# Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers Version 3.2

# User Guide

# Notes and Cautions

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

**CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.**

---

**Information in this publication is subject to change without notice.**
**© 2011 Dell Inc. All rights reserved.**

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL™ logo, OpenManage™, and PowerEdge™, are trademarks of Dell Inc.. Microsoft®, Windows®, Windows Server®, Internet Explorer®, Windows Vista®, MS-DOS™, ActiveX™, and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and other countries. Novell® and SUSE® are registered trademarks of Novell, Inc. in the United States and other countries. Intel® and Pentium® are registered trademarks of Intel Corporation in the U.S. and other countries. UNIX® is a registered trademark of The Open Group in the United States and other countries. Thawte® is a registered trademark of Thawte Consulting (Pty) Ltd. VeriSign® is a registered trademark of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. Sun™ and Java™ are trademarks or registered trademarks of Oracle Corporation or its subsidiaries in the United States and other countries. Mozilla® and Firefox® are registered trademarks of Mozilla Foundation. Fedora™ is a trademark of Red Hat, Inc.

Copyright 1998-2009 The OpenLDAP Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License. A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at **OpenLDAP.org/license.html**. OpenLDAP is a registered trademark of the OpenLDAP Foundation. Individual files and/or contributed packages may be copyrighted by other parties and subject to additional restrictions. This work is derived from the University of Michigan LDAP v3.3 distribution. This work also contains materials derived from public sources. Information about OpenLDAP can be obtained at **openldap.org/**. Portions Copyright 1998-2004 Kurt D. Zeilenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License. Portions Copyright 1999-2003 Howard Y.H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Hallvard B. Furuseth. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided "as is" without express or implied warranty. Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

**2011 - 03**

# Contents

1 iDRAC6 Enterprise Overview . . . . . 19

**What's New in This Release** . . . . . **20**

**IPv6 Ready Logo Certification** . . . . . **20**

**iDRAC6 Security Features** . . . . . **21**

**iDRAC6 Enterprise and vFlash Media** . . . . . **22**

**Supported Platforms** . . . . . **24**

**Supported Operating Systems** . . . . . **24**

**Supported Web Browsers** . . . . . **25**

**Supported Remote Access Connections** . . . . . **25**

**iDRAC6 Ports** . . . . . **25**

**Other Documents You May Need** . . . . . **27**

2 Configuring iDRAC6 Enterprise . . . . . 31

**Before You Begin** . . . . . **31**

**Interfaces for Configuring iDRAC6** . . . . . **31**

**Configuration Tasks** . . . . . **35**

Configure the Management Station . . . . . 35

Configure iDRAC6 Networking . . . . . 35

Configure iDRAC6 Users . . . . . 36

Configure Directory Services . . . . . 36
Configure IP Filtering and IP Blocking . . . . . 37
Configure Platform Events . . . . . 37
Enabling or Disabling Local Configuration Access . . . . . 37
Configure iDRAC6 Services . . . . . 38
Configure Secure Sockets Layer (SSL) . . . . . 38
Configure Virtual Media . . . . . 38
Configure a vFlash Media Card . . . . . 38
Install the Managed Server Software . . . . . 39
Configure the Managed Server for the Last Crash Screen Feature . . . . . 39

**Configuring Network Settings Using CMC Web Interface . . . . . 39**
Launching iDRAC6 Web Interface From CMC . . . . . 39
Configuring Networking for iDRAC6 . . . . . 41

**Viewing FlexAddress Mezzanine Card Fabric Connections . . . . . 42**
FlexAddress MAC for iDRAC6 . . . . . 43

**Remote Syslog . . . . . 44**

**First Boot Device . . . . . 46**

**Remote File Share . . . . . 47**

**Internal Dual SD Module . . . . . 50**
Viewing Internal Dual SD Module Status Using GUI . . . . . 51

**Updating iDRAC6 Firmware . . . . . 52**
Downloading the Firmware or Update Package . . . . . 52
Executing the Firmware Update . . . . . 52

Verifying the Digital Signature for Linux DUPs . . . . . 53
Using iDRAC6 Web Interface . . . . . 57
Updating iDRAC6 Firmware Using RACADM . . . . . 58
Using the DOS Update Utility . . . . . 58
Using WSMAN Interface . . . . . 59

**Updating the USC Repair Package . . . . . 59**

**Configuring iDRAC6 For Use With IT Assistant . . . . . 59**

**Using iDRAC6 Configuration Utility to Enable Discovery and Monitoring . . . . . 60**

**Using iDRAC6 Web Interface to Enable Discovery and Monitoring . . . . . 61**

**Using IT Assistant to View iDRAC6 Status and Events . . . . . 63**

3 Configuring the Management Station . . . . . 65

**Management Station Set Up Steps . . . . . 65**

**Management Station Network Requirements . . . . . 65**

**Configuring a Supported Web Browser . . . . . 66**
Opening Your Web Browser . . . . . 66
Configuring Your Web Browser to Connect to the Web Interface . . . . . 66
Adding iDRAC6 to the List of Trusted Domains . . . . . 69
Viewing Localized Versions of the Web Interface . . . . . 70
Setting the Locale in Linux . . . . . 71
Disabling the Whitelist Feature in Firefox . . . . . 72

**Installing iDRAC6 Software on the Management Station** . . . . . **73**

Installing and Uninstalling RACADM on a Management Station . . . . . 73

Installing and Uninstalling RACADM on Linux . . . . . 73

**Installing a Java Runtime Environment (JRE)** . . . . . **74**

**Installing Telnet or SSH Clients** . . . . . **75**

Telnet with iDRAC6 . . . . . 75

Configuring the Backspace Key For Telnet Sessions . . . . . 75

SSH With iDRAC6 . . . . . 76

**Installing a TFTP Server** . . . . . **78**

**Installing Dell OpenManage IT Assistant** . . . . . **78**

**Installing Dell Management Console** . . . . . **79**

4 Configuring the Managed Server . . . . . 81

**Installing the Software on the Managed Server** . . . . **81**

**Configuring the Managed Server to Capture the Last Crash Screen** . . . . . **82**

**Disabling the Windows Automatic Reboot Option** . . . **83**

5 Configuring iDRAC6 Enterprise Using the Web Interface . . . . . 85

**Accessing the Web Interface** . . . . . **86**

Logging In . . . . . 86

Logging Out . . . . . 87

Using Multiple Browser Tabs and Windows . . . . . 87

**Configuring iDRAC6 NIC** . . . . . **88**

Configuring the Network, IPMI, and VLAN Settings . . . . . 88

Configuring IP Filtering and IP Blocking . . . . . 92

**Configuring Platform Events** . . . . . **94**

Configuring Platform Event Filters (PEF) . . . . . 95

Configuring Platform Event Traps (PET) . . . . . 95

Configuring E-Mail Alerts . . . . . 96

**Configuring IPMI Over LAN** . . . . . **98**

**Adding and Configuring iDRAC6 Users** . . . . . **99**

Public Key Authentication over SSH . . . . . 99

**Securing iDRAC6 Communications Using SSL and Digital Certificates** . . . . . **107**

Secure Sockets Layer (SSL) . . . . . 107

Certificate Signing Request (CSR) . . . . . 108

Accessing the SSL Main Menu . . . . . 108

Generating a New Certificate Signing Request . . . . . 109

Uploading a Server Certificate . . . . . 110

Viewing a Server Certificate . . . . . 111

**Configuring and Managing Microsoft Active Directory Certificates** . . . . . **111**

Configuring Active Directory (Standard Schema and Extended Schema) . . . . . 112

Viewing an Active Directory CA Certificate . . . . 119

**Enabling or Disabling Local Configuration Access** . . . . . **119**

Enabling Local Configuration Access . . . . . 119

Disabling Local Configuration Access . . . . . 120

**Configuring iDRAC6 Services . . . . . 120**

**Updating iDRAC6 Firmware . . . . . 123**

Updating iDRAC6 Firmware Using CMC . . . . . 124

iDRAC6 Firmware Rollback . . . . . 125

6 Using iDRAC6 Directory Service . . . . . 127

**Using iDRAC6 With Microsoft Active Directory. . . . 127**

**Prerequisites for Enabling Active Directory Authentication for iDRAC6 . . . . . 129**

Enabling SSL on a Domain Controller. . . . . 129

**Supported Active Directory Authentication Mechanisms . . . . . 132**

**Extended Schema Active Directory Overview . . . . 132**

Active Directory Schema Extensions. . . . . 132

Overview of iDRAC6 Schema Extensions. . . . . 133

Active Directory Object Overview . . . . . 133

Accumulating Privileges Using Extended Schema. . . . . 135

**Configuring Extended Schema Active Directory to Access iDRAC6 . . . . . 136**

Extending the Active Directory Schema . . . . . 137

Installing the Dell Extension to the Active Directory Users and Computers Snap-In. . . . . 143

Adding iDRAC6 Users and Privileges to Active Directory . . . . . 144

Configuring Microsoft Active Directory With Extended Schema Using iDRAC6 Web Interface . . . . . 146

Configuring Active Directory With Extended Schema Using RACADM . . . . . 149

**Standard Schema Active Directory Overview . . . . . 152**

Single Domain Versus Multiple Domain Scenarios . . . . . 153

**Configuring Standard Schema Active Directory to Access iDRAC6 . . . . . 154**

Configuring Active Directory With Standard Schema Using iDRAC6 Web Interface . . . . . 154

Configuring Active Directory With Standard Schema Using RACADM . . . . . 158

**Testing Your Configurations . . . . . 161**

**Using iDRAC6 with LDAP Directory Service . . . . . 161**

Login Syntax (Directory User versus Local User) . . . . . 161

Configuring Generic LDAP Directory Service Using iDRAC6 Web-Based Interface . . . . . 162

**Frequently Asked Questions . . . . . 165**

Active Directory Log In Issues . . . . . 165

Active Directory Certificate Validation . . . . . 168

Extended and Standard Schema . . . . . 169

Miscellaneous . . . . . 170

7 Configuring iDRAC6 for Single Sign-On and Smart Card Login . . . . . 171

**About Kerberos Authentication . . . . . 171**

**Prerequisites for Active Directory SSO and Smart Card Authentication . . . . . 172**

**Using Active Directory SSO** . . . . . **175**
Configuring iDRAC6 to Use SSO . . . . . 175
Logging Into iDRAC6 Using SSO . . . . . 177

**Configuring Smart Card Authentication** . . . . . **178**

**Configuring Smart Card Login in iDRAC6** . . . . . **178**

**Logging Into iDRAC6 Using Active Directory Smart Card Authentication** . . . . . **180**

**Frequently Asked Questions About SSO**. . . . . **180**

**Troubleshooting the Smart Card Logon in iDRAC6** . . . . . **181**

8 Viewing the Configuration and Health of the Managed Server . . . . 185

**System Summary** . . . . . **185**

**System Details** . . . . . **185**
Main System Enclosure. . . . . 185
Integrated Dell Remote Access Controller 6 - Enterprise. . . . . 187

**WWN/MAC**. . . . . **190**

**Server Health**. . . . . **190**
iDRAC6 . . . . . 190
CMC . . . . . 191
Batteries . . . . . 191
Temperatures . . . . . 191
Voltages. . . . . 191
Power Monitoring. . . . . 192
CPU . . . . . 192
POST . . . . . 192

Misc Health . . . . . 193

**System Inventory** . . . . . **193**

Troubleshooting . . . . . 194

9 Configuring and Using Serial Over LAN . . . . . 197

**Enabling Serial Over LAN in the BIOS** . . . . . **197**

**Configuring Serial Over LAN in iDRAC6 Web GUI** . . . . . **198**

**Using Serial Over LAN (SOL)** . . . . . **200**

Model for Redirecting SOL Over Telnet or SSH . . . . . 200

Model for the SOL Proxy . . . . . 201

Model for Redirecting SOL Over IPMItool . . . . . 201

Disconnecting SOL session in iDRAC6 Command Line Console . . . . . 202

Using SOL over PuTTY . . . . . 202

Using SOL over Telnet with Linux . . . . . 203

Using SOL over OpenSSH with Linux . . . . . 203

Using SOL over IPMItool . . . . . 204

Opening SOL with SOL proxy . . . . . 205

**Operating System Configuration** . . . . . **210**

Linux Enterprise Operating System . . . . . 210

Windows 2003 Enterprise . . . . . 216

10 Using GUI Virtual Console . . . . . 219

**Overview** . . . . . **219**

**Using Virtual Console** . . . . . **219**

Clear Your Browser's Cache . . . . . 220
Supported Screen Resolutions and Refresh Rates . . . . . 221
Configuring the Management Station . . . . . 221
Configuring Virtual Console and Virtual Media in iDRAC6 Web Interface . . . . . 222
Opening a Virtual Console Session . . . . . 224
Virtual Console Preview . . . . . 226

**Using the Video Viewer . . . . . 226**
Synchronizing the Mouse Pointers . . . . . 230
Disabling or Enabling Local Console . . . . . 231

**Launching Virtual Console and Virtual Media Remotely . . . . . 232**
URL Format . . . . . 232
General Error Scenarios . . . . . 232

**Frequently Asked Questions . . . . . 233**

11 Configuring the vFlash SD Card and Managing vFlash Partitions . . . . . 239

**Installing a vFlash or Standard SD Card . . . . . 240**
Removing a vFlash or Standard SD Card . . . . . 241

**Configuring vFlash or Standard SD Card Using RACADM . . . . . 243**
Displaying the vFlash or Standard SD Card Properties . . . . . 243
Enabling or Disabling the vFlash or Standard SD Card . . . . . 244
Initializing the vFlash or Standard SD Card . . . . . 244
Getting the Last Status on the vFlash or Standard SD Card . . . . . 244

Resetting the vFlash or Standard SD Card . . . . . 245

**Managing vFlash Partitions Using iDRAC6 Web Interface . . . . . 245**

Creating an Empty Partition . . . . . 245

Creating a Partition Using an Image File . . . . . 247

Formatting a Partition. . . . . 249

Viewing Available Partitions . . . . . 251

Modifying a Partition . . . . . 252

Attaching and Detaching Partition . . . . . 252

Deleting Existing Partitions. . . . . 254

Downloading Partition Contents . . . . . 254

Booting to a Partition . . . . . 255

**Managing vFlash Partitions Using RACADM . . . . . 256**

Creating a Partition . . . . . 257

Deleting a Partition . . . . . 258

Getting the Status of a Partition . . . . . 258

Viewing Partition Information . . . . . 258

Booting to a Partition . . . . . 258

Attaching or Detaching a Partition . . . . . 259

Modifying a Partition . . . . . 259

**Frequently Asked Questions. . . . . 259**

12 Configuring and Using Virtual Media . . . . . 261

**Overview . . . . . 261**

Windows-Based Management Station . . . . . 262

Linux-Based Management Station . . . . . 263

**Configuring Virtual Media . . . . . 264**

**Running Virtual Media . . . . . 265**

Disconnecting Virtual Media . . . . . 267
Booting From Virtual Media. . . . . 267
Installing Operating Systems Using Virtual Media . . . . . 268
Using Virtual Media When the Server's Operating System Is Running . . . . . 269

**Frequently Asked Questions** . . . . . **269**

13 Using the RACADM Command Line Interface . . . . . 275

**RACADM Subcommands** . . . . . **276**

**Using local RACADM Commands** . . . . . **278**

**Using the RACADM Utility to Configure iDRAC6** . . . **279**
Displaying Current iDRAC6 Settings . . . . . 279
Managing iDRAC6 Users with RACADM . . . . . 280
Adding an iDRAC6 User. . . . . 281
Enabling an iDRAC6 User With Permissions . . . . . 281
Uploading, Viewing, and Deleting SSH Keys Using RACADM . . . . . 282
Removing an iDRAC6 User . . . . . 283
Testing E-mail Alerting . . . . . 283
Testing iDRAC6 SNMP Trap Alert Feature . . . . 284
Configuring iDRAC6 Network Properties . . . . . 284
Configuring IPMI Over LAN. . . . . 286
Configuring PEF . . . . . 288
Configuring PET. . . . . 288
Configuring IP Filtering (IP Range) . . . . . 290
Configuring IP Blocking. . . . . 292
Configuring iDRAC6 Telnet and SSH Services Using Local RACADM. . . . . 294

**Remote and SSH/Telnet RACADM** . . . . . **295**
Remote RACADM Usage . . . . . 296
Remote RACADM Options . . . . . 296

**Using an iDRAC6 Configuration File** . . . . . **297**
Creating an iDRAC6 Configuration File . . . . . 297
Configuration File Syntax . . . . . 298
Modifying iDRAC6 IP Address in a Configuration File . . . . . 300
Loading the Configuration File Into iDRAC6 . . . . 300

**Configuring Multiple iDRAC6s** . . . . . **302**

14 Power Monitoring and Power Management . . . . . 305

**Configuring and Managing Power** . . . . . **306**

**Power Monitoring** . . . . . **306**
Viewing Power Monitoring . . . . . 307

**Power Budgeting** . . . . . **309**
Viewing Power Budget . . . . . 311
Power Budget Threshold . . . . . 312
Viewing and Modifying PCIe Power Allocation . . . . . 313

**Power Control** . . . . . **314**
Executing Power Control Operations on the Server . . . . . 314

15 Using iDRAC6 Enterprise SM-CLP Command Line Interface . . . . . 317

**System Management With SM-CLP** . . . . . **318**

**iDRAC6 SM-CLP Support** . . . . . **318**
How to start an SM–CLP session . . . . . 318

**SM-CLP Features** . . . . . **319**

**Navigating the MAP Address Space** . . . . . **322**
Targets . . . . . 322

**Using the Show Verb** . . . . . **322**
Using the -display Option . . . . . 322
Using the -level Option . . . . . 323
Using the -output Option . . . . . 323

**iDRAC6 SM-CLP Examples** . . . . . **323**
Server Power Management . . . . . 324
SEL Management . . . . . 324
MAP Target Navigation . . . . . 324

16 Using the WS-MAN Interface . . . . . 329

**WS-Management Features** . . . . . **329**

**Supported CIM Profiles** . . . . . **330**

17 Deploying Your Operating System Using iVMCLI . . . . . 335

**Before You Begin** . . . . . **335**
Remote System Requirements . . . . . 335
Network Requirements . . . . . 335

**Creating a Bootable Image File** . . . . . **336**
Creating an Image File for Linux Systems . . . . 336
Creating an Image File for Windows Systems . . . . . 336

**Preparing for Deployment** . . . . . **336**
Configuring the Remote Systems . . . . . 336

**Deploying the Operating System** . . . . . **337**

**Using the Virtual Media Command Line Interface Utility** . . . . . **339**
Installing the iVMCLI Utility . . . . . 340
Command Line Options . . . . . 340
iVMCLI Parameters . . . . . 341
iVMCLI Operating System Shell Options . . . . . 345

18 Using iDRAC6 Configuration Utility . . . . . 347

**Overview** . . . . . **347**

**Starting iDRAC6 Configuration Utility** . . . . . **348**

**Using iDRAC6 Configuration Utility** . . . . . **348**
iDRAC6 LAN . . . . . 349
IPMI Over LAN . . . . . 349
LAN Parameters . . . . . 350
Virtual Media Configuration . . . . . 353
System Services . . . . . 355
LAN User Configuration . . . . . 355
Reset to Default . . . . . 358
System Event Log Menu . . . . . 358
Exiting iDRAC6 Configuration Utility . . . . . 359

19 Recovering and Troubleshooting the Managed System . . . . . 361

**Safety First – For You and Your System** . . . . . **361**

**Trouble Indicators** . . . . . **362**
LED Indicators . . . . . 362
Hardware Trouble Indicators . . . . . 363
Other Trouble Indicators . . . . . 363

**Problem Solving Tools** . . . . . **364**
Checking the System Health . . . . . 364
Checking the System Event Log (SEL) . . . . . 365
Checking the Post Codes . . . . . 367
Viewing the Last System Crash Screen. . . . . 367
Viewing the Most Recent Boot Sequences . . . . . 368
Viewing and Adding Work Notes . . . . . 369
Checking the Server Status Screen for Error Messages . . . . . 369
Viewing iDRAC6 Log . . . . . 377
Viewing System Information . . . . . 379
Identifying the Managed Server in the Chassis . . . . . 379
Using the Diagnostics Console . . . . . 380
Managing Power on a Remote System . . . . . 381

**Troubleshooting and Frequently Asked Questions** . . . . . **383**

Index . . . . . 389

# 1

# iDRAC6 Enterprise Overview

The Integrated Dell Remote Access Controller (iDRAC6) Enterprise is a systems management hardware and software solution that provides remote management capabilities, crashed system recovery, and power control functions for the Dell PowerEdge systems.

iDRAC6 uses an integrated system-on-chip microprocessor for the remote monitor/control system, and co-exists on the system board with the managed Dell PowerEdge server. The server operating system executes application programs; iDRAC6 monitors and manages the server's environment and state outside of the operating system.

You can configure iDRAC to send an e-mail or Simple Network Management Protocol (SNMP) trap alert for warnings or errors. To help you diagnose the cause of a system crash, iDRAC6 can log event data and capture an image of the screen when it detects that the system has crashed.

Managed servers are installed in a Dell M1000e system enclosure (chassis) with modular power supplies, cooling fans, and a Chassis Management Controller (CMC). CMC monitors and manages all components installed in the chassis. Add a redundant CMC to provide hot failover if the primary CMC fails. The chassis provides access to iDRAC6 devices through its LCD display, local console connections, and its Web interface. Each blade in a chassis has an iDRAC6. You can install up to 16 blades in M1000e.

All network connections to iDRAC6 are routed through CMC network interfaces (CMC RJ45 connection port labeled "GB1"). CMC routes traffic to the iDRAC6 devices through a private, internal network. This private management network is outside of the server's data path and outside of the operating system's control—that is, it is *out-of-band*. The managed server's *inband* network interfaces are accessed through I/O modules (IOMs) installed in the chassis.

**NOTE:** It is recommended that you isolate or separate the chassis management network, used by iDRAC6 and CMC, from your production network(s). Mixing management and production or application network traffic may cause congestion or network saturation resulting in CMC and iDRAC6 communication delays. The delays may cause unpredictable chassis behavior such as CMC displaying that iDRAC6 is offline even though it is operating properly. This may also cause other unpredictable behavior.

iDRAC6 network interface is disabled by default. Configure iDRAC6 network interface before iDRAC6 is made accessible. After iDRAC6 is enabled and configured on the network, you can access iDRAC throught its assigned IP address with iDRAC6 Web interface, Telnet or SSH, and supported network management protocols, such as Intelligent Platform Management Interface (IPMI).

## What's New in This Release

- View system hardware and firmware inventory
- View Lifecycle Controller work notes
- View Lifecycle Controller version number on GUI and CLI
- Filter the IPMI OEM messages from System Event Log
- Add additional Mezzanine cards
- Add additional LOM cards for Dell PowerEdge M710HD
- View the Express Service Code on GUI and CLI
- Reset the default Web certificate
- Perform one-to-many updates through CMC
- Remotely-manage MAC addresses

## IPv6 Ready Logo Certification

The IPv6 Ready Logo Committee's mission is to define the test specifications for IPv6 conformance and interoperability testing, to provide access to self-test tools, and to deliver the IPv6 Ready Logo.

iDRAC6 is **Phase-2 IPv6 Ready Logo** certified and the Logo ID is **02-C-000380**. For information on the IPv6 Ready Logo Program, see **URL ipv6ready.org/**.

## iDRAC6 Security Features

The following features are available in iDRAC security:

- User authentication through Microsoft Active Directory, generic LDAP Directory Service, or locally administered user IDs and passwords
- Two-factor authentication provided by the Smart–Card logon feature. The two-factor authentication is based on what the users *have* (the Smart– Card) and what they *know* (the PIN)
- Role-based authorization, which enables an administrator to configure specific privileges for each user
- User ID and password configuration
- SM-CLP 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 (where applicable)
- Secure Shell (SSH), which 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
- Configurable client IP address range for clients connecting to iDRAC6

# iDRAC6 Enterprise and vFlash Media

iDRAC6 Enterprise provides SD card slots for vFlash Media. For more information about iDRAC6 Enterprise and vFlash Media, see the *Hardware Owner's Manual* at **support.dell.com/manuals**.

Table 1-1 lists the features available for iDRAC6 Enterprise and vFlash Media.

**Table 1-1. iDRAC6 Feature List**

| Feature | iDRAC6 Enterprise | iDRAC6 Enterprise with vFlash Media |
|---|---|---|
| **Interface and Standards Support** | | |
| IPMI 2.0 | ✔ | ✔ |
| Web GUI | ✔ | ✔ |
| SNMP | ✔ | ✔ |
| WS–MAN | ✔ | ✔ |
| SM-CLP | ✔ | ✔ |
| RACADM Command Line | ✔ | ✔ |
| **Connectivity** | | |
| Shared/Failover Network Modes | ✔ | ✔ |
| IPv4 | ✔ | ✔ |
| VLAN Tagging | ✔ | ✔ |
| IPv6 | ✔ | ✔ |
| Dynamic DNS | ✔ | ✔ |
| Dedicated NIC | ✔ | ✔ |
| **Security and Authentication** | | |
| Role-based Authorization | ✔ | ✔ |

**Table 1-1. iDRAC6 Feature List *(continued)***

| Feature | iDRAC6 Enterprise | iDRAC6 Enterprise with vFlash Media |
|---|---|---|
| Local Users | ✓ | ✓ |
| Active Directory | ✓ | ✓ |
| Two-factor Authentication | ✓ | ✓ |
| Single sign-on | ✓ | ✓ |
| SSL Encryption | ✓ | ✓ |
| **Remote Management and Remediation** | | |
| Remote Firmware Update | ✓ | ✓ |
| Server Power Control | ✓ | ✓ |
| Serial-over-LAN (with proxy) | ✓ | ✓ |
| Serial-over-LAN (no proxy) | ✓ | ✓ |
| Power Capping | ✓ | ✓ |
| Last Crash Screen Capture | ✓ | ✓ |
| Boot Capture | ✓ | ✓ |
| Virtual Media | ✓ | ✓ |
| Remote File Share | ✓ | ✓ |
| Virtual Console | ✓ | ✓ |
| Virtual Console Sharing | ✓ | ✓ |
| vFlash | ✗ | ✓ |
| **Monitoring** | | |
| Sensor Monitoring and Alerting | ✓ | ✓ |
| Real-time Power Monitoring | ✓ | ✓ |

**Table 1-1. iDRAC6 Feature List *(continued)***

| Feature | iDRAC6 Enterprise | iDRAC6 Enterprise with vFlash Media |
|---|---|---|
| Real-time Power Graphing | ✓ | ✓ |
| Historical Power Counters | ✓ | ✓ |
| System Inventory | ✓ | ✓ |
| **Logging** | | |
| System Event Log (SEL) | ✓ | ✓ |
| RAC Log | ✓ | ✓ |
| Trace Log | ✓ | ✓ |
| Remote Syslog | ✓ | ✓ |
| Work Notes | ✓ | ✓ |

✓ = Supported; ✗=Not Supported

# Supported Platforms

For the latest supported platforms, see iDRAC6 Readme file and the *Dell Systems Software Support Matrix* available at **support.dell.com/manuals**.

# Supported Operating Systems

For the latest information, see iDRAC6 Readme file and the *Dell Systems Software Support Matrix* available at **support.dell.com/manuals**.

## Supported Web Browsers

For the latest information, see the readme file and the *Dell Systems Software Support Matrix* available at **support.dell.com/manuals**. On the **Manuals** page, click **Software→ Systems Management**. Click on the appropriate product link on the right-side to access the documents.

**NOTE:** Support for SSL 2.0 has been discontinued because of security flaws. Ensure that your browser is configured to enable SSL 3.0.

## Supported Remote Access Connections

Table 1-2 lists the connection features.

**Table 1-2. Supported Remote Access Connections**

| Connection | Features |
|---|---|
| iDRAC6 NIC | • 10Mbps/100Mbs/1Gbps Ethernet via CMC Gb Ethernet port.<br>• DHCP support.<br>• SNMP traps and e-mail event notification.<br>• SM–CLP shell and RACADM commands for operations such as iDRAC6 configuration, system boot, reset, power on, and shutdown commands are supported through SSH and Telnet.<br>• Support for IPMI utilities, such as IPMItool and ipmish. |

## iDRAC6 Ports

Table 1-3 lists the ports on which iDRAC6 listens for connections. Table 1-4 identifies the ports that iDRAC6 uses as a client. This information is required when opening firewalls for remote access to an iDRAC6.

**CAUTION: iDRAC6 does not check for conflicts between configurable ports. When setting port configurations, verify that the port assignments do not conflict with each other.**

**Table 1-3. iDRAC6 Server Listening Ports**

| Port Number | Function |
|---|---|
| 22* | Secure Shell (SSH) |
| 23* | Telnet |
| 80* | HTTP |
| 443* | HTTPS |
| 623 | RMCP/RMCP+ |
| 3668, 3669 | Virtual Media Service |
| 3670, 3671 | Virtual Media Secure Service |
| 5900* | Virtual Console keyboard/mouse |
| 5901* | Virtual Console video |
| 5988 | Used for WSMAN |

* Configurable port

**Table 1-4. iDRAC6 Client Ports**

| Port Number | Function |
|---|---|
| 25 | SMTP |
| 53 | DNS |
| 68 | DHCP-assigned IP address |
| 69 | TFTP |
| 162 | SNMP trap |
| 636 | LDAPS |
| 3269 | LDAPS for global catalog (GC) |

## Other Documents You May Need

In addition to this guide, the following documents provide additional information about the setup and operation of iDRAC6 in your system. You can access these guides available on the Dell Support website at **support.dell.com/manuals**. On the **Manuals** page, click **Software→ Systems Management**. Click on the appropriate product link on the right-side to access the documents.

- iDRAC6 online help provides information about using the Web interface.
- The *Dell Systems Software Support Matrix* provides information about the various Dell systems, the operating systems supported by these systems, and the installable Dell OpenManage components on these systems.
- 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 Chassis Management Controller User Guide* provide information about using the controller that manages all modules in the chassis containing your Dell PowerEdge server.
- The *Dell OpenManage IT Assistant User's Guide* provides information about using IT Assistant.
- The *Dell Management Console User's Guide* provides information about using Dell Management Console.
- The *Dell OpenManage Server Administrator User's Guide* provides information about installing and using Server Administrator.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.
- The *Dell Lifecycle Controller User Guide* provides information on the Unified Server Configurator (USC), the Unified Server Configurator – Lifecycle Controller Enabled (USC – LCE), and Remote Services.

- The *iDRAC6 CIM Element Mapping* and *iDRAC6 SM-CLP Property Database* documents available on the Dell Enterprise Technology Center at **delltechcenter.com** provide information on iDRAC6 SM–CLP Property Database, mappings between WS–MAN classes and SM–CLP targets and Dell implementation details.
- The *Dell RACADM Command Line Reference Guide for iDRAC6 and CMC* provides information about the RACADM subcommands, supported RACADM interfaces, and property database groups and object definitions for iDRAC6 Enterprise on Blade Servers, iDRAC6 Enterprise or Express on Rack and Tower Servers, and CMC.
- The *Glossary* provides information about the terms used in this document.

The following system documents are also available to provide more information about the system in which iDRAC6 is installed:

- 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 *Getting Started Guide* provides an overview of system features, setting up your system, and technical specifications.
- The *Hardware Owner's Manual* provides information about system features and describes how to troubleshoot the system and install or replace system components.
- Systems management software documentation describes the features, requirements, installation, and basic operation of the software.
- Operating system documentation describes how to install (if necessary), configure, and use the operating system software.
- Documentation for any components you purchased separately provides information to configure and install these options.

- Updates are sometimes included with the system to describe changes to the system, software, and/or documentation.

  **NOTE:** Always read the updates first because they often supersede information in other documents.

- Release notes or readme files are included to provide last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians.

# 2

# Configuring iDRAC6 Enterprise

This section provides information about how to establish access to iDRAC6 and to configure your management environment to use iDRAC6.

## Before You Begin

Gather the following items prior to configuring iDRAC6:

- *Dell Chassis Management Controller Firmware User Guide*
- *Dell Systems Management Tools and Documentation* DVD

The *Dell Systems Management Tools and Documentation* DVD includes the following components:

- DVD root — Contains the Dell Systems Build and Update Utility, which provides server setup and system installation information
- SYSMGMT — Contains the systems management software products including Dell OpenManage Server Administrator

For more information, see the *Dell OpenManage Server Administrator Installation Guide* and the *Dell OpenManage Management Station Software Installation Guide* available on the Dell Support website at **support.dell.com/manuals**.

## Interfaces for Configuring iDRAC6

You can configure iDRAC6 using iDRAC6 Configuration Utility, iDRAC6 Web interface, Chassis Management Controller (CMC) Web interface, Chassis LCD Panel, the local and remote RACADM CLI, iVMCLI, or the SM-CLP CLI. The local RACADM CLI is available after you have installed the operating system and the Dell OpenManage software on the managed server. Table 2-1 describes these interfaces.

For greater security, access to iDRAC6 configuration through iDRAC6 Configuration Utility or disable the local RACADM CLI using a RACADM command (see *RACADM Command Line Reference Guide for iDRAC and CMC* available on **support.dell.com/manuals**) or from the GUI (see "Enabling or Disabling Local Configuration Access" on page 119.)

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

**Table 2-1. Configuration Interfaces**

| Interface | Description |
|---|---|
| iDRAC6 Configuration Utility | Accessed at boot time, iDRAC6 Configuration Utility is useful when installing a new Dell PowerEdge server. Use it for setting up the network and basic security features and for enabling other features. |
| iDRAC6 Web Interface | iDRAC6 Web interface is a browser-based management application that you can use to interactively manage iDRAC6 and monitor the managed server. It is the primary interface for day-to-day tasks, such as monitoring system health, viewing the system event log, managing local iDRAC6 users, and launching CMC Web interface and Virtual Console sessions. |
| CMC Web Interface | In addition to monitoring and managing the chassis, use the CMC Web interface to view the status of a managed server, update iDRAC6 firmware, configure iDRAC6 network settings, logon to iDRAC6 Web interface, and to start, stop, or reset the managed server. |

**Table 2-1. Configuration Interfaces *(continued)***

| Interface | Description |
|---|---|
| Chassis LCD Panel | Use the LCD panel on the chassis containing iDRAC6 to view the high-level status of the servers in the chassis. During initial configuration of CMC, the configuration wizard allows you to enable DHCP configuration of iDRAC6 networking. |
| Local and Remote RACADM | The local RACADM command line interface runs on the managed server.<br>Remote RACADM is a client utility which runs on a management station. It uses the out-of-band network interface to run RACADM commands on the managed server. The **–r** option runs the RACADM command over a network.<br>RACADM commands provide access to nearly all iDRAC6 features. You can inspect sensor data, system event log records, and the current status and configuration values maintained in iDRAC6. You can alter iDRAC6 configuration values, manage local users, enable and disable features, and perform power functions such as shutting down or rebooting the managed server. |
| iVMCLI | iDRAC6 Virtual Media Command Line Interface (iVMCLI) provides the managed server access to media on the management station. It is useful for developing scripts to install operating systems on multiple managed servers. |

**Table 2-1. Configuration Interfaces *(continued)***

| Interface | Description |
|---|---|
| SM-CLP | SM-CLP is the Server Management Workgroup Server Management-Command Line Protocol (SM-CLP) implementation incorporated in iDRAC6. The SM-CLP command line is accessed by logging in to iDRAC6 using Telnet or SSH and typing `smclp` at the CLI prompt.<br><br>SM-CLP commands implement a useful 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. |
| IPMI | IPMI defines a standard way for embedded management subsystems, such as iDRAC6, to communicate with other embedded systems and management applications.<br><br>You can use iDRAC6 Web interface, SM-CLP, or RACADM commands to configure IPMI Platform Event Filters (PEF) and Platform Event Traps (PET).<br><br>PEFs cause iDRAC6 to perform specific actions (for example, rebooting the managed server) when it detects a condition. PETs instruct iDRAC6 to send e-mail or IPMI alerts when it detects specified events or conditions.<br><br>You can also use standard IPMI tools such as **IPMItool** and **ipmish** with iDRAC6 when you enable IPMI Over LAN. |

# Configuration Tasks

This section is an overview of the configuration tasks for the management station, iDRAC6, and the managed server. Performable tasks include configuring iDRAC6 for remote accessibility, configuring iDRAC6 features you want to use, installing the operating system on the managed server, and installing management software on your management station and the managed server.

The configuration tasks required to perform each task are listed beneath that task.

**NOTE:** Before performing the configuration procedures in this guide, install CMC and I/O modules in the chassis and configure, and physically install the Dell PowerEdge server in the chassis.

### Configure the Management Station

Set up a management station by installing the Dell OpenManage software, a Web browser, and other software utilities. See "Configuring the Management Station" on page 65.

### Configure iDRAC6 Networking

Enable iDRAC6 network and configure IP, netmask, gateway, and DNS addresses.

**NOTE:** Access to iDRAC6 configuration through iDRAC6 Configuration Utility or disable the local RACADM CLI using a RACADM command (see *RACADM Command Line Reference Guide for iDRAC and CMC* available on **support.dell.com/manuals**) or from the GUI (see "Enabling or Disabling Local Configuration Access" on page 119.)

**NOTE:** Changing iDRAC6 network settings terminates all current network connections to iDRAC6.

**NOTE:** The option to configure the server using the LCD panel is available *only* during CMC initial configuration. Once the chassis is deployed, you cannot reconfigure iDRAC6 using the LCD panel.

**NOTE:** Use the LCD panel only to enable DHCP to configure iDRAC6 network.

- Chassis LCD Panel — See the *Dell Chassis Management Controller Firmware User Guide*.
- iDRAC6 Configuration Utility — See "Using iDRAC6 Configuration Utility" on page 347.
- CMC Web interface — See "Configuring Network Settings Using CMC Web Interface" on page 39.
- Remote and local RACADM — See **cfgLanNetworking** in the *RACADM Command Line Reference Guide for iDRAC and CMC* available on **support.dell.com/manuals**.

### Configure iDRAC6 Users

Set up the local iDRAC6 users and permissions. iDRAC6 holds a table of sixteen local users in firmware. You can set usernames, passwords, and roles for these users.

- iDRAC6 Configuration Utility (configures administrative user only) — See "LAN User Configuration" on page 355.
- iDRAC6 Web interface — See "Adding and Configuring iDRAC6 Users" on page 99.
- Remote and local RACADM — See "Adding an iDRAC6 User" on page 281.

**NOTE:** When using iDRAC6 in an Active Directory / generic LDAP Directory Service environment, ensure that your user names conform to the Active Directory / generic LDAP Directory Service naming convention in force.

### Configure Directory Services

In addition to the local iDRAC6 users, you can use Microsoft Active Directory or generic LDAP Directory Service to authenticate iDRAC6 user logins.

For more information, see "Using iDRAC6 Directory Service" on page 127.

### Configure IP Filtering and IP Blocking

In addition to user authentication, you can prevent unauthorized access by rejecting connection attempts from IP addresses outside of a defined range and by temporarily blocking connections from IP addresses where authentication has failed multiple times within a configurable timespan.

- iDRAC6 Web interface — See "Configuring IP Filtering and IP Blocking" on page 92.
- RACADM — See "Configuring IP Filtering (IP Range)" on page 290 and "Configuring IP Blocking" on page 292.

### Configure Platform Events

Platform events occur when iDRAC6 detects a warning or critical condition from one of the managed server's sensors.

Configure Platform Event Filters (PEF) to choose the actions you want to execute, such as rebooting the system, when an event is detected.

- iDRAC6 Web interface — See "Configuring Platform Event Filters (PEF)" on page 95.
- RACADM — See "Configuring PEF" on page 288.

Configure Platform Event Traps (PET) to send alert notifications to an IP address, such as a management station with management software or to send an e-mail to a specified e-mail address.

- iDRAC6 Web interface — See "Configuring Platform Event Traps (PET)" on page 95.
- RACADM — See "Configuring PET" on page 288.

### Enabling or Disabling Local Configuration Access

You can disable access to critical configuration parameters, such as network configuration and user privileges. Once disabled, the setting remains persistent across reboots. Configuration write access is blocked for both the local RACADM program and iDRAC6 Configuration Utility (at boot). Web access to configuration parameters is unimpeded and configuration data is always available for viewing. For information about iDRAC6 Web interface, see "Enabling or Disabling Local Configuration Access" on page 119.

For RACADM commands, see **cfgRacTuning** in the *RACADM Command Line Reference Guide for iDRAC and CMC* available at **support.dell.com/manuals**.

### Configure iDRAC6 Services

Enable or disable iDRAC6 network services — such as Telnet, SSH, and the Web server interface — and reconfigure ports and other service parameters.

- iDRAC6 Web interface — See "Configuring iDRAC6 Services" on page 120
- RACADM — See "Configuring iDRAC6 Telnet and SSH Services Using Local RACADM" on page 294

### Configure Secure Sockets Layer (SSL)

Configure SSL for iDRAC6 Web server.

- iDRAC6 Web interface — See "Secure Sockets Layer (SSL)" on page 107
- RACADM — See cfgRacSecurity, sslcsrgen, sslcertupload, sslcertdownload, and sslcertview in the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

### Configure Virtual Media

Configure the virtual media feature so that you can install the operating system on the Dell PowerEdge server. 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.

- iDRAC6 Web interface — See "Configuring and Using Virtual Media" on page 261
- iDRAC6 Configuration Utility — See "Virtual Media Configuration" on page 353

### Configure a vFlash Media Card

Install and configure a vFlash Media card for use with iDRAC6.

- iDRAC6 Web interface and Using RACADM — See "Configuring the vFlash SD Card and Managing vFlash Partitions" on page 239

### Install the Managed Server Software

Install the operating system on the Dell PowerEdge server using virtual media and then install the Dell OpenManage software on the managed Dell PowerEdge server and set up the last crash screen feature.

- Virtual Console — See "Installing the Software on the Managed Server" on page 81
- iVMCLI — See "Using the Virtual Media Command Line Interface Utility" on page 339

### Configure the Managed Server for the Last Crash Screen Feature

Set up the managed server so that iDRAC6 can capture the screen image after an operating system crash or freeze.

- Managed server — See "Configuring the Managed Server to Capture the Last Crash Screen" on page 82 and "Disabling the Windows Automatic Reboot Option" on page 83

# Configuring Network Settings Using CMC Web Interface

**NOTE:** You must have Chassis Configuration Administrator privilege to set up iDRAC6 network settings from CMC.

**NOTE:** The default CMC username is **root** and the default password is **calvin**.

### Launching iDRAC6 Web Interface From CMC

CMC provides limited management of individual chassis components, such as servers. For complete management of these individual components, CMC provides a launch point for the server's iDRAC6 Web interface.

