the wait time is not applicable.

The types of diagnostic tests are:

- Express test
- Extended test
- Both in a sequence

The types of reboot are:

- Power cycle system
- Graceful shutdown (waits for operating system to turn off or for system restart)
- Forced Graceful shutdown (signals operating system to turn off and waits for 10 minutes. If the operating system does not turn off, the iDRAC power cycles the system)

Only one diagnostic job can be scheduled or run at one time. A diagnostic job can complete successfully, complete with error, or is unsuccessful. The diagnostic events including the results are recorded in Lifecycle Controller log. You can retrieve the results of the last diagnostic execution using remote RACADM or WSMAN.

You can export the diagnostic results of the last completed diagnostics that were scheduled remotely to a network share such as CIFS or NFS. The maximum file size is 5 MB.

You can cancel a diagnostic job when the status of the job is Unscheduled or Scheduled. If the diagnostic is running, then restart the system to cancel the job.

Before you run the remote diagnostics, make sure that:

- Lifecycle Controller is enabled.
- You have Login and Server Control privileges.

Scheduling Remote Automated Diagnostics Using RACADM

To run the remote diagnostics and save the results on the local system, use the following command:

```
racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e
<Expiration Time>
```

To export the last run remote diagnostics results, use the following command:

```
racadm diagnostics export -f <file name> -l <NFS / CIFS share> -u <username> -p
<password>
```

For more information about the options, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Viewing Post Codes

Post codes are progress indicators from the system BIOS, indicating various stages of the boot sequence from power-on-reset, and allows you to diagnose any faults related to system boot-up. The **Post Codes** page displays the last system post code prior to booting the operating system.

To view the Post Codes, go to **Overview → Server → Troubleshooting → Post Code**.

The **Post Code** page displays the system health indicator, a hexadecimal code, and a description of the code.

Viewing Boot and Crash Capture Videos

You can view the video recordings of:

- Last three boot cycles — A boot cycle video logs the sequence of events for a boot cycle. The boot cycle videos are arranged in the order of latest to oldest.
- Last crash video — A crash video logs the sequence of events leading to the failure.

This is a licensed feature.

iDRAC records fifty frames during boot time. Playback of the boot screens occur at a rate of 1 frame per second. If iDRAC is reset, the boot capture video is not available as it is stored in RAM and is deleted.

NOTE: You must have Access Virtual Console or administrator privileges to playback the Boot Capture and Crash Capture videos.

To view the **Boot Capture** screen, click **Overview → Server → Troubleshooting → Video Capture**.

The **Video Capture** screen displays the video recordings. For more information, see the *iDRAC Online Help*.

Configuring Video Capture Settings

To configure the video capture settings:

1. In the iDRAC Web interface, go to **Overview → Server → Troubleshooting → Video Capture**.
   The **Video Capture** page is displayed.
2. From the **Video Capture Settings** drop-down menu, select any of the following options:
   - **Disable** — Boot capture is disabled.

- **Capture until buffer full** — Boot sequence is captured until the buffer size has reached.
- **Capture until end of POST** — Boot sequence is captured until end of POST.

3. Click **Apply** to apply the settings.

Viewing Logs

You can view System Event Logs (SELs) and Lifecycle logs. For more information, see Viewing System Event Log and Viewing Lifecycle Log .

Viewing Last System Crash Screen

The last crash screen feature captures a screenshot of the most recent system crash, saves, and displays it in iDRAC. This is a licensed feature.

To view the last crash screen:

1. Make sure that the last system crash screen feature is enabled.
2. In iDRAC Web interface, go to **Overview → Server → Troubleshooting → Last Crash Screen**.

   The **Last Crash Screen** page displays the last saved crash screen from the managed system.

   Click **Clear** to delete the last crash screen.

Related Links

Enabling Last Crash Screen

Viewing Front Panel Status

The Front Panel on the managed system summarizes the status of the following components in the system:

- Batteries
- Fans
- Intrusion
- Power Supplies
- Removable Flash Media
- Temperatures
- Voltages

You can view the status of the front panel of the managed system:

- For rack and tower servers: LCD front panel and system ID LED status or LED front panel and system ID LED status.
- For blade servers: Only system ID LEDs.

Viewing System Front Panel LCD Status

To view the LCD front panel status for applicable rack and tower servers, in iDRAC Web interface, go to **Overview → Hardware → Front Panel**. The **Front Panel** page displays.

The **Live Front Panel Feed** section displays the live feed of the messages currently being displayed on the LCD front panel. When the system is operating normally (indicated by Solid Blue color in the LCD front

panel), then both **Hide Error** and **UnHide Error** is grayed-out. You can hide or unhide the errors only for rack and tower servers.

To view LCD front panel status using RACADM, use the objects in the `System.LCD` group. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Related Links

Configuring LCD Setting

Viewing System Front Panel LED Status

To view the current system ID LED status, in iDRAC Web interface, go to **Overview → Hardware → Front Panel**. The **Live Front Panel Feed** section displays the current front panel status:

- Solid blue — No errors present on the managed system.
- Blinking blue — Identify mode is enabled (regardless of managed system error presence).
- Solid amber — Managed system is in failsafe mode.
- Blinking amber — Errors present on managed system.

When the system is operating normally (indicated by blue Health icon on the LED front panel), then both **Hide Error** and **UnHide Error** is grayed-out. You can hide or unhide the errors only for rack and tower servers.

To view system ID LED status using RACADM, use the **getled** command. For more information, see the *iDRAC8 RACADM Command Line Interface Reference Guide* available at **dell.com/support/manuals**.

Related Links

Configuring System ID LED Setting

Hardware Trouble Indicators

The hardware related problems are:

- Failure to power up
- Noisy fans
- Loss of network connectivity
- Hard drive failure
- USB media failure
- Physical damage

Based on the problem, use the following methods to correct the problem:

- Reseat the module or component and restart the system
- In case of a blade server, insert the module into a different bay in the chassis
- Replace hard drives or USB flash drives
- Reconnect or replace the power and network cables

If problem persists, see the *Hardware Owner's Manual* for specific troubleshooting information about the hardware device.

CAUTION: You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that came with the product.

Viewing System Health

iDRAC and CMC (for blade servers) Web interfaces display the status for the following:

- Batteries
- Fans
- Intrusion
- Power Supplies
- Removable Flash Media
- Temperatures
- Voltages
- CPU

In iDRAC Web interface, go to **Overview** → **Server** → **System Summary** → **Server Health** section.

To view CPU health, go to **Overview** → **Hardware** → **CPU**.

The system health indicators are:

- — Indicates a normal status.
- — Indicates a warning status.
- — Indicates a failure status.
- — Indicates an unknown status.

Click any component name in the **Server Health** section to view details about the component.

Generating Technical Support Report

If you have to work with Tech Support on an issue with a server but the security policies restrict direct internet connection, then you can provide Tech Support with necessary data to facilitate troubleshooting of the problem without having to install software or download tools from Dell and without having access to the Internet from the server operating system or iDRAC. You can send the report from an alternate system and be certain that the data collected from your server is not viewable by non-authorized individuals during the transmission to Tech Support.

You can generate a health report of the server and then export the report to a location on the management station (local) or to a shared network location such as Common Internet File System (CIFS) or Network File Share (NFS). You can then share this report directly with the Tech Support. To export to a network share such as CIFS or NFS, direct network connectivity to the iDRAC shared or dedicated network port is required.