To launch iDRAC6 from CMC:

1. Log in to CMC Web interface.
2. In the system tree, select **Server Overview**. The **Servers Status** screen displays the list of available servers.
3. Click **iDRAC** for the server you want to manage. The iDRAC GUI is launched in a new browser window.

To launch iDRAC6 Web interface for a single server from CMC:

1. Log in to CMC Web interface.
2. Expand **Server Overview** in the system tree. All of the servers appear in the expanded **Servers** list.
3. Click the server you want to view. The **Server Status** screen for the server you selected displays.
4. Click **Launch iDRAC6 GUI**.

#### Single Sign-On

Using the single sign-on feature, you can launch iDRAC6 Web interface from CMC without having to log in a second time. Single sign-on policies are described below.

- A CMC user who has **Server Administrator** set under **User Privileges** is automatically logged in to iDRAC6 Web interface using single sign-on. After logging in, the user is automatically granted iDRAC6 Administrator privileges. This is true even if the same user does not have an account on iDRAC6, or if the account does not have Administrator privileges.
- A CMC user who does not have **Server Administrator** set under **User Privileges**, but has the same account on iDRAC6, is automatically logged in to iDRAC6 using single sign-on. Once logged in to iDRAC6 Web interface, this user is granted the privileges that were created for iDRAC6 account.

  **NOTE:** In this context, *the same account* means that the user has the same username and password for CMC as for iDRAC6. A user who has the same username but a different password is not recognized as a valid user.

- A CMC user who does not have **Server Administrator** set under **User Privileges**, or the same account on iDRAC6, is *not* automatically logged in to iDRAC6 using single sign-on. This user is directed to iDRAC6 log in screen after clicking **Launch iDRAC6 GUI**.

  **NOTE:** If iDRAC6 network LAN is disabled (LAN Enabled = No), single sign–on is not available.

  **NOTE:** If the server is removed from the chassis, iDRAC6 IP address is changed, or there is a problem in iDRAC6 network connection, then clicking the **Launch iDRAC6 GUI** icon may display an error screen.

### Configuring Networking for iDRAC6

1. Click **System→ iDRAC Settings→ Network/Security** tab.
2. To enable or disable Serial Over LAN:
   a. Click **Serial Over LAN**.

      The **Serial Over LAN** screen is displayed.

   b. Select the **Enable Serial Over LAN** check box. You may also change the **Baud Rate** and **Channel Privilege Level Limit** settings.

   c. Click **Apply**.
3. To enable or disable IPMI Over LAN:
   a. Click **Network**.

      The **Network** screen is displayed.

   b. Click **IPMI Settings**.

   c. Select the **Enable IPMI Over LAN** check box. You may also change the **Channel Privilege Level Limit** and **Encryption Key** settings.

   d. Click **Apply**.
4. To enable or disable DHCP:
   a. Click **Network**.

      The **Network** screen is displayed.

   b. In the **IPv4 Settings** section, select the **DHCP Enable** and **Use DHCP to obtain DNS Server Addresses** check boxes.

   c. In the **IPv6 Settings** section, select the **Autoconfiguration Enable** and the **Use DHCPv6 to obtain DNS Server Addresses** check boxes.

   d. Click **Apply**.

   **NOTE:** If you choose not to enable DHCP, you must enter the static IP address, netmask, and default gateway for the server.

# Viewing FlexAddress Mezzanine Card Fabric Connections

The M1000e includes FlexAddress, an advanced multilevel, multistandard networking system. FlexAddress allows the use of persistent, chassis-assigned World Wide Names and MAC addresses (WWN/MAC) for each managed server port connection.

**NOTE:** To avoid errors that may lead to an inability to power on the managed server, you *must* have the correct type of mezzanine card installed for each port and fabric connection.

Configuration of the FlexAddress feature is performed using CMC Web interface. For more information on the FlexAddress feature and its configuration, see the *Dell Chassis Management Controller User Guide* and the *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* document.

After the FlexAddress feature has been enabled and configured for the chassis, click **System→ Properties** tab→ **WWN/MAC** to view a list of installed mezzanine cards, the fabrics to which they are connected, type of fabric, and server-assigned or chassis-assigned MAC addresses for each installed embedded Ethernet and optional mezzanine card port.

The **Server–Assigned** column displays the server–assigned WWN/MAC addresses embedded in the controller's hardware. WWN/MAC addresses showing **N/A** indicate that an interface for the specified fabric is not installed.

The **Chassis–Assigned** column displays the chassis–assigned WWN/MAC addresses used for the particular slot. WWN/MAC addresses showing **N/A** indicate that the FlexAddress feature is not installed.

The **Remotely-Assigned** column displays the user-assigned WWN/MAC address through WSMAN. This is displayed only if the FlexAddress is disabled and remote management is enabled. See the *Dell Lifecycle Controller User's Guide* and the *iDRAC6 CIM Element Mapping* for more information.

A check mark in the **Server–Assigned**, **Chassis–Assigned**, and **Remotely-Assigned** columns indicates the active addresses.

When chassis flex address is enabled, iDRAC GUI displays the CMC assigned MAC address and not remotely-assigned MAC address. The server-assigned MAC address is displayed but is not active.

When the remotely-assigned MAC addresses are active, the CMC Web interface page displays the MAC address as remotely managed for a particular slot in the chassis.

The remotely-assigned addresses are displayed only on the iDRAC Out-Of-Band (OOB) GUI and not through other interfaces such as RACADM and IPMI tools.

### FlexAddress MAC for iDRAC6

The FlexAddress feature replaces the server–assigned MAC addresses with chassis–assigned MAC addresses and is implemented for iDRAC6 along with blade LOMs, mezzanine cards and I/O modules. The iDRAC6 FlexAddress feature supports preservation of slot specific MAC address for iDRAC6s in a chassis. The chassis–assigned MAC address is stored in CMC non–volatile memory and is sent to iDRAC6 during an iDRAC6 boot or when CMC FlexAddress page settings are changed.

If CMC enables chassis–assigned MAC addresses, iDRAC6 displays the value in the **MAC Address** field on the following screens:

- **System→ Properties** tab**→ System Details→ iDRAC6 Information**
- **System→ Properties** tab**→ WWN/MAC**
- **System→ iDRAC Settings→ Properties** tab**→ Remote Access Information→ Network Settings**
- **System→ iDRAC Settings→ Network/Security** tab**→ Network→ Network Interface Card Settings**

**CAUTION: With FlexAddress enabled, if you switch from a server–assigned MAC address to a chassis–assigned MAC address and vice–versa, iDRAC6 IP address also changes.**

**NOTE:** You can enable or disable the FlexAddress feature only through CMC. iDRAC6 GUI only reports the status. Any existing Virtual Console or Virtual Media session terminates if the FlexAddress setting is changed in the CMC FlexAddress page.

#### Enabling FlexAddress through RACADM

You cannot enable FlexAddress from iDRAC6. Enable FlexAddress at the slot and fabric levels from CMC.

1. From CMC console, enable FlexAddress for the managed server on the slot with the following RACADM command:

   `racadm setflexaddr -i <slot_no> 1`, where `<slot_no>` is the slot number on which to enable FlexAddress.

2. Next, from CMC console, enable FlexAddress at the fabric level by executing the following RACADM command:

   `racadm setflexaddr -f <fabric_name> 1`, where `<fabric_name>` is A, B, or C.

3. To enable FlexAddress for all iDRAC6s in the chassis, from the CMC console, execute the following RACADM command:

   ```
   racadm setflexaddr -f idrac 1
   ```

See the *RACADM Command Line Reference Guide for iDRAC and CMC* for more information on CMC RACADM subcommands.

## Remote Syslog

iDRAC6 Remote Syslog feature allows you to remotely write the RAC log and the System Event Log (SEL) to an external syslog server. You can read all logs from the entire server farm from a central log.

The Remote Syslog protocol does not need any user authentication. To enter logs in the Remote Syslog server, ensure that there is proper network connectivity between iDRAC6 and the Remote Syslog server and that the Remote Syslog server is running on the same network as iDRAC6. The Remote Syslog entries are carried in UDP packets sent to the Remote Syslog server's syslog port. If network failures occur, iDRAC6 does not send the same log again. The remote logging happens real time as and when the logs are recorded in iDRAC6's RAC log and SEL log. You can also change iDRAC6 Remote Syslog settings through CMC.

To enable Remote Syslog through the remote Web interface:

1. Open a supported Web browser window.
2. Log in to iDRAC6 Web interface.
3. In the system tree, select **System→ Setup** tab**→ Remote Syslog Settings**. The **Remote Syslog Settings** screen is displayed.

Table 2-2 lists the Remote Syslog settings.

**Table 2-2. Remote Syslog Settings**

| Attribute | Description |
|---|---|
| **Remote Syslog Enabled** | Select this option to enable the transmission and remote capture of the syslog on the specified server. Once syslog is enabled, new log entries are sent to the Syslog server(s). |
| **Syslog Server 1–3** | Enter the Remote Syslog server address to log iDRAC6 messages like SEL Log and RAC Log. Syslog server addresses allows alphanumeric, -, ., :, and _ symbols. |
| **Port Number** | Enter the port number of the Remote Syslog server. Provide a value between 1 to 65535. Default is 514. |

**NOTE:** The severity levels defined by the Remote Syslog protocol differ from the standard IPMI System Event Log (SEL) severity levels. Hence all iDRAC6 Remote Syslog entries are reported in the syslog server with severity level as **Notice**.

The following example shows the configuration objects and the RACADM command usage to change remote syslog settings:

```
racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogEnable [1/0] ; default is 0

racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogServer1 <servername1> ; default is
blank

racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogServer2 <servername2>; default is
blank
```

```
racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogServer3 <servername3>; default is
blank

racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogPort <portnumber>; default is 514
```

# First Boot Device

This feature allows you to select the first boot device for your system and enable boot once. 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 iDRAC6 GUI or from the BIOS Boot sequence. If Boot Once is enabled, the system boots from the selected device only once. Subsequently, the system boots according to the BIOS Boot sequence.

To select the first boot device through the remote Web interface:

1. Open a supported Web browser window.
2. Log in to iDRAC6 Web interface.
3. In the system tree, select **System**→ **Setup** tab→ **First Boot Device**. The **First Boot Device** screen is displayed.

Table 2-3 lists the **First Boot Device** settings.

**Table 2-3. First Boot Device**

| Attribute | Description |
|---|---|
| **First Boot Device** | Select the first boot device from the drop-down list. The system will boot from the selected device on next and subsequent reboots. |
| **Boot Once** | Selected = Enabled; Deselected = Disabled. Check this option to boot from the selected device on the next boot. Thereafter, the system will boot from the first boot device in the BIOS boot order. |

# Remote File Share

iDRAC6 Remote File Share (RFS) feature allows you to specify a CD/DVD ISO image file located 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.

**NOTE:** This feature works only with IPv4 addresses. IPv6 addresses are currently not supported.

**NOTE:** 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 ensure 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 will display 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.

The format of the CIFS shared image path is:

```
//<ipaddress or domain
name>/<share_name>/<pathtoimage>
```

The format of the NFS shared image path is:

```
<ipadddress>:/<pathtoimage>
```

If a username contains a domain name, then the username must be entered in the form of *<user name>@<domain>*. For example, **user1@dell.com** is a valid username whereas **dell\user1** is not.

A filename that ends with the IMG extension is redirected as a Virtual Floppy and a filename ending with the ISO extension is redirected as a Virtual CDROM. Remote file share supports only .IMG and .ISO image file formats.

The RFS feature utilizes the underlying virtual media implementation in iDRAC6. You must have Virtual Media privileges to perform an RFS mounting. If a virtual drive is already used by Virtual Media, then the drive will not be available to mount as RFS and vice versa. For RFS to work, Virtual Media in iDRAC6 must be in the *Attach* or *Auto–Attach* modes.

The connection status for RFS is available in iDRAC6 log. Once connected, an RFS mounted virtual drive does not disconnect even if you log out from iDRAC6. The RFS connection is closed if iDRAC6 is reset or the network connection is dropped. GUI and command line options are also available in CMC and iDRAC6 to close the RFS connection. The RFS connection from CMC always overrides an existing RFS mount in iDRAC6.

**NOTE:** iDRAC6 vFlash feature and RFS are not related.

To enable remote file sharing through iDRAC6 Web interface, do the following:

1. Open a supported Web browser window.
2. Log in to iDRAC6 Web interface.
3. Select **System→ Remote File Share** tab.

   The **Remote File Share** screen is displayed.

Table 2-4 lists the remote file share settings.

**Table 2-4. Remote File Server Settings**

| Attribute | Description |
|---|---|
| **User Name** | Username to connect for NFS/CIFS file system. |
| **Password** | Password to connect for NFS/CIFS file system. |
| **Image File Path** | Path of the file to be shared through remote file share. |
| **Status** | **Connected**: The file is shared.<br>**Not Connected**: The file is not shared.<br>**Connecting... :** Busy connecting to the share |

4. Click **Connect** to establish a file share connection. The **Connect** button is disabled after successfully establishing a connection.

**NOTE:** Even if you have configured remote file sharing, the GUI does not display user credential information due to security reasons.

For remote file share, the remote RACADM command is

`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

`-s` ; display current status

**CAUTION: All characters including alphanumeric and special characters are allowed as part of username, password, and image_location except the following characters: ' (single quote), "(double quote), ,(comma), < (less than), and > (greater than). When using remote file share, the characters listed above are not allowed as part of the user name, password, and image_location.**

# Internal Dual SD Module

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. The iDRAC6 vFlash SD card, with the second SD card, can be set to IDSDM by setting the **Redundancy** option to **Mirror mode** in the **Integrated Devices** screen of the system BIOS setup. When the IDSDM feature is enabled, the vFlash functionality of iDRAC6 vFlash SD card is not available and this card is set as the secondary SD card in IDSDM. For more information about the BIOS options for IDSDM, see the *Hardware Owner's Manual* available on the Dell Support website at **support.dell.com/manuals**.

**NOTE:** In the BIOS setup, **Integrated Devices** screen, the **Internal USB Port** option must be set to **On**. If this is set to **Off**, the IDSDM will not be visible to the system as a boot device.

Either of the two SD cards can be the master. For example, if two new SD cards are installed in the IDSDM, SD1 will become the Active or master card. SD2 will be the standby card, and all file system IDSDM writes will go to both cards, but reads will occur only from SD1. At any time if SD1 fails or is removed, SD2 will automatically become the Active (master) card.

**Table 2-5. IDSDM Status**

| IDSDM - Mirror Mode | SD Card | vFlash SD Card |
|---|---|---|
| Enabled | Active (SD1 Card) | vFlash Inactive, Standby SD2 |
| Disabled | Active (SD2 Card) | Only vFlash Active |

Using iDRAC you can view the status, health, and availability of IDSDM.

The SD card redundancy status and failure events are logged to SEL, displayed on LCD, and PET alerts are generated if alerts are enabled.

### Viewing Internal Dual SD Module Status Using GUI

1. Log in to iDRAC Web GUI.
2. In the **System** tree, click **Removable Flash Media**. The **Removable vFlash Media** page is displayed. This page displays the following two sections:

- **Internal Dual SD Module** — Displayed only if IDSDM is in redundant mode. The **Redundancy Status** is displayed as **Full**. If this section is not present, then the card is in the non-redundant mode state. The valid **Redundancy Status** indications are:
  - **Full** — SD card 1 and 2 are functioning properly.
  - **Lost** — Either one or both the SD cards are not functioning properly.
- **Internal SD Module Status** — Displays the SD card state for SD1 and SD2 with the following information:
  - Status:
    - — Indicates that the card is ok.
    - — Indicates that the card is offline or write-protected.
    - — Indicates that an alert has been issued.
  - Location — Location of the SD cards.
  - Online Status — SD1 and SD2 cards can be in one of the states listed in Table 2-6.

**Table 2-6. SD1 and SD2 Card States**

| State | Description |
|---|---|
| Boot | The controller is powering up. |
| Active | The card receives all SD writes and is used for SD reads. |
| Standby | The card is the secondary card. It is receiving a copy of the all the SD writes. |
| Failed | An error is reported during a SD card read or write |
| Absent | The SD card is not detected |
| Offline | At boot, the CID signature of the card is different from the NV storage value or the card is the destination of a copy operation that is in-progress. |
| Write Protected | The card is write protected by the physical latch on the SD card. IDSDM cannot use a write-protected card. |

# Updating iDRAC6 Firmware

Updating iDRAC6 firmware installs a new firmware image in the flash memory. You can update the firmware using any of the following methods:

- iDRAC6 Web interface
- RACADM CLI
- Dell Update Package (for Linux or Microsoft Windows)
- DOS iDRAC6 firmware update utility
- CMC Web interface
- WSMAN interface

## Downloading the Firmware or Update Package

Download the firmware from **support.dell.com**. The firmware image is available in several different formats to support the different update methods available.

To update iDRAC6 firmware using iDRAC6 Web interface or to recover iDRAC6 using CMC Web interface, download the binary image packaged as a self-extracting archive.

To update iDRAC6 firmware from the managed server, download the operating system-specific Dell Update Package (DUP) for the operating system running on the server whose iDRAC6 you are updating.

To update iDRAC6 firmware using the DOS iDRAC6 Firmware update utility, download both the update utility and the binary image, which are packaged in self-extracting archive files.

## Executing the Firmware Update

**NOTE:** When iDRAC6 firmware update begins, all existing iDRAC6 sessions are disconnected and new sessions are not permitted until the update process is completed.

**NOTE:** The chassis fans run at 100% during iDRAC6 firmware update. When the update is complete, normal fan speed regulation resumes. This is normal behavior, designed to protect the server from overheating during a time when it cannot send sensor information to CMC.

To use a Dell Update Package for Linux or Microsoft Windows, execute the operating system-specific DUP on the managed server.

When using iDRAC6 Web interface or CMC Web interface, place the firmware binary image on a disk that is accessible to the management station from which you are running the Web interface. See "Updating iDRAC6 Firmware" on page 123.

**NOTE:** iDRAC6 Web interface also allows you to reset iDRAC6 configuration to the factory defaults.

**NOTE:** If the configuration is not preserved during firmware update, iDRAC6 generates new SHA1 and MD5 keys for the SSL certificate. Because the keys are different from those in the open Web browser, all browser windows that are connected to iDRAC6 must be closed after the firmware update is complete. If the browser windows are not closed, an **Invalid Certificate** error message is displayed.

You can use CMC Web interface or CMC RACADM to update iDRAC6 firmware. This feature is available when iDRAC6 firmware is in Normal mode, as well as when it is corrupted. See "Updating iDRAC6 Firmware Using CMC" on page 124.

**NOTE:** If you are rolling back iDRAC6 firmware to an earlier version, delete the existing Internet Explorer ActiveX browser plug-in on any Windows-based management station to allow the firmware to install a compatible version of the ActiveX plug-in.

### Verifying the Digital Signature for Linux DUPs

A digital signature is used to authenticate the identity of the signer of a file and to certify that the original content of the file has not been modified since it was signed.

If you do not already have it installed on your system, you must install the GNU Privacy Guard (GPG) to verify a digital signature.

To use the standard verification procedure, perform the following steps:

1. Download the Dell Linux public GnuPG key by navigating to **lists.us.dell.com** and clicking the **Dell Public GPG key** link. Save the file to your local system. The default name is **linux-security-publickey.txt**.
2. Import the public key to your GPG trust database by running the following command:

   ```
   gpg --import <Public Key Filename>
   ```

3 To prevent a distrusted-key warning, change the trust level for the Dell Public GPG key.

a Enter the following command:

```
gpg --edit-key 23B66A9D
```

b Within the GPG key editor, enter `fpr`. The following message is displayed:

```
pub 1024D/23B66A9D 2001-04-16 Dell, Inc.
(Product Group) <linux-security@dell.com>
Primary key fingerprint: 4172 E2CE 955A 1776
A5E6 1BB7 CA77 951D 23B6 6A9D
```

If the fingerprint of your imported key is the same as above, you have a correct copy of the key.

c While still in the GPG key editor, enter `trust`. The following menu is displayed:

```
Please decide how far you trust this user to
correctly verify other users' keys (by looking
at passports, checking fingerprints from
different sources, etc.)


  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu

Your decision?
```

d Enter `5`, then press <Enter>. The following prompt is displayed:

```
Do you really want to set this key to ultimate
trust? (y/N)
```

e Enter `y` <Enter> to confirm your choice.

f Enter `quit` <Enter> to exit the GPG key editor.

You must import and validate the public key only once.

4 Obtain the package you need (for example, the Linux DUP or self-extracting archive) and its associated signature file from the Dell Support website at **support.dell.com/support/downloads**.

**NOTE:** Each Linux Update Package has a separate signature file, which is shown on the same Web page as the Update Package. You need both the Update Package and its associated signature file for verification. By default, the signature file has the same name as the DUP filename with a **.sign** extension. For example, iDRAC6 firmware image has an associated **.sign** file (**IDRAC_FRMW_LX_2.2.BIN.sign**), which is included in the self-extracting archive with the firmware image (**IDRAC_FRMW_LX_2.2.BIN**). To download the files, right-click the **Download** link and use the **Save Target As** option.

5 Verify the Update Package:

```
gpg --verify <Linux Update Package signature
filename> <Linux Update Package filename>
```

The following example illustrates the steps that you must follow to verify a Dell PowerEdge M610 iDRAC6 Update Package:

1 Download the following two files from **support.dell.com**:

- IDRAC_FRMW_LX_2.2.BIN.sign
- IDRAC_FRMW_LX_2.2.BIN

2 Import the public key by running the following command line:

```
gpg --import <linux-security-publickey.txt>
```

The following output message is displayed:

```
gpg: key 23B66A9D: "Dell Computer Corporation
(Linux Systems Group) <linux-
security@dell.com>" not changed
gpg: Total number processed: 1
gpg: unchanged: 1
```

3 Set the GPG trust level for the Dell public key, if you have not done so previously.

a Enter the following command:

```
gpg --edit-key 23B66A9D
```

b At the command prompt, enter the following commands:

```
fpr
trust
```

c Enter `5`, then press <Enter> to choose `I trust ultimately` from the menu.

d Enter `y` <Enter> to confirm your choice.

e Enter `quit` <Enter> to exit the GPG key editor.

This completes validation of the Dell public key.

4 Verify the Dell PowerEdge M610 iDRAC6 package digital signature by running the following command:

```
gpg --verify IDRAC_FRMW_LX_2.2.BIN.sign
IDRAC_FRMW_LX_2.2.BIN
```

The following output message is displayed:

```
gpg: Signature made Fri Jul 11 15:03:47 2008
CDT using DSA key ID 23B66A9D
gpg: Good signature from "Dell, Inc. (Product
Group) <linux-security@dell.com>"
```

If you have not validated the key as shown in step 3, you will receive additional messages:

```
gpg: WARNING: This key is not certified with a trusted
signature!
gpg: There is no indication that the signature belongs
to the owner.
Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7
CA77 951D 23B6 6A9D
```

### Using iDRAC6 Web Interface

**NOTE:** If iDRAC6 firmware update progress is interrupted before it completes, iDRAC6 firmware may be corrupted. In such cases, you can recover iDRAC6 using CMC Web interface.

**NOTE:** The firmware update, by default, retains the current iDRAC6 settings. During the update process, you have the option to reset iDRAC6 configuration to the factory defaults. If you set the configuration to the factory defaults, external network access will be disabled when the update completes. You must enable and configure the network using iDRAC6 Configuration Utility.

1. Start iDRAC6 Web interface.
2. In the system tree, select **System→ iDRAC Settings**.
3. Click the **Update** tab.

   The **Firmware Update** screen is displayed.

   **NOTE:** To update the firmware, iDRAC6 must be placed in an update mode. Once in this mode, iDRAC6 will automatically reset, even if you cancel the update process.
4. In the **Upload** section, click **Browse** to locate the firmware image that you downloaded. The default firmware image name is **firmimg.imc**.
5. Click **Upload**.

   The file uploads to iDRAC6. This may take several minutes to complete.

   **NOTE:** During the upload process, you abort the firmware upgrade process by clicking **Cancel**. Clicking **Cancel** resets iDRAC6 to normal operating mode.

   When the upload is complete, the **Upload (Step 2 of 3)** screen displays.

   - If the image file uploaded successfully and passed all verification checks, a message is displayed indicating that the firmware image has been verified.
   - If the image did not upload successfully, or it did not pass the verification checks, the firmware update returns to the **Firmware Update** screen. You can try upgrading iDRAC6 again or click **Cancel** to reset iDRAC6 to normal operating mode.

   **NOTE:** If you deselect the **Preserve Configuration** check box, iDRAC6 resets to its default settings. In the default settings, the LAN is disabled, and you cannot log in to iDRAC6 Web interface. You must reconfigure the LAN settings using **iDRAC6 Configuration Utility** during BIOS POST or through CMC.

6 By default, the **Preserve Configuration** option is enabled (checked) to preserve the current settings on iDRAC6 after an upgrade. If you do not want the settings to be preserved, clear the **Preserve Configuration** check box.

7 Click **Begin Update** to start the upgrade process. Do not interrupt the upgrade process.

8 In the **Upload (Step 3 of 3)** window, you will see the status of the update. The progress of the firmware upgrade operation, measured in percentage, is displayed in the **Progress** column.

9 Once the firmware update is complete, the **Upload (Step 3 of 3)** window will refresh with the result and iDRAC6 will reset automatically. You must close the current browser window and reconnect to iDRAC6 using a new browser window.

### Updating iDRAC6 Firmware Using RACADM

You can update iDRAC6 firmware using remote RACADM.

1 Download iDRAC6 firmware image from the Dell Support website at **support.dell.com** to the TFTP server.

For example:

**C:\downloads\firmimg.imc**

2 Run the following RACADM command:

For example:

```
racadm -r <iDRAC6 IP address> -u <username> -p
<password> fwupdate -g -u -a <path>
```

where *path* is the location on the TFTP server where **firmimg.imc** is stored.

### Using the DOS Update Utility

To update iDRAC6 firmware using the DOS update utility, boot the managed server to DOS, and execute the **idrac16d** command. The syntax for the command is:

```
idrac16d [-f] [-i=<filename>] [-l=<logfile>]
```

When executed with no options, the **idrac16d** command updates iDRAC6 firmware using the firmware image file **firmimg.imc** in the current directory.

The options are as follows:

- `-f` — Forces the update. The `-f` option can be used to *downgrade* the firmware to an earlier image.
- `-i=<filename>` — Specifies the file name of the firmware image. This option is required if the firmware file name has been changed from the default name **firmimg.imc**.
- `-l=<logfile>` — Logs output from the update activity. This option is used for debugging.

**NOTE:** If you enter incorrect arguments to the **idrac16d** command, or supply the `-h` option, you may notice an additional option, `-nopresconfig` in the usage output. This option is used to update the firmware without preserving any configuration information. It is recommended to **not** use this option because it *deletes* all of your existing iDRAC6 configuration information such as IP addresses, users, and passwords.

### Using WSMAN Interface

For information to update the firmware using WSMAN, see the documentation available on the Dell Enterprise Technology Center at **delltechcenter.com**.

# Updating the USC Repair Package

See the *Dell Lifecycle Controller User Guide* for information on updating the USC repair package from iDRAC6 Web interface.

# Configuring iDRAC6 For Use With IT Assistant

Dell OpenManage IT Assistant can discover managed devices that comply with Simple Network Management Protocol (SNMP) v1 and v2c and Intelligent Platform Management Interface (IPMI) v2.0.

iDRAC6 complies with IPMI v2.0. This section describes the steps necessary to configure iDRAC6 for discovery and monitoring by IT Assistant. There are two ways to accomplish this: through iDRAC6 Configuration Utility and through iDRAC6 graphical Web interface.

# Using iDRAC6 Configuration Utility to Enable Discovery and Monitoring

To set up iDRAC6 for IPMI discovery and sending alert traps at iDRAC6 Configuration Utility level, restart your managed server (blade) and observe its power-up using the Virtual Console and either a remote monitor and console keyboard or a Serial over LAN (SOL) connection. When `Press <Ctrl-E> for Remote Access Setup` displays, press <Ctrl><E>.

When iDRAC6 **Configuration Utility** screen is displayed, use the arrow keys to scroll down.

1. Enable **IPMI over LAN**.
2. Enter your site's **RMCP+ Encryption Key**, if used.

   **NOTE:** See your senior Network Administrator or CIO to discuss implementing this option because it adds valuable security protection and must be implemented site-wide in order to function properly.
3. At **LAN Parameters**, press <Enter> to enter the sub-screen. Use Up and Down arrows to navigate.
4. Toggle **LAN Alert Enabled** to **On** using the spacebar.
5. Enter the IP address of your Management Station into **Alert Destination** 1.
6. Enter a name string into **iDRAC6 Name** with a consistent naming convention across your data center. The default is `iDRAC6-{Service Tag}`.

Exit iDRAC6 Configuration Utility by pressing <Esc>, <Esc>, and then pressing <Enter> to save your changes. Your server will now boot into normal operation, and it will be discovered during IT Assistant's next scheduled Discovery pass.

**NOTE:** You can also use Dell Management Console, the next generation one-to-many systems management application, to enable discovery and monitoring. See the *Dell Management Console User's Guide* on the Dell Support site at **support.dell.com/manuals** for more information.

## Using iDRAC6 Web Interface to Enable Discovery and Monitoring

IPMI Discovery can also be enabled through the remote Web interface:

1. Open a supported Web browser window.
2. Log in to iDRAC6 Web interface using a login and password with Administrator rights.
3. In the system tree, select **System→ iDRAC Settings→ Network/Security** tab.

   The **Network** screen is displayed.
4. In the **IPMI Settings** section, ensure the **Enable IPMI Over LAN** check box is selected (checked).
5. From the **Channel Privilege Level Limit** drop-down menu, select **Administrator**.
6. Enter your site's **RMCP+ Encryption Key**, if used.
7. Click **Apply** if you made any changes on this screen.
8. In the system tree, select **System→ Alert Management** tab**→ Platform Events**.

   The **Platform Events** screen is displayed, displaying a list of events for which you can configure iDRAC6 to generate alerts.
9. Enable alerts for one or more events by selecting the check box in the **Generate Alert** column.
10. Click **Apply** if you made any changes on this screen.
11. Click **Trap Settings**. The **Trap Settings** screen is displayed.
12. In the **IPv4 Destination List** section, in the first available **Destination IP Address** field, select the **Enabled** check box, and then enter the IP address of your Management Station.
13. Repeat step 12 for the **IPv6 Destination List** section.
14. Click **Apply**. You can click **Send** to send a test trap alert.
15. Click **Email Alert Settings**. The **Email Alert Settings** screen is displayed.

16 In the **Destination Email Addresses** section, in the first available **Email Alert** field, type the email address that must receive the alert messages, and then click **Apply**.

17 You can click **Send** to send a test email alert message.

It is highly recommended that for security purposes you create a separate User for IPMI commands with its own user name, IPMI over LAN privileges, and password:

1 In the system tree, select **System→ iDRAC Settings**.

2 Click the **Network/Security** tab, and then click **Users**.

The **Users** screen displays a list of all users (defined or undefined).

3 Click the **User ID** of an undefined User.

The **User Configuration** screen for the selected User ID is displayed.

4 Select the **Enable User** check box, and then enter the user's name and password.

5 In the **IPMI LAN Privilege** section, ensure that **Maximum LAN User Privilege Granted** is set to **Administrator**.

6 Set other user privileges as needed.

7 Click **Apply** to save the new User settings.

# Using IT Assistant to View iDRAC6 Status and Events

After discovery is complete, iDRAC6 devices appear in the **Servers** category of the **ITA Devices detail** screen, and iDRAC6 information can be seen by clicking the iDRAC6 name. This is different from DRAC 5 systems, where the management card shows up in the RAC group.

iDRAC6 error and warning traps can now be seen in the primary **Alert Log** of IT Assistant. They display in the **Unknown** category, but the trap description and severity will be accurate.

For more information on using IT Assistant to manage your data center, see the *Dell OpenManage IT Assistant User's Guide*.

**NOTE:** You can also use Dell Management Console, the next generation one-to-many systems management application, to view iDRAC6 status and events. See the *Dell Management Console User's Guide* on the Dell Support website at **support.dell.com/manuals** for more information.

# 3

# Configuring the Management Station

A management station is a computer used to monitor and manage the Dell PowerEdge servers and other modules in the chassis. This section describes software installation and configuration tasks that set up a management station to work with iDRAC6 Enterprise. Before you begin configuring iDRAC6, follow the procedures in this section to ensure that you have installed and configured the tools you will need.

## Management Station Set Up Steps

To set up your Management Station, perform the following steps:

1. Set up the management station network.
2. Install and configure a supported Web browser.
3. Install a Java Runtime Environment (JRE) (required if using Java plug-in type).
4. Install Telnet or SSH clients, if required.
5. Install a TFTP server, if required.
6. Install Dell OpenManage IT Assistant (optional).
7. Install Dell Management Console (optional).

## Management Station Network Requirements

To access iDRAC6, the management station must be on the same network as CMC RJ45 connection port labeled "GB1". It is possible to isolate CMC network from the network the managed server is on, so that your., management station may have LAN access to iDRAC6 but not to the managed server.

Using iDRAC6 Virtual Console feature (see "Configuring and Using Serial Over LAN" on page 197), you can access the managed server's console even if you do not have network access to the server's ports. You can also perform several management functions on the managed server, such as rebooting the computer and using iDRAC6 facilities. To access network and application services hosted on the managed server, however, you may need an additional NIC in the managed server.

# Configuring a Supported Web Browser

The following sections provide instructions for configuring the supported Web browsers for use with iDRAC6 Web interface.

## Opening Your Web Browser

iDRAC6 Web interface is designed to be viewed in a supported Web browser at a minimum screen resolution of 800 pixels wide by 600 pixels high. In order to view the interface and access all features, ensure that your resolution is set to at least 800 by 600 pixels and/or resize your browser, as needed.

**NOTE:** In some situations, most often during the first session after a firmware update, users of Internet Explorer may see the message **Done, with errors** displayed in the browser status bar along with a partially rendered screen in the main browser window. This error can also occur if you are experiencing connectivity problems. This is a known issue with Internet Explorer. Close the browser and start again.

## Configuring Your Web Browser to Connect to the Web Interface

If you are connecting to iDRAC6 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 this server.

To configure the Internet Explorer Web browser to access a proxy server, perform the following steps:

1. Open a Web browser window.
2. Click **Tools**, and click **Internet Options**.

   The **Internet Options** window is displayed.
3. Select **Tools→ Internet Options→ Security→ Local Network**.
4. Click the **Custom Level**.

5 Select **Medium-Low** from the drop-down menu and click **Reset**. Click **OK** to confirm. You will need to re-enter the **Custom Level** dialog by clicking its button.

6 Scroll down to the section labeled ActiveX controls and plug-ins and check each setting, as different versions of IE have differing settings in **Medium-Low** state:

- 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

In the section on **Downloads**:

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

In the **Miscellaneous** section:

- 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 nonencrypted form data: Enable
- Use Pop-up Blocker: Disable

In the **Scripting** section:

- Active scripting: Enable
- Allow paste operations via script: Enable
- Scripting of Java applets: Enable

7 Select **Tools→ Internet Options→ Advanced**.

8 Make sure the following items are checked or unchecked:

In the **Browsing** section:

- Always send URLs as UTF-8: checked
- Disable script debugging (Internet Explorer): checked
- Disable script debugging: (Other): checked
- Display a notification about every script error: unchecked
- Enable Install On demand (Other): checked
- Enable page transitions: checked
- Enable third-party browser extensions: checked
- Reuse windows for launching shortcuts: unchecked

In the **HTTP 1.1 settings** section:

- Use HTTP 1.1: checked
- Use HTTP 1.1 through proxy connections: checked

In the **Java (Sun)** section:

- Use JRE 1.6.x_yz: checked (optional; version may differ)

In the **Multimedia** section:

- Enable automatic image resizing: checked
- Play animations in Web pages: checked
- Play videos in Web pages: checked
- Show pictures: checked

In the **Security** section:

- Check for publishers' certificate revocation: unchecked
- Check for signatures on downloaded programs: unchecked

- Check for signatures on downloaded programs: checked
- Use SSL 2.0: unchecked
- Use SSL 3.0: checked
- Use TLS 1.0: checked
- Warn about invalid site certificates: checked
- Warn if changing between secure and not secure mode: checked
- Warn if forms submittal is being redirected: checked

**NOTE:** If you choose to alter any of the above settings, It is recommended that you learn and understand the consequences of doing so. For example, if you choose to block pop-ups, portions of iDRAC6 Web interface will not function properly.

9 Click **Apply**, then **OK**.

10 Click the **Connections** tab.

11 Under **Local Area Network (LAN) settings**, click **LAN Settings**.

12 If the **Use a proxy server** box is selected, select the **Bypass proxy server for local addresses** box.

13 Click **OK** twice.

14 Close and restart your browser to make sure all changes take effect.

### Adding iDRAC6 to the List of Trusted Domains

When you access iDRAC6 Web interface through the Web browser, you may be prompted to add iDRAC6 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 iDRAC6 Web interface.

On some operating systems, Internet Explorer (IE) 8 may not prompt you to add iDRAC6 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 ensure security.

To add iDRAC6 IP address to the list of trusted domains in IE8, do the following:

1. Select **Tools→ Internet Options→ Security→ Trusted sites→ Sites**.
2. Enter iDRAC6 IP address to the **Add this website to the zone**.
3. Click **Add**.
4. Click **OK**.
5. Click **Close**.
6. Click **OK** and then refresh your browser.

When you launch Virtual Console for the first time through IE8 with Active-X plug-in, a "`Certificate Error: Navigation Blocked`" message may be displayed.

1. Click **Continue to this website**.
2. Click **Install** to install Active-X controls on the **Security Warning** window.

   The Virtual Console session is launched.

### Viewing Localized Versions of the Web Interface

iDRAC6 Web interface is supported for the following operating system languages:

- English (en-us)
- French (fr)
- German (de)
- Spanish (es)
- Japanese (ja)
- Simplified Chinese (zh-cn)

The ISO identifiers in parentheses denote the specific language variants which are supported. Use of the interface with other dialects or languages is not supported and may not function as intended. For some supported languages, resizing the browser window to 1024 pixels wide may be necessary in order to view all features.

iDRAC6 Web interface is designed to work with localized keyboards for the specific language variants listed above. Some features of iDRAC6 Web interface, such as Virtual Console, may require additional steps to access

certain functions/letters. For more details on how to use localized keyboards in these situations, see "Using the Video Viewer" on page 226. Use of other keyboards is 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 iDRAC6 Web interface.

### Setting the Locale in Linux

The Virtual Console viewer requires a UTF-8 character set to display correctly. If your display is garbled, check your locale and reset the character set if needed.

To set the character set on a Linux client with a Simplified Chinese GUI:

1. Open a command terminal.
2. Enter `locale` and press <Enter>. Output similar to the following output is displayed:

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3. If the values include `zh_CN.UTF-8`, no changes are required. If the values do not include `zh_CN.UTF-8`, go to step 4.
4. Edit the **/etc/sysconfig/i18n** file with a text editor.

5 In the file, apply the following changes:

Current entry:

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

Updated entry:

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-
8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

6 Log out and then log in to the operating system.

When you switch from any other language, ensure that this fix is still valid. If not, repeat this procedure.

### Disabling the Whitelist Feature in Firefox

Firefox has a "whitelist" security feature that requires user permission to install plugins for each distinct site that hosts a plugin. If enabled, the whitelist feature requires you to install a Virtual Console viewer for each iDRAC6 you visit, even though the viewer versions are identical.

To disable the whitelist feature and avoid unnecessary plugin 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** value changes to **false**.

4 In the **Preferences Name** column, locate **xpinstall.enabled**.

Ensure that **Value** is **true**. If not, double-click **xpinstall.enabled** to set **Value** to **true**.

# Installing iDRAC6 Software on the Management Station

Your system includes the *Dell Systems Management Tools and Documentation* DVD. This DVD includes the following components:

- DVD root - Contains the Dell Systems Build and Update Utility, which provides server setup and system installation information
- SYSMGMT - Contains the systems management software products including Dell OpenManage Server Administrator

### Installing and Uninstalling RACADM on a Management Station

To use the remote RACADM functions, install RACADM on a management station. See the *Dell OpenManage Management Station Software Installation Guide* available at **support.dell.com/manuals** for information on how to install DRAC Tools on a management station running Microsoft Windows operating system.

### Installing and Uninstalling RACADM on Linux

1. Log on as root to the system where you want to install the management station components.
2. If necessary, mount the *Dell Systems Management Tools and Documentation* DVD using the following command or a similar command:

   ```
   mount /media/cdrom
   ```

3. Navigate to the **/linux/rac** directory and execute the following command:

   ```
   rpm -ivh *.rpm
   ```

For help with the RACADM command, type **racadm help** after issuing the previous commands.

To uninstall RACADM, open a command prompt and type:

```
rpm -e <racadm_package_name>
```

where <*racadm_package_name*> is the RPM package used to install iDRAC6 software.

For example, if the RPM package name is **srvadmin-racadm5**, type:

```
rpm -e srvadmin-racadm5
```

# Installing a Java Runtime Environment (JRE)

**NOTE:** If you use Internet Explorer, an ActiveX control is provided for the Virtual Console viewer. You can also use the Java Virtual Console viewer with Firefox if you install a JRE and configure the Virtual Console viewer in iDRAC6 Web interface before you launch the viewer. See "Configuring Virtual Console and Virtual Media in iDRAC6 Web Interface" on page 222 for more information.

You can choose to use the Java viewer instead before you launch the viewer.

If you use the Firefox browser you must install a JRE (or a Java Development Kit [JDK]) to use the Virtual Console feature. The Virtual Console viewer is a Java application that is downloaded to the management station from iDRAC6 Web interface and then launched with Java Web Start on the management station.

Go to **java.com** to install a JRE or JDK. Version 1.6 (Java 6.0) or higher is recommended.

The Java Web Start program is automatically installed with the JRE or JDK. The file **jviewer.jnlp** is downloaded to your desktop and a dialog box prompts you for what action to take. It may be necessary to associate the **.jnlp** extension type with the Java Web Start application in your browser. Otherwise, click **Open with** and then select the javaws application, which is located in the bin subdirectory of your JRE installation directory.

**NOTE:** If the **.jnlp** file type is not associated with Java Web Start after installing JRE or JDK, you can set the association manually. For Windows (**javaws.exe**) click **Start**→ **Control Panel**→ **Appearance and Themes**→ **Folder Options**. Under the **File Types** tab, highlight **.jnlp** under **Registered file types**, and then click **Change**. For Linux (**javaws**), start Firefox, and click **Edit**→ **Preferences**→ **Downloads**, and then click **View and Edit Actions**.

For Linux, once you have installed either JRE or JDK, add a path to the Java bin directory to the front of your system PATH. For example, if Java is installed in /usr/java, add the following line to your local .bashrc or /etc/profile:

```
PATH=/usr/java/bin:$PATH; export PATH
```

**NOTE:** There may already be PATH-modification lines in the files. Ensure that the path information you enter does not create conflicts.

# Installing Telnet or SSH Clients

By default, iDRAC6 Telnet service is disabled and the SSH service is enabled. Since Telnet is an insecure protocol, you should use it only if you cannot install an SSH client or your network connection is otherwise secured.

**NOTE:** iDRAC6 supports up to 4 Telnet sessions and 4 SSH sessions simultaneously.

### Telnet with iDRAC6

Telnet client is included in Windows and Linux operating systems, and can be run from a command shell. You may also choose to install a commercial or freely available Telnet client with more convenience features than the standard version included with your operating system.

### Configuring the Backspace Key For Telnet Sessions

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 Microsoft Telnet clients to use the <Backspace> key, perform the following steps:

1. Open a command prompt window (if required).
2. If you are not running a Telnet session, enter:

   ```
   telnet
   ```

   If you are running a Telnet session, press <Ctrl><]>.
3. At the prompt, enter:

   ```
   set bsasdel
   ```

   The following message is displayed:

   ```
   Backspace will be sent as delete.
   ```

To configure a Linux Telnet session to use the <Backspace> key, perform the following steps:

1. Open a shell and enter:

   ```
   stty erase ^h
   ```

2. At the prompt, enter:

   ```
   telnet
   ```

### SSH With iDRAC6

Secure Shell (SSH) is a command line connection with the same capabilities as a Telnet session, but with session negotiation and encryption to improve security. iDRAC6 supports SSH version 2 with password authentication. SSH is enabled by default on iDRAC6.

You can use free programs like PuTTY or OpenSSH on a management station to connect to the managed server's iDRAC6. When an error occurs during the login procedure, the **SSH** client issues an error message. The message text is dependent on the client and is not controlled by iDRAC6.

**NOTE:** OpenSSH should be run 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).

iDRAC6 supports up to 4 Telnet sessions and 4 SSH sessions simultaneously. However, only one of those 8 potential sessions may use SM-CLP. That is, iDRAC6 supports only one SM-CLP session at a time. The session timeout is controlled by the `cfgSsnMgtSshIdleTimeout` property as described in see *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

iDRAC6 SSH implementation supports multiple cryptography schemes, as shown in Table 3-1.

**NOTE:** SSHv1 is not supported.

**Table 3-1. Cryptography Schemes**

| Scheme Type | Scheme |
|---|---|
| Asymmetric Cryptography | Diffie-Hellman DSA/DSS 512-1024 (random) bits per NIST specification |
| Symmetric Cryptography | • AES256-CBC<br>• RIJNDAEL256-CBC<br>• AES192-CBC<br>• RIJNDAEL192-CBC<br>• AES128-CBC<br>• RIJNDAEL128-CBC<br>• BLOWFISH-128-CBC<br>• 3DES-192-CBC<br>• ARCFOUR-128 |
| Message Integrity | • HMAC-SHA1-160<br>• HMAC-SHA1-96<br>• HMAC-MD5-128<br>• HMAC-MD5-96 |
| Authentication | • Password |

## Installing a TFTP Server

Trivial File Transfer Protocol (TFTP) is a simplified form of the File Transfer Protocol (FTP). It is used with the SM-CLP and RACADM command line interfaces to transfer files to and from iDRAC6.

**NOTE:** If you use only iDRAC6 Web interface to transfer SSL certificates and upload new iDRAC6 firmware, no TFTP server is required.

The only times when you need to copy files to or from iDRAC6 are when you update iDRAC6 firmware or install certificates on iDRAC6. If you choose to use RACADM when you perform these tasks, a TFTP server must be running on a computer iDRAC6 can access through IP address or DNS name.

You can use the `netstat -a` command on Windows or Linux operating systems to see if a TFTP server is already listening. Port 69 is the TFTP default port. If no server is running, you have the following options:

- Find another computer on the network running a TFTP service.
- If you are using Linux, install a TFTP server from your distribution.
- If you are using Windows, install a commercial or free TFTP server.

## Installing Dell OpenManage IT Assistant

Your system includes the Dell OpenManage system management software kit. This kit includes, but is not limited to, the following components:

- *Dell Systems Management Tools and Documentation* DVD
- Dell Support website and Readme files — Check Readme files and the Dell Support website at **support.dell.com/manuals** for the most recent information about your Dell products.

For information on installing IT Assistant, see the *Dell OpenManage IT Assistant User's Guide* available at **support.dell.com/manuals**.

## Installing Dell Management Console

Dell Management Console (DMC) is the next generation one-to-many systems management application that provides similar functionality as the Dell OpenManage IT Assistant and also provides enhanced discovery, inventory, monitoring, and reporting features. It is a Web–based GUI, which is installed on a management station in a networked environment.

You can install DMC from the *Dell Management Console* DVD or download and install it from the Dell website at **dell.com/openmanage**.

See the *Dell Management Console User's Guide* available at **support.dell.com/manuals** for instructions on installing this software.

# 4

# Configuring the Managed Server

This section describes tasks to set up the managed server to enhance your remote management capabilities. These tasks include installing the Dell Open Manage Server Administrator software and configuring the managed server to capture the last crash screen.

## Installing the Software on the Managed Server

The Dell management software includes the following features:

- RACADM CLI — Allows you to configure and administer iDRAC6. It is a powerful tool for scripting configuration and management tasks.
- Server Administrator — Is required to use iDRAC6 last-crash-screen feature.
- Server Administrator Instrumentation Service — Provides access to detailed fault and performance information gathered by industry-standard systems management agents and allows remote administration of monitored systems, including shutdown, startup, and security.
- Server Administration Storage Management Service — Provides storage management information in an integrated graphical view.
- Server Administrator Logs — Displays logs of commands issued to or by the system, monitored hardware events, POST events, and system alerts. You can view logs on the home page, print or save them as reports, and send them by e-mail to a designated service contact.

Use the *Dell Systems Management Tools and Documentation* DVD to install Dell OpenManage Server Administrator. For instructions on installing this software, see the *Dell OpenManage Server Administrator Installation Guide* available at **support.dell.com/manuals**. On the **Manuals** page, click **Software→ Systems Management**. Click on the appropriate product link on the right-side to access the documents.

# Configuring the Managed Server to Capture the Last Crash Screen

iDRAC6 can capture the last crash screen so that you can view it in the Web interface to help troubleshoot the cause of the managed server crash.

**NOTE:** You can capture the last crash screen only if the managed server is running on a Windows operating system.

Follow these steps to enable the last crash screen feature.

1. Install the managed server software. For more information, see the *Dell OpenManage Server Administrator Installation Guide* and the *Dell OpenManage Management Station Software Installation Guide*. You can access these documents on the Dell Support website at **support.dell.com/manuals**.
2. Ensure that **Automatically Reboot** is deselected in the **Windows Startup and Recovery Settings**. See "Disabling the Windows Automatic Reboot Option" on page 83.
3. Enable the **Last Crash Screen** (disabled by default) in iDRAC6 Web interface.

   To enable the **Last Crash Screen** in iDRAC6 Web interface, click **System**→ **iDRAC Settings**→ **Network/Security** tab→ **Services**, then check the **Enabled** check box under the **Automated System Recovery Agent** Settings heading.

   To enable the Last Crash Screen using local RACADM, open a command prompt on the managed server and enter the following command:

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

4. In the Server Administrator Web interface, enable the **Auto Recovery** timer and set the **Auto Recovery** action to **Reset**, **Power Off**, or **Power Cycle**.

For information about how to configure the **Auto Recovery** timer, see the *Dell OpenManage Server Administrator User's Guide*. To ensure that the last crash screen can be captured, the **Auto Recovery** timer should be set to 60 seconds. The default setting is 480 seconds.

The last crash screen is not available when the **Auto Recovery** action is set to **Shutdown** or **Power Cycle** if the managed server is powered off.

## Disabling the Windows Automatic Reboot Option

To ensure that iDRAC6 can capture the last crash screen, disable the **Automatic Reboot** option on managed servers running Windows Server or Windows Vista.

1. Open the Windows **Control Panel** and double-click the **System** icon.
2. Click the **Advanced** tab.
3. Under **Startup and Recovery**, click **Settings**.
4. Deselect the **Automatically Reboot** check box.
5. Click **OK** twice.

# 5

# Configuring iDRAC6 Enterprise Using the Web Interface

iDRAC6 provides a Web interface that enables you to configure iDRAC6 properties and users, perform remote management tasks, and troubleshoot a remote (managed) system for problems. You would typically use the Web interface to perform your daily system management tasks. This chapter provides information about how to perform common systems management tasks with iDRAC6 Web interface and provides links to related information.

Most configuration tasks for which you would use the Web interface could also be performed with local or remote RACADM commands or with SM-CLP commands.

Local RACADM commands are executed from the managed server. Remote RACADM is a client utility run on a management station, and makes use of the out-of-band interface to communicate with the managed server. This utility is used with the **–r** option to execute commands over a network. For more information about RACADM, see "Using the RACADM Command Line Interface" on page 275.

SM-CLP commands are executed in a shell that can be accessed remotely with a Telnet or Secure Shell (SSH) connection. For more information about SM-CLP, see "Using iDRAC6 Enterprise SM-CLP Command Line Interface" on page 317.

# Accessing the Web Interface

To access iDRAC6 Web interface, perform the following steps:

1. Open a supported Web browser window.
2. In the **Address** field, enter `https://<iDRAC6-IP-address>` and press <Enter>.

   If the default HTTPS port number (port 443) has been changed, enter:

   `https://<iDRAC6-IP-address>:<port-number>`

   where *iDRAC6-IP-address* is the IP address for iDRAC6 and *port-number* is the HTTPS port number.

   The iDRAC6 **Log in** window is displayed.

### Logging In

You can log in as either an iDRAC6 user, a Microsoft Active Directory user, or an LDAP user. The default user name and password are **root** and **calvin**, respectively.

You must have been granted **Login to iDRAC** privilege by the administrator to log in to iDRAC6.

To log in, perform the following steps:

1. In the **Username** field, enter one of the following:
   - Your iDRAC6 user name.

     **NOTE:** The user name for local users is *case-sensitive*. Examples are root, it_user, IT_user, or john_doe.

   - Your Active Directory (AD) user name. The AD domain name can also be selected from the drop-down menu.

     You can use any of the following forms for Active Directory names: <*domain*>\<*username*>, <*domain*>/<*username*>, or <*user*>@<*domain*>. They are not case-sensitive. Examples are `dell.com\john_doe`, or `JOHN_DOE@DELL.COM`. Alternatively, you can enter the domain in the **Domain** field.

   - LDAP user name (with no domain name).

2 In the **Password** field, enter either your iDRAC6 user password, Active Directory user password, or LDAP password. Passwords are case-sensitive.

3 Click **OK** or press <Enter>.

## Logging Out

1 In the upper-right corner of the main window, click **Log out** to close the session.

2 Close the browser window.

**NOTE:** The **Log out** button does not appear until you log in.

**NOTE:** Closing the browser without gracefully logging out may cause the session to remain active until the session timeout is reached. It is recommended that you click the **Log out** button to end a session.

**NOTE:** Closing iDRAC6 Web interface within Internet Explorer using the close button ("x") at the top right corner of the window may generate an application error. To fix this issue, download the latest Cumulative Security Update for Internet Explorer from the Microsoft Support website, located at **support.microsoft.com**.

**CAUTION: If you have opened multiple Web GUI sessions either through <Ctrl+T> or <Ctrl+N> to access the same iDRAC6 from the same management station, and then log out of any one session, all the Web GUI sessions will be terminated.**

## Using Multiple Browser Tabs and Windows

Different versions of Web browsers exhibit different behaviors when opening new tabs and windows. Internet Explorer (IE) 7 and IE 8 have the option to open tabs as well as windows. Each tab inherits the characteristics of the most recently opened tab. Press `<Ctrl–T>` to open a new tab and `<Ctrl–N>` to open a new browser window from the active session. Automatic login only occurs with <Ctrl-N>. When you open a new tab, you have to login again. Closing any one tab expires all iDRAC6 Web interface tabs. Also, if a user logs in with Power User privileges on one tab, and then logs in as Administrator on another tab, both open tabs then have Administrator privileges.

Tab behavior in Firefox 3 is the same as IE 7 and IE 8; new tabs are new sessions. Window behavior in Firefox is different. Firefox windows will operate with the same privileges as the latest window opened. For example, if one Firefox window is open with a Power User logged in and another window is opened with Administrator privileges, **both** users will now have Administrator privileges.

**Table 5-1. User Privilege Behavior in Supported Browsers**

| Browser | Tab Behavior | Window Behavior |
|---|---|---|
| Microsoft IE7 and IE8 | From latest session opened | New session |
| Firefox 3 | From latest session opened | From latest session opened |

# Configuring iDRAC6 NIC

This section assumes that iDRAC6 has already been configured and is accessible on the network. See "Configure iDRAC6 Networking" on page 35 for help with the initial iDRAC6 network configuration.

## Configuring the Network, IPMI, and VLAN Settings

**NOTE:** You must have **Configure iDRAC6** privilege to perform the following steps.

**NOTE:** Most DHCP servers require a server to store a client identifier token in its reservations table. The client (iDRAC6, for example) must provide this token during DHCP negotiation. iDRAC6 supplies the client identifier option using a one-byte interface number (0) followed by a six-byte MAC address.

1. Click **System→ iDRAC Settings**.
2. Click the **Network/Security** tab.

   The **Network** screen is displayed.
3. Configure the Network, IPMI, and VLAN settings as needed. See Table 5-2, Table 5-3, and Table 5-4 for descriptions of the **Network, IPMI**, and **VLAN Settings** options.
4. Click **Apply**.
5. Click the appropriate button to continue.

**Table 5-2. Network Settings**

| Setting | Description |
|---|---|
| **Network Interface Card Settings** | |
| **MAC Address** | Displays the Media Access Control (MAC) address that uniquely identifies each node in a network. The MAC address cannot be changed. |
| **Enable NIC** | When checked, indicates that the NIC is enabled and activates the remaining controls in this group. When a NIC is disabled, all communication to and from iDRAC6 through the network is blocked.<br>The default is **Unchecked**. |
| **Common Settings** | |
| **Register iDRAC6 on DNS** | Registers iDRAC6 name on the DNS server.<br>The default is **Unchecked**. |
| **DNS iDRAC6 Name** | Displays iDRAC6 name. The default name is idrac-*service_tag*, where *service_tag* is the service tag number of the Dell server. For example: iDRAC-HM8912S. |
| **Use DHCP for DNS Domain Name** | **Checked**: Enable acquisition of DNS domain name from DHCP server.<br>**Unchecked**: Disable acquisition of DNS domain name from DHCP server. |
| **DNS Domain Name** | The default **DNS Domain Name** is blank. When the **Use DHCP for DNS Domain Name** check box is selected, this option is grayed out and the field cannot be modified. |
| **IPv4 Settings** | |
| **Enabled** | Enables (**Checked**) or disables (**Unchecked**) IPv4 protocol support. The **Enable NIC** option should be checked to activate this setting. |
| **DHCP Enable** | If **Checked**, the Server Administrator obtains the IP address for iDRAC6 NIC from the DHCP server. It also deactivates the **IP Address**, **Subnet Mask**, and **Gateway** fields. |
| **IP Address** | Allows you to enter or edit a static IP address for iDRAC6 NIC. To change this setting, deselect the **DHCP Enable** option. |

**Table 5-2. Network Settings *(continued)***

| Setting | Description |
|---|---|
| **Subnet Mask** | Allows you to enter or edit a subnet mask for iDRAC6 NIC. To change this setting, deselect the **DHCP Enable** option. |
| **Gateway** | Allows you to enter or edit a static IPv4 gateway for iDRAC6 NIC. To change this setting, deselect the **DHCP Enable** option. |
| **Use DHCP to obtain DNS server addresses** | Select the **DHCP Enable** option to obtain DNS server addresses by selecting the **Use DHCP to obtain DNS server addresses** check box. When not using DHCP to obtain the DNS server addresses, provide the IP addresses in the **Preferred DNS Server** and **Alternate DNS Server** fields. |
| **Preferred DNS Server** | Allows you to enter or edit a static IP address for the preferred DNS server. To change this setting, first deselect the **Use DHCP to obtain DNS server addresses** option. |
| **Alternate DNS Server** | Uses the secondary DNS server IP address when **Use DHCP to obtain DNS server addresses** is **not selected**. Enter an IP address of 0.0.0.0 if there is no alternate DNS server. |
| **IPv6 Settings** | |
| **Enabled** | If the check box is **Checked**, IPv6 is enabled. If the check box is **Unchecked**, IPv6 is disabled. The default is **Unchecked**. |
| **Autoconfiguration Enable** | Selecting this option allows iDRAC6 to obtain the IPv6 address for iDRAC6 NIC from the Dynamic Host Configuration Protocol (DHCPv6) server. Enabling **Autoconfiguration Enable** also deactivates and flushes out the static values for **IPv6 Address**, **Prefix Length**, and **Gateway**. |
| **IPv6 Address** | Configures the IPv6 address for iDRAC6 NIC. To change this setting, you must first disable **Autoconfiguration Enable** by deselecting the associated check box.<br>**NOTE:** Only two IPv6 addresses (Link Local address and the global address) are displayed if your network setup has IPv6 DHCP configured and all sixteen IPv6 addresses are displayed if you have configured your network router to send Router Advertisement messages.<br>**NOTE:** iDRAC6 does not allow you to save the settings if you enter an IPv6 Address consisting of more than eight groups. |

**Table 5-2. Network Settings *(continued)***

| Setting | Description |
|---|---|
| **Prefix Length** | Configures the prefix length of the IPv6 address. It can be a value between 1 and 128 inclusive. To change this setting, you must first disable **Autoconfiguration Enable** by deselecting the associated check box. |
| **Gateway** | Configures the static IPv6 gateway for iDRAC6 NIC. To change this setting, you must first disable **Autoconfiguration Enable** by deselecting the associated check box. |
| **Use DHCPv6 to obtain DNS Server addresses** | Enable DHCP to obtain IPv6 DNS server addresses by selecting the **Use DHCPv6 to obtain DNS Server addresses** check box. When not using DHCP to obtain the DNS server addresses, provide the IP addresses in the **Preferred DNS Server** and **Alternate DNS Server** fields. The default value is **Unchecked**.<br>**NOTE:** When the **Use DHCPv6 to obtain DNS Server addresses** check box is selected, IP addresses cannot be entered into the **Preferred DNS Server** and **Alternate DNS Server** fields. |
| **Preferred DNS Server** | Configures the static IPv6 address for the preferred DNS server. To change this setting, deselect **Use DHCPv6 to obtain DNS Server Addresses**. |
| **Alternate DNS Server** | Configures the static IPv6 address for the alternate DNS server. To change this setting, deselect **Use DHCPv6 to obtain DNS Server Addresses**. |

**Table 5-3. IPMI Settings**

| Setting | Description |
|---|---|
| **Enable IPMI Over LAN** | When selected, indicates that the IPMI LAN channel is enabled. The default is **Unchecked**. |
| **Channel Privilege Level Limit** | Configures the maximum privilege level for the user that can be accepted on the LAN channel. Select one of the following options: **Administrator, Operator**, or **User**. The default is **Administrator**. |
| **Encryption Key** | Configures the encryption key. The encryption key must consist of an even number of hexadecimal characters with a maximum of 40 characters with no spaces. The default IPMI encryption key is all zeros. |

**Table 5-4. VLAN Settings**

| Button | Description |
|---|---|
| Enable VLAN ID | **Yes**—Enabled. **No**—Disabled. If enabled, only matched Virtual LAN (VLAN) ID traffic is accepted.<br>**NOTE:** The VLAN settings can only be configured through CMC Web Interface. iDRAC6 only displays the current enablement status; you can not modify the settings on this screen. |
| VLAN ID | VLAN ID field of 802.1g fields. Displays a value from 1 to 4094 except 4001 to 4020. |
| Priority | Priority field of 802.1g fields. This is used to identify the priority of the VLAN ID and displays a value from 0 to 7 for the VLAN Priority. |

**Table 5-5. Network Configuration Buttons**

| Button | Description |
|---|---|
| Advanced Settings | Displays the **Network Security** screen, allowing you to enter the IP Range and IP Blocking attributes. |
| Apply | Saves any new settings made to the network configuration screen.<br>**NOTE:** Changes to the NIC IP address settings close all user sessions and require users to reconnect to iDRAC6 Web interface using the updated IP address settings. All other changes require the NIC to be reset, which may cause a brief loss in connectivity. |

## Configuring IP Filtering and IP Blocking

**NOTE:** You must have **Configure iDRAC6** privilege to perform the following steps.

1. Click **System→ iDRAC Settings.**
2. Click the **Network/Security** tab.

   The **Network** screen is displayed.
3. Click **Advanced Settings**.

   The **Network Security** screen is displayed.

4 Configure IP filtering and blocking settings as needed. See Table 5-6 for descriptions of the IP filtering and blocking settings.

5 Click **Apply** to save the settings.

**Table 5-6. IP Filtering and Blocking Settings**

| Settings | Description |
|---|---|
| **IP Range Enabled** | Enables the IP Range checking feature, which defines a range of IP addresses that can access iDRAC6. The default is **Disabled**. |
| **IP Range Address** | Determines the acceptable IP subnet address. The default is **192.168.1.0**. |
| **IP Range Subnet Mask** | Defines the significant bit positions in the IP address. The subnet mask should be in the form of a netmask, where the more significant bits are all 1's with a single transition to all zeros in the lower-order bits. The default is **255.255.255.0**. |
| **IP Blocking Enabled** | Enables the IP address blocking feature, which limits the number of failed login attempts from a specific IP address for a preselected time span. The default is **Disabled**. |
| **IP Blocking Fail Count** | Sets the number of login failures attempted from an IP address before the login attempts are rejected from that address. The default is **10**. |
| **IP Blocking Fail Window** | Determines the time span in seconds within which IP Block Fail Count failures must occur to trigger the IP Block Penalty Time. The default is **3600**. |
| **IP Blocking Penalty Time** | The time span in seconds that login attempts from an IP address with excessive failures are rejected. The default is **3600.** |

# Configuring Platform Events

Platform event configuration provides a mechanism for configuring iDRAC6 to perform selected actions on certain event messages. The actions include no action, reboot system, power cycle system, power off system, and generate an alert (Platform Event Trap [PET] and/or e-mail).

The filterable platform events are listed in Table 5-7.

**Table 5-7. Filterable Platform Events**

| Index | Platform Event |
|---|---|
| 1 | Battery Warning Assert Filter |
| 2 | Battery Critical Assert Filter |
| 3 | Voltage Critical Assert Filter |
| 4 | Temperature Warning Assert Filter |
| 5 | Temperature Critical Assert Filter |
| 6 | Processor Critical Assert Filter |
| 7 | Processor Absent Critical Assert Filter |
| 8 | Event Log Critical Assert Filter |
| 9 | Watchdog Critical Assert Filter |
| 10 | Removable Flash Media Warning Assert Filter |
| 11 | Removable Flash Media Absent Informational Assert Filter |
| 12 | Removable Flash Media Critical Assert Filter |
| 13 | Redundancy Lost Filter |
| 14 | Key Management Critical Assert Filter |

When a platform event occurs (for example, a *Battery Probe Warning*), a system event is generated and recorded in the System Event Log (SEL). If this event matches a platform event filter (PEF) that is enabled and you have configured the filter to generate an alert (PET or e-mail), then a PET or e-mail alert is sent to one or more configured destinations.

If the same platform event filter is also configured to perform an action (such as rebooting the system), the action is performed.

## Configuring Platform Event Filters (PEF)

**NOTE:** Configure platform event filters before you configure the platform event traps or e-mail alert settings.

1. Log in to iDRAC6 Web interface.
2. Click **System**, and then click the **Alert Management** tab.

   The **Platform Events** screen is displayed.
3. Select the **Enable Paltform Event Filter Alerts** checkbox. You must select this option for any platform alert to be sent to a valid destination.
4. Select one of the following action you want to enable for each event:
   - Reboot System - When an event occurs, the system restarts (a warm boot).
   - Power Cycle System - When an event occurs, the system shuts down, powers off, and restarts (a cold boot).
   - Power Off System - When an event occurs, the system shuts down and powers off.
   - No Action - When an event occurs, no action is performed. This is the default setting for an event.
5. Select the **Generate Alert** option beside each event for which you want an alert to be generated.

**NOTE:** You can enable or disable alert generation for all events by selecting or deselecting the check box next to the **Generate Alert** column heading.

6. Click **Apply**.

## Configuring Platform Event Traps (PET)

**NOTE:** You must have **Configure iDRAC** permission to add or enable/disable an SNMP alert. The following options will not be available if you do not have **Configure iDRAC** permission.

1. Log in to iDRAC6 Web interface.
2. Ensure that you followed the procedures in "Configuring Platform Event Filters (PEF)" on page 95.
3. Click **System**, and then click the **Alert Management** tab.

   The **Platform Events** screen is displayed.

4 Click **Trap Settings**.

The **Trap Settings** screen is displayed.

5 Configure your PET destination IP address:

a Select the **Enabled** check box for the **Destination Number** you would like to activate.

b Enter an IP address in the appropriate IPv4 or IPv6 **Destination IP Address** box.

c Click **Apply**.

**NOTE:** To successfully send a trap, configure the **Community String** value. The **Community String** value indicates the community string to use in a Simple Network Management Protocol (SNMP) alert trap sent from iDRAC6. SNMP alert traps are transmitted by iDRAC6 when a platform event occurs. The default setting for the **Community String** is **Public**.

d To test the configured alert, click **Send**.

e To add an additional destination IP address, repeat step a through step d. You may specify up to four IPv4 and four IPv6 destination addresses.

## Configuring E-Mail Alerts

1 Log in to iDRAC6 Web interface.

2 Ensure that you followed the procedures in "Configuring Platform Event Filters (PEF)" on page 95.

3 Click **System**, and then click the **Alert Management** tab.

The **Platform Events** screen is displayed.

4 Click **Email Alert Settings**.

The **Email Alert Settings** screen is displayed.

5 Configure your e-mail alert destination.

a Select the **Enabled** check box for the first undefined e-mail alert.

b Enter a valid e-mail address in the **Destination Email Address** field.

c Click **Apply**.

**NOTE:** To successfully send a test e-mail, the SMTP (Email) Server must be configured in the **SMTP (Email) Server Address Settings** section of the **Email Alert Settings** screen. Specify an SMTP server in the field provided using either the dot separated format (for example, 192.168.1.1) or the DNS name. The IP address of the SMTP Server sends sends e-mail alerts to iDRAC when a platform event occurs.

d In the **Modify Source Email Name** field, enter the originator e-mail for the alert, or leave it blank to use the default e-mail originator. The default is blade_slot@iDRAC6 IP Address.

- If the **Modify Source Email Name** field is blank, iDRAC6 host name is configured, and DNS Domain Name is active, then the source e-mail address is:<iDRAC6 host name>@<DNS Domain name>.
- If the field is blank, iDRAC6 host name is blank, and the DNS Domain Name is active, then the source e-mail address is: <iDRAC6 Slot*x*>@<DNS Domain name>.
- If the field is blank, iDRAC6 host name is blank, and the DNS Domain Name is blank, then the source e-mail address is: <iDRAC6 Slot*x*>@<iDRAC6 IP Address>.
- If the field is "a string without @", and DNS Domain Name is active, then the source e-mail address is: <a string without @>@<DNS Domain name>.
- If the field is "a string without @", and DNS Domain Name is blank, then the source e-mail address is :<a string without @>@<iDRAC6 IP Address>.
- If the field is "a string with @", and DNS Domain Name is active, then the source e-mail address is:<a string with @>@<DNS Domain name>.
- If the field is "a string with @", and the DNS Domain Name is blank, then the source e-mail address is:<a string with @>@<iDRAC6 IP Address>.

e Click **Send** to test the configured e-mail alert (if desired).

f To add an additional e-mail alert destination, repeat **step a** through **step e**. You may specify up to four e-mail alert destinations.

# Configuring IPMI Over LAN

1 Log in to iDRAC6 Web interface.

2 Configure IPMI over LAN:

a Click **System→ iDRAC Settings**, and then click the **Network/Security** tab.

The **Network** screen is displayed.

b Click **IPMI Settings**.

c Select the **Enable IPMI Over LAN** check box.

d Update the **Channel Privilege Level Limit**, if required:

**NOTE:** This setting determines the IPMI commands that can be executed from the IPMI over LAN interface. For more information, see the IPMI 2.0 specifications.

Under **IPMI Settings**, click the **Channel Privilege Level Limit** drop-down menu, select **Administrator**, **Operator**, or **User**, and then click **Apply**.

e Set the IPMI LAN channel encryption key, if required.

**NOTE:** iDRAC6 IPMI supports the RMCP+ protocol.

Under **IPMI Settings** in the **Encryption Key** field, enter the encryption key.

f Click **Apply**.

3 Configure IPMI Serial over LAN (SOL):

a Click **System→ iDRAC Settings**, and then click the **Network/Security** tab.

The **Network** screen is displayed.

b Click the **Serial Over LAN** tab.

c Select **Enable Serial Over LAN**.

d Update the IPMI SOL **Baud Rate**, if needed, by selecting a data speed from the **Baud Rate** drop-down menu.

**NOTE:** To redirect the serial console over the LAN, ensure that the SOL **Baud Rate** is identical to your managed server's baud rate.

e Click **Apply**.

f Configure IP filtering and blocking settings as needed in the **Advanced Settings** page.

# Adding and Configuring iDRAC6 Users

To manage your system with iDRAC6 and maintain system security, create unique users with specific administrative permissions (or *role-based authority*).

To add and configure iDRAC6 users, perform the following steps:

**NOTE:** You must have **Configure iDRAC** permission to perform the following steps.

1 Click **System→ iDRAC Settings→ Network/Security→ Users**.

The **Users** screen displays each user's User ID, State, User Name, IPMI LAN Privileges, iDRAC6 Privileges, and Serial Over LAN capability.

**NOTE:** User-1 is reserved for the IPMI anonymous user and is not configurable.

2 In the **User ID** column, click a user ID number.

3 On the **User Main Menu** page (see Table 5-8, Table 5-9, and Table 5-10), you can either configure a user, upload a SSH public key file, or view or delete a specified SSH key or all SSH keys.

## Public Key Authentication over SSH

iDRAC6 supports the Public Key Authentication (PKA) over SSH. This authentication method improves SSH scripting automation by removing the need to embed or prompt for a user ID/password.

### Before you Begin

You can configure up to 4 public keys *per user* that can be used over an SSH interface. Before adding or deleting public keys, ensure that you use the view command to see what keys are already set up, so a key is not accidentally

overwritten or deleted. When the PKA over SSH is set up and used correctly, you do not have to enter the password when logging into iDRAC6. This can be very useful for setting up automated scripts to perform various functions.

When getting ready to set up this functionality, be aware of the following:

- You can manage this feature with RACADM and also from the GUI.
- When adding new public keys, ensure that the existing keys are not already at the index where the new key is added. iDRAC6 does not perform checks to ensure previous keys are deleted before a new one is added. As soon as a new key is added, it is automatically in effect as long as the SSH interface is enabled.

#### Generating Public Keys for Windows

Before adding an account, a public key is required from the system that will access iDRAC6 over SSH. There are two ways to generate the public/private key pair: using *PuTTY Key Generator* application for clients running Windows or *ssh-keygen* CLI for clients running Linux. The *ssh-keygen* CLI utility comes by default on all standard installations.

This section describes simple instructions to generate a public/private key pair for both applications. For additional or advanced usage of these tools, see the application Help.

To use the *PuTTY Key Generator* for Windows clients 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.
2. Enter the number of bits for the key. The supported key generation algorithms are RSA and DSA only. The number must be between 768 and 4096 bits for RSA and 1024 bits for DSA.
3. Click **Generate** and move the mouse in the window as directed. After the key is created, you can modify the key comment field. You can also enter a passphrase to make the key secure. Ensure that you save the private key.
4. You can save the public key to a file using the **Save public key** option to upload it later. All uploaded keys must be in RFC 4716 or openSSH formats. If not, you must convert the same into those formats.

#### Generating Public Keys for Linux

The *ssh-keygen* application for Linux clients is a command line tool with no graphical user interface.

Open a terminal window and at the shell prompt, enter:

```
ssh-keygen –t rsa –b 1024 –C testing
```

**NOTE:** The options are case-sensitive.

where,

**-t** can be either *dsa* or *rsa*.

**–b** specifies the bit encryption size between 768 and 4096.

**–C** allows modifying the public key comment and is optional.

After the command executes, upload the public file.

**NOTE:** Keys generated from the Linux management station using ssh-keygen are not in RFC4716 but openSSH format. The openSSH public keys can be uploaded to iDRAC6. iDRAC6 public key algorithm validates both the openSSH and RFC4716 keys, internally converts the RFC4716 keys to the openSSH format, and then internally stores the keys.

**NOTE:** iDRAC6 does not support ssh-agent forward of keys.

#### Logging in Using Public Key Authentication

After the public keys are uploaded, you can log into iDRAC6 over SSH without entering a password. You also have the option of sending a single RACADM command as a command line argument to the SSH application. The command line options behave like 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 iDRAC6.

Sending RACADM commands:

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

See "Uploading, Viewing, and Deleting SSH Keys Using RACADM" on page 282 for information on how to upload, view, and delete SSH keys using RACADM.

**Table 5-8. SSH Key Configurations**

| Option | Description |
|---|---|
| **Upload SSH Key(s)** | Allows the local user to upload a SSH public key file. If a key is uploaded, the content of the key file is displayed in a non-editable text box on the **User Configuration** page. |
| **View/Remove SSH Key(s)** | Allows the local user to view or delete a specified SSH key or all SSH keys. |

The **Upload SSH Key(s)** page allows you to upload a SSH public key file. If a key is uploaded, the contents of the key file is displayed in a non-editable text box on the **View/Remove SSH Key(s)** page.

**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. For more information, see Table 5-13.**

**Table 5-9. Upload SSH Key(s)**

| Option | Description |
|---|---|
| **File/Text** | Select the **File** option and type the path where the key is located. You can also select the **Text** option and paste the contents of the key file in the box. You can upload new key(s) or overwrite existing key(s). To upload a key file, click **Browse**, select the file, and then click the **Apply** button.<br>**NOTE:** The Key text paste option is supported for public keys in the openSSH format. Text paste option for the RFC4716 format key is not supported. |
| **Browse** | Click this button to locate the full path and file name of the key. |

The **View/Remove SSH Key(s)** page enables you to view or remove the user's SSH public keys.

**Table 5-10. View/Remove SSH Key(s)**

| Option | Description |
|---|---|
| **Remove** | The uploaded key is displayed in the box. Select the **Remove** option and click **Apply** to delete the existing key. |

1. If you select **Configure User** and click **Next**, the **User Configuration** page is displayed.
2. On the **User Configuration** screen, configure the user's properties and privileges.

   Table 5-11 describes the **General** settings for configuring an iDRAC6 user name and password.

   Table 5-12 describes the **IPMI LAN Privileges** for configuring the user's LAN privileges.

   Table 5-13 describes the **User Group** permissions for the **IPMI LAN Privileges** and iDRAC6 **User Privileges** settings.

   Table 5-14 describes **iDRAC6 Group** permissions. If you add an **iDRAC6 User Privilege** to the **Administrator**, **Power User**, or **Guest User**, iDRAC6 **Group** will change to the **Custom** group.
3. When completed, click **Apply** to save the settings.

**Table 5-11. General Properties**

| Property | Description |
|---|---|
| **User ID** | Contains one of 16 preset User ID numbers. This field cannot be edited. |
| **Enable User** | When **Checked**, indicates that the user's access to iDRAC6 is enabled. When **Unchecked**, user access is disabled. |

**Table 5-11. General Properties *(continued)***

| Property | Description |
|---|---|
| **User Name** | Specifies an iDRAC6 user name with up to 16 characters. Each user must have a unique user name.<br>• 0-9<br>• A-Z<br>• a-z<br>• Special characters:<br>+ % = , - { ] §<br>! ( ? ; _ } I<br># ) * : $ [ \|<br>**NOTE:** If the user name is changed, the new name will not appear in the user interface until the next user login. |
| **Change Password** | Enables the **New Password** and **Confirm New Password** fields. When deselected, the user's Password cannot be changed. |
| **New Password** | Enables editing iDRAC6 user's password. Enter a **Password** with up to 20 characters. The characters will not display.<br>• 0-9<br>• A-Z<br>• a-z<br>• Special characters:<br>+ % = , - { ] .<br>! ( ? ; _ } I \|<br># ) * : $ [ / @ |
| **Confirm New Password** | Re-enter iDRAC6 user's password to confirm. |

**NOTE:** iDRAC6 allows to create usernames with the supported characters described in table 5-12. However, a few delimiter characters are not supported in all the user interfaces like RACADM. Directory services also have restrictions on user name format.

**Table 5-12. IPMI LAN Privilege**

| Property | Description |
|---|---|
| **Maximum LAN User Privilege Granted** | Specifies the user's maximum privilege on the IPMI LAN channel to one of the following user groups: **None**, **Administrator**, **Operator**, or **User**. |
| **Enable Serial Over LAN** | Allows the user to use IPMI Serial Over LAN. When **Checked**, this privilege is enabled. |

**Table 5-13. Other Privilege**

| Property | Description |
|---|---|
| **iDRAC6 Group** | Specifies the user's maximum iDRAC6 user privilege as one of the following: **Administrator**, **Power User**, **Guest User**, **Custom**, or **None**.<br>See Table 5-14 for **iDRAC6 Group** permissions. |
| **Login to iDRAC6** | Enables the user to log in to iDRAC6. |
| **Configure iDRAC6** | Enables the user to configure iDRAC6. |
| **Configure Users** | Enables the user to allow specific users to access the system.<br>**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.** |
| **Clear Logs** | Enables the user to clear iDRAC6 logs. |
| **Execute Server Control Commands** | Enables the user to execute RACADM commands. |

**Table 5-13. Other Privilege *(continued)***

| Property | Description |
|---|---|
| Access Virtual Console | Enables the user to run Virtual Console.<br>**CAUTION: This privilege is normally reserved for users who are members of the Administrator or Power User group on iDRAC. In addition to being able to use the Virtual Console, users with the Access Virtual Console privilege are allowed to view in the iDRAC6 Web interface the activities of anyone using the Virtual Console. For these reasons, assign this privilege carefully.** |
| Access Virtual Media | Enables the user to run and use Virtual Media. |
| Test Alerts | Enables the user to send test alerts (e-mail and PET) to all currently configured alert recipients. |
| Execute Diagnostic Commands | Enables the user to run diagnostic commands. |

**Table 5-14. iDRAC6 Group Permissions**

| User Group | Permissions Granted |
|---|---|
| Administrator | Login to iDRAC6, Configure iDRAC6, Configure Users, Clear Logs, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands |
| Power User | Login to iDRAC6, Clear Logs, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts |
| Guest User | Login to iDRAC6 |
| Custom | Selects any combination of the following permissions: Login to iDRAC6, Configure iDRAC6, Configure Users, Clear Logs, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands |
| None | No assigned permissions |

# Securing iDRAC6 Communications Using SSL and Digital Certificates

This section provides information about the following data security features that are incorporated in iDRAC6:

- Secure Sockets Layer (SSL)
- Certificate Signing Request (CSR)
- Accessing the SSL main menu
- Generating a new CSR
- Uploading a server certificate
- Viewing a server certificate

## Secure Sockets Layer (SSL)

iDRAC6 includes a Web server that is configured to use the industry-standard SSL security protocol to transfer encrypted data over a network. Built upon public-key and private-key encryption technology, SSL is a widely accepted technology 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 client to authenticate itself to the server
- Allow both systems to establish an encrypted connection

The encryption process provides a high level of data protection. iDRAC6 employs the 128-bit SSL encryption standard, the most secure form of encryption generally available for Internet browsers in North America.

iDRAC6 Web server has a Dell self-signed SSL digital certificate (Server ID) by default. To ensure high security over the Internet, replace the Web server 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

signed certificate, you can use iDRAC6 Web interface to generate a Certificate Signing Request (CSR) with your company's information. You can then submit the generated CSR to a CA such as VeriSign or Thawte.

### Certificate Signing Request (CSR)

A CSR is a digital request to a Certificate Authority (CA) for a secure server certificate. Secure 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 certificate that uniquely identifies that applicant for transactions over networks and on the Internet.

After the CA approves the CSR and sends the certificate, upload the certificate to iDRAC6 firmware. The CSR information stored on iDRAC6 firmware must match the information contained in the certificate, that is, the certificate must have been generated in response to the CSR created by iDRAC6.

### Accessing the SSL Main Menu

1. Click **System→ iDRAC Settings→ Network/Security** tab.
2. Click **SSL** to open the **SSL** screen.

Table 5-15 describes the options available when generating a CSR.

**Table 5-15. SSL Main Menu Options**

| Field | Description |
|---|---|
| **Generate a New Certificate Signing Request (CSR)** | Select the option and click **Next** to open the **Generate Certificate Signing Request (CSR)** screen. See "Generating a New Certificate Signing Request" on page 109 for more information.<br>**NOTE:** Each new CSR overwrites any previous CSR data stored in the firmware. The information in the CSR should match the information in the certificate. Otherwise, iDRAC6 will not accept the certificate. |

**Table 5-15. SSL Main Menu Options *(continued)***

| Field | Description |
|---|---|
| Upload Server Certificate | Select the option and click **Next** to open the **Certificate Upload** screen and upload the certificate sent to you by the CA. See "Uploading a Server Certificate" on page 110 for more information.<br>**NOTE:** Only X509 v3, Base 64-encoded certificates are accepted by iDRAC6. DER-encoded certificates are not accepted. |
| View Server Certificate | Select the option and click **Next** to open the **View Server Certificate** screen and view the existing server certificate. See "Viewing a Server Certificate" on page 111 for more information. |

## Generating a New Certificate Signing Request

**NOTE:** Each new CSR overwrites any previous CSR data stored in the firmware. The information in the CSR should match the information in the certificate. Otherwise, iDRAC6 will not accept the certificate.