The report is generated in the standard ZIP format. The report contains information that is similar to the information available in the DSET report such as:

- Hardware inventory for all components
- System, Lifecycle Controller, and component attributes
- Operating system and application information
- Active Lifecycle Controller logs (archived entries are not included)
- PCIe SSD logs
- Storage controller logs

After the report is generated, you can view the report. It contains a bunch of XML files and log files. The report must be shared with tech support to troubleshoot the issue.

Each time the data collection is performed, an event is recorded in the Lifecycle Controller log. The event includes information such as the interface used, the date and time of export, and iDRAC user name.

You can generate the OS Application and Logs report in two ways:

- Automatic — Using iDRAC Service Module that automatically invokes the OS Collector tool.
- Manual — By manually executing the OS Collector executable from the server OS. iDRAC exposes the OS Collector executable to the server OS as a USB device with label DRACRW.

NOTE:

- OS Collector tool is not applicable for Dell Precision PR7910 systems.
- The OS log collection feature is not supported on CentOS operating system.

Before generating the health report, make sure:

- Lifecycle Controller is enabled.
- Collect System Inventory On Reboot (CSIOR) is enabled.
- You have Login and Server Control privileges.

Related Links

Generating Technical Support Report Automatically
Generating Technical Support Report Manually

Generating Technical Support Report Automatically

If iDRAC Service Module is installed and running, you can automatically generate the Tech Support Report. The iDRAC Service Module invokes the appropriate OS collector file on the host operating system, collects the data, and transfers to iDRAC. You can then save the report to the required location.

Generating Tech Support Report Automatically Using iDRAC Web Interface

To generate the Tech Support Report automatically:

1. In the iDRAC Web interface, go to **Overview → Server → Troubleshooting → Tech Support Report**. The **Tech Support Report** page is displayed.
2. Select options for which you want to collect the data:
   - **Hardware**
   - **OS and Application Data**

NOTE: While specifying the network share settings, it is recommended to avoid special characters for user name and password or percent encode the special characters.

- Click **Advanced Export Options** to select the following additional options:
  - **RAID Controller Log**
  - **Enable Report Filtering** under **OS and Application Data**

Based on the options selected, the time taken to collect the data is displayed next to these options.

3. Select the **I agree to allow Technical Support to use this data** option and click **Export**.
4. After the iDRAC Service Module has completed transferring the OS and application data to iDRAC, it is packaged along with the hardware data and the final report is generated. A message appears to save the report.
5. Specify the location to save the tech support report.

Generating Technical Support Report Manually

When iSM is not installed, you can manually run the OS collector tool to generate the Technical Support Report. You must run OS Collector tool on the server OS to export the OS and application data. A virtual USB device labeled DRACRW appears in the server operating system. This device contains the OS Collector file that is specific for the host operating system. Run the file specific for the operating system from the server OS to collect and transfer the data to iDRAC. You can then export the report to a local or network shared location.

In 13th generation Dell PowerEdge systems, the OS collector DUP is installed in factory. However, if you determine that OS Collector is not present in iDRAC, then you can download the DUP file from the Dell support site and then upload the file to iDRAC using the Firmware Update process.

Before you manually generate the Technical Support Report using the OS collector tool, do the following on the host operating system:

- On Linux operating system: Check if the IPMI service is running. If it is not running, you must manually start the service. The following table provides the commands that you can use to check the IPMI service status and start the service (if required) for each Linux OS.

Linux Operating System	Command to Check the IPMI Service Status	Command to Start the IPMI Service
Red Hat Enterprise Linux 5 64-bit Red Hat Enterprise Linux 6 SUSE Linux Enterprise Server 11 CentOS 6 Oracle VM Oracle Linux 6.4	`$ service ipmi status`	`$ service ipmi start`
Red Hat Enterprise Linux 7	`$ systemctl status ipmi.service`	`$ systemctl start ipmi.service`

NOTE:

- CentOS is supported only for iDRAC Service Module 2.0 or later.
- If the IPMI modules are not present, then you can install the respective modules from the OS distribution media. The service starts once the installation is complete.

- On Windows operating system:
  - Check if the WMI service is running:
    * If WMI is stopped, OS Collector starts the WMI automatically and continues with the collection.
    * If WMI is disabled, OS Collector collection stops with an error message.
  - Check the appropriate privilege levels and make sure there is no Firewall or security settings that is preventing to get the registry or software data.

Generating Technical Support Report Manually Using iDRAC Web Interface

To generate the technical support report manually:

1. In the iDRAC Web interface, go to **Overview → Server → Troubleshooting → Tech Support Report**.
   The **Tech Support Report** page is displayed.
2. Select options for which you want to collect the data:
   - **Hardware** to export the report to a location on the local system
   - **OS and Application Data** to export the report to a network share and specify the network settings.

     NOTE: While specifying the network share settings, it is recommended to avoid special characters for user name and password or percent encode the special characters.
   - Click **Advanced Export Options** to select the following additional options:
     - **RAID Controller Log**
     - **Enable Report Filtering** under **OS and Application Data**

   Based on the options selected, the time taken to collect the data is displayed next to these options.

   If OS Collector tool was not run on the system, then the OS and Application Data option is grayed-out and it is not selectable. The message OS and Application Data (Timestamp: Never) is displayed.

   If OS Collector was run on the system in the past, then the timestamp displays when the operating system and application data was last collected: Last Collected: <timestamp>
3. Click **Attach OS Collector**.
   You are directed to access the host OS. A message asking you to launch Virtual Console is displayed.
4. After you launch the Virtual Console, click the pop-up message to run and use the OS Collector tool to collect the data.
5. Navigate to the DRACRW virtual USB device that is presented to the system by the iDRAC.
6. Invoke the OS Collector file appropriate for the host operating system:
   - For Windows, run **Windows_OSCollector_Startup.bat**.
   - For Linux, run **Linux_OSCollector_Startup.exe**.
7. After the OS collector has completed transferring the data to iDRAC, the USB device is removed automatically by iDRAC.
8. Return to the **Tech Support Report** page, click the **Refresh** icon to reflect the new timestamp.
9. To export the data, under **Export Location**, select **Local** or **Network**.
10. If you have selected **Network**, enter the network location details.

11. Select the **I agree to allow Technical Support to use this data** option and click **Export** to export the data to the specified location.

Generating Technical Support Report Manually Using RACADM

To generate the TSR using RACADM, use the **techsupreport** subcommand. For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals.com**.

Checking Server Status Screen for Error Messages

When a flashing amber LED is blinking, and a particular server has an error, the main Server Status Screen on the LCD highlights the affected server in orange. Use the LCD navigation buttons to highlight the affected server, then click the center button. Error and warning messages will be displayed on the second line. For the list of error messages displayed on the LCD panel, see the server's Owner's Manual.

Restarting iDRAC

You can perform a hard or soft iDRAC restart without turning off the server:

- Hard restart — On the server, press and hold the LED button for 15 seconds.
- Soft restart — Using iDRAC Web interface or RACADM.

Resetting iDRAC Using iDRAC Web Interface

To restart iDRAC, do one of the following in the iDRAC Web interface:

- Go to **Overview → Server → Summary**. Under **Quick Launch Tasks**, click **Reset iDRAC**.
- Go to **Overview → Server → Troubleshooting → Diagnostics**. Click **Reset iDRAC**.

Resetting iDRAC Using RACADM

To restart iDRAC, use the **racreset** command. For more information, see the *RACADM Reference Guide for iDRAC and CMC* available at **dell.com/support/manuals**.