1. On the **SSL** screen, select **Generate a New Certificate Signing Request (CSR)** and click **Next**.
2. On the **Generate Certificate Signing Request (CSR)** screen, enter a value for each CSR attribute.

   Table 5-16 describes the **Generate Certificate Signing Request (CSR)** screen options.
3. Click **Generate** to create the CSR.
4. Click **Download** to save the CSR file to your remote management station.

**Table 5-16. Generate Certificate Signing Request (CSR) Options**

| Field | Description |
|---|---|
| Common Name | The exact name being certified (usually the Web server's domain name, for example, **xyzcompany.com**). All characters except for '$' is supported. |
| Organization Name | The name associated with this organization (for example, XYZ Corporation). All characters except for '$' is supported. |

**Table 5-16. Generate Certificate Signing Request (CSR) Options *(continued)***

| Field | Description |
|---|---|
| **Organization Unit** | The name associated with an organizational unit, such as a department (for example, Information Technology). All characters except for '$' is supported. |
| **Locality** | The city or other location of the entity being certified (for example, Round Rock). Only alphanumeric characters and spaces are valid. Do not separate words using an underscore or other character. |
| **State Name** | The state or province where the entity who is applying for a certification is located (for example, Texas). Only alphanumeric characters and spaces are valid. Do not use abbreviations. |
| **Country Code** | The name of the country where the entity applying for certification is located. |
| **Email** | The e-mail address associated with the CSR. Enter the company's e-mail address, or any e-mail address associated with the CSR. This field is optional. |
| **Key Size** | The size of the Certificate Signing Request (CSR) Key to be generated. The size may be 1024 KB or 2048 KB. |

## Uploading a Server Certificate

1. In the **SSL** screen, select **Upload Server Certificate** and click **Next**.

   The **Certificate Upload** screen is displayed.

2. In the **File Path** field, click **Browse** to navigate to and specify the certificate file on the management station.

   **NOTE:** The **File Path** value displays the file path of the certificate you are uploading, which includes the full path, the complete file name, and file extension.

3. Click **Apply** to upload the certificate to iDRAC6 firmware.

### Viewing a Server Certificate

1 On the SSL screen, select **View Server Certificate** and click **Next**.

Table 5-17 describes the fields and associated descriptions listed in the **View Server Certificate** window.

**Table 5-17. View Server Certificate Information**

| Field | Description |
|---|---|
| Serial Number | Certificate serial number |
| Subject Information | Certificate attributes entered by the subject |
| Issuer Information | Certificate attributes returned by the issuer |
| Valid From | Issue date of the certificate |
| Valid To | Expiration date of the certificate |

# Configuring and Managing Microsoft Active Directory Certificates

**NOTE:** You must have **Configure iDRAC** permission to configure Active Directory and upload, download, and view an Active Directory certificate.

**NOTE:** For more information about Active Directory configuration and how to configure Active Directory with the standard schema or an extended schema, see "Using iDRAC6 Directory Service" on page 127.

To access the **Microsoft Active Directory** summary screen, click **System**→ **iDRAC Settings**→ **Network/Security** tab→ **Directory Service**→ **Microsoft Active Directory**.

Table 5-18 lists the **Active Directory** summary options. Click the appropriate button to continue.

**Table 5-18. Active Directory Options**

| Field | Description |
|---|---|
| **Common Settings** | Displays commonly configured Active Directory settings. |
| **Active Directory CA Certificate** | Displays the certificate of the CA that signs all the domain controller's SSL server certificates. |
| **Standard Schema Settings/Extended Schema Settings** | Depending on the current Active Directory configuration, Extended Schema Settings or Standard Schema Settings are displayed. |
| **Configure Active Directory** | Click this option to configure Step 1 of 4 in Active Directory Settings. The **Step 1 of 4 Active Directory** page allows you to upload an Active Directory CA certificate to iDRAC6, view the current Active Directory CA Certificate that has been uploaded to iDRAC6, or enable certificate validation. |
| **Test Settings** | Click this option to test the Active Directory configuration using the settings you specified. |
| **Kerberos Keytab Upload** | Click this option to upload the Kerberos Keytab to iDRAC6. For information on how to create a keytab file, see "Configuring iDRAC6 for Single Sign-On and Smart Card Login" on page 171. |

## Configuring Active Directory (Standard Schema and Extended Schema)

1. On the **Active Directory** summary screen, click **Configure Active Directory**.
2. On the **Step 1 of 4 Active Directory** screen, you can either enable certificate validation, upload the Active Directory CA certificate in iDRAC6, or view the current Active Directory CA certificate.

   Table 5-19 describes the settings and selections for each step in the **Active Directory Configuration and Management** process. Click the appropriate button to continue.

**Table 5-19. Active Directory Configuration Settings**

| Setting | Description |
|---|---|
| Step 1 of 4 Active Directory Configuration and Management | |
| **Certificate Validation Enabled** | Specifies whether Certificate validation is enabled or disabled. If **Checked**, Certificate Validation is enabled. iDRAC6 uses LDAP over Secure Socket Layer (SSL) while connecting to Active Directory. By default, iDRAC6 provides strong security by using the CA certificate loaded in iDRAC6 to validate the SSL server certificate of the domain controllers during SSL handshake. Certificate validation can be disabled for testing purposes. |
| **Upload Active Directory CA Certificate** | To upload an Active Directory CA certificate, click **Browse**, select the file, and click **Upload**. Ensure that the domain controller's SSL certificates have been signed by the same CA and that this Certificate is available on the management station accessing iDRAC6. The **File Path** value displays the file path of the certificate you are uploading. If you choose not to browse to the certificate, enter the file path which includes the full path and the complete file name and file extension. |
| **Current Active Directory CA Certificate** | Displays the Active Directory CA Certificate that was uploaded to iDRAC6. |
| Step 2 of 4 Active Directory Configuration and Management | |
| **Active Directory Enabled** | Select this option if you want to enable Active Directory. |
| **Enable Smart–Card Login** | Select this option to enable Smart Card login. You are prompted for a Smart Card logon during any subsequent logon attempts using the GUI.<br>**NOTE:** The Smart Card based Two Factor Authentication (TFA) and Single Sign–on are supported only in Microsoft Windows operating systems with Internet Explorer. Also, Terminal Services (Remote Desktop) under Windows XP does not support Smart Card operation. However, Windows Vista supports such usage. |

**Table 5-19. Active Directory Configuration Settings *(continued)***

| Setting | Description |
|---|---|
| **Enable Single Sign-on** | Select this option if you want to log into iDRAC6 without entering your domain user authentication credentials, such as user name and password. If you enable Single Sign-on (SSO) and then logout, you can log back in using SSO. If you are already logged in using SSO and then logout or if SSO fails, the normal login webpage is displayed.<br>**NOTE:** Enabling Smart–Card logon **or** Single Sign-on does not disable any command line out–of–band interfaces including SSH, Telnet, remote RACADM, and IPMI over LAN.<br>**NOTE:** In this release, the Smart Card based Two Factor Authentication (TFA) feature is not supported if the Active directory is configured for Extended schema. The Single Sign-On (SSO) feature is supported for both Standard and Extended schema. |
| **User Domain Name** | Enter the User Domain Name entries. If configured, a list of user domain names are displayed on the login page as a drop-down menu. If not configured, Active Directory users can still log in by entering the user name in the format user_name@domain_name or domain_name\user_name. **Add**: Adds a new User Domain Name entry to the list. **Edit**: Modifies an existing User Domain Name entry. **Delete**: Deletes a User Domain Name entry from the list. |
| **Timeout** | Enter the maximum time (in seconds) to wait for Active Directory queries to complete. |

**Table 5-19. Active Directory Configuration Settings *(continued)***

| Setting | Description |
|---|---|
| **Look Up Domain Controllers with DNS** | Select the **Look Up Domain Controllers with DNS** option to obtain the Active Directory domain controllers from a DNS lookup. When this option is selected, Domain Controller Server Addresses 1-3 are ignored. Select **User Domain from Login** to perform the DNS lookup with the domain name of the login user. Otherwise, select **Specify a Domain** and enter the domain name to use on the DNS lookup. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS look up) one by one until it makes a successful connection.<br><br>If **Extended Schema** is selected, the domain controllers are where iDRAC6 device object and the Association objects are located. If **Standard Schema** is selected, the domain controllers are where the user accounts and the role groups are located. |
| **Specify Domain Controller Addresses** | Select the **Specify Domain Controller Addresses** option to allow iDRAC6 to use the Active Directory Domain Controller server addresses that are specified. When this option is selected, DNS lookup is not performed. Specify the IP address or the Fully Qualified Domain Name (FQDN) of the domain controllers. When the **Specify Domain Controller Addresses** option is selected, at least one of the three addresses is required to be configured. iDRAC6 attempts to connect to each of the configured addresses one by one until it makes a successful connection.<br><br>If **Standard Schema** is selected, these are the addresses of the domain controllers where the user accounts and the role groups are located. If **Extended Schema** is selected, these are the addresses of the domain controllers where iDRAC6 device object and the Association objects are located. |

**Step 3 of 4 Active Directory Configuration and Management**

**Table 5-19. Active Directory Configuration Settings *(continued)***

| Setting | Description |
|---|---|
| Extended Schema Selection | Select this option if you want to use Extended Schema with Active Directory.<br><br>Click **Next** to display the **Step 4 of 4 Active Directory Configuration and Management** page.<br><br>**iDRAC6 Name**: Specifies the name that uniquely identifies iDRAC6 in Active Directory. This value is NULL by default.<br><br>**iDRAC6 Domain Name**: The DNS name (string) of the domain where the Active Directory iDRAC object resides. This value is NULL by default.<br><br>These settings are displayed only if iDRAC6 has been configured for use with an Extended Active Directory Schema. |

**Table 5-19. Active Directory Configuration Settings *(continued)***

| Setting | Description |
|---|---|
| **Standard Schema Selection** | Select this option if you want to use Standard Schema with Active Directory.<br><br>Click **Next** to display the **Step 4a of 4 Active Directory** page.<br><br>Select the **Look Up Global Catalog Servers with DNS** option and enter the **Root Domain Name** to use on a DNS lookup to obtain the Active Directory Global Catalog Servers. When this option is selected, **Global Catalog Server Addresses 1-3** are ignored. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS lookup) one by one until it makes a successful connection. A Global Catalog server is required only for Standard Schema in the case that the user accounts and the role groups are in different domains.<br><br>Select the **Specify Global Catalog Server Addresses** option and enter the IP address or the FQDN of the Global Catalog server(s). When this option is selected, DNS lookup is not performed. At least one of the three addresses must be configured. iDRAC6 attempts to connect to each of the configured addresses one by one until it makes a successful connection. Global Catalog server is required only for Standard Schema in the case that the user accounts and the role groups are in different domains.<br><br>**Role Groups**: Specifies the list of role groups associated with iDRAC6.<br><br>**Group Name**: Specifies the name that identifies the role group in the Active Directory associated with iDRAC6.<br><br>**Group Domain**: Specifies the group domain type where the Role Group resides.<br><br>**Role Group Privileges**: Specifies the group privilege level. (see Table 5-20)<br><br>These settings are displayed only if iDRAC6 has been configured for use with a Standard Active Directory Schema. |

**Table 5-20. Role Group Privileges**

| Setting | Description |
|---|---|
| Role Group Privilege Level | Specifies the user's maximum iDRAC6 user privilege as one of the following: **Administrator**, **Power User**, **Guest User**, **None**, or **Custom**.<br>See Table 5-21 for **Role Group** permissions. |
| Login to iDRAC6 | Allows the group login access to iDRAC6. |
| Configure iDRAC6 | Allows the group permission to configure iDRAC6. |
| Configure Users | Allows the group permission to configure users. |
| Clear Logs | Allows the group permission to clear logs. |
| Execute Server Control Commands | Allows the group permission to execute server control commands. |
| Access Virtual Console | Allows the group access to Virtual Console. |
| Access Virtual Media | Allows the group access to Virtual Media. |
| Test Alerts | Allows the group to send test alerts (e-mail and PET) to a specific user. |
| Execute Diagnostic Commands | Allows the group permission to execute diagnostic commands. |

**Table 5-21. Role Group Permissions**

| Property | Description |
|---|---|
| Administrator | Login to iDRAC6, Configure iDRAC6, Configure Users, Clear Logs, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands |
| Power User | Login to iDRAC6, Clear Logs, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts |
| Guest User | Login to iDRAC6 |

**Table 5-21. Role Group Permissions *(continued)***

| Property | Description |
|---|---|
| Custom | Selects any combination of the following permissions: Login to iDRAC6, Configure iDRAC6, Configure Users, Clear Logs, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands |
| None | No assigned permissions |

### Viewing an Active Directory CA Certificate

On the **Active Directory** summary page, click **Configure Active Directory**. The **Current Active Directory CA Certificate** section is displayed. See Table 5-22.

**Table 5-22. Active Directory CA Certificate Information**

| Field | Description |
|---|---|
| Serial Number | Certificate serial number. |
| Subject Information | Certificate attributes entered by the subject. |
| Issuer Information | Certificate attributes returned by the issuer. |
| Valid From | Certificate issue date. |
| Valid To | Certificate expiration date. |

# Enabling or Disabling Local Configuration Access

**NOTE:** The default setting for local configuration access is **Enabled**.

### Enabling Local Configuration Access

1. Click **System**→ **iDRAC Settings**→ **Network/Security**→ **Services**.
2. Under **Local Configuration**, click to **Uncheck** the **Disable iDRAC6 local USER Configuration Updates** to enable access.
3. Click **Apply**.

### Disabling Local Configuration Access

1. Click **System→ iDRAC Settings→ Network/Security→ Services**.
2. Under **Local Configuration**, click to select **Disable iDRAC6 local USER Configuration Updates** to disable access.
3. Click **Apply**.

## Configuring iDRAC6 Services

**NOTE:** To modify these settings, you must have **Configure iDRAC6** permission.

**NOTE:** When you apply changes to services, the changes take effect immediately. Existing connections may be terminated without warning.

**NOTE:** There is a known issue with the Telnet client supplied with Microsoft Windows. Use another Telnet client such as HyperTerminal or PuTTY.

1. Click **System→ iDRAC Settings→ Network/Security** tab.
2. Click **Services** to open the **Services** configuration screen.
3. Configure the following services, as required:
   - Web server — see Table 5-23 for Web server settings
   - SSH — see Table 5-24 for SSH settings
   - Telnet — see Table 5-25 for Telnet settings
   - SNMP Agent — see Table 5-26 for SNMP agent settings
   - Automated System Recovery Agent — see Table 5-27 for Automated System Recovery Agent settings
4. Click **Apply**.

**Table 5-23. Web Server Settings**

| Setting | Description |
|---|---|
| **Enabled** | Enables or disables iDRAC6 Web server. When **Checked**, indicates that the Web server is enabled. The default value is **Checked**. |
| **Max Sessions** | The maximum number of simultaneous Web server sessions allowed for this system. This field is not editable. There can be 4 simultaneous Web server sessions. |
| **Active Sessions** | The number of current sessions on the system, less than or equal to the **Max Sessions**. This field is not editable. |
| **Timeout** | The time, in seconds, that a connection is allowed to remain idle. The session is cancelled when the timeout is reached. Changes to the timeout setting take affect immediately and will reset the Web server. Timeout range is 60 to 10800 seconds. The default is **1800** seconds. |
| **HTTP Port Number** | The port on which iDRAC6 listens for a browser connection. The default is **80**. |
| **HTTPS Port Number** | The port on which iDRAC6 listens for a secure browser connection. The default is **443**. |

**Table 5-24. SSH Settings**

| Setting | Description |
|---|---|
| **Enabled** | Enables or disables SSH. When **Checked**, the check box indicates that SSH is enabled. |
| **Max Sessions** | The maximum number of simultaneous SSH sessions allowed for this system. 4 simultaneous SSH sessions are supported. You can not edit this field. |
| **Active Sessions** | The number of current sessions on the system. You can not edit this field. |
| **Timeout** | The secure shell idle timeout, in seconds. Timeout range is 60 to 10800 seconds. Enter 0 seconds to disable the Timeout feature. The default is **1800**. |
| **Port Number** | The port on which iDRAC6 listens for an SSH connection. The default is **22**. |

**Table 5-25. Telnet Settings**

| Setting | Description |
|---|---|
| **Enabled** | Enables or disables Telnet. When **Checked**, Telnet is enabled. The default value is **Unchecked**. |
| **Max Sessions** | The maximum number of simultaneous Telnet sessions allowed for this system. 4 simultaneous Telnet sessions are supported. You can not edit this field. |
| **Active Sessions** | The number of current Telnet sessions on the system. You can not edit this field. |
| **Timeout** | The Telnet idle timeout, in seconds. Timeout range is 60 to 10800 seconds. Enter 0 seconds to disable the Timeout feature. The default is **1800**. |
| **Port Number** | The port on which iDRAC6 listens for a Telnet connection. The default is **23**. |

**Table 5-26. SNMP Settings**

| Setting | Description |
|---|---|
| **Enabled** | Enables/disables SNMP. When checked, SNMP is enabled. |
| **SNMP Community Name** | Enter the SNMP community name. The default is **public**. |

**Table 5-27. Automated System Recovery Agent**

| Setting | Description |
|---|---|
| **Enabled** | Enables the Automated System Recovery Agent. |

# Updating iDRAC6 Firmware

**NOTE:** If iDRAC6 firmware becomes corrupted, as could occur if iDRAC6 firmware update is interrupted before it completes, you can recover iDRAC6 using CMC. See your *CMC Firmware User Guide* for instructions.

**NOTE:** The firmware update, by default, retains the current iDRAC6 settings. During the update process, you have the option to reset iDRAC6 configuration to the factory defaults. If you set the configuration to the factory defaults, external network access will be disabled when the update completes. You must enable and configure the network using iDRAC6 Configuration Utility or CMC Web interface.

1. Start iDRAC6 Web interface.
2. Click **System→ iDRAC Settings→ Update** tab.

   The **Firmware Update** screen is displayed.

   **NOTE:** To update the firmware, iDRAC6 must be placed in an update mode. Once in this mode, iDRAC6 will automatically reset, even if you cancel the update process.
3. In the **Upload** section, click **Browse** and select the firmware image.

   The default firmware image name is **firmimg.imc**.
4. Click **Upload**. The file will be uploaded to iDRAC6. This may take several minutes to complete.
5. In the **Upload (Step 2 of 3)** screen, you will see the results of the validation performed on the image file you uploaded.
   - If the image file is uploaded successfully and passed all verification checks, a message will appear indicating that the firmware image has been verified.
   - If the image did not upload successfully, or it did not pass the verification checks, reset iDRAC6, close the current session, and then try updating again.

   **NOTE:** If you clear the **Preserve Configuration** check box, after completing update firmware, iDRAC6 resets to its default configuration. In the default settings, the LAN is disabled. You will not be able to log in to iDRAC6 Web interface. You will have to reconfigure the LAN settings using CMC Web interface or by using iDRAC6 Configuration Utility during BIOS POST.

6 By default the **Preserve Configuration** check box is selected to preserve the current settings on iDRAC6 after an upgrade. If you do not want the settings to be preserved, clear the **Preserve Configuration** check box.

7 Click **Begin Update** to start the upgrade process. Do not interrupt the upgrade process.

8 In the **Upload (step 3 of 3)** window, you will see the status of the upgrade. The progress of the firmware upgrade operation, measured in percent, will appear in the **Progress** column.

9 Once the firmware update is complete, the **Upload (step 3 of 3)** window will refresh with the result and iDRAC6 will reset automatically. To continue accessing iDRAC6 through the Web interface, close the current browser window and reconnect to iDRAC6 using a new browser window.

### Updating iDRAC6 Firmware Using CMC

Typically, iDRAC6 firmware is updated using iDRAC6 utilities, such as iDRAC6 Web interface or operating system specific update packages downloaded from **support.dell.com**.

You can use CMC Web interface or RACADM to update iDRAC6 firmware. This feature is available both when iDRAC6 firmware is in Normal mode, as well as when it is corrupted.

**NOTE:** See the *Chassis Management Controller Firmware User Guide* for instructions for using CMC Web interface.

To update iDRAC6 firmware, perform the following steps:

1 Download the latest iDRAC6 firmware to your management station from **support.dell.com**.

2 Log in to CMC Web interface.

3 Click **Chassis Overview** in the system tree.

4 Click the **Update** tab. The **Firmware Update** screen is displayed.

5 In the **iDRAC6 Enterprise Firmware** section→ **Update Targets** column, select the iDRAC6s to be updated.

6 Click **Apply iDRAC6 Enterprise Update**.

7 Click **Browse**, browse to iDRAC6 firmware image you downloaded, and click **Open**.

8 Click **Begin Firmware Update**.

After the firmware image file has been uploaded to CMC, iDRAC6 updates itself with the image.

**NOTE:** The configuration is always preserved when iDRAC is updated using the CMC Web interface.

### iDRAC6 Firmware Rollback

iDRAC6 has the provision to maintain two simultaneous firmware images. You can choose to boot from (or rollback to) the firmware image of your choice.

1. Open iDRAC6 Web interface and log in to the remote system.
2. Click **System→ iDRAC Settings→ Update** tab.
3. Click **Rollback**. The current and the rollback firmware versions are displayed on the **Rollback (Step 2 of 3)** page.
4. Click **Next** to start the firmware rollback process.

   On the **Rollback (Step 3 of 3)** page, you see the status of the rollback operation. On successful completion, it shows that the process completed successfully.

   If the firmware rollback is successful, iDRAC6 will reset automatically. To continue working with iDRAC6 through the Web interface, close the current browser and reconnect to iDRAC6 using a new browser window. An appropriate error message is displayed if an error occurs.

   **NOTE:** The **Preserve Configuration** feature does not work if you want to rollback iDRAC6 firmware from version 2.2 to version 2.1.

# 6

# Using iDRAC6 Directory Service

A directory service maintains a common database for storing information about users, computers, printers, and so on on a network. If your company uses either the Microsoft Active Directory or the LDAP Directory Service software, you can configure the software to provide access to iDRAC6, allowing you to add and control iDRAC6 user privileges to your existing users in your directory service.

## Using iDRAC6 With Microsoft Active Directory

**NOTE:** Using Active Directory to recognize iDRAC6 users is supported on the Microsoft Windows 2000, Windows Server 2003, and Windows Server 2008 operating systems.

You can configure user authentication through Microsoft Active Directory to log in to the iDRAC6. You can also provide role-based authority, which enables an administrator to configure specific privileges for each user. For more information, see the subsequent sections.

Table 6-1 shows iDRAC6 Active Directory user privileges.

**Table 6-1. iDRAC6 User Privileges**

| Privilege | Description |
|---|---|
| Login to iDRAC6 | Enables the user to log in to iDRAC6 |
| Configure iDRAC6 | Enables the user to configure iDRAC6 |
| Configure Users | Enables the user to allow specific users to access the system |
| Clear Logs | Enables the user to clear iDRAC6 logs |
| Execute Server Control Commands | Enables the user to execute RACADM commands |
| Access Virtual Console | Enables the user to run Virtual Console |
| Access Virtual Media | Enables the user to run and use Virtual Media |
| Test Alerts | Enables the user to send test alerts (e-mail and PET) to a specific user |

**Table 6-1. iDRAC6 User Privileges *(continued)***

| Privilege | Description |
|---|---|
| **Execute Diagnostic Commands** | Enables the user to run diagnostic commands |

You can use Active Directory to log in to iDRAC6 using one of the following methods:

- Web interface
- Local RACADM
- SSH or Telnet console for SM-CLP CLI

The login syntax is the same for all three methods:

*<username@domain>*

or

*<domain>**<username>* or *<domain>*/*<username>*

where *username* is an ASCII string of 1–256 bytes.

White space and special characters (such as \, /, or @) cannot be used in the user name or the domain name.

**NOTE:** You cannot specify NetBIOS domain names, such as *Americas*, because these names cannot be resolved.

If you log in from the Web interface and you have configured user domains, the Web interface log in screen will list all the user domains in the pull-down menu for you to choose. If you select a user domain from the pull-down menu, you should only enter the user name. If you select **This iDRAC**, you can still log in as an Active Directory user if you use the login syntax described above in "Using iDRAC6 With Microsoft Active Directory" on page 127.

# Prerequisites for Enabling Active Directory Authentication for iDRAC6

To use the Active Directory authentication feature of iDRAC6, you must have already deployed an Active Directory infrastructure. See the Microsoft website for information on how to set up an Active Directory infrastructure, if you don't already have one.

iDRAC6 uses the standard Public Key Infrastructure (PKI) mechanism to authenticate securely into the Active Directory; therefore, you would also require an integrated PKI into the Active Directory infrastructure.

See the Microsoft website for more information on the PKI setup.

To correctly authenticate to all the domain controllers, you also need to enable the Secure Socket Layer (SSL) on all domain controllers that iDRAC6 connects to. See "Enabling SSL on a Domain Controller" on page 129 for more specific information.

## Enabling SSL on a Domain Controller

When iDRAC6 authenticates users against an Active Directory domain controller, it starts an SSL session with the domain controller. At this time, the domain controller should publish a certificate signed by the Certificate Authority (CA)—the root certificate of which is also uploaded into iDRAC6. In other words, for iDRAC6 to authenticate to *any* domain controller—whether it is the root or the child domain controller—that domain controller should 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, perform the following steps to enable SSL on each domain controller:

1. Enable SSL on each of your domain controllers by installing the SSL certificate for each controller.
   a. Click **Start**→ **Administrative Tools**→ **Domain Security Policy**.
   b. Expand the **Public Key Policies** folder, right-click **Automatic Certificate Request Settings** and click **Automatic Certificate Request**.
   c. In the **Automatic Certificate Request Setup Wizard**, click **Next** and select **Domain Controller**.
   d. Click **Next** and click **Finish**.

### Exporting the Domain Controller Root CA Certificate to iDRAC6

**NOTE:** If your system is running Windows 2000, the following steps may vary.

**NOTE:** If you are using a standalone CA, the following steps may vary.

1. Locate the domain controller that is running the Microsoft Enterprise CA service.
2. Click **Start**→ **Run**.
3. In the **Run** field, 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** account and click **Next**.
8. Select **Local Computer** and click **Finish**.
9. Click **OK**.
10. In the **Console 1** window, expand the **Certificates** folder, expand the **Personal** folder, and click the **Certificates** folder.
11. Locate and right-click the root CA certificate, select **All Tasks**, and click **Export...**.
12. In the **Certificate Export Wizard**, click **Next**, and select **No do not export the private key**.
13. Click **Next** and select **Base-64 encoded X.509 (.cer)** as the format.
14. Click **Next** and save the certificate to a directory on your system.
15. Upload the certificate you saved in step 14 to iDRAC6.

    To upload the certificate using RACADM, see "Configuring Active Directory With Standard Schema Using RACADM" on page 158.

    To upload the certificate using the Web interface, see "Configuring Active Directory With Standard Schema Using iDRAC6 Web Interface" on page 154.

#### Importing iDRAC6 Firmware SSL Certificate

**NOTE:** If the Active Directory Server is set to authenticate the client during an SSL session initialization phase, you need to upload iDRAC6 Server certificate to the Active Directory Domain controller as well. 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 iDRAC6 firmware SSL certificate is signed by a well-known CA and the certificate of that CA is already in the domain controller's Trusted Root Certificate Authority list, you are not required to perform the steps in this section.

iDRAC6 SSL certificate is the identical certificate used for iDRAC6 Web server. All iDRAC6 controllers are shipped with a default self-signed certificate.

To import iDRAC6 firmware SSL certificate to all domain controller trusted certificate lists:

1. To download iDRAC6 SSL certificate, run 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 iDRAC6 SSL Certificate in each domain controller's **Trusted Root Certification Authority**.

   If you have installed your own certificate, ensure 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 would like 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**.

# Supported Active Directory Authentication Mechanisms

You can use Active Directory to define user access on iDRAC6 through two methods: you can use the *extended schema* solution, which Dell has customized to add Dell-defined Active Directory objects. Or, you can use the *standard schema* solution, which uses Active Directory group objects only. See the sections that follow for more information about these solutions.

When using Active Directory to configure access to iDRAC6, you must choose either the extended schema or the standard schema solution.

The advantages of using the extended schema solution are:

- All of the access control objects are maintained in Active Directory.
- Maximum flexibility is provided in configuring user access on different iDRAC6 cards with varying privilege levels.

The advantage of using the standard schema solution is that no schema extension is required because all of the necessary object classes are provided by Microsoft's default configuration of the Active Directory schema.

# Extended Schema Active Directory Overview

Using the extended schema solution requires the Active Directory schema extension, as described in the following section.

### 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. Companies can extend the Active Directory database by adding their own unique Attributes and Classes to solve environment-specific needs. Dell has extended the schema to include the necessary changes to support remote management Authentication and Authorization.

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 our attributes and classes that are added into the directory service.

- Dell extension is: `dell`
- Dell base OID is: `1.2.840.113556.1.8000.1280`
- RAC LinkID range is: `12070 to 12079`

### Overview of iDRAC6 Schema Extensions

To provide the greatest flexibility in the multitude of customer environments, Dell provides a group of properties that can be configured by the user depending on the desired results. 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 iDRAC6 devices. This model provides an Administrator maximum flexibility over the different combinations of users, iDRAC6 privileges, and iDRAC6 devices on the network without adding too much complexity.

### Active Directory Object Overview

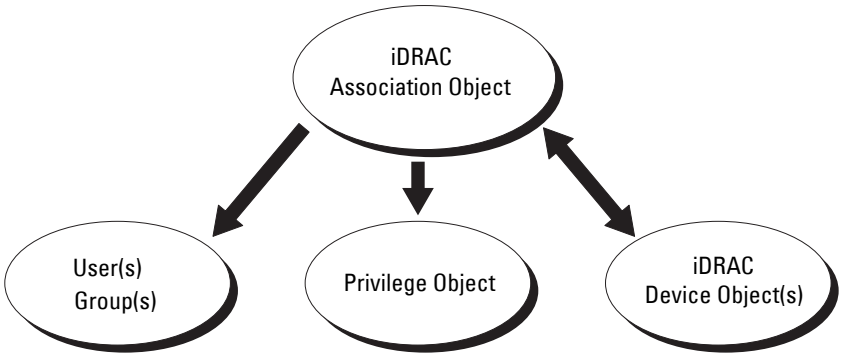
For each physical iDRAC6 device on the network that you want to integrate with Active Directory for Authentication and Authorization, create at least one Association Object and one iDRAC6 Device Object. You can create multiple Association Objects, and each Association Object can be linked to as many users, groups of users, or iDRAC6 Device Objects as required. The users and iDRAC6 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 iDRAC6 Device Objects) to only one Privilege Object. This example allows an Administrator to control each user's privileges on specific iDRAC6 devices.

iDRAC6 Device object is the link to iDRAC6 firmware for querying Active Directory for authentication and authorization. When iDRAC6 is added to the network, the Administrator must configure iDRAC6 and its device object with its Active Directory name so users can perform authentication and authorization with Active Directory. Additionally, the Administrator must add iDRAC6 to at least one Association Object in order for users to authenticate.

Figure 6-1 illustrates that the Association Object provides the connection that is needed for all of the Authentication and Authorization.

**Figure 6-1. 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 iDRAC6 Device Object for each iDRAC6 device on the network that you want to integrate with Active Directory for Authentication and Authorization with iDRAC6.

The Association Object allows for as many or as few users and/or groups as well as iDRAC6 Device Objects. However, the Association Object only includes one Privilege Object per Association Object. The Association Object connects the *Users* who have *Privileges* on iDRAC6 devices.

The Dell extension to the ADUC MMC Snap-in only allows associating the Privilege Object and iDRAC6 Objects from the same domain with the Association Object. The Dell extension does not allow a group or an iDRAC6 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 will not work with Universal Groups from other domains.

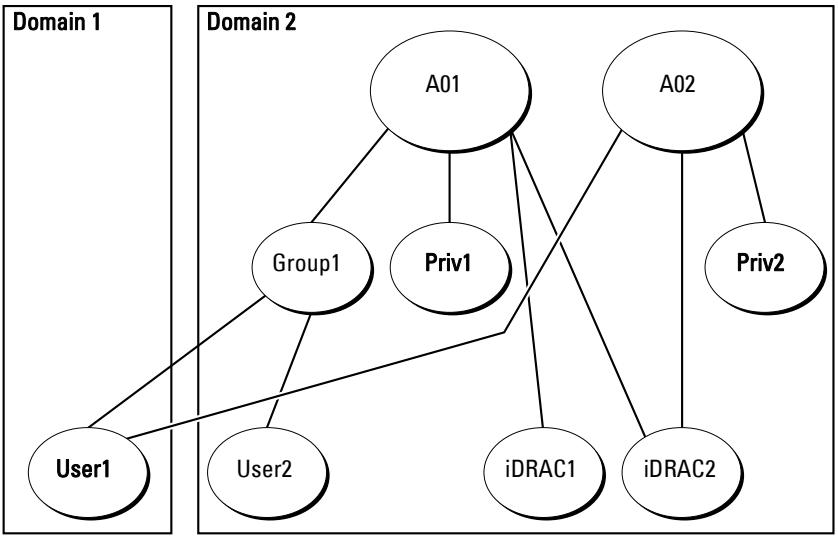
Users, user groups, or nested user groups from any domain can be added into the Association Object. Extended Schema solutions support any user group type and any user group nesting across multiple domains allowed by Microsoft Active Directory.

### 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.

Figure 6-2 provides an example of accumulating privileges using Extended Schema.

**Figure 6-2. Privilege Accumulation for a User**




The figure shows two Association Objects—A01 and A02. User1 is associated to iDRAC2 through both association objects. Therefore, User1 has accumulated privileges that are the result of combining the privileges set for objects Priv1 and Priv2 on iDRAC2.

For example, Priv1 has these privileges: Login, Virtual Media, and Clear Logs and Priv2 has these privileges: Login to iDRAC, Configure iDRAC, and Test Alerts. As a result, User1 now has the privilege set: Login to iDRAC, Virtual Media, Clear Logs, Configure iDRAC, and Test Alerts, which is the combined privilege set of Priv1 and Priv2.

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 configuration, 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 Access iDRAC6

Before using Active Directory to access iDRAC6, configure the Active Directory software and iDRAC6 by performing the following steps in order:

1. Extend the Active Directory schema (see "Extending the Active Directory Schema" on page 137.)
2. Extend the Active Directory Users and Computers Snap-in (see "Installing the Dell Extension to the Active Directory Users and Computers Snap-In" on page 143).
3. Add iDRAC6 users and their privileges to Active Directory (see "Adding iDRAC6 Users and Privileges to Active Directory" on page 144).
4. Configure iDRAC6 Active Directory properties using either iDRAC6 Web interface or the RACADM (see "Configuring Microsoft Active Directory With Extended Schema Using iDRAC6 Web Interface" on page 146 or "Configuring Active Directory With Extended Schema Using RACADM" on page 149).

### Extending the Active Directory Schema

**Important:** The schema extension for this product is different from the previous generations of Dell Remote Management products. You must extend the new schema and install the new **Active Directory Users and Computers Microsoft Management Console (MMC) Snap-in** on your directory. The old schema does not work with this product.

**NOTE:** Extending the new schema or installing the new extension to Active Directory User and Computer Snap-in has no impact on previous versions of the product.

The schema extender and Active Directory Users and Computers MMC Snap-in extension are available on the *Dell Systems Management Tools and Documentation* DVD. For information on installing, see "Installing the Dell Extension to the Active Directory Users and Computers Snap-In" on page 143. For further details on extending the schema for iDRAC6 and installing the Active Directory Users and Computers MMC Snap-in, see the *Dell OpenManage Installation and Security User's Guide* available on **support.dell.com/manuals**.

**NOTE:** When you create iDRAC6 Association Objects or iDRAC6 Device Objects, select **Dell Remote Management Object Advanced**.

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, ensure that you have Schema Admin privileges on the Schema Master Flexible Single Master Operation (FSMO) Role Owner of the domain forest.

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 will not be 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:

- *DVD drive*:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- <*DVD drive*>:\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. To use the Dell Schema Extender to extend the Active Directory Schema, see "Using the Dell Schema Extender" on page 138.

You can copy and run the Schema Extender or LDIF files from any location.

### Using the Dell Schema Extender

**CAUTION: The Dell Schema Extender uses the SchemaExtenderOem.ini file. To ensure 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 following exist:

   - Classes (see Table 6-2 through Table 6-7)
   - Attributes (Table 6-8)

   See your Microsoft documentation for details about using the MMC and the Active Directory Schema Snap-in.

**Table 6-2. 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 6-3. dellRacDevice Class**

| OID | 1.2.840.113556.1.8000.1280.1.7.1.1 |
|---|---|
| Description | Represents the Dell iDRAC6 device. iDRAC6 must be configured as delliDRACDevice in Active Directory. This configuration enables iDRAC6 to send Lightweight Directory Access Protocol (LDAP) queries to Active Directory. |
| Class Type | Structural Class |
| SuperClasses | dellProduct |
| Attributes | **dellSchemaVersion**<br>**dellRacType** |

**Table 6-4. 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**<br>**dellPrivilegeMember** |

**Table 6-5. dellRAC4Privileges Class**

| OID | 1.2.840.113556.1.8000.1280.1.1.1.3 |
|---|---|
| Description | Defines the privileges (Authorization Rights) for iDRAC6 |
| Class Type | Auxiliary Class |
| SuperClasses | None |

**Table 6-5. dellRAC4Privileges Class *(continued)***

| OID | 1.2.840.113556.1.8000.1280.1.1.1.3 |
|---|---|
| Attributes | **dellIsLoginUser** |
| | **dellIsCardConfigAdmin** |
| | **dellIsUserConfigAdmin** |
| | **dellIsLogClearAdmin** |
| | **dellIsServerResetUser** |
| | **dellIsConsoleRedirectUser** |
| | **dellIsVirtualMediaUser** |
| | **dellIsTestAlertUser** |
| | **dellIsDebugCommandAdmin** |

**Table 6-6. 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 6-7. 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 6-8. List of Attributes Added to the Active Directory Schema**

| Attribute Name/Description | Assigned OID/Syntax Object Identifier | Single Valued |
|---|---|---|
| **dellPrivilegeMember**<br>List of dellPrivilege Objects that belong to this Attribute. | 1.2.840.113556.1.8000.1280.1.1.2.1<br>Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| **dellProductMembers**<br>List of dellRacDevice and DelliDRACDevice Objects that belong to this role. This attribute is the forward link to the dellAssociationMembers backward link.<br>Link ID: 12070 | 1.2.840.113556.1.8000.1280.1.1.2.2<br>Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| **dellIsLoginUser**<br>TRUE if the user has Login rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.3<br>Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsCardConfigAdmin**<br>TRUE if the user has Card Configuration rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.4<br>Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsUserConfigAdmin**<br>TRUE if the user has User Configuration rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.5<br>Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **delIsLogClearAdmin**<br>TRUE if the user has Log Clearing rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.6<br>Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsServerResetUser**<br>TRUE if the user has Server Reset rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.7<br>Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsConsoleRedirectUser**<br>TRUE if the user has Virtual Console rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.8<br>Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |

**Table 6-8. List of Attributes Added to the Active Directory Schema *(continued)***

| Attribute Name/Description | Assigned OID/Syntax Object Identifier | Single Valued |
|---|---|---|
| **dellIsVirtualMediaUser**<br>TRUE if the user has Virtual Media rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.9<br>Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsTestAlertUser**<br>TRUE if the user has Test Alert User rights on the device. | 1.2.840.113556.1.8000.1280.1.1.2.10<br>Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsDebugCommandAdmin**<br>TRUE if the user has Debug Command Admin rights on the vdevice. | 1.2.840.113556.1.8000.1280.1.1.2.11<br>Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellSchemaVersion**<br>The Current Schema Version is used to update the schema. | 1.2.840.113556.1.8000.1280.1.1.2.12<br>Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| **dellRacType**<br>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<br>Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| **dellAssociationMembers**<br>List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers linked attribute.<br>Link ID: 12071 | 1.2.840.113556.1.8000.1280.1.1.2.14<br>Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |

## Installing the 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 iDRAC6 devices, Users and User Groups, iDRAC6 Associations, and iDRAC6 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:

**<DVD drive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64**

For more information about the Active Directory Users and Computers Snap-in, see your Microsoft documentation.

### Installing the Administrator Pack

You must install the Administrator Pack on each system that is managing the Active Directory iDRAC6 Objects. If you do not install the Administrator Pack, you cannot view the Dell iDRAC6 Object in the container.

See "Opening the Active Directory Users and Computers Snap-In" on page 143 for more information.

### Opening the Active Directory Users and Computers Snap-In

To open the Active Directory Users and Computers Snap-in:

1. If you are logged in to the domain controller, click **Start Admin Tools→ Active Directory Users and Computers**.

   If you are not logged in to the domain controller, you must have the appropriate Microsoft Administrator Pack installed on your local system. To install this Administrator Pack, click **Start→ Run**, enter `MMC`, and press **Enter**.

   The MMC is displayed.

2. In the **Console 1** window, click **File** (or **Console** on systems running Windows 2000).

3 Click **Add/Remove Snap-in**.

4 Select the **Active Directory Users and Computers Snap-in** and click **Add**.

5 Click **Close** and click **OK**.

## Adding iDRAC6 Users and Privileges to Active Directory

Using the Dell-extended Active Directory Users and Computers Snap-in, you can add iDRAC6 users and privileges by creating iDRAC6, Association, and Privilege objects. To add each object type, perform the following procedures:

- Create an iDRAC6 device Object
- Create a Privilege Object
- Create an Association Object
- Add objects to an Association Object

### Creating an iDRAC6 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 iDRAC6 name that you will enter in Step A of "Configuring Microsoft Active Directory With Extended Schema Using iDRAC6 Web Interface" on page 146.

4 Select **iDRAC Device Object**.

5 Click **OK**.

### Creating a Privilege Object

**NOTE:** A Privilege Object must be created 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**.

5 Click **OK**.

6 Right-click the privilege object that you created, and select **Properties**.

7 Click the **Remote Management Privileges** tab and select the privileges that you want the user or group to have (see Table 5-13).

#### Creating an Association Object

**NOTE:** iDRAC6 Association Object is derived from 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 opens the **New Object** window.

3 Enter a name for the new object.

4 Select **Association Object**.

5 Select the scope for the **Association Object**.

6 Click **OK**.

7 Provide access privileges to the authenticated users for accessing the created association objects. To do this:

a Go to **Administrative Tools→ ADSI Edit**. The **ADSI Edit** window is displayed.

b In the right-pane, navigate to the created association object, right-click and select **Properties**.

c In the **Security** tab, click **Add**.

d Type `Authenticated Users`, click **Check Names**, and click **OK**. The **Authenticated Users** is added to the list of **Groups and user names**.

e Click **OK**.