Erasing System and User Data

You can erase system component(s) and user data for those components. The system components include:

- Lifecycle Controller Data
- Embedded Diagnostics
- Embedded OS Driver Pack
- BIOS reset to default
- iDRAC reset to default

Before performing system erase, make sure that:

- You have iDRAC Server Control privilege.
- Lifecycle Controller is enabled.

The Lifecycle Controller Data option erases any content such as the LC Log, configuration database, rollback firmware, factory as-shipped logs, and the configuration information from the FP SPI (or management riser).

NOTE: The Lifecycle Controller log contains the information about the system erase request and any information generated when the iDRAC restarts. Prior information does not exist.

You can delete individual or multiple system components using the **SystemErase** command:

```
racadm systemErase <BIOS | DIAG | DRVPACK | LCDATA | IDRAC >
```

where,

- BIOS — BIOS reset to default
- DIAG — Embedded Diagnostics
- DRVPACK— Embedded OS Driver Pack
- LCDATA — Clear the Lifecycle Controller Data
- IDRAC — iDRAC reset to default

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

Resetting iDRAC to Factory Default Settings

You can reset iDRAC to the factory default settings using the iDRAC Settings utility or the iDRAC Web interface.

Resetting iDRAC to Factory Default Settings Using iDRAC Web Interface

To reset iDRAC to factory default settings using the iDRAC Web interface:

1. Go to **Overview → Server → Troubleshooting → Diagnostics**.
   The **Diagnostics Console** page is displayed.
2. Click **Reset iDRAC to Default Settings**.
   The completion status is displayed in percentage. iDRAC reboots and is restored to factory defaults. The iDRAC IP is reset and is not accessible. You can configure the IP using the front panel or BIOS.

Resetting iDRAC to Factory Default Settings Using iDRAC Settings Utility

To reset iDRAC to factory default values using the iDRAC Settings utility:

1. Go to **Reset iDRAC configurations to defaults**.
   The **iDRAC Settings Reset iDRAC configurations to defaults** page is displayed.
2. Click **Yes**.
   iDRAC reset starts.
3. Click **Back** and navigate to the same **Reset iDRAC configurations to defaults** page to view the success message.

24

Frequently Asked Questions

This section lists the frequently asked questions for the following:

- System Event Log
- Network Security
- Active Directory
- Single Sign On
- Smart Card Login
- Virtual Console
- Virtual Media
- vFlash SD Card
- SNMP Authentication
- Storage Devices
- iDRAC Service Module
- RACADM
- Miscellaneous

System Event Log

While using iDRAC Web interface through Internet Explorer, why does SEL not save using the Save As option?

This is due to a browser setting. To resolve this:

1. In Internet Explorer, go to **Tools** → **Internet Options** → **Security** and select the zone you are attempting to download in.

   For example, if the iDRAC device is on the local intranet, select **Local Intranet** and click **Custom level...**.
2. In the **Security Settings** window, under **Downloads** make sure that the following options are enabled:

   - Automatic prompting for file downloads (if this option is available)
   - File download

   CAUTION: To make sure that the computer used to access iDRAC is safe, under Miscellaneous, do not enable the Launching applications and unsafe files option.

Network Security

While accessing the iDRAC Web interface, a security warning appears stating that the SSL certificate issued by the Certificate Authority (CA) is not trusted.

iDRAC includes a default iDRAC server certificate to ensure network security while accessing through the Web-based interface and remote RACADM. This certificate is not issued by a trusted CA. To resolve this, upload a iDRAC server certificate issued by a trusted CA (for example, Microsoft Certificate Authority, Thawte or Verisign).

Why the DNS server not registering iDRAC?

Some DNS servers register iDRAC names that contain only up to 31 characters.

When accessing the iDRAC Web-based interface, a security warning is displayed stating that the SSL certificate host name does not match the iDRAC host name.

iDRAC includes a default iDRAC server certificate to ensure network security while accessing through the Web-based interface and remote RACADM. When this certificate is used, the Web browser displays a security warning because the default certificate that is issued to iDRAC does not match the iDRAC host name (for example, the IP address).

To resolve this, upload an iDRAC server certificate issued to the IP address or the iDRAC host name. When generating the CSR (used for issuing the certificate), make sure that the common name (CN) of the CSR matches the iDRAC IP address (if certificate issued to IP) or the registered DNS iDRAC name (if certificate is issued to iDRAC registered name).

To make sure that the CSR matches the registered DNS iDRAC name:

1. In iDRAC Web interface, go to **Overview → iDRAC Settings → Network**. The **Network** page is displayed.
2. In the **Common Settings** section:
   - Select the **Register iDRAC on DNS** option.
   - In the **DNS iDRAC Name** field, enter the iDRAC name.
3. Click **Apply**.

Active Directory

Active Directory login failed. How to resolve this?

To diagnose the problem, on the **Active Directory Configuration and Management** page, click **Test Settings**. Review the test results and fix the problem. Change the configuration and run the test until the test user passes the authorization step.

In general, check the following:

- While logging in, make sure that you use the correct user domain name and not the NetBIOS name. If you have a local iDRAC user account, log into iDRAC using the local credentials. After logging in, make sure that:

- The **Active Directory Enabled** option is selected on the **Active Directory Configuration and Management** page.
- The DNS setting is correct on the **iDRAC Networking configuration** page.
- The correct Active Directory root CA certificate is uploaded to iDRAC if certificate validation was enabled.
- The iDRAC name and iDRAC Domain name matches the Active Directory environment configuration if you are using extended schema.
- The Group Name and Group Domain Name matches the Active Directory configuration if you are using standard schema.
- If the user and the iDRAC object is in different domain, then do not select the **User Domain from Login** option. Instead select **Specify a Domain** option and enter the domain name where the iDRAC object resides.

- Check the domain controller SSL certificates to make sure that the iDRAC time is within the valid period of the certificate.

Active Directory login fails even if certificate validation is enabled. The test results display the following error message. Why does this occur and how to resolve this?

```
ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check
the correct Certificate Authority (CA) certificate has been uploaded to iDRAC.
Please also check if the iDRAC date is within the valid period of the
certificates and if the Domain Controller Address configured in iDRAC matches
the subject of the Directory Server Certificate.
```

If certificate validation is enabled, when iDRAC establishes the SSL connection with the directory server, iDRAC uses the uploaded CA certificate to verify the directory server certificate. The most common reasons for failing certification validation are:

- iDRAC date is not within the validity period of the server certificate or CA certificate. Check the iDRAC time and the validity period of your certificate.
- The domain controller addresses configured in iDRAC does not match the Subject or Subject Alternative Name of the directory server certificate. If you are using an IP address, read the next question. If you are using FQDN, make sure you are using the FQDN of the domain controller and not the domain. For example, **servername.example.com** instead of **example.com**.

Certificate validation fails even if IP address is used as the domain controller address. How to resolve this?

Check the Subject or Subject Alternative Name field of your domain controller certificate. Normally, Active Directory uses the host name and not the IP address of the domain controller in the Subject or Subject Alternative Name field of the domain controller certificate. To resolve this, do any of the following:

- Configure the host name (FQDN) of the domain controller as the *domain controller address(es)* on iDRAC to match the Subject or Subject Alternative Name of the server certificate.
- Reissue the server certificate to use an IP address in the Subject or Subject Alternative Name field, so that it matches the IP address configured in iDRAC.
- Disable certificate validation if you choose to trust this domain controller without certificate validation during the SSL handshake.

How to configure the domain controller address(es) when using extended schema in a multiple domain environment?

This must be the host name (FQDN) or the IP address of the domain controller(s) that serves the domain in which the iDRAC object resides.

When to configure Global Catalog Address(es)?

If you are using standard schema and the users and role groups are from different domains, Global Catalog Address(es) are required. In this case, you can use only Universal Group.

If you are using standard schema and all the users and role groups are in the same domain, Global Catalog Address(es) are not required.

If you are using extended schema, the Global Catalog Address is not used.

How does standard schema query work?

iDRAC connects to the configured domain controller address(es) first. If the user and role groups are in that domain, the privileges are saved.

If Global Controller Address(es) is configured, iDRAC continues to query the Global Catalog. If additional privileges are retrieved from the Global Catalog, these privileges are accumulated.

Does iDRAC always use LDAP over SSL?

Yes. All the transportation is over secure port 636 and/or 3269. During test setting, iDRAC does a LDAP CONNECT only to isolate the problem, but it does not do an LDAP BIND on an insecure connection.

Why does iDRAC enable certificate validation by default?

iDRAC enforces strong security to ensure the identity of the domain controller that iDRAC connects to. Without certificate validation, a hacker can spoof a domain controller and hijack the SSL connection. If you choose to trust all the domain controllers in your security boundary without certificate validation, you can disable it through the Web interface or RACADM.

Does iDRAC support the NetBIOS name?

Not in this release.

Why does it take up to four minutes to log in to iDRAC using Active Directory Single Sign–On or Smart Card Login?

The Active Directory Single Sign–On or Smart Card log in normally takes less than 10 seconds, but it may take up to four minutes to log in if you have specified the preferred DNS server and the alternate DNS server, and the preferred DNS server has failed. DNS time-outs are expected when a DNS server is down. iDRAC logs you in using the alternate DNS server.

The Active Directory is configured for a domain present in Windows Server 2008 Active Directory. A child or sub domain is present for the domain, the user and group is present in the same child domain, and the user is a member of that group. When trying to log in to iDRAC using the user present in the child domain, Active Directory Single Sign-On login fails.

This may be because of the an incorrect group type. There are two kinds of Group types in the Active Directory server:

- Security — Security groups allow you to manage user and computer access to shared resources and to filter group policy settings.
- Distribution — Distribution groups are intended to be used only as email distribution lists.

Always make sure that the group type is Security. You cannot use distribution groups to assign permission on any object, however use them to filter group policy settings.

Single Sign-On

SSO login fails on Windows Server 2008 R2 x64. What are the settings required to resolve this?

1. Run the **technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** for the domain controller and domain policy.
2. Configure the computers to use the DES-CBC-MD5 cipher suite.

   These settings may affect compatibility with client computers or services and applications in your environment. The Configure encryption types allowed for Kerberos policy setting is located at **Computer Configuration → Security Settings → Local Policies → Security Options**.
3. Make sure that the domain clients have the updated GPO.
4. At the command line, type `gpupdate /force` and delete the old key tab with `klist purge` command.
5. After the GPO is updated, create the new keytab.
6. Upload the keytab to iDRAC.

You can now log in to iDRAC using SSO.

Why does SSO login fail with Active Directory users on Windows 7 and Windows Server 2008 R2?

You must enable the encryption types for Windows 7 and Windows Server 2008 R2. To enable the encryption types:

1. Log in as administrator or as a user with administrative privilege.
2. Go to **Start** and run **gpedit.msc**. The **Local Group Policy Editor** window is displayed.
3. Go to **Local Computer Settings → Windows Settings → Security Settings → Local Policies → Security Options**.
4. Right-click **Network Security: Configure encryption types allowed for kerberos** and select **Properties**.
5. Enable all the options.
6. Click **OK**. You can now log in to iDRAC using SSO.

Perform the following additional settings for Extended Schema:

1. In the **Local Group Policy Editor** window, navigate to **Local Computer Settings → Windows Settings → Security Settings → Local Policies → Security Options** .
2. Right-click **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote server** and select **Properties**.
3. Select **Allow all**, click **OK**, and close the **Local Group Policy Editor** window.
4. Go to **Start** and run cmd. The command prompt window is displayed.
5. Run the command `gpupdate /force`. The group policies are updated. Close the command prompt window.
6. Go to **Start** and run regedit. The **Registry Editor** window is displayed.

7. Navigate to **HKEY_LOCAL_MACHINE → System → CurrentControlSet → Control → LSA** .
8. In the right-pane, right-click and select **New → DWORD (32-bit) Value**.
9. Name the new key as **SuppressExtendedProtection**.
10. Right-click **SuppressExtendedProtection** and click **Modify**.
11. In the **Value** data field, type **1** and click **OK**.
12. Close the **Registry Editor** window. You can now log in to iDRAC using SSO.

If you have enabled SSO for iDRAC and you are using Internet Explorer to log in to iDRAC, SSO fails and you are prompted to enter your user name and password. How to resolve this?

Make sure that the iDRAC IP address is listed in the **Tools → Internet Options → Security → Trusted sites**. If it is not listed, SSO fails and you are prompted to enter your user name and password. Click **Cancel** and proceed.

Smart Card Login

It takes up to four minutes to log into iDRAC using Active Directory Smart Card login.

The normal Active Directory Smart Card login normally takes less than 10 seconds, however it may take up to four minutes if you have specified the preferred DNS server and the alternate DNS server in the **Network** page, and the preferred DNS server has failed. DNS time-outs are expected when a DNS server is down. iDRAC logs you in using the alternate DNS server.

ActiveX plug-in unable to detect the Smart Card reader.

Make sure that the smart card is supported on the Microsoft Windows operating system. Windows supports a limited number of smart card Cryptographic Service Providers (CSPs).

In general, check if the smart card CSPs are present on a particular client, insert the smart card in the reader at the Windows logon (Ctrl-Alt-Del) screen and check if Windows detects the smart card and displays the PIN dialog-box.

Incorrect Smart Card PIN.

Check if the smart card is locked due to too many attempts with an incorrect PIN. In such cases, contact the smart card issuer in the organization to get a new smart card.

Virtual Console

Virtual Console session is active even if you have logged out of iDRAC Web interface. Is this the expected behavior?

Yes. Close the Virtual Console Viewer window to log out of the corresponding session.

Can a new remote console video session be started when the local video on the server is turned off?

Yes.

Why does it take 15 seconds to turn off the local video on the server after requesting to turn off the local video?

It gives a local user an opportunity to take any action before the video is switched off.

Is there a time delay when turning on the local video?

No, after a local video turn ON request is received by iDRAC, the video is turned on instantly.

Can the local user also turn off or turn on the video?

When the local console is disabled, the local user cannot turn off or turn on the video.

Does switching off the local video also switch off the local keyboard and mouse?

No.

Does turning off the local console turn off the video on the remote console session?

No, turning the local video on or off is independent of the remote console session.

What privileges are required for an iDRAC user to turn on or turn off the local server video?

Any user with iDRAC configuration privileges can turn on or turn off the local console.

How to get the current status of the local server video?

The status is displayed on the Virtual Console page.

Use the RACADM command `racadm getconfig –g cfgRacTuning` to display the status in the object `cfgRacTuneLocalServerVideo`.