#### Adding Objects to an Association Object

Using the **Association Object Properties** window, you can associate users or user groups, privilege objects, and iDRAC6 devices or iDRAC6 device groups.

You can add groups of Users and iDRAC6 devices. The procedure for creating Dell-related groups and non-Dell-related groups is identical.

#### Adding 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

1. Select the **Privileges Object** tab and click **Add**.
2. Enter the Privilege Object name and click **OK**.

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 iDRAC6 device. Only one privilege object can be added to an Association Object.

#### Adding iDRAC6 Devices or iDRAC6 Device Groups

To add iDRAC6 devices or iDRAC6 device groups:

1. Select the **Products** tab and click **Add**.
2. Enter iDRAC6 devices or iDRAC6 device group name and click **OK**.
3. In the **Properties** window, click **Apply** and click **OK**.

Click the **Products** tab to add one iDRAC6 device connected to the network that is available for the defined users or user groups. You can add multiple iDRAC6 devices to an Association Object.

### Configuring Microsoft Active Directory With Extended Schema Using iDRAC6 Web Interface

1. Open a supported Web browser window.
2. Log in to iDRAC6 Web interface.
3. In the system tree, select **System→ iDRAC Settings→ Network/Security** tab**→ Directory Service→ Microsoft Active Directory**.

   The **Active Directory** summary screen is displayed.
4. Scroll to the bottom of the screen and click **Configure Active Directory**.

   The **Step 1 of 4 Active Directory** screen is displayed.
5. To validate the SSL certificate of your Active Directory servers, select the **Certificate Validation Enabled** check box under **Certificate Settings**.

If you do not want to validate the SSL certificate of your Active Directory servers, skip to step 7.

6 Under **Upload Active Directory CA Certificate**, enter the file path of the certificate or browse to find the certificate file, and then click **Upload**.

**NOTE:** You must enter the absolute file path which includes the full path, complete file name, and file extension.

The certificate information for the Active Directory CA certificate that you uploaded is displayed in the **Current Active Directory CA Certificate** section.

7 Click **Next**.

The **Step 2 of 4 Active Directory Configuration and Management** screen is displayed.

8 Select the **Active Directory Enabled** check box.

**NOTE:** In this release, the Smart Card based Two Factor Authentication (TFA) feature is not supported if the Active directory is configured for Extended schema. The Single Sign-On (SSO) feature is supported for both Standard and Extended schema.

9 Click **Add** to enter the **User Domain Name**. Enter the domain name in the text field, and then click **OK**. Note that this step is optional. If you configure a list of user domains, the list will be available in the Web interface login screen. You can choose from the list, and then you only need to enter the user name.

10 In the **Timeout** field, enter the number of seconds you want iDRAC6 to wait for Active Directory responses.

11 Select the **Look Up Domain Controllers with DNS** option to obtain the Active Directory domain controllers from a DNS lookup. If already configured, the **Domain Controller Server Addresses 1-3** are ignored. Select **User Domain from Login** to perform the DNS lookup with the domain name of the login user. Otherwise, select **Specify a Domain** and enter the domain name to use for the DNS lookup. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS look up) one by one until it makes a successful connection. If **Extended Schema** is selected, the domain controllers are where iDRAC6 device object and the Association objects are located.

If **Standard Schema** is selected, the domain controllers are where the user accounts and the role groups are located.

**NOTE:** iDRAC6 does not failover to the specified domain controllers when DNS lookup fails, or none of the servers returned by the DNS lookup works.

12 Select the **Specify Domain Controller Addresses** option to allow iDRAC6 to use the Active Directory Domain Controller server addresses that are specified. DNS lookup is not performed. Specify the IP address or the FQDN of the domain controllers. When the **Specify Domain Controller Addresses** option is selected, at least one of the three addresses is required to be configured. iDRAC6 attempts to connect to each of the configured addresses one by one until it makes a successful connection. If **Extended Schema** is selected, these are the addresses of the domain controllers where iDRAC6 device object and the Association objects are located.

**NOTE:** 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.

13 Click **Next**.

The **Step 3 of 4 Active Directory Configuration and Management** screen is displayed.

14 Under **Schema Selection**, select the **Extended Schema Selection** check box.

15 Click **Next**.

The **Step 4 of 4 Active Directory** screen is displayed.

16 Under **Extended Schema Settings**, enter **iDRAC6 Name** and **iDRAC6 Domain Name** to configure iDRAC6 device object and its location in Active Directory.

17 Click **Finish** to save your changes, and then **Done**.

The main **Active Directory Configuration and Management** summary page is displayed. Next, test the Active Directory settings you just configured.

18 Scroll to the bottom of the screen and click **Test Settings**.

The **Test Active Directory Settings** screen is displayed.

19 Enter your iDRAC6 user name and password, and then click **Start Test**.

The test results and the test log displays. For additional information, see "Testing Your Configurations" on page 161.

**NOTE:** You must have a DNS server configured properly on iDRAC6 to support Active Directory log in. Navigate to the **Network** screen (click **System→ iDRAC Settings→ Network/Security→ Network**) to configure DNS server(s) manually or use DHCP to get DNS server(s).

You have completed the Active Directory configuration with Extended Schema.

### Configuring Active Directory With Extended Schema Using RACADM

Use the following commands to configure iDRAC6 Active Directory feature with Extended Schema using the RACADM command line interface (CLI) tool instead of the Web interface.

1 Open a command prompt and enter the following RACADM commands:

```
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>
```

**NOTE:** You must configure at least one of the three addresses. iDRAC6 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 iDRAC6 device is located. Global catalog servers are not used in extended schema mode at all.

If you want to disable the certificate validation during SSL handshake, enter the following RACADM command:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

In this case, you do not have to upload a CA certificate.

If you want to enforce the certificate validation during SSL handshake, enter the following RACADM command:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 1
```

In this case, you must upload a CA certificate using the following RACADM command:

```
racadm sslcertupload -t 0x2 -f <ADS root CA
certificate>
```

Using the following RACADM command may be optional. See "Importing iDRAC6 Firmware SSL Certificate" on page 131 for additional information.

```
racadm sslcertdownload -t 0x1 -f <RAC SSL
certificate>
```

2 If DHCP is enabled on iDRAC6 and you want to use the DNS provided by the DHCP server, enter the following RACADM command:

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 1
```

3 If DHCP is disabled in iDRAC6 or you want to manually input your DNS IP address, enter the following RACADM commands:

```
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>
```

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 iDRAC6 Web interface, enter the following command:

```
racadm config -g cfgUserDomain -o
cfgUserDomainName <fully qualified domain name or
IP Address of the domain controller> -i <index>
```

You can configure up to 40 user domains with index numbers between 1 and 40.

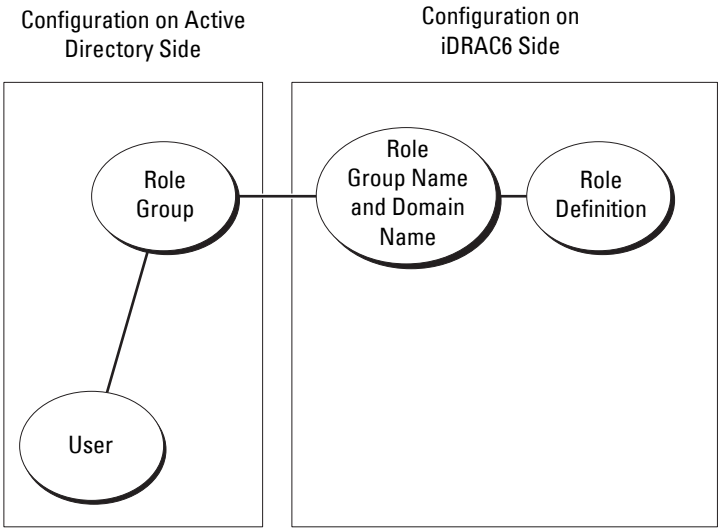
See "Using iDRAC6 With Microsoft Active Directory" on page 127 for details about user domains.

5 Press **Enter** to complete the Active Directory configuration with Extended Schema.

## Standard Schema Active Directory Overview

As shown in Figure 6-3, using standard schema for Active Directory integration requires configuration on both Active Directory and iDRAC6.

**Figure 6-3. Configuration of iDRAC6 with Microsoft Active Directory and Standard Schema**




On the Active Directory side, a standard group object is used as a role group. A user who has iDRAC6 access will be a member of the role group. To give this user access to a specific iDRAC6 card, the role group name and its domain name need to be configured on the specific iDRAC6 card. Unlike the extended schema solution, the role and the privilege level is defined on each iDRAC6 card, not in the Active Directory. Up to five role groups can be configured and defined in each iDRAC6. Table 6-9 shows the default role group privileges.

**Table 6-9. 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 of the login users and role groups, as well as the nested groups, are in the same domain, then only the domain controllers' addresses must be configured on iDRAC6. In this single domain scenario, any group type is supported.

If all of the login users and role groups, or any of the nested groups, are from multiple domains, then Global Catalog server addresses are required to be configured on iDRAC6. In this multiple domain scenario, all of the role groups and nested groups, if any, must be Universal Group type.

# Configuring Standard Schema Active Directory to Access iDRAC6

You must perform the following steps to configure Active Directory before an Active Directory user can access iDRAC6:

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 iDRAC6.
3. Configure the name of the group and the domain name on iDRAC6 by using either the Web interface or RACADM (see "Configuring Active Directory With Standard Schema Using iDRAC6 Web Interface" on page 154 or "Configuring Active Directory With Standard Schema Using RACADM" on page 158).

## Configuring Active Directory With Standard Schema Using iDRAC6 Web Interface

1. Open a supported Web browser window.
2. Log in to iDRAC6 Web interface.
3. In the system tree, select **System→ iDRAC Settings→ Network/Security** tab**→ Directory Service→ Microsoft Active Directory**.

   The **Active Directory** summary page is displayed.
4. Scroll to the bottom of the screen and click **Configure Active Directory**.

   The **Step 1 of 4 Active Directory** screen is displayed.
5. Under **Certificate Settings**, select **Certificate Validation Enabled**.
6. Under **Upload Active Directory CA Certificate**, enter the file path of the certificate or browse to find the certificate file, and then click **Upload**.

   **NOTE:** You must enter the absolute file path, which includes the full path and the complete file name and file extension.

   The certificate information for the Active Directory CA certificate that you uploaded is displayed in the **Current Active Directory CA Certificate** section.

7 Click **Next**.

The **Step 2 of 4 Active Directory Configuration and Management** screen is displayed.

8 Select the **Active Directory Enabled** check box.

9 Select **Enable smart card Login** to enable Smart–Card login. You are prompted for a Smart–Card logon during any subsequent logon attempts using the GUI. This is optional.

10 Select **Enable Single Sign-on** if you want to log into iDRAC6 without entering your domain user authentication credentials, such as user name and password.

11 Click **Add** to enter the **User Domain Name**. Enter the domain name in the text field, and then click **OK**. Note that this step is optional. If you configure a list of user domains, the list will be available in the Web interface login screen. You can choose from the list, and then you only need to enter the user name.

12 In the **Timeout** field, enter the number of seconds you want iDRAC6 to wait for Active Directory responses.

13 Select the **Look Up Domain Controllers with DNS** option to obtain the Active Directory domain controllers from a DNS lookup. If already configured, the **Domain Controller Server Addresses 1-3** are ignored. Select **User Domain from Login** to perform the DNS lookup with the domain name of the login user. Otherwise, select **Specify a Domain** and enter the domain name to use for the DNS lookup. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS look up) one by one until it makes a successful connection. If **Standard Schema** is selected, the domain controllers are where the user accounts and the role groups are located.

14 Select the **Specify Domain Controller Addresses** option to allow iDRAC6 to use the Active Directory Domain Controller server addresses that are specified. DNS lookup is not performed. Specify the IP address or the FQDN of the domain controllers. When the **Specify Domain Controller Addresses** option is selected, at least one of the three addresses is required to be configured. iDRAC6 attempts to connect to each of the configured addresses one by one until it makes a successful connection.

If **Standard Schema** is selected, these are the addresses of the domain controllers where the user accounts and the role groups are located.

**NOTE:** iDRAC6 does not failover to the specified domain controllers when DNS lookup fails, or none of the servers returned by the DNS lookup works.

**15** Click **Next**.

The **Step 3 of 4 Active Directory Configuration and Management** screen is displayed.

**16** Under **Schema Selection**, select the **Standard Schema Selection** check box.

**17** Click **Next**.

The **Step 4a of 4 Active Directory** screen is displayed.

**18** Under **Standard Schema Settings**, select the **Look Up Global Catalog Servers with DNS** option and enter the **Root Domain Name** to use on a DNS lookup to obtain the Active Directory Global Catalog Servers. If already configured, the Global Catalog Server Addresses 1-3 are ignored. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS lookup) one by one until it makes a successful connection. A Global Catalog server is required only for Standard Schema in the case that the user accounts and the role groups are in different domains.

**NOTE:** iDRAC6 does not failover to the specified Global Catalog servers when DNS lookup fails, or none of the servers returned by the DNS lookup work.

**19** Select the **Specify Global Catalog Server Addresses** option and enter the IP address or the Fully Qualified Domain Name (FQDN) of the Global Catalog server(s). DNS lookup is not performed. At least one of the three addresses is required to be configured. iDRAC6 attempts to connect to each of the configured addresses one by one until it makes a successful connection.

**NOTE:** The Global Catalog server is required only for Standard Schema when the user accounts and role groups are in different domains. And, in this multiple domain case, only the Universal Group can be used. If you use iDRAC6 Web GUI to configure Active Directory, you need to enter a Global Address even though the user and group are in the same domain.

**20** Click a **Role Group** button to add a role group.

The **Step 4b of 4 Configure Role Group** screen is displayed.

21 Enter the **Group Name**. The group name identifies the role group in the Active Directory associated with iDRAC6.

22 Enter the **Group Domain**. The **Group Domain** is the fully qualified root domain name for the forest.

23 In the **Role Group Privileges** section, set the group privileges. See Table 5-13 for information on role group privileges.

**NOTE:** If you modify any of the permissions, the existing role group privilege (Administrator, Power User, or Guest User) will change to either the Custom Group or the appropriate role group privilege based on the permissions you modified.

24 Click **OK** to save the role group settings.

An alert dialog is displayed, indicating that your settings are changed. Click **OK** to return to the **Step 4a of 4 Active Directory Configuration and Management** screen.

25 To add an additional role group, repeat step 20 through step 24.

26 Click **Finish**, and the click **Done**.

The main **Active Directory Configuration and Management** summary screen is displayed. Test the Active Directory settings you just configured.

27 Scroll to the bottom of the screen and click **Test Settings**.

The **Test Active Directory Settings** screen is displayed.

28 Enter your iDRAC6 user name and password, and then click **Start Test**.

The test results and the test log displays. For additional information, see "Testing Your Configurations" on page 161.

**NOTE:** You must have a DNS server configured properly on iDRAC6 to support Active Directory log in. Navigate to the **Network** screen (click **System→ iDRAC Settings**, and then click the **Network/Security→ Network** tab) to configure DNS server(s) manually or use DHCP to get DNS server(s).

You have completed the Active Directory configuration with Standard Schema.

### Configuring Active Directory With Standard Schema Using RACADM

Use the following commands to configure iDRAC6 Active Directory Feature with Standard Schema using the RACADM CLI instead of the Web-based interface.

1 Open a command prompt and enter the following RACADM commands:

```
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>
```

**NOTE:** For Bit Mask values for specific Role Group permissions, see Table 6-9.

```
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>
```

**NOTE:** Enter the FQDN of the domain controller, *not* the FQDN of the domain. For example, enter `servername.dell.com` instead of `dell.com`.

**NOTE:** At least one of the 3 addresses is required to be configured. iDRAC6 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.

```
racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog1 <fully qualified domain name or IP
address of the domain controller>
```

```
racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog2 <fully qualified domain name or IP
address of the domain controller>
```

```
racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog3 <fully qualified domain name or IP
address of the domain controller>
```

**NOTE:** The Global Catalog server is only required for standard schema when the user accounts and role groups are in different domains. And, in this multiple domain case, only the Universal Group can be used.

**NOTE:** 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:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

In this case, no Certificate Authority (CA) certificate needs to be uploaded.

If you want to enforce the certificate validation during SSL handshake, enter the following RACADM command:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 1
```

In this case, you must also upload the CA certificate using the following RACADM command:

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

Using the following RACADM command may be optional. See "Importing iDRAC6 Firmware SSL Certificate" on page 131 for additional information.

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```

2 If DHCP is enabled on iDRAC6 and you want to use the DNS provided by the DHCP server, enter the following RACADM commands:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3 If DHCP is disabled on iDRAC6 or you want manually to input your DNS IP address, enter the following RACADM commands:

```
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>
```

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:

```
racadm config -g cfgUserDomain -o cfgUserDomainName <fully qualified domain name or IP Address of the domain controller> -i <index>
```

Up to 40 user domains can be configured with index numbers between 1 and 40.

See "Using iDRAC6 With Microsoft Active Directory" on page 127 for details about user domains.

# Testing Your Configurations

If you want to verify whether your configuration works, or if you need to diagnose the problem with your failed Active Directory log in, you can test your settings from iDRAC6 Web interface.

After you finish configuring settings in iDRAC6 Web interface, click **Test Settings** at the bottom of the screen. You will be required to enter a test user's name (for example, **username@domain.com**) and password to run the test. Depending on your configuration, it may take some time for all of the test steps to complete and display the results of each step. A detailed test log will display at the bottom of the results screen.

If there is a failure in any step, examine the details in the test log to identify the problem and a possible solution. For most common errors, see "Frequently Asked Questions" on page 165.

If you need to make changes to your settings, click the **Active Directory** tab and change the configuration step-by-step.

# Using iDRAC6 with LDAP Directory Service

iDRAC6 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 iDRAC6 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 iDRAC6.

### Login Syntax (Directory User versus Local User)

Unlike Active Directory, special characters ("@", "\", and "/") are not used to differentiate an LDAP user from a local user. The login user must enter the user name, excluding the domain name. iDRAC6 takes the user name as is and does not break it down to the user name and user domain.

When generic LDAP is enabled, iDRAC6 first tries to login the user as a directory user. If it fails, local user lookup is enabled.

**NOTE:** There is no behavior change on the Active Directory login syntax. When generic LDAP is enabled, the GUI login page displays only **This iDRAC** in the drop-down menu.

**NOTE:** In this release, only openLDAP, openDS, Novell eDir and Fedora based directory services are supported. "<" and ">" characters are not allowed in the user name.

### Configuring Generic LDAP Directory Service Using iDRAC6 Web-Based Interface

1. Open a supported Web browser window.
2. Log in to iDRAC6 Web-based interface.
3. Click **System→ iDRAC Settings→ Network/Security** tab**→ Directory Service→ Generic LDAP Directory Service**.
4. The **Generic LDAP Configuration and Management** page displays the current iDRAC6 generic LDAP settings. Scroll to the bottom of the **Generic LDAP Configuration and Management** page, and click **Configure Generic LDAP**.

   The **Step 1 of 3 Generic LDAP Configuration and Management** page is displayed. Use this page to configure the digital certificate used during initiation of SSL connections when communicating with a generic LDAP server. These communications use LDAP over SSL (LDAPS). If you enable certificate validation, upload the certificate of the Certificate Authority (CA) that issued the certificate used by the LDAP server during initiation of SSL connections. The CA's certificate is used to validate the authenticity of the certificate provided by the LDAP server during SSL initiation.

   **NOTE:** In this release, non-SSL port based LDAP bind is not supported. Only LDAP over SSL is supported.
5. Under **Certificate Settings**, check **Enable Certificate Validation** to enable certificate validation. If enabled, iDRAC6 uses the CA certificate to validate the LDAP server certificate during Secure Socket Layer (SSL) handshake; if disabled, iDRAC6 skips the certificate validation step of the

SSL handshake. You can disable certificate validation during testing or if your system administrator chooses to trust the domain controllers in the security boundary without validating their SSL certificates.

**CAUTION: Ensure that CN = open LDAP FQDN is set (for example, CN= openldap.lab) in the subject field of the LDAP server certificate during certificate generation. The CN field in the server certificate should be set to match the LDAP server address field in iDRAC6 for certificate validation to work.**

6 Under **Upload Directory Service CA Certificate**, type the file path of the certificate or browse to find the certificate file.

**NOTE:** You must type the absolute file path, which includes the full path and the complete file name and file extension.

7 Click **Upload**.

The certificate of the root CA that signs all the domain controllers' Security Socket Layer (SSL) server certificates will be uploaded.

8 Click **Next** to go to the **Step 2 of 3 Generic LDAP Configuration and Management** page. Use this page to configure location information about generic LDAP servers and user accounts.

**NOTE:** In this release, the Smart Card based Two Factor Authentication (TFA) and the single sign-on (SSO) features are not supported for Generic LDAP Directory Service.

9 Select **Enable Generic LDAP**.

**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.

10 Select the **Use Distinguished Name to Search Group Membership** option to use the Distinguished Name (DN) as group members. iDRAC6 compares the User DN retrieved from the directory to compare with the members of the group. If unchecked, user name provided by the login user is used to compare with the members of the group.

11 In the **LDAP Server Address** field, enter the FQDN or the IP address of the LDAP server. To specify multiple redundant LDAP servers that serve the same domain, provide the list of all servers separated by commas. iDRAC6 tries to connect to each server in turn, until it makes a successful connection.

12 Enter the port used for LDAP over SSL in the **LDAP Server Port** field. The default is 636.

13 In the **Bind DN** field, enter the DN of a user used to bind to the server when searching for the login user's DN. If not specified, an anonymous bind is used.

14 Enter the **Bind Password** to use in conjunction with the **Bind DN**. This is required if anonymous bind is not allowed.

15 In the **Base DN to Search** field, enter the DN of the branch of the directory where all searches should start.

16 In the **Attribute of User Login** field, enter the user attribute to search for. Default is UID. It is recommended that this be unique within the chosen Base DN, else a search filter must be configured to ensure the uniqueness of the login user. If the user DN cannot be uniquely identified by the search combination of attribute and search filter, the login will fail.

17 In the **Attribute of Group Membership** field, specify which LDAP attribute should be used to check for group membership. This should be an attribute of the group class. If not specified, iDRAC6 uses the *member* and *uniquemember* attributes.

18 In the **Search Filter** field, enter a valid LDAP search filter. Use the filter if the user attribute cannot uniquely identify the login user within the chosen Base DN. If not specified, the value defaults to *objectClass=**, which searches for all objects in the tree. This additional search filter configured by the user applies only to userDN search and not the group membership search.

19 Click **Next** to go to the **Step 3a of 3 Generic LDAP Configuration and Management** page. Use this page to configure the privilege groups used to authorize users. When generic LDAP is enabled, Role Group(s) are used to specify authorization policy for iDRAC6 users.

20 Under **Role Groups**, click a **Role Group**.

The **Step 3b of 3 Generic LDAP Configuration and Management** page is displayed. Use this page to configure each Role Group used to control authorization policy for users.

21 Enter the **Group Distinguished Name (DN)** that identifies the role group in the generic LDAP Directory Service associated with iDRAC6.

22 In the **Role Group Privileges** section, specify the privileges associated with the group by selecting the **Role Group Privilege Level**. For example, if you select **Administrator**, all of the privileges are selected for that level of permission.

23 Click **Apply** to save Role Group settings.

iDRAC6 Web server automatically returns you to the **Step 3a of 3 Generic LDAP Configuration and Management** page where your Role Group settings are displayed.

24 Configure additional Role Groups if required.

25 Click **Finish** to return to the **Generic LDAP Configuration and Management** summary page.

26 Click **Test Settings** to check the generic LDAP settings.

27 Enter the user name and password of a directory user that is chosen to test the LDAP settings. The format depends on what *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, iDRAC6 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 iDRAC6 is not able to communicate with the LDAP server.

The test results and the test log are displayed. You have completed the **Generic LDAP Directory Service** configuration.

# Frequently Asked Questions

## Active Directory Log In Issues

### It takes nearly 4 minutes to log into iDRAC6 using Active Directory Single Sign–On.

The normal Active Directory Single Sign–On login usually takes less than 10 seconds but it may take nearly 4 minutes to log into iDRAC6 using Active Directory Single Sign–On if you have specified the **Preferred DNS Server** and the **Alternate DNS Server** in iDRAC6 **Network** page, and the preferred DNS server has failed. DNS timeouts are expected when a DNS server is down. iDRAC6 logs you in using the alternate DNS server.

**I have configured Active Directory for a domain present in Windows Server 2008 Active Directory and have made these configurations. 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. Now if I try to log in to iDRAC6 using the User present in the child domain, Active Directory Single Sign-On login fails.**

This may be because of the wrong 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 e–mail distribution lists.

Always ensure that the Group Type is **Security**. You cannot use distribution groups to assign permission on any objects and use them to filter Group Policy settings.

**My Active Directory log in failed. What do I do?**

iDRAC6 provides a diagnostic tool in the Web interface.

1. Log in as a local user with administrator privilege from the Web interface.
2. In the system tree, select **System**→ **iDRAC Settings**→ **Network/Security** tab→ **Directory Service**→ **Microsoft Active Directory**.

   The **Active Directory** summary screen is displayed.
3. Scroll to the bottom of the screen and click **Test Settings**.

   The **Test Active Directory Settings** screen is displayed.
4. Enter a test user name and password, and then click **Start Test**.

   iDRAC6 runs the tests step-by-step and displays the result for each step. iDRAC6 also logs a detailed test result to help you resolve any problems.

   If problems persist, configure your Active Directory settings, change your user configuration, and run the test again until the test user passes the authorization step.

**I enabled certificate validation but my Active Directory log in failed. I ran the diagnostics from the GUI and the test results show the following error message. What could the problem be and how do I fix it?**

```
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, iDRAC6 uses the uploaded CA certificate to verify the directory server certificate when iDRAC6 establishes the SSL connection with the directory server. The most common reasons for failing certification validation are:

- iDRAC6 date is not within the valid period of the server certificate or CA certificate. Check iDRAC6 time and the valid period of your certificate.
- The Domain Controller Addresses configured in iDRAC6 do not match the Subject or Subject Alternative Name of the directory server certificate.
  - If you are using an IP address, see "I am using an IP address for a Domain Controller Address, and I failed certificate validation. What is the problem?" on page 168.
  - If you are using FQDN, ensure you are using the FQDN of the domain controller, and not the domain itself. For example, use `servername.example.com` and *not* `example.com`.

**What should I check if I cannot log in to iDRAC6 using Active Directory?**

First, diagnose the problem using the Test Settings feature. For directions, see "My Active Directory log in failed. What do I do?" on page 166.

Then, fix the specific problem indicated by the test results. For additional information, see "Testing Your Configurations" on page 161.

Most common issues are explained in this section. However, in general, you should check the following:

1. Ensure that you use the correct user domain name during a log in and not the NetBIOS name.
2. If you have a local iDRAC6 user account, log in to iDRAC6 using your local credentials.
   a. Ensure that the **Active Directory Enabled** check box is selected in the **Step 2 of 4 Active Directory Configuration and Management** page.
   b. If you have enabled certificate validation, ensure that you have uploaded the correct Active Directory root CA certificate to iDRAC6. The certificate is displayed in the **Current Active Directory CA Certificate** area. Ensure that iDRAC6 time is within the valid period of the CA certificate.
   c. If you are using the Extended Schema, ensure that **iDRAC6 Name** and **iDRAC6 Domain Name** match your Active Directory environment configuration.

      If you are using the Standard Schema, ensure that the **Group Name** and **Group Domain** match your Active Directory configuration.
   d. Navigate to the **Network** screen. Select **System→ iDRAC Settings→ Network/Security→ Network**.
      Ensure that the DNS settings are correct.
   e. Check the Domain Controller SSL certificates to ensure that iDRAC6 time is within the valid period of the certificate.

## Active Directory Certificate Validation

#### I am using an IP address for a Domain Controller Address, and I failed certificate validation. What is the problem?

Check the Subject or Subject Alternative Name field of your domain controller certificate. Usually Active Directory uses the hostname, not the IP address, of the domain controller in the Subject or Subject Alternative Name field of the domain controller certificate.

You can fix the problem by taking any of the following actions:

- Configure the hostname (FQDN) of the domain controller as the *domain controller address(es)* on iDRAC6 to match the Subject or Subject Alternative Name of the server certificate.
- Re-issue the server certificate to use an IP address in the Subject or Subject Alternative Name field so it matches the IP address configured in iDRAC6.
- Disable certificate validation if you choose to trust this domain controller without certificate validation during the SSL handshake.

#### Why does iDRAC6 enable certificate validation by default?

iDRAC6 enforces strong security to ensure the identity of the domain controller that iDRAC6 connects to. Without certificate validation, a hacker could 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 GUI or the CLI.

## Extended and Standard Schema

#### I'm using extended schema in a multiple domain environment. How do I configure the domain controller address(es)?

Use the host name (FQDN) or the IP address of the domain controller(s) that serves the domain in which iDRAC6 object resides.

#### Do I need to configure Global Catalog Address(es)?

If you are using extended schema, you cannot configure global catalog addresses, because they are not used with extended schema.

If you are using standard schema, and users and role groups are from different domains, you must configure global catalog address(es). In this case, you can use only Universal Group.

If you are using standard schema, and all the users and all the role groups are in the same domain, you are not required to configure global catalog address(es).

#### How does standard schema query work?

iDRAC6 connects to the configured domain controller address(es) first. If the user and role groups reside in that domain, the privileges are saved.

If global controller address(es) is configured, iDRAC6 continues to query the Global Catalog. If additional privileges are retrieved from the Global Catalog, these privileges are accumulated.

### Miscellaneous

#### Does iDRAC6 always use LDAP over SSL?

Yes. All the transportation is over secure port 636 and/or 3269.

During *test settings*, iDRAC6 does a LDAP CONNECT only to help isolate the problem, but it does not do an LDAP BIND on an insecure connection.

#### Does iDRAC6 support the NetBIOS name?

Not in this release.

# 7

# Configuring iDRAC6 for Single Sign-On and Smart Card Login

This section provides information to configure iDRAC6 for Smart Card login for local users and Active Directory users, and Single Sign-On (SSO) login for Active Directory users.

iDRAC6 supports Kerberos based Active Directory authentication to support Active Directory Smart Card and Single Sign-On (SSO) logins.

## About Kerberos Authentication

Kerberos is a network authentication protocol that allows systems to communicate securely over a non-secure network. It achieves this by allowing the systems to prove their authenticity. To keep with the higher authentication enforcement standards, iDRAC6 now supports Kerberos based Active Directory authentication to support Active Directory Smart Card and single sign-on (SSO) logins.

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008 use Kerberos as their default authentication method.

iDRAC6 uses Kerberos to support two types of authentication mechanisms—Active Directory single sign-on and Active Directory Smart Card logins. For single-sign on login, iDRAC6 uses the user credentials cached in the operating system after the user has logged in using a valid Active Directory account.

For Active Directory smart card login, iDRAC6 uses smart card-based two factor authentication (TFA) as credentials to enable an Active Directory login.

Kerberos authentication on iDRAC6 fails if iDRAC6 time differs from the Domain Controller time. A maximum offset of 5 minutes is allowed. To enable successful authentication, synchronize the server time with the Domain Controller time and then **reset** iDRAC6.

You can also use the following RACADM time zone offset command to synchronize the time:

```
racadm config -g cfgRacTuning -o
cfgRacTuneTimeZoneOffset <offset value>
```

# Prerequisites for Active Directory SSO and Smart Card Authentication

The pre-requisites for both Active Directory SSO and Smart Card authentication are:

- Configure iDRAC6 for Active Directory login. For more information, see "Using iDRAC6 Directory Service" on page 127.
- Register iDRAC6 as a computer in the Active Directory root domain.
  - **a** Click **System→ iDRAC Settings→ Network/Security→ Network** subtab.
  - **b** Provide a valid **Preferred/Alternate DNS Server** IP address. This value is the IP address of the DNS that is part of the root domain, which authenticates the Active Directory accounts of the users.
  - **c** Select **Register iDRAC6 on DNS**.
  - **d** Provide a valid **DNS Domain Name**.
  - **e** Verify that network DNS configuration matches with the Active Directory DNS information.

    See iDRAC6 Online Help for more information.
- To support the two new types of authentication mechanisms, iDRAC6 supports the configuration to enable itself as a kerberized service on a Windows Kerberos network. The Kerberos configuration on iDRAC6 entails the same steps as configuring a non–Windows Server Kerberos service as a security principal in Windows Server Active Directory.

  The Microsoft tool **ktpass** (supplied by 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.

The keytab obtained from the ktpass utility is made available to iDRAC6 as a file upload and is enabled to be a kerberized service on the network.

Since iDRAC6 is a device with a non-Windows operating system, run the **ktpass** utility—part of Microsoft Windows—on the Domain Controller (Active Directory server) where you want to map iDRAC6 to a user account in Active Directory.

For example, use the following **ktpass** command to create the Kerberos keytab file:

```
C:\> ktpass.exe -princ
HTTP/idracname.domainname.com@DOMAINNAME.COM -
mapuser DOMAINNAME\username -mapOp set -crypto
DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass
<password> +DesOnly -out c:\krbkeytab
```

**NOTE:** If you find any issues with iDRAC6 user the keytab file is created for, create a new user and a new keytab file. If the same keytab file which was initially created is again executed, it will not configure correctly.

After the above command executes successfully, run the following command:

```
C:\>setspn -a HTTP/idracname.domainname.com
username
```

The encryption type that iDRAC6 uses for Kerberos authentication is DES-CBC-MD5. The principal type is KRB5_NT_PRINCIPAL. The properties of the user account that the Service Principal Name is mapped to should have Use DES encryption types for this account property enabled.

**NOTE:** You must create an Active Directory user account for use with the -mapuser option of the **ktpass** command. Also, you should have the same name as iDRAC6 DNS name to which you will upload the generated keytab file.

**NOTE:** It is recommended that you use the latest **ktpass** utility to create the keytab file. Also, while generating the keytab file, use *lowercase* letters for the **idracname** and the **Service Principal Name**.

This procedure will produce a keytab file that you should upload to iDRAC6.

**NOTE:** The keytab contains an encryption key and should be kept secure.

For more information on the **ktpass** utility, see the Microsoft website at: **http://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

- iDRAC6 time should be synchronized with the Active Directory domain controller.

### Browser Settings to Enable Active Directory SSO

To configure the browser settings for Internet Explorer:

1. Open Internet Explorer Web browser.
2. Select **Tools→ Internet Options→ Security→ Local Intranet**.
3. Click **Sites**.
4. Select the following options only:
   - Include all local (intranet) sites not listed on other zones.
   - Include all sites that bypass the proxy server.
5. Click **Advanced**.
6. Add all relative domain names that will be used for iDRAC instances that is part of the SSO configuration (for example, myhost.example.com.)
7. Click **Close** and click **OK**.
8. Click **OK**.

To configure the browser settings for Firefox:

1. Open Firefox Web browser.
2. In the address bar, enter `about:config`.
3. In **Filter**, enter `network.negotiate`.
4. Add the iDRAC name to network.negotiate-auth.trusted-uris (using comma separated list.)
5. Add the iDRAC name to network.negotiate-auth.delegation-uris (using comma separated list.)

# Using Active Directory SSO

You can enable iDRAC6 to use Kerberos—a network authentication protocol—to enable single sign-on. For more information on setting up iDRAC6 to use the Active Directory single sign-on feature, see "Prerequisites for Active Directory SSO and Smart Card Authentication" on page 172.

## Configuring iDRAC6 to Use SSO

1. Ensure you have done the following:
   a. Created the device object, privilege object, and association object in the Active Directory server.
   b. Set access privileges to the created privilege object. It is recommended not to provide administrator privileges as this could bypass some security checks.
   c. Associate the device object and privilege object using the association object.
   d. Add the preceding SSO user (login user) to the device object.
   e. Provide access privilege to *Authenticated Users* for accessing the created association object.

      For information about how to perform these steps, see "Adding iDRAC6 Users and Privileges to Active Directory" on page 144.
2. Open a supported Web browser window.
3. Log in to iDRAC6 Web interface.
4. In the system tree, select **System→ iDRAC Settings→ Network/Security** tab→ **Network**. In the **Network** page, verify whether the **DNS iDRAC6 Name** is correct and matches with the name used for iDRAC6 fully qualified domain name.
5. In the system tree, select **System→ iDRAC Settings→ Network/Security** tab→ **Directory Service→ Microsoft Active Directory**.

   The **Active Directory** summary screen is displayed.
6. Scroll to the bottom of the screen and click **Configure Active Directory**.

   The **Active Directory Configuration and Management Step 1 of 4** screen is displayed.

7 To validate the SSL certificate of the Active Directory servers, select the **Enable Certificate Validation** check box under **Certificate Settings**.

If you do not want to validate the SSL certificate of your Active Directory servers, take no action, and skip to step 9.

8 Under **Upload Active Directory CA Certificate**, enter the file path of the certificate or browse to find the certificate file, and then click **Upload**.

**NOTE:** You must enter the absolute file path, which includes the full path and the complete file name and file extension.

The certificate information for the Active Directory CA certificate that you uploaded is displayed in the **Current Active Directory CA Certificate** section.

9 Click **Next**.

The **Active Directory Configuration and Management Step 2 of 4** screen is displayed.

10 Select the **Enable Active Directory** check box.

11 Select **Enable Single Sign-on** if you want to log into iDRAC6 directly after logging into your workstation without entering your domain user authentication credentials, such as user name and password.

To log into iDRAC6 using this feature, you should have already logged into your system using a valid Active Directory user account. Also you should have already configured the user account to log into iDRAC6 using the Active Directory credentials. iDRAC6 uses the cached Active Directory credentials to log you in.

To enable SSO using the CLI, run the RACADM command:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

12 Add **User Domain Name**, and enter the IP address of the Domain Controller Server Address. Select either the **Look Up Domain Controllers with DNS** or **Specify Domain Controller Addresses**. Select **Next**. The **Active Directory Configuration and Management Step 3 of 4** screen is displayed.

13 Select the **Standard Schema** or **Extended Schema** option and click **Next**.

If you have selected **Standard Schema,** go to step 13. If you have selected **Extended Schema**, go to step 14.

14 For standard schema:

a In the **Active Directory Step 4a of 4** screen, enter the IP Address of the **Global Catalog Server** or select the **Look Up Global Catalog Servers with DNS** option and enter the **Root Domain Name** to use for a DNS lookup to obtain the Active Directory Global Catalog Servers.

b Click any of the Role Groups and add the Role Group information that your valid Active Directory user is a member. The **Active Directory Step 4b of 4** screen is displayed.

c Enter the Role Group name, Group Domain, Role Group Privileges level, and the required privileges and click **Finish**. The message "Configuration set successfully" is displayed. Click **OK**. The **Step 4a of 4** screen displays the created Role Group Name, Group Domain, and the Group Privelege level.

d Click **Finish**. The success message is displayed.

15 For extended schema, in the **Active Directory Step 4 of 4** screen, enter the **iDRAC6 Name** and the **iDRAC6 Domain Name** and click **Finish**. The success message is displayed.

### Logging Into iDRAC6 Using SSO

1 Log into your management station using your valid Active Directory network account.

2 Log into iDRAC6 Web page using iDRAC6 fully qualified domain name:

**http://idracname.domain.com.**

iDRAC6 logs you in, using your credentials that were cached in the operating system when you logged in using your valid Active Directory network account.

# Configuring Smart Card Authentication

iDRAC6 supports the two factor authentication (TFA) feature by enabling **Smart Card Logon**.

The traditional authentication schemes use user name and password to authenticate users. This provides minimal security.

TFA, on the other hand, provides a higher-level of security by making the users provide two factors of authentication—what you have and what you know—what you have is the Smart Card, a physical device, and what you know—a secret code like a password or PIN.

The two-factor authentication requires users to verify their identities by providing *both* factors.

# Configuring Smart Card Login in iDRAC6

To enable iDRAC6 Smart Card login feature from the Web interface:

1. Open a supported Web browser window.
2. Log in to iDRAC6 Web interface.
3. Go to the **Step 1 of 4 Active Directory Configuration and Management** screen.
4. To validate the SSL certificate of your Active Directory servers, select the **Certificate Validation Enabled** check box under **Certificate Settings**. If you do not want to validate the SSL certificate of your Active Directory servers, skip to step 6.
5. Under **Upload Active Directory CA Certificate**, enter the file path of the certificate or browse to find the certificate file, and then click **Upload**. You must enter the absolute file path, which includes the full path and the complete file name and file extension. The certificate information for the Active Directory CA certificate that you uploaded is displayed in the **Current Active Directory CA Certificate** section.
6. Click Next. The **Step 2 of 4 Active Directory Configuration and Management** screen is displayed.
7. Select the **Active Directory Enabled** check box.

8. Select **Enable Smart–Card Login** to enable Smart Card login. You are prompted for a Smart Card logon during any subsequent logon attempts using the GUI.
9. Add **User Domain Name**, and enter the IP address of the Domain Controller Server Address. Select **Next**.
10. Select **Standard Schema Settings** on **Step 3 of 4 Active Directory Configuration and Management** page. Select **Next**.
11. On **Step 4a of 4 Active Directory** page, enter the IP Address of the **Global Catalog Server**. Add the Role Group information that your valid Active Directory user is a member of, by selecting one of the Role Groups (**Step 4B of 4 Configure Role Group** page). Enter the **Group Name**, the **Group Domain**, and the **Role Group Privileges**. Select **OK** and then **Finish**. After selecting **Done**, scroll back to the bottom of the **Active Directory** summary page and select **Kerberos Keytab Upload**.
12. Upload a valid Kerberos Keytab file. Ensure that the Active Directory Server and iDRAC6 times are synchronized. Verify that both time and time zones are correct before uploading the keytab file. For more information on creating a keytab file, see "Configuring iDRAC6 for Single Sign-On and Smart Card Login" on page 171.

Clear the **Enable Smart–Card Login** option to disable the TFA Smart Card logon feature. The next time you login to iDRAC6 GUI, you are prompted for a Microsoft Active Directory or local logon username and password, which occurs as the default login prompt from the Web interface.

# Logging Into iDRAC6 Using Active Directory Smart Card Authentication

**NOTE:** Depending on your browser settings, you may be prompted to download and install the Smart Card reader ActiveX plug-in when using this feature for the first time.

1. Log into iDRAC6 using https.

   `https://<IP address>`

   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 iDRAC6 and *port number* is the HTTPS port number.

   iDRAC6 Login page is displayed prompting you to insert the Smart Card.

2. Insert the Smart Card.
3. Enter the PIN and click **Log in**.

   You are logged into iDRAC6 with your credentials as set in Active Directory.