Or, use the following RACADM command from a Telnet, SSH, or a remote session:

```
racadm -r (iDrac IP) -u (username) -p (password) getconfig -g cfgRacTuning
```

The status is also seen on the Virtual Console OSCAR display. When the local console is enabled, a green status is displayed next to the server name. When disabled, a yellow dot indicates that iDRAC has locked the local console.

Why is the bottom of the system screen not seen from the Virtual Console window?

Make sure that the management station's monitor resolution is set to 1280 x 1024.

Why is the Virtual Console Viewer window garbled on Linux operating system?

The console viewer on Linux requires a UTF-8 character set. Check your locale and reset the character set if required.

Why does the mouse not synchronize under the Linux text console in Lifecycle Controller?

Virtual Console requires the USB mouse driver, but the USB mouse driver is available only under the X-Window operating system. In the Virtual Console viewer, do any of the following:

- Go to**Tools** → **Session Options** → **Mouse** tab. Under **Mouse Acceleration**, select **Linux**.
- Under the **Tools** menu, select **Single Cursor** option .

How to synchronize the mouse pointers on the Virtual Console Viewer window?

Before starting a Virtual Console session, make sure that the correct mouse is selected for your operating system.

Make sure that the **Single Cursor** option under **Tools** in the iDRAC Virtual Console menu is selected on iDRAC Virtual Console client. The default is two cursor mode.

Can a keyboard or mouse be used while installing a Microsoft operating system remotely through the Virtual Console?

No. When you remotely install a supported Microsoft operating system on a system with Virtual Console enabled in the BIOS, an EMS Connection Message is sent that requires that you select **OK** remotely. You must either select **OK** on the local system or restart the remotely managed server, reinstall, and then turn off the Virtual Console in BIOS.

This message is generated by Microsoft to alert the user that Virtual Console is enabled.To make sure that this message does not appear, always turn off Virtual Console in the iDRAC Settings utility before remotely installing an operating system.

Why does the Num Lock indicator on the management station not reflect the status of the Num Lock on the remote server?

When accessed through the iDRAC, the Num Lock indicator on the management station does not necessarily coincide with the state of the Num Lock on the remote server. The state of the Num Lock is dependent on the setting on the remote server when the remote session is connected, regardless of the state of the Num Lock on the management station.

Why do multiple Session Viewer windows appear when a Virtual Console session is established from the local host?

You are configuring a Virtual Console session from the local system. This is not supported.

If a Virtual Console session is in-progress and a local user accesses the managed server, does the first user receive a warning message?

No. If a local user accesses the system, both have control of the system.

How much bandwidth is required to run a Virtual Console session?

It is recommended to have a 5 MBPS connection for good performance. A 1 MBPS connection is required for minimal performance.

What are the minimum system requirements for the management station to run Virtual Console?

The management station requires an Intel Pentium III 500 MHz processor with at least 256 MB of RAM.

Why doe Virtual Console Viewer window sometimes displays No Signal message?

You may see this message because the iDRAC Virtual Console plug-in is not receiving the remote server desktop video. Generally, this behavior may occur when the remote server is turned off. Occasionally, the message may be displayed due to a remote server desktop video reception malfunction.

Why does Virtual Console Viewer window sometimes display an Out of Range message?

You may see this message because a parameter necessary to capture video is beyond the range for which the iDRAC can capture the video. Parameters such as display resolution or refresh rate too high will cause and out of range condition. Normally, physical limitations such as video memory size or bandwidth sets the maximum range of parameters.

When starting a Virtual Console session from iDRAC Web interface, why is an ActiveX security popup displayed?

iDRAC may not be in the trusted site list. To prevent the security popup from appearing every time you begin a Virtual Console session, add iDRAC to the trusted site list in the client browser:

1. Click **Tools** → **Internet Options** → **Security** → **Trusted sites**.
2. Click **Sites** and enter the IP address or the DNS name of iDRAC
3. Click **Add**.
4. Click **Custom Level**.
5. In the **Security Settings** window, select **Prompt** under **Download unsigned ActiveX Controls**.

Why is the Virtual Console Viewer window blank?

If you have Virtual Media privilege, but not Virtual Console privilege, you can start the viewer to access the virtual media feature, but the managed server's console is not displayed.

Why doesn't the mouse synchronize in DOS when using Virtual Console?

The Dell BIOS is emulating the mouse driver as a PS/2 mouse. By design, the PS/2 mouse uses relative position for the mouse pointer, which causes the lag in syncing. iDRAC has a USB mouse driver, that allows absolute position and closer tracking of the mouse pointer. Even if iDRAC passes the USB absolute mouse position to the Dell BIOS, the BIOS emulation converts it back to relative position and the behavior remains. To fix this problem, set the mouse mode to USC/Diags in the Configuration screen.

After launching the Virtual Console, the mouse cursor is active on the Virtual Console, but not on the local system. Why does this occur and how to resolve this?

This occurs if the **Mouse Mode** is set to **USC/Diags**. Press **Alt + M** hot key to use the mouse on the local system. Press **Alt + M** again to use the mouse on the Virtual Console.

When iDRAC Web interface is launched from the CMC Web interface soon after Virtual Console is launched, why does GUI session time-out?

When launching the Virtual Console to iDRAC from the CMC Web interface a popup is opened to launch the Virtual Console. The popup closes shortly after the Virtual Console opens.

When launching both the GUI and Virtual Console to the same iDRAC system on a management station, a session time-out for the iDRAC GUI occurs if the GUI is launched before the popup closes. If the iDRAC GUI is launched from the CMC Web interface after the popup with the Virtual Console closed, this issue does not appear.

Why does Linux SysRq key not work with Internet Explorer?

The Linux SysRq key behavior is different when using Virtual Console from Internet Explorer. To send the SysRq key, press the **Print Screen** key and release while holding the **Ctrl** and **Alt** keys. To send the SysRq key to a remote Linux server though iDRAC, while using Internet Explorer:

1. Activate the magic key function on the remote Linux server. You can use the following command to activate it on the Linux terminal:
   ```
   echo 1 > /proc/sys/kernel/sysrq
   ```
2. Activate the keyboard pass-through mode of Active X Viewer.
3. Press **Ctrl + Alt +Print Screen**.
4. Release only **Print Screen**.
5. Press **Print Screen+Ctrl+Alt**.

NOTE: The SysRq feature is currently not supported with Internet Explorer and Java.

Why is the "Link Interrupted" message displayed at the bottom of the Virtual Console?

When using the shared network port during a server reboot, iDRAC is disconnected while BIOS is resetting the network card. This duration is longer on 10 Gb cards, and is also exceptionally long if the connected network switch has Spanning Tree Protocol (STP) enabled. In this case, it is recommended to enable "portfast" for the switch port connected to the server. In most cases, the Virtual Console restores itself.

Virtual Media

Why does the Virtual Media client connection sometimes drop?

When a network time-out occurs, iDRAC firmware drops the connection, disconnecting the link between the server and the virtual drive.

If you change the CD in the client system, the new CD may have an autostart feature. In this case, the firmware can time-out and the connection is lost if the client system takes too long to read the CD. If a connection is lost, reconnect from the GUI and continue the previous operation.

If the Virtual Media configuration settings are changed in the iDRAC Web interface or through local RACADM commands, any connected media is disconnected when the configuration change is applied.

To reconnect to the Virtual Drive, use the Virtual Media **Client View** window.

Why does a Windows operating system installation through Virtual Media takes an extended amount of time?

If you are installing the Windows operating system using the *Dell Systems Management Tools and Documentation DVD* and the network connection is slow, the installation procedure may require an extended amount of time to access iDRAC Web interface due to network latency. The installation window does not indicate the installation progress.

How to configure the virtual device as a bootable device?

On the managed system, access BIOS Setup and go to the boot menu. Locate the virtual CD, virtual floppy, or vFlash and change the device boot order as required. Also, press the "spacebar" key in the boot sequence in the CMOS setup to make the virtual device bootable. For example, to boot from a CD drive, configure the CD drive as the first device in the boot order.

What are the types of media that can be set as a bootable device?

iDRAC allows you to boot from the following bootable media:

- CDROM/DVD Data media
- ISO 9660 image
- 1.44 Floppy disk or floppy image
- A USB key that is recognized by the operating system as a removable disk
- A USB key image

How to make the USB key a bootable device?

You can also boot with a Windows 98 startup disk and copy system files from the startup disk to the USB key. For example, from the DOS prompt, type the following command:

```
sys a: x: /s
```

where, x: is the USB key that is required to be set as a bootable device.

The Virtual Media is attached and connected to the remote floppy. But, cannot locate the Virtual Floppy/Virtual CD device on a system running Red Hat Enterprise Linux or the SUSE Linux operating system. How to resolve this?

Some Linux versions do not auto-mount the virtual floppy drive and the virtual CD drive in the same method. To mount the virtual floppy drive, locate the device node that Linux assigns to the virtual floppy drive. To mount the virtual floppy drive:

1. Open a Linux command prompt and run the following command:
   ```
   grep "Virtual Floppy" /var/log/messages
   ```
2. Locate the last entry to that message and note the time.
3. At the Linux prompt, run the following command:
   ```
   grep "hh:mm:ss" /var/log/messages
   ```
   where, hh:mm:ss is the time stamp of the message returned by grep in step 1.
4. In step 3, read the result of the grep command and locate the device name that is given to the Virtual Floppy.
5. Make sure that you are attached and connected to the virtual floppy drive.
6. At the Linux prompt, run the following command:
   ```
   mount /dev/sdx /mnt/floppy
   ```
   where, `/dev/sdx` is the device name found in step 4 and `/mnt/floppy` is the mount point.

To mount the virtual CD drive, locate the device node that Linux assigns to the virtual CD drive. To mount the virtual CD drive:

1. Open a Linux command prompt and run the following command:
   ```
   grep "Virtual CD" /var/log/messages
   ```
2. Locate the last entry to that message and note the time.
3. At the Linux prompt, run the following command:
   ```
   grep "hh:mm:ss" /var/log/messages
   ```
   where, hh:mm:ss is the timestamp of the message returned by grep in step 1.
4. In step 3, read the result of the grep command and locate the device name that is given to the *Dell Virtual* CD.
5. Make sure that the Virtual CD Drive is attached and connected.

6. At the Linux prompt, run the following command:
   `mount /dev/sdx /mnt/CD`

   where: `/dev/sdx` is the device name found in step 4 and `/mnt/floppy` is the mount point.

Why are the virtual drives attached the server removed after performing a remote firmware update using the iDRAC Web interface?

Firmware updates cause the iDRAC to reset, drop the remote connection, and unmount the virtual drives. The drives reappear when iDRAC reset is complete.

Why are all the USB devices detached after connecting a USB device?

Virtual media devices and vFlash devices are connected as a composite USB device to the Host USB BUS, and they share a common USB port. Whenever any virtual media or vFlash USB device is connected to or disconnected from the host USB bus, all the Virtual Media and vFlash devices are disconnected momentarily from the host USB bus, and then they are re-connected. If the host operating system uses a virtual media device, do not attach or detach one or more virtual media or vFlash devices. It is recommended that you connect all the required USB devices first before using them.

What does the USB Reset do?

It resets the remote and local USB devices connected to the server.

How to maximize Virtual Media performance?

To maximize Virtual Media performance, launch the Virtual Media with the Virtual Console disabled or do one of the following:

- Change the performance slider to Maximum Speed.
- Disable encryption for both Virtual Media and Virtual Console.

  NOTE: In this case, the data transfer between managed server and iDRAC for Virtual Media and Virtual Console will not be secured.
- If you are using any Windows server operating systems, stop the Windows service named Windows Event Collector. To do this, go to **Start** → **Administrative Tools** → **Services**. Right-click **Windows Event Collector** and click **Stop**.

While viewing the contents of a floppy drive or USB key, a connection failure message is displayed if the same drive is attached through the virtual media?

Simultaneous access to virtual floppy drives are not allowed. Close the application used to view the drive contents before attempting to virtualize the drive.

What file system types are supported on the Virtual Floppy Drive?

The virtual floppy drive supports FAT16 or FAT32 file systems.

Why is an error message displayed when trying to connect a DVD/USB through virtual media even though the virtual media is currently not in use?

The error message is displayed if Remote File Share (RFS) feature is also in use. At a time, you can use RFS or Virtual Media and not both.

vFlash SD Card

When is the vFlash SD card locked?

The vFlash SD card is locked when an operation is in-progress. For example, during an initialize operation.

SNMP Authentication

Why is the message 'Remote Access: SNMP Authentication Failure' displayed?

As part of discovery, IT Assistant attempts to verify the get and set community names of the device. In IT Assistant, you have the get community name = public and the set community name = private. By default, the SNMP agent community name for iDRAC agent is public. When IT Assistant sends out a set request, the iDRAC agent generates the SNMP authentication error because it accepts requests only from community = public.

To prevent SNMP authentication errors from being generated, you must enter community names that are accepted by the agent. Since the iDRAC only allows one community name, you must use the same get and set community name for IT Assistant discovery setup.

Storage Devices

Information for all the storage devices connected to the system are not displayed and OpenManage Storage Management displays more storage devices that iDRAC. Why?

iDRAC displays information for only the Comprehensive Embedded Management (CEM) supported devices.

iDRAC Service Module

Before installing or running the iDRAC Service Module, should the Open Manage Server Administrator be uninstalled?

No you do not have to uninstall Server Administrator. Before you install or run the iDRAC Service Module, make sure that you have stopped the features of Server Administrator that the iDRAC Service Module provides.

How to check whether iDRAC Service Module is installed in the system?

To know if the iDRAC Service Module is installed on the system,

- On Windows:
  Run the `service.msc` command. In the list of services displayed, see if there is a service called **DSM iDRAC Service Module**.
- On Linux:
  Run the command `/etc/init.d/dcismeng status`. If the iDRAC Service Module is installed and running, the status displayed is **running**.

NOTE: Use the `systemctl status dcismeng.service` command instead of the `init.d` command to check if the iDRAC Service Module is installed on RedHat Enterprise Linux 7 operating system.

How to check the version number of the iDRAC Service Module installed in the system?

To check the version of the iDRAC Service Module in the system, do any of the following:

- Click **Start** → **Control Panel** → **Programs and Features**. The version of the installed iDRAC Service Module is listed in the **Version** tab.
- Go to **My Computer** → **Uninstall or change a program**.

What is the minimum permission level required to install the iDRAC Service Module?

To install the iDRAC Service Module, you must have administrator level privileges.

While installing the iDRAC Service Module, it displays an error message This is not a supported server. Consult the User Guide for additional information about the supported servers. How to resolve this?

Before installing the iDRAC Service Module, make sure that the server is a 12th generation PowerEdge sever or later. Also, make sure that you have a 64-bit system.