   **NOTE:** You need not keep your Smart Card in the reader to stay logged in.

# Frequently Asked Questions About SSO

**SSO login fails on Windows 7 and Windows Server 2008 R2.**

You must enable the encryption types DES_CBC_CRC and DES_CBC_MD5 for Windows 7 and Windows Server 2008 R2. To enable the encryption types:

1. Log in as administrator or as a user with adminstrative privilege.
2. Go to **Start** and run **gpedit**. 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 and click **OK**.

# Troubleshooting the Smart Card Logon in iDRAC6

Use the following tips to help you debug an inaccessible Smart Card:

#### It takes nearly 4 minutes to log into iDRAC6 using Active Directory Smart Card login.

The normal Active Directory Smart Card login usually takes less than 10 seconds but it may take nearly 4 minutes to log into iDRAC6 using Active Directory Smart Card login if you have specified the **Preferred DNS Server** and the **Alternate DNS Server** in iDRAC6 **Network** page, and the preferred DNS server has failed. DNS timeouts are expected when a DNS server is down. iDRAC6 logs you in using the alternate DNS server.

#### ActiveX plug-in unable to detect the Smart Card reader

Ensure that the Smart Card is supported on the Microsoft Windows operating system. Windows supports a limited number of Smart Card cryptographic service providers (CSPs).

Tip: As a general check to see 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 to see if Windows detects the Smart Card and displays the PIN dialog-box.

#### Incorrect Smart Card PIN

Check to see if the Smart Card has been locked out due to too many attempts with an incorrect PIN. In such cases, the issuer of the Smart Card in the organization will be able to help you get a new Smart Card.

#### Unable to Log into iDRAC6 as an Active Directory User

- If you cannot log into iDRAC6 as an Active Directory user, try to log into iDRAC6 without enabling the Smart Card logon. You can disable the Smart Card logon through RACADM using the following command:

  ```
  racadm config –g cfgSmartCard –o
  cfgSmartCardLogonEnable 0
  ```

- For 64–bit Windows platforms, iDRAC6 authentication plug–in is not installed properly if a 64–bit version of Microsoft Visual C++ 2005 Redistributable Package is deployed. You need to deploy the 32–bit version of Microsoft Visual C++ 2005 Redistributable Package for the plug–in to install and run properly.
- If you receive the following error message "`Not able to load the Smart Card Plug-in. Please check your IE settings or you may have insufficient privileges to use the Smart Card Plug-in`", then install the Microsoft Visual C++ 2005 Redistributable Package. This file is available on the Microsoft Website at **microsoft.com**. Two distributed versions of the C++ Redistributable Package have been tested and they allow the Dell Smart Card plug–in to load:

**Table 7-1. Distributed Versions of the C++ Redistributable Package**

| Redistributable Package File Name | Version | Release Date | Size | Description |
|---|---|---|---|---|
| vcredist_x86.exe | 6.0.2900.2180 | March 21, 2006 | 2.56 MB | MS Redistributable 2005 |
| vcredist_x86.exe | 9.0.21022.8 | November 7, 2007 | 1.73 MB | MS Redistributable 2008 |

- Ensure that iDRAC6 time and the domain controller time at the domain controller server are within 5 minutes of each other for Kerberos authentication to work. See **iDRAC6 time** on the **System→ iDRAC Settings→ Properties→ Remote Access Information** page, and the domain controller time by right clicking on the time in the bottom right hand corner of the screen. The timezone offset is displayed in the pop up

display. For US Central Standard Time (CST), this is –6. Use the following RACADM timezone offset command to synchronize iDRAC6 time (through Remote or Telnet/SSH RACADM): `racadm config -g cfgRacTuning –o cfgRacTuneTimeZoneOffset <offset value in minutes>.` For example, if the system time is GMT -6 (US CST) and time is 2PM, set iDRAC6 time to GMT time of 18:00 which would require you to enter "360" in the above command for the offset. You can also use `cfgRacTuneDaylightoffset` to allow for daylight savings variation. This saves you from having to change the time on those two occasions every year when the daylight savings adjustments are made, or just allow for it in the above offset using "300" in the preceding example.

# 8

# Viewing the Configuration and Health of the Managed Server

## System Summary

The **System Summary** page allows you to view your system's health and other basic iDRAC6 information at a glance and provides you with links to access the system health and information pages. Also, you can quickly launch common tasks from this page and view recent events logged in the System Event Log (SEL).

To access the **System Summary** page, click **System→ Properties** tab→ **System Summary**. See *iDRAC6 Online Help* for detailed information on each section in the **System Summary** page.

## System Details

The **System Details** page displays information about the following system components:

- Main System Enclosure
- Integrated Dell Remote Access Controller 6 - Enterprise

### Main System Enclosure

#### System Information

This section of iDRAC6's Web interface provides the following basic information about the managed server:

- Description — The model number or name of the managed server.
- BIOS Version — The version number of the managed server's BIOS.
- Service Tag — The Service Tag number of the server.

- Express Service Code — The system's service code number. It is the decimal numerical representation of the Service Tag.
- Host Name — The DNS hostname associated with the managed server.
- OS Name — The name of the operating system installed on the managed server.

  **NOTE:** The **OS Name** field is populated only if Dell OpenManage Server Administrator is installed on the managed system. An exception to this are VMware operating system names which are displayed even if Server Administrator is not installed on the managed system. In certain operating systems, it may take several minutes after server boot up for the operating system name to be updated in iDRAC.
- System Revision — The chassis revision number.
- Lifecycle Controller Firmware — The Lifecycle Controller firmware version.

#### I/O Mezzanine Card

This section of iDRAC6 Web interface provides the following information about the I/O Mezzanine cards installed on the managed server:

- Location — Lists the I/O Mezzanine card(s) installed on the managed server. The list also displays the I/O Mezzanine cards for platforms that support expansion-cards.
- Presence Status — Indicates whether the Mezzanine card is present or not, or if it is an extension of another fabric's Mezzanine card slot.
- Card Type — The physical type of the installed Mezzanine card/connection
- Model Name — The model number, type, or description of the installed Mezzanine card(s)

#### Integrated Storage Card

This section of iDRAC6 Web interface provides information about the integrated Storage Controller Card installed on the managed server:

- Card Type — Displays the model name of the installed storage card, for example, SAS6/iR.

#### Integrated Network Card

This section of the iDRAC6 Web interface provides information about the integrated network card installed on the managed server. It is displayed only for applicable platforms.

- Card Type— Displays the card type of the integrated network card installed on the board, for example, Gigabit Ethernet.
- Model Name — Displays the model name of the integrated network card.

For more information about Integrated Network Card, see the *Hardware Owner's Manual* available on the Dell Support website at **support.dell.com/manuals**.

#### Auto Recovery

This section of iDRAC6 Web interface details the current mode of operation of the Auto Recovery feature of the managed server as set by Open Manage Server Administrator:

- Recovery Action — Action to be performed when a system fault or *hang* is detected. Available actions are **No Action**, **Hard Reset**, **Power Down**, or **Power Cycle**.
- Initial Countdown — The amount of time (in seconds) after a system hang is detected at which time iDRAC6 performs a recovery action.
- Present Countdown — The current value (in seconds) of the countdown timer.

### Integrated Dell Remote Access Controller 6 - Enterprise

#### iDRAC6 Information

This section of iDRAC6 Web interface provides the following information about iDRAC6 itself:

- Date/Time — Displays the current date and time (as of last page refresh) of iDRAC6.
- Firmware Version — Displays the current version of iDRAC6 firmware installed on the managed system.
- CPLD Version — Displays the board complex programmable logic device (CPLD) version.

- Extended CPLD Version — Displays the extended board CPLD version.
- Firmware Updated — Displays the date and time of the last successful iDRAC6 firmware update.
- MAC Address — Displays the MAC address associated with the LOM (LAN on Motherboard) Network Interface Controller of iDRAC6.

#### IPv4 Settings

- Enabled — Displays whether IPv4 protocol support is enabled or disabled

  **NOTE:** The IPv4 protocol option is enabled by default.
- DHCP Enabled — Enabled if iDRAC6 is set to fetch its IP address and associated info from a DHCP server.
- IP Address — Displays the IP address associated with iDRAC6 (not the managed server.)
- Subnet Mask — Displays the TCP/IP Subnet Mask configured for iDRAC6.
- Gateway — Displays the IP address of the network gateway configured for iDRAC6.
- Use DHCP to obtain DNS server addresses — Displays whether DHCP is used to obtain DNS Server Addresses.
- Preferred DNS Server — Displays the currently active primary DNS server.
- Alternate DNS Server — Displays the alternate DNS server address.

#### IPv6 Settings

- Enabled — Displays whether IPv6 protocol support is enabled or disabled.
- Autoconfiguration Enabled — Displays whether Autoconfiguration is enabled or disabled.
- Link Local Address — Displays the link local IPv6 address for iDRAC6 NIC.
- IPv6 Address 1-16 — Displays up to 16 IPv6 addresses (IPv6 Address 1 to IPv6 Address 16) for iDRAC6 NIC.
- Gateway — Displays the IP address of the network gateway configured for iDRAC6.

- Use DHCPv6 to obtain DNS server addresses — Displays whether DHCP is used to obtain DNS Server Addresses.
- Preferred DNS Server — Displays the currently active primary DNS server.
- Alternate DNS Server — Displays the alternate DNS server address.

**NOTE:** This information is also available at **System→ iDRAC Settings→ Properties→ Remote Access Information**.

#### Embedded NIC MAC Addresses

- NIC 1 — Displays the Media Access Control (MAC) address(es) of the embedded Network Interface Controller (NIC) 1.

  MAC addresses uniquely identify each node in a network at the Media Access Control layer.

  Internet Small Computer System Interface (iSCSI) NIC is a network interface controller with the iSCSI stack running on the host computer.

  Ethernet NICs support the wired Ethernet standard and plug into the system bus of the server.
- NIC 2 — Displays the MAC address(es) of the embedded NIC 2 that uniquely identifies it in the network.
- NIC 3 — Displays the MAC address(es) of the embedded NIC 3 that uniquely identifies it in the network. Embedded NIC 3 MAC addresses may not be displayed on all systems.
- NIC 4 — Displays the MAC address(es) of the embedded NIC 4 that uniquely identifies it in the network. Embedded NIC 4 MAC addresses may not be displayed on all systems.

The embedded NIC MAC addresses returned by racadm `getSysInfo` command and the MAC address displayed under **System→ Properties→ System Details** are the server-assigned MAC addresses. If the MAC addresses are remotely managed or chassis assigned, the active MAC addresses are displayed under **System→ Properties→ WWN/MAC**.

# WWN/MAC

Click **System→ Properties** tab**→ WWN/MAC** to view the current configuration of installed I/O Mezzanine cards and their associated network fabrics. You can also view the remotely-assigned MAC addresses. If the FlexAddress feature is enabled in CMC, the globally assigned (Chassis-Assigned) persistent MAC addresses supersede the hardwired values of each LOM.

# Server Health

Click **System→ Properties tab→ System Summary**. In the **Server Health** section, you can click the links to view important information about the health of iDRAC6 and components monitored by iDRAC6. The **Status** column shows the status for each component. For a list of status icons and their meaning, see Table 19-3. Click the component name in the **Component** column for more detailed information about the component.

**NOTE:** Component information can also be obtained by clicking the component name in the left pane of the window. Components remain visible in the left pane independent of the tab/screen that is selected.

The component links available in the **Server Health** section are explained in detail in the following sections.

## iDRAC6

The **Remote Access Information** screen lists a number of important details about iDRAC6, such as name, firmware revision, firmware updated, iDRAC6 time, IPMI version, CPLD version, server type, and network parameters. Additional details are available by clicking the appropriate tab at the top of the screen.

The **iDRAC Time** displays either the BIOS time or the CMC time. BIOS sends the time to iDRAC when the system reboots. If the host system is powered on when iDRAC boots, iDRAC gets its time from BIOS. If the host system is not powered on when iDRAC boots, iDRAC gets its time from CMC. That is, BIOS is the preferred source, but to get the BIOS time, the host server must be powered on.

The firmware time stamp always matches the time stamp iDRAC last had prior to the firmware update, which can be BIOS time if the system had been booted or rebooted prior to the firmware update or the CMC time.

### CMC

**CMC** screen displays the health status, firmware revision, and IP addresses of the Chassis Management Controller. You can also launch CMC Web interface by clicking the **Launch the CMC Web Interface** button. See the *Chassis Management Controller Firmware User Guide* for more information.

**NOTE:** Launching CMC Web GUI from iDRAC6 directs your search with the same IP address format. For example, if you open iDRAC6 Web GUI with an IPv6 address format, CMC Web page will also open with a valid IPv6 address.

### Batteries

The **Batteries** screen displays the status of the system board coin-cell battery that maintains the Real-Time Clock (RTC) and CMOS configuration data storage of the managed system.

### Temperatures

The **Temperatures** screen displays the status and readings of the on–board ambient temperature probe. Minimum and maximum temperature thresholds for *warning* and *failure* states are shown, along with the current health status of the probe.

**NOTE:** Depending on the model of your server, temperature thresholds for *warning* and *failure* states and/or the health status of the probe may not be displayed.

### Voltages

The **Voltage Probes** screen displays the status and reading of the Voltage probes, providing such information as the status of the on-board voltage rail and CPU core sensors.

### Power Monitoring

The **Power Monitoring** screen enables you to view the following monitoring and power statistics information:

- Power Monitoring — Displays the amount of power being used (one minute average power value measured in AC watts) by the server as reported by the System Board Current Monitor.
- Amperage — Displays the current consumption (AC in Amperes) in the active Power Supply unit.
- Power Tracking Statistics — Displays information about the amount of power used by the system since the reading was last reset.
- Peak Statistics — Displays information about the peak amount of power used by the system since the reading was last reset.
- Power Consumption — Displays the average, minimum, and maximum power consumption, and the maximum and minimum power times in the system for the last minute, hour, day, and week.
- Show Graph — Displays a graphical representation of power consumption for 1 Hour, 24 Hours, 3 Days, and 1 Week.

**NOTE:** Power and Amperage are measured in AC.

### CPU

The **CPU** screen reports the health of each CPU on the managed server. This health status is a roll-up of a number of individual thermal, power, and functional tests.

### POST

The **Post Code** screen displays the last system post code (in hexadecimal) prior to booting the operating system of the managed server.

### Misc Health

The **Misc Health** screen provides access to the following system logs:

- System Event Log — Displays system-critical events that occur on the managed system.
- Post Code — Displays the last system post code (in hexadecimal) prior to booting the operating system of the managed server.
- Last Crash Screen — Displays the most recent crash screen and time.
- Boot Capture — Provides playback of the last three boot screens.

**NOTE:** This information is also available at **System**→ **Logs** tab→ **System Event Log**.

## System Inventory

The **System Inventory** page displays the hardware and firmware components installed on the managed system.

To access the System Inventory page, click **System**→ **Properties**→ **System Inventory**.

The **Hardware Inventory** section displays the information for components that include the iDRAC, the RAID controller installed, all CPUs installed, all DIMMs installed, all HDDs installed, the host NICs (integrated and embedded), the video card installed, and the SD card if installed.

The **Firmware Inventory** section displays the firmware version for the firmware components and includes the BIOS, Lifecycle Controller version (USC), and iDRAC firmware.

Each field can only display up to 48 characters. If it is greater than 48, the string is truncated.

For more information, see the *iDRAC6 Online Help*.

To ensure that the Systems Inventory feature is working, do the following:

1. System must be configured to collect system inventory. To do this, use the iDRAC Option ROM utility during system startup (Ctrl-E). In the **System Services** menu, enable the **Collect System Inventory on Restart (CSIOR)** option.
2. After enabling CSIOR, the host system reboots and starts, in the output screen, towards the end of the BIOS startup, the message "Collecting System Inventory" is displayed after several minutes.

3 After the host reboots and the system inventory is collected, reboot iDRAC only.

4 Once the iDRAC boots, the hardware inventory is accessible.

After iDRAC reboots, the internal components necessary for servicing the requests that provide the hardware inventory will not be ready immediately. Therefore, after the reboot, wait for 5 minutes and then connect to iDRAC to display the hardware inventory. This can be several minutes after iDRAC was first reset. Alternativley, use WSMAN check for the Remote Services availability on the iDRAC to determine when the hardware inventory is ready. To invoke, use the GetRSStatus method of the DCIM_LCService class. For more details, see the Dell DCIM LC Service MOF available at **delltechcenter.com**. The Remote Service must be available before the hardware inventory is ready. This applies if the iDRAC has been rebooted (step 3) or not.

## Troubleshooting

#### Hardware Inventory page displays that hardware inventory information is not available.

Ensure the steps described for properly enabling the hardware inventory are followed. This includes the minimum wait time required on the iDRAC before trying to display the page after an iDRAC reboot. Any iDRAC reboot (including firmware update) requires this minimum wait time. Run the Remote Services availability WSMAN check to check when the hardware inventory is ready.

#### Hardware Inventory is missing some hardware attribute values.

Some values may not be properly populated on the hardware component and thus the underlying elements that retrieve the data will obtain blank fields. This is reflected in the GUI. The iDRAC GUI properly displays the information it obtains. If data is missing, the same data will be missing in the USC hardware inventory. If the hardware component can be reseated, try to reseat it to see if the issue is cleared. If the hardware component can be swapped, replace it and the problem should be resolved. After replacing or reseating a component ensure CSIOR is run and use the Remote Services availability WSMAN check before attempting to view the updated inventory.

**Hardware Inventory has mostly blank data and is missing many supported components.**

This problem is typically a result of the CSIOR feature not being enabled or the data was lost from a previous collection. To gather the full inventory allow the system to boot and make sure the CSIOR feature is enabled in the Ctrl-E setup for System Services. As the system is booting make sure the screen shows a message "Collecting System Inventory" before the host boots.

**Firmware Inventory data is missing or LC Version on System Summary and System Details page shows as Not Found.**

In this case an option is to reboot the iDRAC. It may also be necessary to update the iDRAC firmware even if the update is to the currently installed firmware.

# 9

# Configuring and Using Serial Over LAN

Serial Over LAN (SOL) is an IPMI feature that allows a managed server's text based console data that would traditionally be sent to the serial I/O port to be redirected over iDRAC6's dedicated Out of Band Ethernet management network. The SOL out-of-band console enables system administrators to remotely manage the blade server's text-based console from any location with network access. Benefits of SOL are as follows:

- Remotely access operating systems with no timeout.
- Diagnose host systems on Emergency Management Services (EMS) or Special Administrator Console (SAC) for Windows or in a Linux shell.
- View the progress of a blade server during POST and reconfigure the BIOS setup program (while redirected to a serial port).

## Enabling Serial Over LAN in the BIOS

To configure the server for Serial Over LAN, the following configuration steps are required and will be explained in detail.

1. Configure Serial Over LAN in BIOS (disabled by default.)
2. Configure iDRAC6 for Serial over LAN.
3. Select a method to initialize Serial Over LAN (SSH, Telnet, SOL Proxy, or IPMI Tool.)
4. Configure the operating system for SOL.

Serial communication is **off** by default in BIOS. In order to redirect the host text console data to Serial over LAN, you must enable Virtual Console through COM1.

To change the BIOS setting:

1. Boot the managed server.
2. Press <F2> to enter the BIOS setup utility during POST.
3. Scroll down to Serial Communication and press <Enter>.

   In the pop-up window, the serial communication list is presented with the following options:

   - Off
   - On without Virtual Console
   - On with Virtual Console

   Use the arrow keys to navigate between options.
4. Ensure that **On with Virtual Console** is enabled. Ensure that **Serial Port Address** is COM1.
5. Ensure that the **Failsafe Baud Rate** is identical to SOL baud rate that is configured on iDRAC6. The default value for both the failsafe baud rate and iDRAC6's SOL baud rate setting is 115.2 kbps.
6. Ensure that **Redirection After Boot** is enabled. This option enables BIOS SOL redirection across subsequent reboots. BIOS has the **Remote Terminal Type** values VT100/VT220 and ANSI.
7. Save the changes and exit.

   The managed server reboots.

# Configuring Serial Over LAN in iDRAC6 Web GUI

1. Open the **Serial Over LAN Configuration** screen by selecting **System→ iDRAC Settings→ Network/Security→ Serial Over LAN**.
2. Ensure the **Enable Serial Over LAN** option is selected (enabled). By default it is enabled.
3. From the **Baud Rate** drop-down menu, select the IPMI SOL baud rate (data speed). The options are 9600 bps, 19.2 kbps, 57.6 kbps, and 115.2 kbps. The default value is 115.2 kbps.

4 From the **Channel Privilege Level Limit** drop-down menu, select a privilege level limit for SOL.

**NOTE:** Ensure that the SOL baud rate is identical to the Failsafe Baud Rate that was set in BIOS.

5 Click **Apply** to save the settings.

6 Click **Advanced Settings**. The **Serial Over LAN Configuration Advanced Settings** screen is displayed that allows you to adjust the SOL performance. See Table 9-1.

**Table 9-1. Serial Over LAN Configuration Advanced Settings**

| Setting | Description |
|---|---|
| **Character Accumulate Interval** | The typical amount of time iDRAC6 waits before sending a partial SOL data packet. This parameter is specified in milliseconds. It is recommended to use 10 milliseconds for optimal performance. |
| **Character Send Threshold** | Specifies the number of characters per SOL data packet. As soon as the number of characters accepted by iDRAC6 is equal to or greater than the Character Send Threshold value, iDRAC6 starts transmitting SOL data packets that contain numbers of characters equal to or less than the Character Send Threshold value. If a packet contains fewer characters than this value, it is defined to be a partial SOL data packet.<br>It is recommended to use 255 characters for optimal performance. |

**NOTE:** If you change these values to lower values, the Virtual Console feature of SOL may experience a reduction in performance. Furthermore, the SOL session must wait to receive an acknowledgement for each packet before sending the next packet. As a result, the performance is significantly reduced.

7 Click **Apply** to save the settings.

8 Configure SSH and Telnet for SOL at **System→ iDRAC Settings→ Network/Security** tab→ **Services**.

**NOTE:** Each blade server supports only one active SOL session.

**NOTE:** SSH protocol is enabled by default. Telnet protocol is disabled by default.

9 Click **Services** to open the **Services** screen.

**NOTE:** SSH and Telnet programs both provide access on a remote machine.

10 Click **Enabled** on either **SSH** or **Telnet** as required.

11 Click **Apply**.

**NOTE:** SSH is a recommended method due to better security and encryption mechanisms.

**NOTE:** SSH/Telnet session duration can be infinite as long as the timeout value is set to 0. The default timeout value is 1800 seconds.

12 Enable iDRAC6 Out-of-Band interface (IPMI over LAN) by selecting **System→ iDRAC Settings→ Network/Security→ Network**.

13 Select the **Enable IPMI Over LAN** option under **IPMI Settings**.

14 Click **Apply**.

# Using Serial Over LAN (SOL)

This section provides several methods to initialize a Serial-Over-LAN session including a Telnet program, an SSH client, IPMItool, and SOL Proxy. The purpose of Serial Over LAN feature is to redirect the serial port of the managed server through iDRAC6 into the console of your management station.

## Model for Redirecting SOL Over Telnet or SSH

Telnet (port 23)/ SSH (port 22) client ←→ WAN connection ←→ iDRAC6 server

The IPMI-based SOL over SSH/Telnet implementation eliminates the need for an additional utility because the serial to network translation happens within iDRAC6. The SSH or Telnet console that you use should be able to interpret and respond to the data arriving from the managed server'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 your SSH or Telnet console.

To initiate a SOL session, attach to iDRAC6 through SSH/Telnet which takes you to iDRAC6 command line console. Then enter `connect` at the dollar prompt.

See "Installing Telnet or SSH Clients" on page 75 for more information about using Telnet and SSH clients with iDRAC6.

### Model for the SOL Proxy

Telnet Client (port 623) ←→ WAN connection ←→ SOL Proxy ←→ iDRAC6 server

When the SOL Proxy communicates with the Telnet client on a management station, it uses the TCP/IP protocol. However, SOL proxy communicates with the managed server's iDRAC6 over the RMCP/IPMI/SOL protocol, which is a UDP-based protocol. Therefore if you communicate with your managed system's iDRAC6 from SOL Proxy over a WAN connection, you may experience network performance issues. The recommended usage model is to have the SOL Proxy and iDRAC6 server on the same LAN. The management station with the Telnet client can then connect to the SOL Proxy over a WAN connection. In this usage model, SOL Proxy will function as desired.

### Model for Redirecting SOL Over IPMItool

IPMItool ←→ WAN connection ←→ iDRAC6 server

The IPMI-based SOL utility, IPMItool, uses RMCP+ protocol delivered using UDP datagrams to port 623. iDRAC6 requires this RMCP+ connection to be encrypted. The encryption key (KG key) must contains characters of zero or NULL that can be configured in iDRAC6 Web GUI or in iDRAC6 Configuration Utility. You can also wipe out the encryption key by pressing the backspace key so that iDRAC6 will provide NULL characters as the encryption key by default. The advantage of using RMCP+ is improved authentication, data integrity checks, encryption, and the ability to carry multiple types of payloads. See "Using SOL over IPMItool" on page 204 or the IPMItool website for more information: **http://ipmitool.sourceforge.net/manpage.html**.

### Disconnecting SOL session in iDRAC6 Command Line Console

Commands to disconnect a SOL session are utility oriented. You can exit the utility only when a SOL session is fully terminated. To disconnect a SOL session, terminate the SOL session from iDRAC6 command line console.

When you are ready to quit SOL redirection, press <Enter>, <Esc>, and then <t> (press the keys in sequence, one after the other). The SOL session will close accordingly. The escape sequence is also printed on screen as soon as a SOL session is connected. When the managed server is off, it takes a bit longer to establish the SOL session.

**NOTE:** If a SOL session is not closed successfully in the utility, more SOL sessions may not be available. The way to resolve this situation is to terminate the command line console in the Web GUI under **System→ iDRAC Settings→ Network/Security→ Sessions**.

### Using SOL over PuTTY

To start SOL from PuTTY on a Windows management station, follow these steps:

**NOTE:** If required, you can change the default SSH/Telnet timeout at **System→ iDRAC Settings→ Network/Security→ Services**.

1. Connect to iDRAC6 with the following command at the command prompt:

   ```
   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. Enter the following command at the command prompt to start SOL:

   ```
   connect
   ```

   This connects you to the managed server's serial port. Once a SOL session is established successfully, iDRAC6 command line console is no longer available to you. Follow the escape sequence properly to reach iDRAC6 command line console. Quit the SOL session using the command sequence detailed in "Disconnecting SOL session in iDRAC6 Command Line Console" on page 202, and start a new one.

**NOTE:** 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 as mentioned in "Disconnecting SOL session in iDRAC6 Command Line Console" on page 202, close the terminal, open another terminal and start the SOL session using the same command described above.

### Using SOL over Telnet with Linux

To start SOL from Telnet on a Linux management station, follow these steps:

**NOTE:** If required, you can change the default Telnet timeout at **System→ iDRAC Settings→ Network/Security→ Services**.

1. Start a shell.
2. Connect to iDRAC6 with the following command:

   ```
   telnet <iDRAC6-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 the following command at the command prompt to start SOL:

   ```
   connect
   ```

4. To quit a SOL session from Telnet on Linux, press <Ctrl>+] (hold down the control key, press the right-square-bracket key, and then release). A Telnet prompt displays. Enter `quit` to exit Telnet.

### Using SOL over OpenSSH with Linux

OpenSSH is an open source utility for using the SSH protocol. To start SOL from OpenSSH on a Linux management station, follow these steps:

**NOTE:** If required, you can change the default SSH session timeout at **System→ iDRAC Settings→ Network/Security→ Services**.

1. Start a shell.
2. Connect to iDRAC6 with the following command:

   ```
   ssh <iDRAC-ip-address> -l <login name>
   ```

3. Enter the following command at the command prompt to start SOL:

   ```
   connect
   ```

This connects you to the managed server's serial port. Once a SOL session is established successfully, iDRAC6 command line console is no longer available to you. Follow the escape sequence properly to reach iDRAC6 command line console. Quit the SOL session (see "Disconnecting SOL session in iDRAC6 Command Line Console" on page 202 to close an active SOL session).

### Using SOL over IPMItool

The *Dell Systems Management Tools and Documentation* DVD provides the IPMItool which can be installed on various operating systems. See the *Software Quick Installation Guide* for installation details. To start SOL with IPMItool on a management station, follow these steps:

**NOTE:** If required, you can change the default SOL timeout at **System→ iDRAC Settings→ Network/Security→ Services**.

1. Locate **IPMItool.exe** under the proper directory.

   The default path in Windows 32–bit operating system is **C:\Program Files\Dell\SysMgt\bmc** and in Windows 64–bit operating system is **C:\Program Files (x86)\Dell\SysMgt\bmc**.

2. Ensure the **Encryption Key** is all zeroes at **System→ iDRAC Settings→ Network/Security→ Network→ IPMI Settings**.

3. Enter the following command in the Windows command prompt or in the Linux shell prompt to start SOL from iDRAC:

   ```
   ipmitool -H <iDRAC-ip-address> -I lanplus -U
   <login name> -P <login password> sol activate
   ```

   This connects you to the managed server's serial port.

4. To quit a SOL session from IPMItool, press <~> and <.> (press the tilde and period keys in sequence, one after the other). Try more than once since iDRAC6 may be busy to accept the keys. The SOL session will close.

**NOTE:** If a user does not terminate the SOL session correctly, enter the following command to reboot iDRAC. Allow iDRAC6 upto two minutes to complete booting. For more details, see the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

```
racadm racreset
```

## Opening SOL with SOL proxy

Serial-Over-LAN Proxy (SOL Proxy) is a Telnet daemon that allows LAN-based administration of remote systems using the Serial over LAN (SOL) and IPMI protocols. Any standard Telnet client application, such as HyperTerminal on Microsoft Windows or Telnet on Linux, can be used to access the daemon's features. SOL can be used either in the menu mode or command mode. The SOL protocol coupled with the remote system's BIOS Virtual Console allows administrators to remotely view and change a managed system's BIOS settings over a LAN. The Linux serial console and Microsoft's EMS/SAC interfaces can also be accessed over a LAN using SOL.

**NOTE:** All versions of the Windows operating system include HyperTerminal terminal emulation software. However, the included version does not provide many functions required during Virtual Console. Instead, you can use any terminal emulation software that supports VT100/VT220 or ANSI emulation mode. One example of a full VT100/VT220 or ANSI terminal emulator that supports Virtual Console on your system is Hilgraeve's HyperTerminal Private Edition 6.1 or later. Also, use of the command line window to perform Telnet serial Virtual Console may display garbage characters.

**NOTE:** See your system's User's Guide for more information about Virtual Console, including hardware and software requirements and instructions for configuring host and client systems to use Virtual Console.

**NOTE:** HyperTerminal and Telnet settings must be consistent with the settings on the managed system. For example, the baud rates and terminal modes should match.

**NOTE:** The Windows `telnet` command that is run from a MS-DOS prompt supports ANSI terminal emulation, and the BIOS needs to be set for ANSI emulation to display all the screens correctly.

### Before Using SOL proxy

Before using SOL proxy, see the *Baseboard Management Controller Utilities User's Guide* to learn how to configure your management stations. By default, BMC Management Utilities are installed in the following directory on Windows operating systems:

**C:\Program Files\Dell\SysMgt\bmc** — (32–bit operating system)

**C:\Program Files (x86)\Dell\SysMgt\bmc** — (64–bit operating system)

The installation program copies the files to the following locations on Linux Enterprise Operating Systems:

**/etc/init.d/SOLPROXY.cfg**

**/etc/SOLPROXY.cfg**

**/usr/sbin/dsm_bmu_solproxy32d**

**/usr/sbin/solconfig**

**/usr/sbin/ipmish**

#### Initiating the SOL Proxy session

##### *For Windows 2003*

To start the SOL Proxy service on Windows system after installation, you can reboot the system (SOL Proxy automatically starts on a reboot). Or, you can start the SOL Proxy service manually by completing the following steps:

1. Right-click **My Computer** and click **Manage**.

   The **Computer Management** window is displayed.

2. Click **Services and Applications** and then click **Services**.

   Available services are displayed to the right.

3. Locate **DSM_BMU_SOLProxy** in the list of services and right-click to start the service.

Depending on the console you use, there are different steps for accessing SOL Proxy. Throughout this section, the management station where the SOL Proxy is running is referred as the SOL Proxy Server.

##### *For Linux*

The SOL Proxy will start automatically during system startup. Alternatively, you can go to directory **/etc/init.d** and use the following commands to manage the SOL Proxy service:

```
solproxy status

dsm_bmu_solproxy32d start

dsm_bmu_solproxy32d stop

solproxy restart
```

### Using Telnet with SOL Proxy

This assumes that the SOL Proxy service is already up and running on the management station.

***For Windows 2003:***

1. Open a command prompt window on your management station.
2. Enter the `telnet` command in the command-line and provide `localhost` as the IP address if the SOL Proxy server is running in the same machine and the port number that you specified in the SOL Proxy installation (the default value is `623`). For example:

   ```
   telnet localhost 623
   ```

***For Linux:***

1. Open a Linux shell on your management station.
2. Enter the `telnet` command and provide `localhost` as the IP address of the SOL Proxy server and the port number that you specified in the SOL Proxy installation (the default value is `623`). For example:

   ```
   telnet localhost 623
   ```

**NOTE:** Whether your host operating system is Windows or Linux, if the SOL Proxy server is running on a different machine than your management station, input SOL Proxy server IP address instead of localhost.

```
telnet <SOL Proxy server IP address> 623
```

### Using HyperTerminal with SOL Proxy

1. From the remote station, open **HyperTerminal.exe**.
2. Choose **TCPIP(Winsock)**.
3. Enter host address `localhost` and port number `623`.

#### Connecting to the Remote Managed System's BMC

After a SOL Proxy session is established successfully, you are presented with the following choices:

```
1. Connect to the Remote Server's BMC

2. Configure the Serial-Over-LAN for the Remote
Server

3. Activate Virtual Console

4. Reboot and Activate Virtual Console

5. Help

6. Exit
```

**NOTE:** While multiple SOL sessions can be active at the same time, only one Virtual Console session can be active at any given time for a managed system.

**NOTE:** To exit an active SOL session, use the <~><.> character sequence. This sequence terminates SOL and returns you to the top-level menu.

1. Select option 1 in the main menu.
2. Enter iDRAC6 **IP Address** of the remote managed system.
3. Provide iDRAC6 **Username** and **Password** for iDRAC6 on the managed system. iDRAC6 username and password must be assigned and stored in iDRAC6 non-volatile storage.

**NOTE:** Only one SOL Virtual Console session with iDRAC6 is permitted at one time.

**NOTE:** If required, extend SOL session duration to infinite by changing the Telnet **Timeout** value to zero in iDRAC6 Web GUI under **System→ iDRAC Settings→ Network/Security→ Services**.

4. Provide the IPMI encryption key if it was configured in iDRAC6.

**NOTE:** You can locate the IPMI encryption key in iDRAC6 GUI on **System→ iDRAC Settings→ Network/Security→ Network→ IPMI Settings→ Encryption Key**.

**NOTE:** The default IPMI encryption key is all zeros. If you press <Enter> for the encryption option, iDRAC6 will use this default encryption key.

5. Select **Configure the Serial-Over-LAN for the Remote Server** (option 2) in the main menu.

The SOL configuration menu is displayed. According to the current SOL status, the content of the SOL configuration menu varies:

- If SOL is already enabled, the current settings are displayed and you are presented with three choices:

  ```
  1. Disable Serial-Over-LAN
  2. Change Serial-Over-LAN settings
  3. Cancel
  ```

- If SOL is enabled, ensure that the SOL baud rate is consistent with iDRAC6's and that the user has the administrator privilege.
- If SOL is currently disabled, enter `Y` to enable SOL or `N` to keep SOL disabled.

6 Select **Activate Virtual Console** (option 3) in the main menu.

The remote managed system's text console is redirected to your management station.

7 Select **Reboot and Activate Virtual Console** (option 4) in the main menu (optional).

The power state of the remote managed system is confirmed. If power is on, you are asked to decide between a graceful or forceful shutdown.

The power state is monitored until the state changes to **On**. Virtual Console begins, and the remote managed system text console is redirected to your management station.

While the managed system reboots, you can enter BIOS system setup program to view or configure BIOS settings.

8 Select **Help** (option 5) in the main menu to display a detailed description for each option.

9 Select **Exit** (option 6) in the main menu to end your Telnet session and disconnect from SOL Proxy.

**NOTE:** If a user does not terminate the SOL session correctly, issue the following command to reboot iDRAC. Allow iDRAC6 1-2 minutes to complete booting. For more details, see *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

```
racadm racreset
```

# Operating System Configuration

To configure generic operating systems, perform the steps relevant to your operating system. This configuration is based on default installations of Red Hat Enterprise Linux 5.0, SUSE Linux Enterprise Server 10 SP1, and Windows 2003 Enterprise.

### Linux Enterprise Operating System

1. Edit the **/etc/inittab** file to enable hardware flow control and to allow users to log in through the SOL console. Add the line below to the end of `#Run gettys in standard runlevels` section.