The following message is displayed in the OS log, even when the OS to iDRAC Pass-through over USBNIC is configured properly. Why?

```
The iDRAC Service Module is unable to communicate with iDRAC using the OS to
iDRAC Pass-through channel
```

iDRAC Service Module uses the OS to iDRAC pass-through over USB NIC feature to establish the communication with iDRAC. Sometimes, the communication is not established though the USB NIC interface is configured with the correct IP endpoints. This may happen when the host operating system routing table has multiple entries for the same destination mask and the USB NIC destination is not listed as the first one in routing order.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
default	10.94.148.1	0.0.0.0	UG	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

In the example **enp0s20u12u3** is the USB NIC interface. The link-local destination mask is repeated and the USB NIC is not the first one in the order. This results in the connectivity issue between iDRAC Service Module and iDRAC over the OS to iDRAC Pass-through. To troubleshoot the connectivity issue, make sure that the iDRAC USBNIC IPv4 address (by default it is 169.254.0.1) is reachable from the host operating system.

If not:

- Change the iDRAC USBNIC address on a unique destination mask.

- Delete the entries that are not required from the routing table to make sure that USB NIC is chosen by route when the host wants to reach the iDRAC USB NIC IPv4 address.

When uninstalling iDRAC Service Module from a VMware ESXi server, the virtual switch is named as vSwitchiDRACvusb and port group as iDRAC Network on the Vsphere client. How to delete them?

While installing iDRAC Service Module VIB on a VMware ESXi server, iDRAC Service Module creates the vSwtich and Portgroup to communicate with iDRAC over the OS to iDRAC Pass-through in USB NIC mode. After the uninstallation, the virtual switch **vSwitchiDRACvusb** and the port group **iDRAC Network** are not deleted. To delete it manually, perform one of the following steps:

- Go to vSphere Client Configuration wizard and delete the entries.
- Go to the Esxcli and type the following commands:
  - To remove port group: `esxcfg-vmknic -d -p "iDRAC Network"`
  - To remove vSwitch: `esxcfg-vswitch -d vSwitchiDRACvusb`

  NOTE: You can reinstall iDRAC Service Module on the Vmware ESXi server as this is not a functional issue for the server.

Where is the Replicated LifeCycle log available on the Operating System?

To view the replicated Lifecycle logs:

Operating System	Location
Microsoft Windows	**Event viewer** → **Windows Logs** → **System**. All the iDRAC Service Module Lifecycle logs are replicated under the source name **iDRAC Service Module**.
Red Hat Enterprise Linux , SUSE Linux, CentOS, and Citrix XenServer	/var/log/messages
VMware ESXi	/var/log/syslog.log

What are the Linux dependent packages or executables available for installation while completing the Linux installation?

To see the list of Linux dependent packages, see the *Linux Dependencies* section in the *iDRAC Service Module Installation Guide*.

RACADM

After performing an iDRAC reset (using the racadm racreset command), if any command is issued, the following message is displayed. What does this indicate?

```
ERROR: Unable to connect to RAC at specified IP address
```

The message indicates that you must wait until the iDRAC completes the reset before issuing another command.

When using RACADM commands and subcommands, some errors are not clear.

You may see one or more of the following errors when using the RACADM commands and subcommands:

- Local RACADM error messages — Problems such as syntax, typographical errors, and incorrect names.
- Remote RACADM error messages — Problems such as incorrect IP Address, incorrect user name, or incorrect password.

During a ping test to iDRAC, if the network mode is switched between Dedicated and Shared modes, there is no ping response.

Clear the ARP table on your system.

Remote RACADM fails to connect to iDRAC from SUSE Linux Enterprise Server (SLES) 11 SP1.

Make sure that the official openssl and libopenssl versions are installed. Run the following command to install the RPM packages:

```
rpm -ivh --force < filename >
```

where, `filename` is the openssl or libopenssl rpm package file.

For example:

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
```

```
rpm -ivh --force libopenssl0_9_8-0.9.8h-30.22.21.1.x86_64.rpm
```

Why are the remote RACADM and Web-based services unavailable after a property change?

It may take a while for the remote RACADM services and the Web-based interface to become available after the iDRAC Web server resets.

The iDRAC Web server is reset when:
- The network configuration or network security properties are changed using the iDRAC Web user interface.
- The cfgRacTuneHttpsPort property is changed (including when a `config -f (config file)` changes it).
- The racresetcfg command is used.
- iDRAC is reset.
- A new SSL server certificate is uploaded.

Why is an error message displayed if you try to delete a partition after creating it using local RACADM?

This occurs because the create partition operation is in-progress. However, the partition is deleted after sometime and a message that the partition is deleted is displayed. If not, wait until the create partition operation is completed and then delete the partition.

Miscellaneous

How to find an iDRAC IP address for a blade server?

You can find the iDRAC IP address using any of the following methods:

Using CMC Web interface: Go to **Chassis** → **Servers** → **Setup** → **Deploy** and in the displayed table, view the IP address for the server.

Using the Virtual Console: Reboot the server to view the iDRAC IP address during POST. Select the "Dell CMC" console in the OSCAR to log in to CMC through a local serial connection. CMC RACADM

commands can be sent from this connection. See the *iDRAC8 RACADM Command Line Interface Reference Guide* for a complete list of CMC RACADM subcommands.

From local RACADM, Use the command: `racadm getsysinfo` For example:

```
$ racadm getniccfg -m server-1
DHCP Enabled        = 1
IP Address          = 192.168.0.1
Subnet Mask         = 255.255.255.0
Gateway             = 192.168.0.1
```

Using LCD: On the Main Menu, highlight the Server and press the check button and select the required server and press the check button.

How to find the CMC IP address related to the blade server?

From iDRAC Web interface: Click **Overview → iDRAC Settings → CMC** . The **CMC Summary** page displays the CMC IP address.

From the Virtual Console: Select the "Dell CMC" console in the OSCAR to log in to CMC through a local serial connection. CMC RACADM commands can be issued from this connection. See the *iDRAC8 RACADM Command Line Interface Reference Guide* for a complete list of CMC RACADM subcommands

```
$ racadm getniccfg -m chassis
NIC Enabled         = 1
DHCP Enabled        = 1
Static IP Address   = 192.168.0.120
Static Subnet Mask  = 255.255.255.0
Static Gateway      = 192.168.0.1
Current IP Address  = 10.35.155.151
Current Subnet Mask = 255.255.255.0
Current Gateway     = 10.35.155.1
Speed               = Autonegotiate
Duplex              = Autonegotiate
```

NOTE: You can also perform this using remote RACADM.

How to find iDRAC IP address for rack and tower server?

From iDRAC Web Interface: Go to **Overview → Server → Properties → Summary**. The **System Summary** page displays the iDRAC IP address.

From Local RACADM: Use the command `racadm getsysinfo`.

From LCD: On the physical server, use the LCD panel navigation buttons to view the iDRAC IP address. Go to **Setup View → View → iDRAC IP → IPv4** or **IPv6 → IP**.

From OpenManage Server Administrator: In the Server Administrator Web interface, go to **Modular Enclosure → System/Server Module → Main System Chassis/Main System → Remote Access**.

iDRAC network connection is not working.

For blade servers:

- Make sure that the LAN cable is connected to CMC.
- Make sure that NIC settings, IPv4 or IPv6 settings, and either Static or DHCP is enabled for your network.

For rack and tower servers:

- In shared mode, make sure the LAN cable is connected to the NIC port where the wrench symbol is present.
- In Dedicated mode, make sure the LAN cable is connected to the iDRAC LAN port.
- Make sure that NIC settings, IPv4 and IPv6 settings and either Static or DHCP is enabled for your network.

Inserted the blade server into the chassis and pressed the power switch, but it did not power on.

- iDRAC requires up to two minutes to initialize before the server can power on.
- Check CMC power budget. The chassis power budget may have exceeded.

How to retieve an iDRAC administrative user name and password?

You must restore iDRAC to its default settings. For more information, see Resetting iDRAC to Factory Default Settings.

How to change the name of the slot for the system in a chassis?

1. Log in to CMC Web interface and go to **Chassis** → **Servers** → **Setup**.
2. Enter the new name for the slot in the row for your server and click **Apply**.

iDRAC on blade server is not responding during boot.

Remove and reinsert the server.

Check CMC Web interface to see if iDRAC is displayed as an upgradable component. If it does, follow the instructions in Updating Firmware Using CMC Web Interface.

If the problem persists, contact technical support.

When attempting to boot the managed server, the power indicator is green, but there is no POST or no video.

This happens due to any of the following conditions:

- Memory is not installed or is inaccessible.
- CPU is not installed or is inaccessible
- Video riser card is missing or not connected properly.

Also, see error messages in iDRAC log using iDRAC Web interface or from the server LCD.

25

Use Case Scenarios

This section helps you in navigating to specific sections in the guide to perform typical use case scenarios.

Troubleshooting An Inaccessible Managed System

After receiving alerts from OpenManage Essentials, Dell Management Console, or a local trap collector, five servers in a data center are not accessible with issues such as hanging operating system or server. Need to identify the cause to troubleshoot and bring up the server using iDRAC.

Before troubleshooting the inaccessible system, make sure that the following prerequisites are met:

- Enable last crash screen
- Alerts are enabled on iDRAC

To identify the cause, check the following in the iDRAC Web interface and re-establish the connection to the system:

NOTE: If you cannot access the iDRAC Web interface, go to the sever, access the LCD panel, write down the IP address or the host name, and then perform the following operations using iDRAC Web interface from your management station:

- Server's LED status — Blinking amber or Solid amber.
- Front Panel LCD status or error message — Amber LCD or error message.
- Operating system image is seen in the Virtual Console. If you can see the image, reset the system (warm boot) and log in again. If you are able to log in, the issue is fixed.
- Last crash screen.
- Boot capture video.
- Crash capture video.
- Server Health status — Red *x* icons for the system components with issues.
- Storage array status — Possible array offline or failed
- Lifecycle log for critical events related to system hardware and firmware and the log entries that were logged at the time of system crash.
- Generate Tech Support report and view the collected data.
- Use the monitoring features provided by iDRAC Service Module

Related Links

Previewing Virtual Console
Viewing Boot and Crash Capture Videos
Viewing System Health
Viewing Logs
Generating Technical Support Report

Inventory and Monitoring Storage Devices
Using iDRAC Service Module

Obtaining System Information and Assess System Health

To obtain system information and assess system health:

- In iDRAC Web interface, go to **Overview → Server → System Summary** to view the system information and access various links on this page to asses system health. For example, you can check the health of the chassis fan.
- You can also configure the chassis locator LED and based on the color, assess the system health.
- If iDRAC Service Module is installed, the operating system host information is displayed.

Related Links

Viewing System Health
Using iDRAC Service Module
Generating Technical Support Report

Setting Up Alerts and Configuring Email Alerts

To set up alerts and configure email alerts:

1. Enable alerts.
2. Configure the email alert and check the ports.
3. Perform a reboot, power off, or power cycle the managed system.
4. Send test alert.

Viewing and Exporting Lifecycle Log and System Event Log

To view and export lifecycle log and system event log (SEL):

1. In iDRAC Web interface, go to **Overview → Server → Logs** to view SEL and **Overview → Server → Logs → Lifecycle Log** to view lifecycle log.

   NOTE: The SEL is also recorded in the lifecycle log. Using the filtering options to view the SEL.
2. Export the SEL or lifecycle log in the XML format to an external location (management station, USB, network share, and so on). Alternatively, you can enable remote system logging, so that all the logs written to the lifecycle log are also simultaneously written to the configured remote server(s).
3. If you are using the iDRAC Service Module, export the Lifecycle log to OS log. For more information, see Using iDRAC Service Module.

Interfaces to Update iDRAC Firmware

Use the following interfaces to update the iDRAC firmware:

- iDRAC Web interface
- RACADM CLI (iDRAC and CMC)
- Dell Update Package (DUP)

- CMC Web interface
- Lifecycle Controller–Remote Services
- Lifecycle Controller
- Dell Remote Access Configuration Tool (DRACT)

Performing Graceful Shutdown

To perform graceful shutdown, in iDRAC Web interface, go to one of the following locations:

- **Overview → Server → Power/Thermal → Power Configuration → Power Control**. The **Power Control** page is displayed. Select **Graceful Shutdown** and click **Apply**.
- **Overview → Server → Power/Thermal → Power Monitoring**. From the **Power Control** drop-down menu, select **Graceful Shutdown** and click **Apply**.

For more information, see the *iDRAC Online Help*.

Creating New Administrator User Account

You can modify the default local administrator user account or create a new administrator user account. To modify the local administrator user account, see Modifying Local Administrator Account Settings.

To create a new administrator account, see the following sections:

- Configuring Local Users
- Configuring Active Directory Users
- Configuring Generic LDAP Users

Launching Server's Remote Console and Mounting a USB Drive

To launch the remote console and mount a USB drive:

1. Connect a USB flash drive (with the required image) to the management station.
2. Use one the following methods to launch virtual console through the iDRAC Web Interface:
   - Go to **Overview → Server → Virtual Console** and click **Launch Virtual Console**.
   - Go to **Overview → Server → Properties** and click **Launch** under **Virtual Console Preview**.

   The **Virtual Console Viewer** is displayed.
3. From the **File** menu, click **Virtual Media → Launch Virtual Media**.
4. Click **Add Image** and select the image that is located on the USB flash drive.
   The image is added to the list of available drives.
5. Select the drive to map it. The image on the USB flash drive is mapped to the managed system.

Installing Bare Metal OS Using Attached Virtual Media and Remote File Share

To do this, see Deploying Operating System Using Remote File Share.

Managing Rack Density

Suppose two servers are installed in a rack. To add two additional servers, need to determine how much capacity is left in the rack.

To assess the capacity of a rack to add additional servers:

1. View the current power consumption data and historical power consumption data for the servers.
2. Based on the data, power infrastructure and cooling system limitations, enable the power cap policy and set the power cap values.

   NOTE: It is recommended that you set a cap close to the peak, and then use that capped level to determine how much capacity is remaining in the rack for adding more servers.

Installing New Electronic License

See License Operations for more information.

Applying I/O Identity Configuration Settings for Multiple Network Cards in Single Host System Reboot

If you have multiple network cards in a server that is part of a Storage Area Network (SAN) environment and you want to apply different virtual addresses, initiator and target configuration settings to those cards, use the I/O Identity Optimization feature to reduce the time in configuring the settings. To do this:

1. Make sure that BIOS, iDRAC, and the network cards are updated to the latest firmware version.
2. Enable IO Identity Optimization.
3. Export the XML configuration file from iDRAC.
4. Edit the I/O Identity optimization settings in the XML file.
5. Import the XML configuration file to iDRAC.

Related Links

Updating Device Firmware
Enabling or Disabling I/O Identity Optimization