   ```
   7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220
   ```

Example of original **/etc/inittab**:

```
#
# inittab    This file describes how the INIT process should set up
#            the system in a certain run-level.
#

SKIP this part of file

# Run gettys in standard runlevels
1:2345:respawn:/sbin/migetty tty1
2:2345:respawn:/sbin/migetty tty1
3:2345:respawn:/sbin/migetty tty1
4:2345:respawn:/sbin/migetty tty1
5:2345:respawn:/sbin/migetty tty1
6:2345:respawn:/sbin/migetty tty1

# Run xdm in runlevel 5
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Example of modified **/etc/inittab**:

```
#
# inittab    This file describes how the INIT process should set up
#            the system in a certain run-level.
#

SKIP this part of file

# Run gettys in standard runlevels
1:2345:respawn:/sbin/migetty tty1
2:2345:respawn:/sbin/migetty tty1
3:2345:respawn:/sbin/migetty tty1
4:2345:respawn:/sbin/migetty tty1
5:2345:respawn:/sbin/migetty tty1
6:2345:respawn:/sbin/migetty tty1
7:2345:respawn:/sbin/agetty -h ttyS0 115200 vt220

# Run xdm in runlevel 5
x:5:respawn:/etc/X11/prefdm -nodaemon
```

2 Edit the **/etc/securetty** file to allow users to log in as root user through the SOL console. Add the following line after `console`:

`ttyS0`

Example of original **/etc/securetty**:

```
console
vc/1
vc/2
vc/3
vc/4
```

```
SKIP the rest of file
```

Example of modified **/etc/securetty**:

```
Console
ttyS0
vc/1
vc/2
vc/3
vc/4

SKIP the rest of file
```

3 Edit the **/boot/grub/grub.conf** or **/boot/grub/menu.list** file to add boot options for SOL:

   a Comment out the graphical display lines in the various Unix-like operating systems:

   - `splashimage=(had0,0)/grub/splash.xpm.gz` in RHEL 5
   - `gfxmenu (hda0,5)/boot/message` in SLES 10

   b Add the following line before the first `title=` … line:

   ```
   # Redirect OS boot via SOL
   ```

   c Append the following entry to the first `title=` … line:

   ```
   SOL redirection
   ```

   d Append the following text to the `kernel/`… line of the first `title=` …:

   ```
   console=tty1 console=ttyS0,115200
   ```

**NOTE: /boot/grub/grub.conf** in Red Hat Enterprise Linux 5 is a symbolic link to **/boot/grub/menu.list**. You can change the settings in either one of them.

Example of original **/boot/grub/grub.conf** in RHEL 5:

```
# grub.conf generated by anaconda
#
# Note that you do not have to return grub after making changes
to this
# file
# NOTICE: You have a /boot partition. This means that
#         all kernel and initrd paths are relative to /boot/,
eg.
#         root (hd0,0)
#         kernel /vmlinux-version ro root=
/dev/VolGroup00/LogVol00
#         initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm/gz
hiddenmenu

title Red Hat Enterprise Linux 5
root (hd0,0)
kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00
rhgb quiet
initrd /initrd-2.6.18-8.el5.img
```

Example of modified **/boot/grub/grub.conf**:

```
# grub.conf generated by anaconda
#
# Note that you do not have to return grub after making changes
to this
# file
# NOTICE: You have a /boot partition. This means that
# all kernel and initrd paths are relative to /boot/, eg.
#         root (hd0,0)
#         kernel /vmlinux-version ro root=
/dev/VolGroup00/LogVol00
#         initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
#splashimage=(hd0,0)/grub/splash.xpm/gz
hiddenmenu

# Redirect the OS boot via SOL
title Red Hat Enterprise Linux 5 SOL redirection
root (hd0,0)
kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00
rhgb quiet console=tty1 console=ttyS0,115200
initrd /initrd-2.6.18-8.el5.img
```

Example of original **/boot/grub/menu.list** in SLES 10:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09
UTC 2008

Default 0

Timeout 8

gfxmenu (hd0.5)/boot/message


###Don't change this comment - YaST2 identifier: Original name:
linux###

title SUSE Linux Enterprise Server 10 SP1

root (hd0,5)

kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-
id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts

initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Example of modified **/boot/grub/menu.list** in SLES 10:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09
UTC 2008

Default 0

Timeout 8

#gfxmenu (hd0.5)/boot/message


###Don't change this comment - YaST2 identifier: Original name:
linux###

title SUSE Linux Enterprise Server 10 SP1 SOL redirection

root (hd0,5)

kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-
id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts
console=tty1 console=ttyS0,115200

initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

### Windows 2003 Enterprise

1. Find out the boot entry ID by entering bootcfg in the Windows command prompt. Locate the boot entry ID for the section with the OS-friendly name **Windows Server 2003 Enterprise**. Press <Enter> to display the boot options on the management station.
2. Enable EMS at a Windows command prompt by entering:

   `bootcfg /EMS ON /PORT COM1 /BAUD 115200 /ID <boot id>`

**NOTE:** *<boot id>* is the boot entry ID from step 1.

3. Press <Enter> to verify that the EMS console setting takes effect.

Example of original `bootcfg` setting:

```
Boot Loader Settings
--------------------
timeout:30
default:multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

Boot Entries
------------
Boot entry ID:    1
Os Friendly Name: Winodws Server 2003, Enterprise
Path:             multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
OS Load Options:  /nonexecute=optout /fastdetect /usepmtimer
/redirect
```

Example of modified `bootcfg` setting:

```
Boot Loader Settings
--------------------
timeout:          30
default:          multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
redirect:         COM1
redirectbaudrate:115200

Boot Entries
------------
Boot entry ID:    1
Os Friendly Name: Windows Server 2003, Enterprise
Path:             multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
OS Load Options:  /nonexecute=optout /fastdetect /usepmtimer
/redirect
```

# 10

# Using GUI Virtual Console

This section provides information about using iDRAC6 Virtual Console feature.

## Overview

iDRAC6 Virtual Console feature enables you to remotely access local consoles in graphic or text mode, allowing you to control one or more iDRAC6-enabled systems from a single location.

## Using Virtual Console

The **Virtual Console** screen enables you to manage the remote system by using the keyboard, video, and mouse on your local management station to control the corresponding devices on a remote managed server. This feature can be used in conjunction with the Virtual Media feature to perform remote software installations.

The following rules apply to a Virtual Console session:

- A maximum of two simultaneous Virtual Console sessions are supported on each blade. Both sessions view the same managed server console simultaneously.
- A Virtual Console session should not be launched from a Web browser on the managed system.
- A minimum available network bandwidth of 1 MB/sec is required.

If a second user requests a Virtual Console session, the first user is notified and is given the option to refuse access, allow only video, 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 not granted to the

second user. During the time that two sessions are concurrently active, the first user sees a message in the upper-right corner of the screen that identifies that the second user has an active session.

If the neither the first or second user has administrator privileges, termination of the first user's active session automatically results in termination of the second user's session.

### Clear Your Browser's Cache

If you encounter issues when operating the Virtual Console, (out of range errors, synchronization issues, and so on) clear the browser's cache to remove/delete any old versions of the viewer that may be stored on the system and try again.

**To clear older 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 **DELL IDRAC AVCView**.

**To clear older 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. From the **Show** drop-down menu, select **All add-ons**.
4. Select the **DELL IDRAC AVCView** and click the **More Information** link.
5. Click **Remove** from the **More Information** window.
6. Close the **More Information** and the **Manage Add-ons** windows.

**To clear older versions of Java viewer in Windows or Linux, do the following:**

1. At the command prompt, run `javaws -viewer`.

   The **Java Cache Viewer** is displayed.

2 Delete the item titled *iDRAC6 Virtual Console Client* and *JViewer*.

You can also run `javaws -uninstall` at the command prompt to remove all applications from the cache.

## Supported Screen Resolutions and Refresh Rates

Table 10-1 lists the supported screen resolutions and corresponding refresh rates for a Virtual Console session that is running on the managed server.

**Table 10-1. Supported Screen Resolutions and Refresh Rates**

| Screen Resolution | Refresh Rate (Hz) |
|---|---|
| 720x400 | 70 |
| 640x480 | 60, 72, 75, 85 |
| 800x600 | 60, 70, 72, 75, 85 |
| 1024x768 | 60, 70, 72, 75, 85 |
| 1280x1024 | 60 |

## Configuring the Management Station

To use Virtual Console on the management station, perform the following procedures:

1 Install and configure a supported Web browser. See "Supported Web Browsers" on page 25 and "Configuring a Supported Web Browser" on page 66.

2 If you are using Firefox or want to use the Java Viewer with Internet Explorer, install a Java Runtime Environment (JRE). See "Installing a Java Runtime Environment (JRE)" on page 74.

3 It is recommended that you configure your monitor display resolution to 1280 x 1024 pixels.

**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 server is running a Linux operating system, an X11 console may not be viewable on the local monitor.
Pressing <Ctrl><Alt><F1> at the Virtual Console will switch Linux to a text console.

4 If you are using Internet Explorer to launch Virtual Console session with Java plug-in, perform the following:

a In Internet Explorer, go to **Tools** →**Internet Options** →**Security** →**Trusted sites** →**Custom level**.

**NOTE:** For Windows 7 64-bit, click **Tools** →**Internet Options** →**Security** →**Internet** →**Custom level**.

b In the **Security Settings** window, select the **Disable** option for **Automatic prompting for file downloads**.

c Click **OK**, and again click **OK**.

## Configuring Virtual Console and Virtual Media in iDRAC6 Web Interface

To configure Virtual Console in iDRAC6 Web interface, perform the following steps:

1. Click **System** and then click the **Virtual Console/Media** tab.
2. Click **Configuration** to open the **Configuration** screen.
3. Configure the Virtual Console properties. Table 10-2 describes the settings for Virtual Console.
4. When completed, click **Apply**.

**Table 10-2. Virtual Console Configuration Properties**

| Property | Description |
|---|---|
| **Enabled** | Select to enable or disable Virtual Console.<br>**Selected** indicates that Virtual Console is enabled.<br>**Deselected** indicates that Virtual Console is disabled.<br>The default is **enabled**. |
| **Max Sessions** | Displays the maximum number of Virtual Console sessions that are possible, **1** or **2**. Use the drop-down menu to change the maximum number of Virtual Console sessions allowed. The default is **2**. |
| **Active Sessions** | Displays the number of Active Console sessions. This field is read-only. |
| **Keyboard and Mouse Port Number** | The network port number used for connecting to the Virtual Console Keyboard/Mouse option. This traffic is always encrypted. You may need to change this number if another program is using the default port. The default is **5900**. |

**Table 10-2. Virtual Console Configuration Properties *(continued)***

| Property | Description |
|---|---|
| Video Port Number | The network port number used for connecting to the Virtual Console Screen service. You may need to change this setting if another program is using the default port. The default is **5901**. |
| Video Encryption Enabled | **Selected** indicates that video encryption is enabled. All traffic going to the video port is encrypted.<br><br>**Deselected** indicates that video encryption is disabled. Traffic going to the video port is not encrypted.<br><br>The default is **Encrypted**. Disabling encryption can improve performance on slower networks. |
| Mouse Mode | Choose **Windows** if the managed server is running on a Windows operating system.<br><br>Choose **Linux** if the managed server is running on Linux.<br><br>Choose **USC/Diags** if your server is not running on a Windows or Linux operating system.<br><br>**NOTE:** You must select **USC/Diags** in HyperV, Dell Diagnostics, or USC (System Services).<br><br>The default is **Windows**. |
| Console Plug-In Type for IE | When using Internet Explorer on a Windows operating system, you can choose from the following viewers:<br><br>**ActiveX** - The *ActiveX Virtual Console* viewer<br><br>**Java** - *Java Virtual Console* viewer<br><br>**NOTE:** Depending on your version of Internet Explorer, additional security restrictions may need to be turned off (see "Configuring and Using Virtual Media" on page 261.)<br><br>**NOTE:** You must have the Java runtime environment installed on your client system to use the Java viewer. |
| Local Server Video Enabled | **Selected** indicates that output to the Virtual Console monitor is enabled during Virtual Console. **Deselected** indicates that the tasks you perform using **Virtual Console** will not be visible on the managed server's local monitor. |

**NOTE:** For information about using Virtual Media with Virtual Console, see "Configuring and Using Virtual Media" on page 261.

## Opening a Virtual Console Session

When you open a Virtual Console session, the Dell Virtual Console Viewer Application (**iDRACView**) starts and the remote system's desktop is displayed in the viewer. Using **iDRACView**, you can control the remote system's mouse and keyboard functions from your local management station.

**NOTE:** Virtual Console launch from a Windows Vista management station may lead to Virtual Console restart messages. To avoid this, set the appropriate timeout values in the following locations: **Control Panel→ Power Options→ Power Saver→ Advanced Settings→ Hard Disk→ Turnoff Hard Disk After <time_out>** and in the **Control Panel→ Power Options→ High–Performance→ Advanced Settings→ Hard Disk→ Turnoff Hard Disk After <time_out>**.

To open a Virtual Console session in the Web interface, perform the following steps:

1. Click **System→ Virtual Console/Media** tab**→ Virtual Console and Virtual Media**.
2. In the **Virtual Console and Virtual Media** screen, use the information in Table 10-3 to ensure that a Virtual Console session is available.

   If you wish to reconfigure any of the property values displayed, see "Configuring Virtual Console and Virtual Media in iDRAC6 Web Interface" on page 222.

**Table 10-3. Virtual Console Information**

| Property | Description |
|---|---|
| Virtual Console Enabled | Yes/No |
| Video Encryption Enabled | Yes/No |
| Max Sessions | Displays the maximum number of supported Virtual Console sessions. |
| Active Sessions | Displays the current number of active Virtual Console sessions. |
| Mouse Mode | Displays the mouse acceleration currently in effect. **Mouse Mode** should be chosen based on the type of operating system installed on the managed server. |

**Table 10-3. Virtual Console Information *(continued)***

| Property | Description |
|---|---|
| Console Plug-in Type | Shows the plug-in type currently configured.<br>**ActiveX** — An Active-X viewer will be launched. Active-X viewer will only work on Internet Explorer while running on a Windows Operating System.<br>**Java** — A Java viewer will be launched. The Java viewer can be used on any browser including Internet Explorer. If your client runs on an operating system other than Windows, then you must use the Java Viewer. If you are accessing iDRAC6 using Internet Explorer while running on a Windows operating system, you may choose either **Active-X** or **Java** as the plug-in type.<br>**NOTE:** Virtual Console may not launch for the first time for Internet Explorer 8, if **Java** is selected as the plug-in type. |
| Local Server Video Enabled | **Yes** indicates that output to the Virtual Console monitor is enabled during Virtual Console. **No** indicates that the tasks you perform using **Virtual Console** are not visible on the managed server's local monitor. |

**NOTE:** For information about using Virtual Media with Virtual Console, see "Configuring and Using Virtual Media" on page 261.

3 If a Virtual Console session is available, click **Launch Virtual Console**.

**NOTE:** Multiple message boxes may appear after you launch the application. To prevent unauthorized access to the application, you must navigate through these message boxes within three minutes. Otherwise, you will be prompted to relaunch the application.

**NOTE:** If one or more **Security Alert** windows appear in the following steps, read the information in the window and click **Yes** to continue.

The management station connects to iDRAC6 and the remote system's desktop is displayed in **iDRACView**.

4 Two mouse pointers appear in the viewer window: one for the remote system and one for your local system. You must synchronize the two mouse pointers so that the remote mouse pointer follows your local mouse pointer. See "Synchronizing the Mouse Pointers" on page 230.

### Virtual Console Preview

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 automatically refreshed every 30 seconds.

**NOTE:** The Virtual Console image is available only if you have enabled Virtual Console.

Table 10-4 provides inforation about the available options.

**Table 10-4. Virtual Console Preview Options**

| Option | Descritpion |
|---|---|
| **Launch** | Click this button to launch the Virtual Console.<br>If only Virtual Media is enabled, then clicking this link directly launches the Virtual Media.<br>This button is disabled if you do not have Virtual Console privileges or if both Virtual Console and Virtual Media are disabled. |
| **Settings** | Click this link to view or edit the Virtual Console configuration settings on the **Virtual Console/Media Configuration** page. |
| **Refresh** | Click this button to refresh the displayed Virtual Console image. |

## Using the Video Viewer

The Video Viewer provides a user interface between the management station and the managed server, allowing you to see the managed server's desktop and control its mouse and keyboard functions from your management station. When you connect to the remote system, the Video Viewer starts in a separate window.

**NOTE:** The Virtual Console 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:
`<DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>`

The Video Viewer provides various control adjustments such as color mode, mouse synchronization, snapshots, keyboard macros, power actions, and access to Virtual Media. Click **Help** for more information on these functions.

When you start a Virtual Console session and the Video Viewer is displayed, you may need to adjust the color mode and synchronize the mouse pointers.

Table 10-5 describes the menu options that are available for use in the viewer.

**Table 10-5. Viewer Menu Bar Selections**

| Menu Item | Item | Description |
|---|---|---|
| **Video** | **Pause** | Temporarily pauses Virtual Console. |
| | **Resume** | Resumes Virtual Console. |
| | **Refresh** | Redraws the viewer screen image. |
| | **Capture Current Screen** | Captures the current remote system screen to a **.bmp** file. A dialog box is displayed that allows you to save the file to a specified location. |
| | **Full Screen** | To make the Video Viewer expand into full screen mode, click on the top right corner of the viewer to get the full screen. |
| | **Exit** | When you have finished using the Console and have logged out (using the remote system's log out procedure), select **Exit** from the **Video** menu to close the **Video Viewer** window. |
| **Keyboard** | Hold Right Alt Key | Select this item before typing keys you want to combine with the right <Alt> key. |
| | Hold Left Alt Key | Select this item before typing keys you want to combine with the left <Alt> key. |
| | Left Windows Key | Select **Hold Down** before typing characters you want to combine with the left Windows key. Select **Press and Release** to send a left Windows key keystroke. |
| | Right Windows Key | Select **Hold Down** before typing characters you want to combine with the right Windows key. Select **Press and Release** to send a right Windows key keystroke. |

**Table 10-5. Viewer Menu Bar Selections *(continued)***

| Menu Item | Item | Description |
|---|---|---|
| | **Macros** | When you select a macro, or enter the hotkey specified for the macro, the action is executed on the remote system. The Video Viewer provides the following macros:<br>• Alt+Ctrl+Del<br>• Alt+Tab<br>• Alt+Esc<br>• Ctrl+Esc<br>• Alt+Space<br>• Alt+Enter<br>• Alt+Hyphen<br>• Alt+F4<br>• PrtScrn<br>• Alt+PrtScrn<br>• F1<br>• Pause<br>• Alt+M<br>• Alt+D<br>• Alt+PrtScrn+M<br>• Alt+PrtScrn+P |
| | **Keyboard Pass-through** | The Keyboard pass-through mode allows all keyboard functions on the client to be redirected to the server. |
| **Mouse** | **Synchronize Cursor** | Synchronizes the cursor so that the mouse on the client is redirected to the mouse on the server. |
| | **Hide Local Cursor** | Only the cursor from the Virtual Console will be displayed. It is recommended this setting when running USC in a Virtual Console. |

**Table 10-5. Viewer Menu Bar Selections *(continued)***

| Menu Item | Item | Description |
|---|---|---|
| Options | Color Mode | Allows you to select a color depth to improve performance over the network. For example, if you are installing software from virtual media, you can choose the lowest color depth, so that less network bandwidth is used by the Virtual Console viewer leaving more bandwidth for transferring data from the media.<br>The color mode can be set to 15-bit color and 7-bit color. |
| Power | Power ON System | Powers on the system. |
| | Power OFF System | Powers off the system. |
| | Graceful Shutdown | Shuts down the system. |
| | Reset System (warm boot) | Reboots the system without powering it off. |
| | Power Cycle System (cold boot) | Powers off, and then reboots the system. |
| Media | Virtual Media Wizard | The **Media** menu provides access to the Virtual Media Wizard, which allows you to redirect to a device or image such as a:<br>• Floppy drive<br>• CD<br>• DVD<br>• Image in ISO format<br>• USB Flash drive<br>For information about the Virtual Media feature, see "Configuring and Using Virtual Media" on page 261.<br>You must keep the Virtual Console viewer window active when using Virtual Media. |

**Table 10-5. Viewer Menu Bar Selections *(continued)***

| Menu Item | Item | Description |
|---|---|---|
| Help | About iDRACView | Displays iDRACView Version. |

## Synchronizing the Mouse Pointers

When you connect to a remote Dell PowerEdge system using Virtual Console, the mouse acceleration speed on the remote system may not synchronize with the mouse pointer on your management station, causing two mouse pointers to appear in the Video Viewer window.

To synchronize the mouse pointers click **Mouse→ Synchronize cursor** or press <Alt><M>.

The Synchronize cursor menu item is a toggle. Ensure that there is a check mark next to the item in the menu so that the mouse synchronization is active.

When using Red Hat Enterprise Linux or Novell SUSE Linux, be sure to configure the mouse mode for Linux before you launch the viewer. See "Configuring Virtual Console and Virtual Media in iDRAC6 Web Interface" on page 222 for help with configuration. The operating system's default mouse settings are used to control the mouse arrow in iDRAC6 **Virtual Console** screen.

When two mouse cursors are seen on the client Virtual Console screen, it indicates that the server's operating system supports Relative Positioning. This is typical for Linux operating systems or Dell's Universal Server Configurator (USC) 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, you can switch to single cursor by selecting Single Cursor from the Tools menu (in the Virtual Console screen) or try to match the mouse acceleration on the server and client.

**NOTE:** This is not applicable for servers running Windows operating systems since they support Absolute Positioning.

When using the iDRAC Virtual Console to connect to a managed server 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, make 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`.

### Disabling or Enabling Local Console

You can configure iDRAC6 to disallow Virtual Console connections using iDRAC6 Web interface. When the local console is disabled, a yellow status dot is displayed in the list of servers (in the local console) to indicate that the console is locked in iDRAC6. When the local console is enabled, the status dot is green.

If you want to ensure that you have exclusive access to the managed server console, you must disable the local console *and* reconfigure the **Max Sessions** to `1` on the **Virtual Console** screen.

**NOTE:** By disabling (turning off) the local video on the server, the monitor, keyboard, and mouse connected to the Virtual Console are disabled.

To disable or enable the local console, perform the following procedure:

1. On your management station, open a supported Web browser and log in to iDRAC6. See "Accessing the Web Interface" on page 86 for more information.
2. Click **System**, click the **Virtual Console/Media** tab, and then click **Configuration**.
3. If you want to disable (turn off) local video on the server, in the **Configuration** screen, deselect **Local Server Video Enabled** and then click **Apply**. The default value is **Enabled (checked)**.
4. If you want to enable (turn on) local video on the server, in the **Configuration** screen, select **Local Server Video Enabled** and then click **Apply**.

The **Virtual Console** screen displays the status of the Local Server Video.

# Launching Virtual Console and Virtual Media Remotely

You can launch Virtual Console or Virtual Media by entering a single URL on a supported browser instead of launching it from iDRAC6 Web GUI. Depending on your system configuration, you will either go through the manual authentication process (login page) or will be directed to the Virtual Console or Virtual Media viewer (iDRACView) automatically.

**NOTE:** Internet Explorer supports Local, Active Directory (AD), Smart Card (SC) and Single Sign-On (SSO) logins. Firefox supports SSO, Local, and AD logins.

## URL Format

If you enter the link **https://<idrac6_ip>/console** in the browser, you may be required to go through the normal manual login procedure depending on the login configuration. If SSO is not enabled and Local, AD, or SC login is enabled, the corresponding login page is displayed. If the login is successful, the Virtual Console or Virtual Media view is not launched. Instead, you are redirected to iDRAC6 GUI home page.

**NOTE:** The URL used to launch **iDRACView** is case-sensitive and should be typed only in lower case.

## General Error Scenarios

Table 10-6 lists general error scenarios, the reasons for those errors, and iDRAC6 behavior.

**Table 10-6. Error Scenarios**

| Error Scenarios | Reason | Behavior |
|---|---|---|
| Login failed | You have entered either an invalid user name or an incorrect password. | Same behavior when *https://<ip>* is specified and login fails. |
| Insufficient Privileges | You do not have Virtual Console and virtual media privileges. | iDRACView is not launched and you are redirected to the Virtual Console/Media configuration GUI page. |

**Table 10-6. Error Scenarios *(continued)***

| Error Scenarios | Reason | Behavior |
|---|---|---|
| Virtual Console disabled | Virtual Console is disabled on your system. | iDRACView is not launched and you are redirected to the Virtual Console/Media configuration GUI page. |
| Unknown URL parameters detected | The URL you have entered contains undefined parameters. | Page not Found (404) message is displayed. |

# Frequently Asked Questions

Table 10-7 lists frequently asked questions and answers.

**Table 10-7. Using Virtual Console: Frequently Asked Questions**

| Question | Answer |
|---|---|
| Virtual Console fails to log out when the out–of–band Web GUI is logged out. | The Virtual Console and Virtual Media sessions stays active even if the Web session is logged off. Close the Virtual Media and Virtual Console viewer applications 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, once a local video turn **ON** request is received by iDRAC6 the video is turned on instantly. |
| Can the local user also turn off the video? | Yes, a local user can use the local RACADM CLI to turn off the video. |
| Can the local user also turn on the video? | No. Once the local console is disabled, the local user's keyboard and mouse are disabled and they are unable to change any settings. |

**Table 10-7. Using Virtual Console: Frequently Asked Questions *(continued)***

| Question | Answer |
|---|---|
| Does switching off the local video also switch off the local keyboard and mouse? | Yes. |
| 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 needed for an iDRAC6 user to turn on or off the local server video? | Any user with iDRAC6 configuration privileges can turn the local console on or off. |
| How can I get the current status of the local server video? | The status is displayed on the **Virtual Console and Virtual Media** screen of iDRAC6 Web interface.<br><br>The RACADM CLI command `racadm getconfig –g cfgRacTuning` displays the status in the object **cfgRacTuneLocalServerVideo**. This racadm command can be executed from Telnet/SSH or a remote session to iDRAC6.<br><br>The remote RACADM command is:<br><br>`racadm -r <idracip> -u <user> -p <password> getconfig -g cfgRacTuning`<br><br>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 the local console is locked by iDRAC6. |
| I cannot see the bottom of the system screen from the Virtual Console window. | Ensure that the management station's monitor resolution is set to 1280x1024. |

**Table 10-7. Using Virtual Console: Frequently Asked Questions *(continued)***

| Question | Answer |
|---|---|
| The console window is garbled. | The Virtual Console viewer on Linux requires a UTF-8 character set. Check your locale and reset the character set if needed. See "Setting the Locale in Linux" on page 71 for more information. |
| Why do I get a blank screen on the managed server when loading the Windows 2000 operating system? | The managed server does not have the correct ATI video driver. Update the video driver. |
| Why doesn't the mouse sync in DOS when performing 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. iDRAC6 has a USB mouse driver, which allows absolute position and closer tracking of the mouse pointer. Even if iDRAC6 passes the USB absolute mouse position to the Dell BIOS, the BIOS emulation would convert it back to relative position and the behavior would remain. To fix this problem, set the mouse mode to **USC/Diags** in the **Configuration** screen. |
| Why doesn't the mouse sync under the Linux text console(either in Dell Unified Server Configurator (USC), Dell Lifecycle Controller (LC) or in Dell Unified Server Configurator Lifecycle Controller Enabled (USC-LCE)? | Virtual Console requires the USB mouse driver, but the USB mouse driver is available only under the X-Window operating system. |

**Table 10-7. Using Virtual Console: Frequently Asked Questions *(continued)***

| Question | Answer |
|---|---|
| I am still having issues with mouse synchronization. | Ensure that the correct mouse is selected for your operating system before starting a Virtual Console session.<br><br>Ensure that **Synchronize Mouse** is checked in the **Mouse** menu. Press <Alt><M> or select **Mouse→ Synchronize mouse** to toggle mouse synchronization. When synchronization is enabled, a check mark is displayed next to the selection in the **Mouse** menu. |
| Why can't I use a keyboard or mouse while installing a Microsoft operating system remotely by using iDRAC6 Virtual Console? | When you remotely install a supported Microsoft operating system on a system with Virtual Console enabled in the BIOS, you receive an EMS Connection Message that requires that you select **OK** before you can continue. You cannot use the mouse to select **OK** remotely. You must either select **OK** on the local system or restart the remotely managed server, reinstall, and then turn Virtual Console off in the BIOS.<br><br>This message is generated by Microsoft to alert the user that Virtual Console is enabled. To ensure that this message does not appear, always turn off Virtual Console in the BIOS before installing an operating system remotely. |
| Why doesn't the Num Lock indicator on my management station reflect the status of the Num Lock on the remote server? | When accessed through iDRAC6, 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. |

**Table 10-7. Using Virtual Console: Frequently Asked Questions *(continued)***

| Question | Answer |
|---|---|
| Why do multiple Session Viewer windows appear when I establish a Virtual Console session from the local host? | You are configuring a Virtual Console session from the local system. This is not supported. |
| If I am running a Virtual Console session and a local user accesses the managed server, do I receive a warning message? | No. If a local user accesses the system, you both have control of the system. |
| How much bandwidth do I need to run a Virtual Console session? | It is recommended that you use a 5 MB/sec connection for good performance. A 1 MB/sec connection is required for minimal performance. |
| What are the minimum system requirements for my management station to run Virtual Console? | The management station requires an Intel Pentium III 500 MHz processor with at least 256 MB of RAM. |
| After launching the Virtual Console, I can only use the mouse on the Virtual Console and not on my local system. Why does this happen and what should I do to use the mouse on the Virtual Console and my local system? | This happens if the **Mouse Mode** is set to **USC/Diags**. Press <Alt><M> hot key to use the mouse on your local system. Press <Alt><M> again to use the mouse on the Virtual Console. |
| When I launch both the GUI and Virtual Console to iDRAC from the CMC Web interface, why does my GUI session timeout? | 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.<br><br>When launching both the GUI and Virtual Console to the same iDRAC system on a management station, a session timeout 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. |

**Table 10-7. Using Virtual Console: Frequently Asked Questions *(continued)***

| Question | Answer |
|---|---|
| Linux SysRq key is not working with Internet Explorer. Why? | The Linux SysRq key behavior is different when using Virtual Console from Internet Explorer. To send the SysRq key, the **Print Screen** key should be pressed and released while holding the **Ctrl** and **Alt** keys. Following are the steps to send the SysRq key to a remote Linux server though iDRAC, when using Internet Explorer:<br>**1** Activate the magic key function on the remote Linux server. You can use the following command to activate it on the Linux terminal.<br>`echo 1 > /proc/sys/kernel/sysrq`<br>**2** Activate the keyboard pass-through mode of Active X Viewer.<br>**3** Press **Ctrl** + **Alt** + **Print Screen**.<br>**4** Release only **Print Screen**.<br>**5** Press **Print Screen** + **Ctrl** + **Alt**.<br>**NOTE:** The SysRq feature is currently not supported with Internet Explorer and Java. |

# 11

# Configuring the vFlash SD Card and Managing vFlash Partitions

The vFlash SD card is a Secure Digital (SD) card that plugs into the optional iDRAC6 Enterprise card slot at the back corner of the system. It provides storage space that behaves like a common USB Flash Key device. It is the storage location for user-defined partition(s) that can be configured to be exposed to the system as a USB device and also used to create a bootable USB device. Depending on the emulation mode selected, the partitions will be exposed to the system as a floppy drive, and hard drive, or a CD/DVD drive. You can set any of these as a bootable device.

The vFlash SD cards and standard SD cards are supported. A *vFlash SD card* refers to the card that supports the new enhanced vFlash features. A *standard SD card* refers to a normal off-the-shelf SD card that supports only limited vFlash features.

With vFlash SD card, you can create up to 16 partitions. You can provide a label name for the partition when you create it and can perform a range of operations to manage and use the partitions. A vFlash SD card can be of any size up to 8 GB. Each partition can be up to 4 GB.

A standard SD card can be of any size but supports only one partition. The size of the partition is limited to 256 MB. The label name for the partition is VFLASH by default.

**NOTE:** Ensure that you only insert a vFlash SD card or standard SD card in the iDRAC6 Enterprise card slot. If you insert a card in any other format (example, Multi-Media Card (MMC)), the following error message is displayed when you initialize the card: *An error has occurred while initializing SD card.*

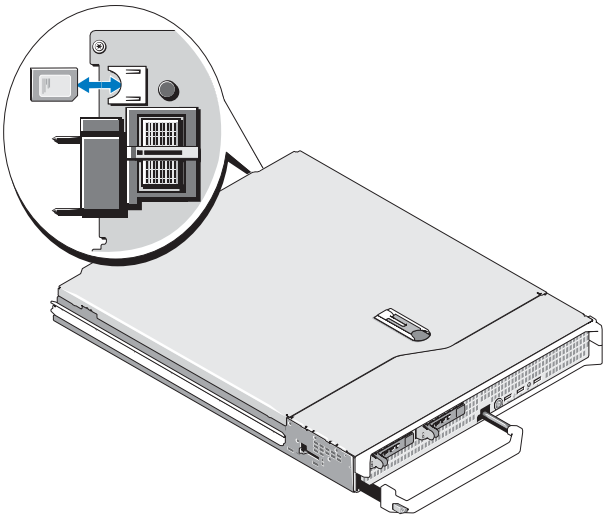
If you are an administrator, you can perform all operations on the vFlash partitions. If not, you must have Access Virtual Media privilege to create, delete, format, attach, detach, or copy the contents for the partition.

**NOTE:** You can only perform a single vFlash operation at a time. The first operation must be completed before you perform another vflash operation. For example, if you start a create from image operation using RACADM, you cannot perform a create, download, or format operation using RACADM or GUI. You must wait until the operation is complete before performing the next vFlash operation.

# Installing a vFlash or Standard SD Card

1. Remove the blade from the chassis.
2. Locate the vFlash media slot at the back corner of the system.

   **NOTE:** You do not need to remove the blade cover to install or remove the card.



3. With the label side facing up, insert the contact-pin end of the SD card into the card slot on the module.

   **NOTE:** The slot is keyed to ensure correct insertion of the card.
4. Press inward on the card to lock it into the slot.
5. Re-install the blade in the chassis.

### Removing a vFlash or Standard SD Card

To remove the vFlash or standard SD card, push inward on the card to release it, and pull the card from the card slot.

# Configuring vFlash or Standard SD Card Using iDRAC6 Web Interface

After you install the vFlash or standard SD card, you can view its properties, enable or disable vFlash, and initialize the card. The card must be enabled to perform partition management. When the card is disabled, you can only view its properties. The initialize operation removes existing partitions and resets the card.

**NOTE:** You must have Configure iDRAC permission to enable or disable vFlash, or to initialize the card.

If a card is not available in the system's iDRAC6 Enterprise card slot, the following error message is displayed.

```
SD card not detected. Please insert an SD card of size
256 MB or greater.
```

To view and configure the vFlash or standard SD card:

1. Open a supported Web browser window and log in to the iDRAC6 Web interface.
2. In the system tree, select **System**.
3. Click the **vFlash** tab. The **SD Card Properties** page is displayed.

   Table 11-1 lists the properties displayed for the SD card.

**Table 11-1. SD Card Properties**

| Attribute | Description |
|---|---|
| **Name** | Displays the name of the card installed in the server's iDRAC6 Enterprise card slot. If the card supports the new enhanced vFlash features, it displays *vFlash SD card*. If it supports limited vFlash features, it displays *SD card*. |
| **Size** | Displays the size of the card in gigabytes (GB). |

**Table 11-1. SD Card Properties *(continued)***

| Attribute | Description |
|---|---|
| Available Space | Displays the unused space on the SD card in MB. This space is available to create more partitions on the vFlash SD card.<br>If the inserted SD card is uninitialized, then the available space displays that the card is uninitialized. |
| Write Protected | Displays whether the card is write-protected or not. |
| Health | Displays the overall health of the SD card. This can be:<br>• OK<br>• Warning<br>• Critical<br>If it is warning, re-initialize the card.<br>If it is critical, reinstall and reinitialize the card. |
| vFlash Enable | Select the checkbox to perform vFlash partition management on the card. Clear the checkbox to disable vFlash partition management. |

4 Click **Apply** to enable or disable vFlash partition management on the card.

If any vFlash partition is attached, you cannot disable vFlash and an error message is displayed.

**NOTE:** If vFlash is disabled, you can only view the SD card properties and will not be able to perform other vFlash operations such as create partition (empty and using an image file), manage partitions, format partitions, and download contents of a partition.

5 Click **Initialize**. All existing partitions are removed and the card is reset. A confirmation message is displayed.

6 Click **OK**. After the initialize operation is complete, a success message is displayed.

**NOTE:** **Initialize** is available only if you select the **vFlash Enable** option.

If any vFlash partition is attached, the initialize operation fails and an error message is displayed.

If you click any option on the vFlash pages when an application such as WSMAN provider, iDRAC6 Configuration Utility, or RACADM is using vFlash, or if you navigate to some other page in the GUI, iDRAC6 may display the following message.

```
SD card is temporarily unavailable. To retry, click
Refresh.
```

# Configuring vFlash or Standard SD Card Using RACADM

You can view and configure the vFlash or standard SD card using RACADM commands from local, remote, or Telnet/SSH console.

**NOTE:** You must have Configure iDRAC permission to enable or disable vFlash, and initialize the card.

## Displaying the vFlash or Standard SD Card Properties

Open a telnet/SSH/Serial console to the server, log in, and enter the following command:

```
racadm getconfig -g cfgvFlashSD
```

The following read-only properties are displayed:

- `cfgvFlashSDSize`
- `cfgvFlashSDLicense`
- `cfgvFlashSDAvailableSize`
- `cfgvFlashSDHealth`

### Enabling or Disabling the vFlash or Standard SD Card

Open a telnet/SSH/Serial console to the server, log in, and enter the following command:

- To enable vFlash or standard SD card:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable
  1
  ```

- To disable vFlash or standard SD card:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable
  0
  ```

**NOTE:** The RACADM command functions only if a vFlash or standard SD card is present. If a card is not present, the following message is displayed: *ERROR: SD Card not present*.

### Initializing the vFlash or Standard SD Card

Open a telnet/SSH/Serial console to the server, log in, and enter the following command:

```
racadm  vflashsd  initialize
```

All existing partitions are deleted and the card is reset.

### Getting the Last Status on the vFlash or Standard SD Card

Open a telnet/SSH/Serial console to the server, log in, and enter the following command to get the status of the last command sent to the vFlash or standard SD card:

```
racadm vFlashsd status
```

### Resetting the vFlash or Standard SD Card

Open a telnet/SSH/Serial console to the server, log in, and enter:

```
racadm vflashsd initialize
```

For more information about `vflashsd`, see the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

**NOTE:** The `racadm vmkey reset` command is deprecated from 1.5 release onwards. The functionality of this command is now covered by `vflashsd initialize`. While execution of the `vmkey reset` command will be successful, it is recommended to use the `vflashsd initialize` command. For more information, see "Initializing the vFlash or Standard SD Card" on page 244.

# Managing vFlash Partitions Using iDRAC6 Web Interface

You can perform the following:

- Create an empty partition
- Create a partition using an image file
- Format a partition
- View available partitions
- Modify a partition
- Attach/Detach a partition
- Delete existing partitions
- Download the contents of a partition
- Boot to a partition

### Creating an Empty Partition

An empty partition is similar to an empty USB key. You can create empty partitions on a vFlash or standard SD card. You can choose to create partitions of type *Floppy* or *Hard Disk*. The partition type CD is not supported for creating empty partitions.

**NOTE:** You must have Access Virtual Media privilege to create empty partitions.

Before creating an empty partition, ensure the following:

- The card is initialized.
- The card is not write-protected.
- An initialize operation is not already being performed on the card.

To create an empty vFlash partition:

1. On the iDRAC6 Web interface, select **System→ vFlash** tab**→ Create Empty Partition** subtab. The **Create Empty Partition** page is displayed.
2. Enter the information mentioned in Table 11-2.
3. Click **Apply**. A new partition is created.

**NOTE:** When create partition is in-progress, the progress or status is not 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 requested partition size is greater than 4 GB.
- An initialize operation is already being performed on the card.

**NOTE:** The new partition is unformatted (RAW).

**Table 11-2. Create Empty Partition Page Options**

| Field | Description |
|---|---|
| **Index** | Select a partition index. Only unused indices are displayed in the drop-down list. The lowest available index is selected by default. You can change it to any other index value from the drop-down list.<br>**NOTE:** For the standard SD card, only index 1 is available. |
| **Label** | Enter a unique label for the new partition. The label name can contain up to six alphanumeric characters. Do not include any space in the label name. The characters are displayed in upper case.<br>**NOTE:** For the standard SD card, the label name must be VFLASH. If not, an error message is displayed. |

**Table 11-2. Create Empty Partition Page Options**

| Field | Description |
|---|---|
| **Emulation Type** | Select the emulation type for the partition from the drop-down list. The available options are **Floppy** and **HDD**. |
| **Size** | Enter the partition size in Megabytes (MB). The maximum partition size is 4 GB, or less than or equal to the available space on the vFlash SD card.<br>**NOTE:** For the standard SD card, the partition size can be up to 256 MB. |

## Creating a Partition Using an Image File

You can create a new partition on vFlash or standard SD card using an image file (available in the **.img** or **.iso** format.) You can create a partition of type Floppy, Hard Disk, or CD. The created partition is read-only.

**NOTE:** You must have Access Virtual Media privileges to create partitions.

The size of the newly created partition is equal to the image file size. The image file size must be:

- Less than or equal to the available space on the card.
- Less than or equal to 4 GB. The maximum partition size is 4 GB.

Using the Web interface, the size of image that can be uploaded to the vFlash SD card is limited to a maximum of 2 GB on both 32-bit and 64-bit browsers (Internet Explorer and FireFox).

Using the RACADM and WSMAN interface, the image size that can be uploaded to a vFlash SD card is a maximum of 4 GB.

For the standard SD card, the image size must be less than or equal to 256 MB.

Before creating a partition from an image file, ensure the following:

- The card is initialized.
- The card is not write-protected.
- An initialize operation is not already being performed on the card.

**NOTE:** When creating partition from an image file, ensure that the image type and the emulation type match. iDRAC emulates the device based on the image type specified. There may be issues when the uploaded image and the emulation type do not match. For example, if the partition is created using an ISO image and the emulation type is specified as Hard Disk, then the BIOS will not be able to boot from this image.

To create a vFlash partition using an image file:

1. On the iDRAC6 Web interface, select **System→ vFlash** tab**→ Create from Image** subtab. The **Create Partition from Image File** page is displayed.
2. Enter the information mentioned in Table 11-3.
3. Click **Apply**. A new partition is created using the image file.

**NOTE:** When create partition is in-progress, the progress or status is not displayed.

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.

**Table 11-3. Create Partition from Image File Page Options**

| Field | Description |
|---|---|
| **Index** | Select a partition index. Only unused indices are displayed in the drop-down list. The lowest available index is selected by default. You can change it to any other index value from the drop-down list.<br>**NOTE:** For the standard SD card, only index 1 is available. |

**Table 11-3. Create Partition from Image File Page Options**

| Field | Description |
|---|---|
| **Label** | Enter a unique label for the new partition. This can contain up to six alphanumeric characters. Do not include spaces in the label name. The characters are displayed in upper case.<br>**NOTE:** For the standard SD card, the label name must be VFLASH. If not, an error message is displayed. |
| **Emulation Type** | Select the emulation type for the partition from the drop-down list. The available options are **Floppy**, **HDD**, and **CDROM**. |
| **Image Location** | Click **Browse** and specify the image file location. Only **.img** or **.iso** file types are 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. The standard SD card with limited vFlash features supports only the FAT32 format.

You can only format Hard Disk or Floppy partitions. Formatting CD partitions is not supported. You cannot format read-only partitions.

**NOTE:** You must have Access Virtual Media privileges to format partitions.

Before formating the partition, ensure the following:

- The card is enabled.
- The partition is not attached.
- The card is not write-protected.
- An initialize operation is not already being performed on the card.

To format vFlash partition:

1. On the iDRAC6 Web interface, select **System**→ **vFlash** tab→ **Format** subtab. The **Format** page is displayed.
2. Enter the information mentioned in Table 11-4.

3 Click **Apply**. A warning message indicating that all the data on the partition will be erased is displayed. Click **OK**. The selected partition is formated with 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.

**Table 11-4. Format Partition Page Options**

| Field | Description |
|---|---|
| **Label** | Select the partition label that you want to format. The first available partition is selected by default.<br>All existing partitions of type Floppy or Hard Disk are available in the drop-down list. Partitions that are attached or that are read-only are not available in the drop-down list. |
| **Type to Format to** | Select the file system type you want to format the partition to. The available options are EXT2, EXT3, FAT16, and FAT32. For the standard SD card, only FAT32 is available. |

### Viewing Available Partitions

Ensure that the vFlash or standard SD card is enabled to view the list of available partitions.

To view the available partitions on the card:

1. On the iDRAC6 Web interface, select **System→ vFlash→ Manage** subtab. The **Manage Partitions** page lists the available partitions.
2. For each partition, you can view the information mentioned in Table 11-5.

**Table 11-5. Viewing Available Partitions**

| Field | Description |
|---|---|
| **Index** | Partitions are indexed from 1 to 16. The partition index is unique for a particular partition. It is specified when the partition is created. |
| **Label** | Identifies the partition. It is specified when the partition is created. |
| **Size** | Size of the partition in Megabytes (MB). |
| **Read Only** | Read-write access state of the partition.<br>• Checked = Read-only partition.<br>• Unchecked=Read-write partition<br>**NOTE:** For the standard SD card, the partition is read-write, and this column is not displayed. |
| **Attached** | Indicates whether the partition is visible to the operating system as a USB device. To attach or detach partitions, see the section "Attaching and Detaching Partition" on page 252. |
| **Type** | Displays whether the partition type is Floppy, Hard Disk or CD. |

### Modifying a Partition

Ensure that the card is enabled to modify the partition.

**NOTE:** You must have Access Virtual Media privileges to modify a vFlash partition.

You can change a read-only partition to read-write or vice-versa. To do this:

1. On the iDRAC6 Web interface, select **System→ vFlash** tab→ **Manage** subtab. The **Manage Partitions** page is displayed.
2. In the **Read Only** column, select the checkbox for the partition(s) that you want to change to read-only or clear the checkbox for the partition(s) that you want to change to read-write.

**NOTE:** If the partition is of type CD, the state is read-only and the checkbox is selected. You cannot change the state to read-write.
If the partition is attached, the checkbox is grayed-out.
For the standard SD card, the partition is read-write and the **Read Only** column is not displayed.

3. Click **Apply**. The partitions are changed to read-only or read-write based on the selections.

### Attaching and Detaching Partition

You can attach one or more paritions as virtual USB mass storage devices such that they are visible to the operating system and BIOS as mass storage devices. When multiple paritions are attached simultaneously, they are presented in ascending order to the host operating system based on the index. The corresponding drive letter assignments are controlled by the operating system.

If you detach a partition, it is no longer seen as a virtual USB mass storage device in the host operating system and it is removed from the BIOS boot order menu.

If you are attaching or detaching a partition, the USB bus of the system is reset. This may affect any applications (like the operating system) that are using vFlash and will disconnect any iDRAC Virtual Media sessions.

**NOTE:** You must have Access Virtual Media privileges to attach or detach a partition.

Before attaching or detaching a partition, ensure the following:

- The card is enabled.
- An initialize operation is not already being performed on the card.

To attach or detach partitions:

1. On the iDRAC6 Web interface, select **System→ vFlash** tab→ **Manage** subtab. The **Manage Partitions** page is displayed.
2. In the **Attached** column, select the checkbox for the partition(s) that you want to attach or clear the checkbox for the partition(s) that you want to detach.

**NOTE:** The detached partitions are not displayed in the boot sequence.

3. Click **Apply**. The partitions are attached or detached based on the selections.

#### Operating System Behavior for Attached Paritions

When partitions are attached and the host operating system is Windows, the drive letters that is assigned to the attached partitions are controlled by the operating system.

If a partition is read-only, it will be read-only as seen in the host operating system.

If the host operating system does not support the file system of an attached partition, you cannot read or modify the contents of the partition from the host operating system. For example, partition type EXT2 cannot be read from Windows operating system.

When you change the label name of an attached partition from the host operating system, it does not impact the label name stored by iDRAC for that partition.

### Deleting Existing Partitions

**NOTE:** You can delete existing partitions for the vFlash or standard SD card.

Before deleting existing partition(s), ensure the following:

- The card is not write-protected.
- The partition is not attached.
- An initialize operation is not already being performed on the card.

**NOTE:** You must have Access Virtual Media privileges to modify a partition.

To delete an existing partition:

1. On the iDRAC6 Web interface, select **System**→ **vFlash** tab→ **Manage** subtab. The **Manage Partitions** page is displayed.
2. In the **Delete** column, click the delete icon for the partition(s) that you want to delete and click **Apply**. The partition(s) are deleted.

### Downloading Partition Contents

You can download the contents of a vFlash partition to a local or remote location as an image file in the **.img** or **.iso** format. Local location is on your management system where iDRAC6 Web interface is operated from. Remote location is on a managed system.

**NOTE:** You must have Access Virtual Media privileges to download partitions.

Before downloading the contents to a local or remote location, ensure the following:

- The card is enabled.
- An initialize operation is not already being performed on the card.
- For a read-write partition, it must not be attached.

To download the contents of the vFlash partition to a location on your system:

1. On the iDRAC6 Web interface, select **System**→ **vFlash** tab→ **Download** subtab. The **Download Partition** page is displayed.
2. From the **Label** drop-down menu, select a partition that you want to download. All existing partitions are displayed in the list except partitions that are attached. The first partition is selected by default.
3. Click **Download**.

4 Specify the location to save the file.

If only the folder location is specified, then the partition label is used as the file name, along with the extension **.iso** for CD type partitions and **.img** for floppy and hard-disk type partitions.

5 Click **Save**. The contents of the selected partition are downloaded to the specified location.

### Booting to a Partition

You can set an attached vFlash partition as the boot device for the next boot operation. The vFlash partition must contain a bootable image (in the **.img** or **.iso** format) to set it as a boot device. Ensure that the card is enabled to set a partition as a boot device and to perform the boot operation.

**NOTE:** You must have Access Virtual Media privileges to set a partition as the boot device.

You can perform the boot operation for the vFlash or standard SD card. For the steps, see the section "First Boot Device" on page 46.

**NOTE:** If the system BIOS does not support vFlash as the first boot device, then the attached vFlash partition(s) may not be listed in the **First Boot Device** drop-down menu. Therefore, ensure that you update the BIOS to the latest version that supports setting the vFlash partition as the first boot device. If the BIOS is the latest version, then rebooting the server will cause the BIOS to inform iDRAC that it supports vFlash as the first boot device and iDRAC lists the vFlash partition in the **First Boot Device** drop-down menu.

## Managing vFlash Partitions Using RACADM

You can use the `vFlashPartition` subcommand to create, delete, list, or view the status of partitions on an already initialized vFlash or standard SD card. The format is:

```
racadm vflashpartition <create | delete | status |
list> <options>
```

**NOTE:** You must have Access Virtual Media privileges to perform vFlash partition management.

**Valid Options**:

| | |
|---|---|
| -i <index> | Index of the partition for which this command applies. <index> must be an integer from 1 to 16.<br>**NOTE:** For the standard SD card, index value is limited to 1 because only one partition of size 256 MB is supported. |

**Options only valid for the create action:**

| | |
|---|---|
| -o <label> | Label that is shown when the partition is mounted on the operating system.<br><label> must be a string up to six alphanumeric characters and must not contain spaces. |
| -e <type> | Emulation type for the partition. <type> must be floppy, cdrom, or HDD. |

-t <type> Create a partition of type <type>. <type> must be:

- empty - Create an empty partition.
  - -s <size> - Partition size in MB.
  - -f <type>- Format type for the partition based on the type of file system. Valid options are RAW, FAT16, FAT32, EXT2, or EXT3.
- image - Create a partition using an image file. The following options are valid with the image type:
  - -l <path> - Specifies the remote path relative to the iDRAC. The path can be on a mounted drive or share:
    SMB path: //<ip or domain>/<share_name>/<path_to_image>
    NFS path: <ipaddress>:/<path_to_image>
  - -u <user> - Username for accessing the remote image.

-p <password> - Password for accessing the remote image.

**Options only valid for the status action:**

-i Displays the status of the partition index.

### Creating a Partition

- To create a 20 MB empty partition:

```
racadm vflashpartition create -i 1 -o drive1 -t
empty -e HDD -f fat16 -s 20
```

- To create a partition using an image file on a remote system:

```
racadm vflashpartition create –i 1 –o drive1 –e
HDD –t image –l //myserver/sharedfolder/foo.iso –u
root –p mypassword
```

**NOTE:** Creating a partition using an image file is not supported in local RACADM.

### Deleting a Partition

- To delete a partition:

  ```
  racadm vflashpartition delete -i 1
  ```

- To delete all partitions, re-initialize the vFlash SD card. For information, see "Initializing the vFlash or Standard SD Card" on page 244.

### Getting the Status of a Partition

- To get the status of an operation on partition 1:

  ```
  racadm vflashpartition status -i 1
  ```

- To get the status of all existing partitions:

  ```
  racadm vflashpartition status -a
  ```

### Viewing Partition Information

To list all existing partitions and their properties:

```
racadm vflashpartition list
```

### Booting to a Partition

- To list the available devices in the boot list:

  ```
  racadm  getconfig –g cfgServerInfo –o
  cfgServerFirstBootDevice
  ```

  If it is a vFlash SD card, the label names of the attached partitions appear in the boot list. If it is a standard SD card and if the partition is attached, then VFLASH is displayed in the boot list.

- To set a vFlash partition as a boot device:

  ```
  racadm  config –g cfgServerInfo –o
  cfgServerFirstBootDevice “<vFlash partition name>”
  ```

  where, <vFlash partition name> is the label name for the vFlash SD card or VFLASH for the standard SD card.

When you run this command, the vFlash partition label is automatically set to boot once, that is, **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.

### Attaching or Detaching a Partition

- 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
```

### Modifying a 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
```

For more information about the RACADM subcommands and iDRAC6 property database group and object definitions, see the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

# Frequently Asked Questions

### When is the vFlash or standard SD card locked?

The virtual flash media is locked by iDRAC when the operation it is performing needs exclusive access to the media. For example, during an initialize operation.

### In local RACADM, sometimes after creating a partition, if you try to delete the same partition, an error message is displayed. Why?

This may happen because the create partition operation is in-progress. However, the partition will be 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.

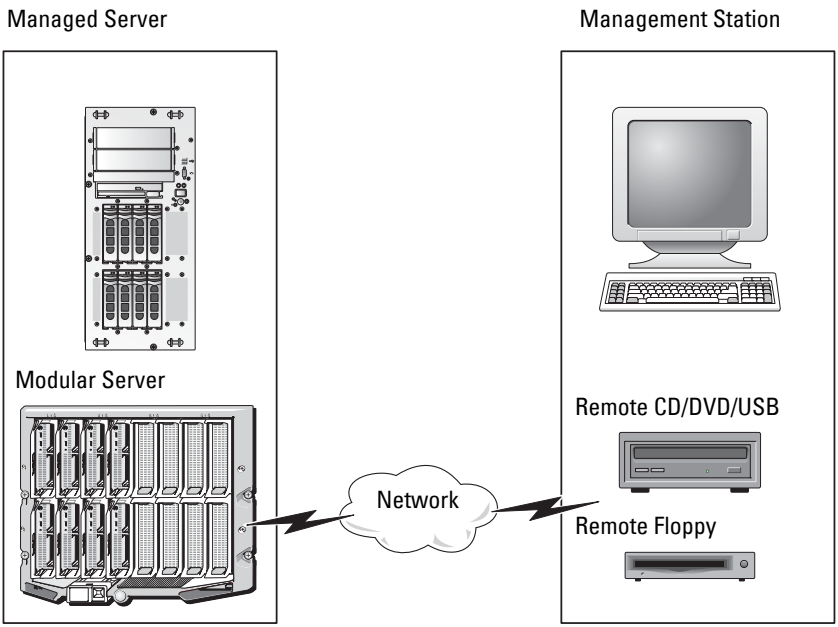
# 12

# Configuring and Using Virtual Media

## Overview

The Virtual Media feature, accessed through the Virtual Console viewer, provides the managed server access to media connected to a remote system on the network. Figure 12-1 shows the overall architecture of Virtual Media.

**Figure 12-1. Overall Architecture of Virtual Media**



Using Virtual Media, administrators can remotely boot their managed servers, install applications, update drivers, or even install new operating systems remotely from the virtual CD/DVD and diskette drives.

**NOTE:** Virtual Media requires a minimum available network bandwidth of 128 Kbps.

Virtual Media defines two devices for the managed server's operating system and BIOS: a floppy disk device and an optical disk device.

The management station provides the physical media or image file across the network. When Virtual Media is connected, all virtual CD/floppy drive access requests from the managed server are directed to the management station across the network. Connecting Virtual Media is displayed the same as inserting media into physical devices on the managed system. When Virtual Media is in attached state, virtual devices on the managed system appear as two drives without the media being installed in the drives.

Table 12-1 lists the supported drive connections for virtual floppy and virtual optical drives.

**NOTE:** Changing Virtual Media while connected could stop the system boot sequence.

**Table 12-1. Supported Drive Connections**

| Supported Virtual Floppy Drive Connections | Supported Virtual Optical Drive Connections |
|---|---|
| Legacy 1.44 floppy drive with a 1.44 floppy diskette | CD-ROM, DVD, CDRW, combination drive with CD-ROM media |
| USB floppy drive with a 1.44 floppy diskette | CD-ROM/DVD image file in the ISO9660 format |
| 1.44 floppy image | USB CD-ROM drive with CD-ROM media |
| USB removable disk (minimum size 128 MB) | |

## Windows-Based Management Station

To run the Virtual Media feature on a management station running the Windows operating system, install a supported version of Internet Explorer with the ActiveX Control plug-in. Set the browser security to **Medium** or a lower setting to enable Internet Explorer to download and install signed ActiveX controls.

Depending on your version of Internet Explorer, a custom security setting for ActiveX may be required:

1. Start Internet Explorer.
2. Click **Tools→ Internet Options**, and then click the **Security** tab.
3. Under **Select a Web content zone to specify its security settings**, click to select the desired zone.
4. Under **Security level for this zone**, click **Custom Level**.

   The **Security Settings** window is displayed.
5. Under **ActiveX controls and plugins**, ensure that the following settings are set to **Enable**:
   - Allow Scriptlets
   - Automatic prompting for ActiveX controls
   - Download signed ActiveX controls
   - Download unsigned ActiveX controls
6. Click **OK** to save any changes and close the **Security Settings** window.
7. Click **OK** to close the **Internet Options** window.
8. Restart Internet Explorer.

You must have administrator rights to install ActiveX. 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.

### Linux-Based Management Station

To run the virtual media feature on a management station running the Linux operating system, install a supported version of Firefox.

A Java Runtime Environment (JRE) is required to run the Virtual Console plugin. You can download a JRE from **java.sun.com**.

# Configuring Virtual Media

1. Log in to iDRAC6 Web interface.
2. Click **System→ Virtual Console/Media→ Configuration**.
3. In the Virtual Media section, select values for the settings. See Table 12-2 for information on Virtual Media configuration values.
4. Click **Apply** to save your settings.

   An alert dialog is displayed with the following message: `You are about to change device configuration. All existing redirection sessions will be closed. Do you want to continue?`
5. Click **OK** to continue.

   An alert dialog is displayed with the following message: `Virtual Media Configuration successfully set.`

**Table 12-2. Virtual Media Configuration Values**

| Attribute | Value |
|---|---|
| Attach Virtual Media | **Attach** — Immediately attaches Virtual Media to the server.<br>**Detach** — Immediately detaches Virtual Media from the server.<br>**Auto-Attach** — Attaches Virtual Media to the server only when a Virtual Media session is started. |
| Maximum Sessions | Displays the maximum number of Virtual Media sessions allowed. This value is always **1**.<br>**NOTE:** Only one virtual media user session is allowed; however, multiple devices can be attached in a single session. See "Running Virtual Media" on page 265. |
| Active Sessions | Displays the number of Virtual Media sessions that are currently active. |
| Virtual Media Encryption Enabled | Enables (checked) or disables (not checked) encryption on Virtual Media connections. |

**Table 12-2. Virtual Media Configuration Values *(continued)***

| Attribute | Value |
|---|---|
| Floppy Emulation | Indicates whether the Virtual Media is displayed as a floppy drive or as a USB key to the server. If **Floppy Emulation** is selected, the Virtual Media device is displayed as a floppy device on the server. If it is deselected, it is displayed as a USB Key drive.<br>**NOTE:** On certain Windows Vista and Red Hat Enterprise Linux environments, you may not be able to virtualize a USB with **Floppy Emulation** enabled. |
| Enable Boot Once | Enables (checked) or disables (not checked) the boot-once option, which automatically terminates the Virtual Media session after the server has booted once. Use this attribute to boot from the Virtual Media. On the next boot, the system will boot from the next device in the boot order. This option is useful for automated deployments. |

# Running Virtual Media

**CAUTION: Do not issue a racreset command when running a Virtual Media session. Otherwise, undesirable results may occur, including data loss.**

**NOTE:** The Virtual Console viewer window application must remain active while you access the virtual media.

1. Open a supported Web browser on your management station.
2. Log in to iDRAC6 Web interface.
3. Click the **Virtual Console/Media** tab.

   The **Virtual Console and Virtual Media** screen is displayed.

To change the values of any of the displayed attributes, see "Configuring Virtual Media" on page 264.

**NOTE:** The **Floppy Image File** under **Floppy Drive** (if applicable) may appear, as this device can be virtualized as a virtual floppy. You can select one optical drive and one floppy at the same time, or a single drive.

**NOTE:** The virtual device drive letters on the managed server do not coincide with the physical drive letters on the management station.

**NOTE:** Virtual Media may not function properly on Windows operating system clients that are configured with Internet Explorer Enhanced Security. To resolve this issue, see your Microsoft operating system documentation or contact your administrator.

4 Click **Launch Virtual Console**.

**NOTE:** On Linux, the file **jviewer.jnlp** is downloaded to your desktop and a dialog box will ask what to do with the file. Choose the option to **Open with program** and then select the **javaws** application, which is located in the **bin** subdirectory of your JRE installation directory.

**iDRACView** application launches in a separate window.

5 Select **Media→ Virtual Media Wizard.**

The **Media Redirection** window is displayed.

6 View the **Status** section at the bottom of the **Media Redirection** window. If media is connected, you can disconnect it before connecting a different media source. To disconnect media, click the **Disconnect** button next to the media in the **Status** window.

7 Select the radio button next to the media types you want to connect.

8 You can select both the **Floppy Image** radio button and one of the radio buttons in the **CD/DVD Drive** section.

**NOTE:** When a management station CD/DVD media is already in use by iDRAC6 blade, the same media can be redirected and made available to another iDRAC6 blade. In other words, iDRAC6 supports same media (Read only) redirection to two different iDRAC6 blades. But with an USB media, you will not be able to attach to two iDRAC6 blades. iDRAC6 displays a warning message indicating the same.

To connect a floppy image or ISO image, enter the path to the image location on your local computer, or click the **Browse** button to navigate to the image location.

**NOTE:** You may not be able to mount remote ISO images if you use the Java based Virtual Media plug–in. For example, Linux clients will not allow you to mount the images since they use the Java based plug–in. To avoid this, copy the ISO image to your local system to make the image file available locally. The Java based Virtual Media plug–in does not allow you to specify the share name using **\\computer\share** format.

9 Click the **Connect** button next to each selected media type.

The media is connected and the **Status** window is updated.

10 Click **Close**.

**NOTE:** Whenever a Virtual Media session is initiated or a vFlash is connected, an extra drive named "LCDRIVE" is displayed on the host operating system and the BIOS. The extra drive disappears when the vFlash or the Virtual Media session is disconnected.

### Disconnecting Virtual Media

1 Select **Media→ Virtual Media Wizard.**

The **Media Redirection Wizard** is displayed.

2 Click **Disconnect** next to the media you wish to disconnect.

The media is disconnected and the **Status** window is updated.

3 Click **Close**.

**NOTE:** When you launch **iDRACview** and then log out of the Web GUI, **iDRACView** does not terminate and remains active.

### Booting From Virtual Media

The system BIOS enables you to boot from virtual optical drives or virtual floppy drives. During POST, enter the BIOS setup window and verify that the virtual drives are enabled and listed in the correct order.

To change the BIOS setting, perform the following steps:

1 Boot the managed server.

2 Press <F2> to enter the BIOS setup window.

3 Scroll to the boot sequence and press <Enter>.

In the pop-up window, the virtual optical drives and virtual floppy drives are listed with the standard boot devices.

4 Ensure 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 Save the changes and exit.

The managed server reboots.

The managed server 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.

### Installing Operating Systems Using Virtual Media

This section describes a manual, interactive method to install the operating system on your management station that may take several hours to complete. A scripted operating system installation procedure using Virtual Media may take fewer than 15 minutes to complete. See "Deploying the Operating System" on page 337 for more information.

1 Verify the following:

- The operating system installation DVD/CD is inserted in the management station's DVD/CD drive.
- The local DVD/CD drive is selected.
- You are connected to the virtual drives.

2 Follow the steps for booting from the Virtual Media in the "Booting From Virtual Media" on page 267 section to ensure that the BIOS is set to boot from the DVD/CD drive from which you are installing.

3 Follow the on-screen instructions to complete the installation.

### Using Virtual Media When the Server's Operating System Is Running

#### Windows-Based Systems

On Windows systems, the Virtual Media drives are automounted if they are attached and configured with a drive letter.

Using the virtual drives from within Windows is similar to using your physical drives. When you connect to the media using the Virtual Media wizard, the media is available at the system by clicking the drive and browsing its content.

#### Linux-Based Systems

Depending on the configuration of the software on your system, the Virtual Media drives may not be automounted. If your drives are not automounted, manually mount the drives using the Linux **mount** command.

## Frequently Asked Questions

Table 12-3 lists frequently asked questions and answers.

**Table 12-3. Using Virtual Media: Frequently Asked Questions**

| Question | Answer |
|---|---|
| Sometimes, I notice my Virtual Media client connection drop. Why? | When a network time-out occurs, iDRAC6 firmware drops the connection, disconnecting the link between the server and the Virtual Drive.<br>If the Virtual Media configuration settings are changed in iDRAC6 Web interface or by local RACADM commands, any connected media is disconnected when the configuration change is applied.<br>To reconnect to the Virtual Drive, use the Virtual Media wizard. |
| Which operating systems support iDRAC6? | See "Supported Operating Systems" on page 24 for a list of supported operating systems. |
| Which Web browsers support iDRAC6? | See "Supported Web Browsers" on page 25 for a list of supported Web browsers. |

**Table 12-3. Using Virtual Media: Frequently Asked Questions *(continued)***

| Question | Answer |
|---|---|
| Why do I sometimes lose my client connection? | • You can sometimes lose your client connection if the network is slow or if you change the CD in the client system CD drive. For example, if you change the CD in the client system's CD drive, the new CD might have an autostart feature. If this is the case, the firmware can time out and the connection can be lost if the client system takes too long before it is ready to read the CD. If a connection is lost, reconnect from the GUI and continue the previous operation.<br>• When a network timeout occurs, iDRAC6 firmware drops the connection, disconnecting the link between the server and the Virtual Drive. Also, someone may have altered the Virtual Media configuration settings in the Web interface or by entering RADACM commands. To reconnect to the Virtual Drive, use the Virtual Media feature. |
| An installation of the Windows operating system seems to take too long. Why? | If you are installing the Windows operating system and have a slow network connection, the installation procedure may require an extended amount of time to access iDRAC6 Web interface due to network latency. While the installation window does not indicate the installation progress, the installation procedure is in progress. |
| I am viewing the contents of a floppy drive or USB memory key. If I try to establish a Virtual Media connection using the same drive, I receive a connection failure message and am asked to retry. Why? | Simultaneous access to Virtual Floppy drives is not allowed. Close the application used to view the drive contents before you attempt to virtualize the drive. |
| How do I configure my virtual device as a bootable device? | On the managed server, access the BIOS Setup and navigate to the boot menu. Locate the virtual CD, Virtual Floppy, or vFlash and change the device boot order as needed. For example, to boot from a CD drive, configure the CD drive as the first drive in the boot order. |

**Table 12-3. Using Virtual Media: Frequently Asked Questions *(continued)***

| Question | Answer |
|---|---|
| What types of media can I boot from? | iDRAC6 allows you to boot from the following bootable media:<br>• CDROM/DVD Data media<br>• ISO 9660 image<br>• 1.44 Floppy disk or floppy image<br>• A USB key that is recognized by the operating system as a removable disk (minimum size 128 MB)<br>• A USB key image |
| How can I make my USB key bootable? | Search **support.dell.com** for the Dell Boot Utility, a Windows program you can use to make your Dell USB key bootable.<br>You can also boot with a Windows 98 startup disk and copy system files from the startup disk to your USB key. For example, from the DOS prompt, enter the following command:<br>`sys a: x: /s`<br>where *x*: is the USB key you want to make bootable. |
| What file system types are supported on my Virtual Floppy Drive? | Your Virtual Floppy Drive supports FAT16 or FAT32 file systems. |
| When I performed a firmware update remotely using iDRAC6 Web interface, my virtual drives at the server were removed. Why? | Firmware updates cause iDRAC6 to reset, drop the remote connection, and unmount the virtual drives. The drives will reappear when iDRAC6 reset is complete. |

**Table 12-3. Using Virtual Media: Frequently Asked Questions *(continued)***

| Question | Answer |
|---|---|
| I cannot locate my Virtual Floppy device on a system running Red Hat Enterprise Linux or the SUSE Linux operating system. My Virtual Media is attached and I am connected to my remote floppy. What should I do? | Some Linux versions do not automount the Virtual Floppy Drive and the Virtual CD drive in a similar manner. To mount the Virtual Floppy Drive, locate the device node that Linux assigns to the Virtual Floppy Drive. Perform the following steps to correctly find and mount the Virtual Floppy Drive:<br>**1** Open a Linux command prompt and run the following command:<br>`grep "Virtual Floppy" /var/log/messages`<br>**2** Locate the last entry to that message and note the time.<br>**3** At the Linux prompt, run the following command:<br>`grep "hh:mm:ss" /var/log/messages` where:<br>`hh:mm:ss` is the time stamp of the message returned by grep in step 1.<br>**4** In step 3, read the result of the grep command and locate the device name that is given to the Dell Virtual Floppy.<br>**5** Ensure that you are attached and connected to the Virtual Floppy Drive.<br>**6** At the Linux prompt, run the following command:<br>mount */dev/sdx* /mnt/floppy<br>where:<br>`/dev/sdx` is the device name found in step 4<br>`/mnt/floppy` is the mount point. |

# 13

# Using the RACADM Command Line Interface

The RACADM command line interface (CLI) provides access to iDRAC6 management features on the managed server. RACADM provides access to most of the features on iDRAC6 Web interface. RACADM can be used in scripts to ease configuration of multiple servers, instead of using the Web interface, which, is more useful for interactive management.

The following interfaces are available for RACADM:

- Local RACADM
- Remote RACADM
- Telnet/SSH RACADM

Local RACADM commands do not use network connections to access iDRAC6 from the managed server. This means that you can use local RACADM commands to configure the initial iDRAC6 networking. Remote RACADM is a client side utility, which can be executed from a management station through the out of band network interface. SSH/Telnet RACADM is used to refer to the RACADM command usage from a SSH or Telnet prompt.

This section provides the following information:

- RACADM commands and supported RACADM interfaces
- Using local RACADM from a command prompt
- Remote RACADM
- SSH/Telnet RACADM
- Configuring iDRAC6 using the **racadm** command
- Using the RACADM configuration file to configure multiple iDRAC6s

**CAUTION: The latest iDRAC6 firmware supports only the latest RACADM version. You may encounter errors if you use an older version of RACADM to query iDRAC6 with the latest firmware. Install the RACADM version shipped with your latest Dell OpenManage DVD media.**

# RACADM Subcommands

Table 13-1 provides a description of each RACADM subcommand that you can run in RACADM. For a detailed listing of RACADM subcommands including syntax and valid entries, see the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

**Table 13-1. RACADM Subcommands**

| Command | Description |
|---|---|
| **arp** | Displays the contents of the ARP table. ARP table entries cannot be added or deleted. |
| **clearasrscreen** | Clears the last crash (ASR) screen. |
| **closessn** | Closes a communication session on the device. |
| **coredump** | Displays the last iDRAC6 core dump. |
| **coredumpdelete** | Deletes the core dump stored in iDRAC6. |
| **clrraclog** | Clears iDRAC6 log. After clearing, a single entry is made to indicate the user and time that the log was cleared. |
| **clrsel** | Clears the iDRAC System Event Log entries. |
| **config** | Configures iDRAC6. |
| **fwupdate** | Updates iDRAC6 firmware. |
| **getconfig** | Displays the current iDRAC6 configuration properties. |
| **getniccfg** | Displays the current IP configuration for the controller. |
| **getraclog** | Displays iDRAC6 log. |
| **getractime** | Displays iDRAC6 time. |
| **getsel** | Displays SEL entries. |
| **getssninfo**[1] | Displays information about active sessions. |
| **getsvctag** | Displays the service tag. |

**Table 13-1. RACADM Subcommands *(continued)***

| Command | Description |
|---|---|
| **getsysinfo** | Displays information about iDRAC6 and the managed server, including IP configuration, hardware model, firmware versions, and operating system information. |
| **gettracelog** | Displays iDRAC6 trace log. If used with `-i`, the command displays the number of entries in iDRAC6 trace log. |
| **help** | Lists iDRAC6 subcommands. |
| **help <subcommand>** | Lists usage statement for the specified subcommand. |
| **ifconfig** | Displays the contents of the network interface table. |
| **krbkeytabupload** | Uploads a Kerberos keytab file. |
| **localconredirdisable** | Performs local Virtual Console disable from the local system. |
| **netstat** | Displays the routing table and the current connections. |
| **ping** | Verifies that the destination IP address is reachable from iDRAC6 with the current routing-table contents. A destination IP address is required. An ICMP echo packet is sent to the destination IP address based on the current routing-table contents. |
| **ping6** | Verifies that the destination IPv6 address is reachable from iDRAC6 with the current routing-table contents. A destination IPv6 address is required. An ICMP echo packet is sent to the destination IPv6 address based on the current routing-table contents. |
| **racdump** | Displays status and general iDRAC6 information. |
| **racreset** | Resets iDRAC6. |
| **racresetcfg** | Resets iDRAC6 to the default configuration. |
| **remoteimage** | Remote file share |
| **serveraction** | Performs power management operations on the managed server. |
| **setniccfg** | Sets the IP configuration for the controller. |
| **sshpkauth** | Enables you to upload up to 4 different SSH public keys, delete existing keys, and view the keys already in iDRAC6. |

**Table 13-1. RACADM Subcommands *(continued)***

| Command | Description |
|---|---|
| **sslcertdownload** | Downloads a CA certificate or server certificate from iDRAC. |
| **sslcertupload** | Uploads a CA certificate or server certificate to iDRAC6. |
| **sslcertview** | Views a CA certificate or server certificate in iDRAC6. |
| **sslcsrgen** | Generates and downloads the SSL CSR. |
| **testemail** | Forces iDRAC6 to send an e-mail over iDRAC6 NIC. |
| **testtrap** | Forces iDRAC6 to send an SNMP alert over iDRAC6 NIC. |
| **traceroute** | Traces the network path of routers that packets take as they are forwarded from your system to a destination IPv4 address. |
| **traceroute6** | Traces the network path of routers that packets take as they are forwarded from your system to a destination IPv6 address. |
| **version** | Displays iDRAC6 version information. |
| **vflashsd** | Initializes or gets the status of the vflash SD card. |
| **vflashpartition** | Creates, deletes, lists, or view the status of partitions on an initialized vFlash SD card. |
| **vmdisconnect** | Closes all open iDRAC6 virtual media connections from remote clients. |
| **vmkey** | Resets the vFlash partition to the default size of 256 MB and removes all data from the partition. |

[1] SOL session information is not included in the response to the getssninfo command.

# Using local RACADM Commands

You run RACADM commands locally (on the managed server) from a command prompt or shell prompt.

Log in to the managed server, start a command shell, and enter local RACADM commands in one of the following formats:

- `racadm <subcommand> [parameters]`
- `racadm <getconfig|config> [-g <group>] [-o <object> <value>]`

Without options, the RACADM command displays general use information. To display the RACADM subcommand list, enter:

```
racadm help
```

or

```
racadm getconfig -h
```

The subcommand list includes all RACADM commands that are supported by iDRAC6.

To get help for a subcommand, enter:

```
racadm help <subcommand>
```

The command displays the syntax and command-line options for the subcommand.

**NOTE:** The usage of characters other than the non-alpha numeric characters such as $ , % , <, > , | etc are not recommended for RACADM command arguments. Usage of them may result in unexpected behavior.

# Using the RACADM Utility to Configure iDRAC6

This section describes how to use RACADM to perform various iDRAC6 configuration tasks.

### Displaying Current iDRAC6 Settings

The RACADM **getconfig** subcommand retrieves current configuration settings from iDRAC6. The configuration values are organized into *groups* containing one or more *objects*, and the objects have *values*.

See the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals** for a complete description of the groups and objects.

To display a list of all iDRAC6 groups, enter this command:

```
racadm getconfig -h
```

To display the objects and values for a particular group, enter this command:

```
racadm getconfig -g <group>
```

For example, to display a list of all **cfgLanNetworking** group object settings, enter the following command:

```
racadm getconfig -g cfgLanNetworking
```

### Managing iDRAC6 Users with RACADM

**NOTE:** Use caution when using the **racresetcfg** command, as *all* configuration parameters are reset to the original defaults. Any previous changes are lost.

**NOTE:** If you are configuring a new iDRAC6 or if you ran the **racadm racresetcfg** command, the only current user is **root** with the password **calvin**.

**NOTE:** Users can be enabled and disabled over time. As a result, a user may have a different index number on each iDRAC6.

**NOTE:** Users and groups created for Active Directory environments must conform to the Active Directory naming convention.

You can configure up to 15 users in iDRAC6 property database. (A sixteenth user is reserved for the IPMI LAN user.) Before you manually enable an iDRAC6 user, verify if any current users exist.

To verify if a user exists, enter the following command at the command prompt:

```
racadm getconfig -u <username>
```

OR

enter the following command once for each index from 1 to 16:

```
racadm getconfig -g cfgUserAdmin -i <index>
```

**NOTE:** You can also enter `racadm getconfig -f <filename>` and view the generated <*filename*> file, which includes all users, as well as all other iDRAC6 configuration parameters.

Several parameters and object IDs are displayed with their current values. Two objects of interest are:

```
# cfgUserAdminIndex=nn
```

```
cfgUserAdminUserName=
```

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 assigned to that user name.

**NOTE:** Users and groups created for Active Directory environments must conform to the Active Directory naming convention.

## Adding an iDRAC6 User

To add a new user to iDRAC6, perform the following steps:

1. Set the user name.
2. Set the password.
3. Set the Login to iDRAC6 user privilege.
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 iDRAC6:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2 123456

racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i 2 0x00000001

racadm config -g cfgUserAdmin -o cfgUserAdminEnable
-i 2 1
```

To verify the new user, use one of the following commands:

```
racadm getconfig -u john

racadm getconfig –g cfgUserAdmin –i 2
```

## Enabling an iDRAC6 User With Permissions

To grant a user a specific administrative (role-based) permissions, set the **cfgUserAdminPrivilege** property to a bitmask constructed from the values show in Table 13-2:

**Table 13-2. Bit Masks for User Privileges**

| User Privilege | Privilege Bit Mask |
|---|---|
| Login to iDRAC6 | 0x00000001 |
| Configure iDRAC6 | 0x00000002 |
| Configure Users | 0x00000004 |

**Table 13-2. Bit Masks for User Privileges *(continued)***

| User Privilege | Privilege Bit Mask |
|---|---|
| Clear Logs | 0x00000008 |
| Execute Server Control Commands | 0x00000010 |
| Access Virtual Console | 0x00000020 |
| Access Virtual Media | 0x00000040 |
| Test Alerts | 0x00000080 |
| Execute Debug Commands | 0x00000100 |

For example, to allow the user **Configure iDRAC6**, **Configure Users**, **Clear Logs,** and **Access Virtual Console** privileges, add the values 0x00000002, 0x00000004, 0x00000008, and 0x00000010 to construct the bitmap 0x0000002E. Then enter the following command to set the privilege:

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i 2 0x0000002E
```

## Uploading, Viewing, and Deleting SSH Keys Using RACADM

### Upload

The upload mode allows you to upload a keyfile or to copy the key text on the command line. You cannot upload and copy a key at the same time.

From local RACADM:

```
racadm sshpkauth -i <2 to 16> -k <1 to 4> -f
<filename>
```

From telnet/ssh RACADM:

```
racadm sshpkauth -i <2 to 16> -k <1 to 4> -t
<key-text>
```

Example:

Upload a valid key to iDRAC6 User 2 in the first key space using a file:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

PK SSH Authentication Key file successfully uploaded to the RAC.

**CAUTION: The "file" option is not supported on telnet/ssh/serial RACADM.**

**View**

The view mode allows the user to view a key specified by the user or all keys.

```
racadm sshpkauth -i <2 to 16> -v -k <1 to 4>
racadm sshpkauth -i <2 to 16> -v -k all
```

**Delete**

The delete mode allows the user to delete a key specified by the user or all keys.

```
racadm sshpkauth -i <2 to 16> -d -k <1 to 4>
racadm sshpkauth -i <2 to 16> -d -k all
```

**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.**

See sshpkauth in the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals** for information on the subcommand options.

## Removing an iDRAC6 User

When using RACADM, the iDRAC user cannot be deleted. The user can only be disabled using the **cfgUserAdminEnable** object. The command syntax is:

```
racadm config –g cfgUserAdmin –o cfgUserAdminEnable –I
<index>
```

For more information on managing user admins, see the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

## Testing E-mail Alerting

iDRAC6 e-mail alert feature allows users to receive e-mail alerts when a critical event occurs on the managed server. The following example shows how to test the e-mail alert feature to ensure that iDRAC6 can properly send e-mail alerts across the network.

```
racadm testemail -i 2
```

(-i 2 is for the index entry #2 in the e–mail alert table)

**NOTE:** Ensure that the SMTP and E-mail Alert settings are configured before testing the e-mail alert feature. See "Configuring E-Mail Alerts" on page 96 for more information.

### Testing iDRAC6 SNMP Trap Alert Feature

iDRAC6 SNMP trap alerting feature allows SNMP trap listener configurations to receive traps for system events that occur on the managed server.

The following example shows how a user can test the SNMP trap alert feature.

```
racadm testtrap -i 2
```

(-i 2 is for the index entry #2 in the e–mail alert table)

**NOTE:** Before you test iDRAC6 SNMP trap alerting feature, ensure that the SNMP and trap settings are configured correctly. See the **testtrap** and **testemail** subcommand descriptions to configure these settings. See "Configuring Platform Event Traps (PET)" on page 95 for more information.

### Configuring iDRAC6 Network Properties

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

```
racadm getconfig -g cfgLanNetworking
```

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

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

The commands provide the same configuration functionality as iDRAC6 Configuration Utility when you are prompted to press <Ctrl><E>. For more information about configuring network properties with iDRAC6 Configuration Utility, see "iDRAC6 LAN" on page 349.

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

```
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
```

**NOTE:** If **cfgNicEnable** is set to **0**, iDRAC6 LAN is disabled even if DHCP is enabled.

### Configuring IPMI Over LAN

1 Configure IPMI over LAN by entering the following command:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

**NOTE:** This setting determines the IPMI commands that can be executed from the IPMI over LAN interface. For more information, see the IPMI 2.0 specifications.

a Update the IPMI channel privileges by entering the following command:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit <level>
```

where `<level>` is one of the following:

- 2 (User)
- 3 (Operator)
- 4 (Administrator)

For example, to set the IPMI LAN channel privilege to 2 (User), enter the following command:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit 2
```

b Set the IPMI LAN channel encryption key, if required, using a command such as the following:

**NOTE:** iDRAC6 IPMI supports the RMCP+ protocol. See the IPMI 2.0 specifications for more information.

```
racadm config -g cfgIpmiLan -o
cfgIpmiEncryptionKey <key>
```

where <*key*> is a 20-character encryption key in a valid hexadecimal format.

2 Configure IPMI Serial over LAN (SOL) using the following command:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

**NOTE:** The IPMI SOL minimum privilege level determines the minimum privilege required to activate IPMI SOL. For more information, see the IPMI 2.0 specification.

**a** Update the IPMI SOL minimum privilege level using the following command:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege <level>
```

where `<level>` is one of the following:

- 2 (User)
- 3 (Operator)
- 4 (Administrator)

For example, to configure the IPMI privileges to 2 (User), enter the following command:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege 2
```

**NOTE:** To redirect the serial console over LAN, ensure that the SOL baud rate is identical to your managed server's baud rate.

**b** Update the IPMI SOL baud rate using the following command:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate <baud-rate>
```

where `<baud-rate>` is 19200, 57600, or 115200 bps.

For example:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate 57600
```

**c** Enable SOL by typing the following command at the command prompt.

**NOTE:** SOL can be enabled or disabled for each individual user.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable 1 -i <id>
```

where `<id>` is the user's unique ID.

## Configuring PEF

You can configure the action you wish iDRAC6 to take for each platform alert. Table 13-3 lists the possible actions and the value to identify them in RACADM.

**Table 13-3. Platform Event Action**

| Action | Value |
|---|---|
| No action | 0 |
| Power off | 1 |
| Reboot | 2 |
| Power Cycle | 3 |

Configure PEF actions using the following command:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction
-i <index> <action-value>
```

where <*index*> is the PEF index (Table 5-7), and <*action-value*> is a value from Table 13-3.

For example, to enable PEF to reboot the system and send an IPMI alert when a processor critical event is detected, enter the following command:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction
-i 9 2
```

## Configuring PET

1. Enable global alerts using the following command:

   ```
   racadm config -g cfgIpmiLan -o
   cfgIpmiLanAlertEnable 1
   ```

2. Enable PET using the following command:

   ```
   racadm config -g cfgIpmiPet -o
   cfgIpmiPetAlertEnable -i <index> <0|1>
   ```

   where <*index*> is the PET destination index and `0` or `1` disable PET or enable PET, respectively.

   For example, to enable PET with index 4, enter the following command:

   ```
   racadm config -g cfgIpmiPet -o
   cfgIpmiPetAlertEnable -i 4 1
   ```

3 Configure your PET policy using the following command:

```
racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertDestIPAddr -i <index> <IP-address>
```

where <*index*> is the PET destination index and <*IP-address*> is the destination IP address of the system that receives the platform event alerts.

4 Configure the Community Name string.

At the command prompt, enter:

```
racadm config -g cfgIpmiLan -o
cfgIpmiPetCommunityName <name>
```

where <*name*> is the PET Community Name.

#### Configuring E-mail Alerts

1 Enable global alerts by entering the following command:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Enable e-mail alerts by entering the following commands:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i <index> <0|1>
```

where <*index*> is the e-mail destination index and 0 disables the e-mail alert or 1 enables the alert. The e-mail destination index can be a value from 1 through 4.

For example, to enable e-mail with index 4, enter the following command:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 4 1
```

3 Configure your e-mail settings by entering the following command:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertAddress -i 1 <email-address>
```

where 1 is the e-mail destination index and <*email-address*> is the destination e-mail address that receives the platform event alerts.

4 To configure the SMTP e–mail server, enter the following command:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSmtpServerIpAddr <SMTP E-mail Server IP
Address>
```

5 To configure a custom message, enter the following command:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertCustomMsg -i <index> <custom-message>
```

where <*index*> is the e-mail destination index and <*custom-message*> is the custom message.

6 Test the configured e-mail alert, if desired, by entering the following command:

```
racadm testemail -i <index>
```

where <*index*> is the e-mail destination index to test.

### Configuring IP Filtering (IP Range)

IP address filtering (or *IP Range Checking*) allows iDRAC6 access only from clients or management workstations whose IP addresses are within a user-specified range. All other login requests are denied.

IP filtering compares the IP address of an incoming login to the IP address range that is specified in the following **cfgRacTuning** properties:

- **cfgRacTuneIpRangeAddr**
- **cfgRacTuneIpRangeMask**

The **cfgRacTuneIpRangeMask** property is applied to both the incoming IP address and to the **cfgRacTuneIpRangeAddr** properties. If the results are identical, the incoming login request is allowed to access iDRAC6. Logins from IP addresses outside this range receive an error.

The login proceeds if the following expression equals zero:

```
cfgRacTuneIpRangeMask & (<incoming-IP-address> ^
cfgRacTuneIpRangeAddr)
```

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

See cfgRacTuning in the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals** for a complete list of cfgRacTuning properties.

**Table 13-4. IP Address Filtering (IPRange) Properties**

| Property | Description |
|---|---|
| **cfgRacTuneIpRangeEnable** | Enables the IP range checking feature. |
| **cfgRacTuneIpRangeAddr** | Determines the acceptable IP address bit pattern, depending on the 1's in the subnet mask.<br>This property is bitwise *and*ed with **cfgRacTuneIpRangeMask** to determine the upper portion of the allowed IP address. Any IP address that contains this bit pattern in its upper bits is allowed to log in. Logins from IP addresses that are outside this range fail. The default values in each property allow an address range from 192.168.1.0 to 192.168.1.255 to log in. |
| **cfgRacTuneIpRangeMask** | Defines the significant bit positions in the IP address. The mask should be in the form of a netmask, where the more significant bits are all 1's with a single transition to all zeros in the lower-order bits. |

Following are examples using local RACADM to set up IP filtering.

**NOTE:** See "Using the RACADM Command Line Interface" on page 275 for more information about RACADM and RACADM commands.

1 The following RACADM commands block all IP addresses except 192.168.0.57:

```
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
```

2 To restrict logins to a small 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, as shown below:

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

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.252
```

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

#### IP Filtering Guidelines

Use the following guidelines when enabling IP filtering:

- Ensure that **cfgRacTuneIpRangeMask** is configured in the form of a netmask, where all most significant bits are 1's (which defines the subnet in the mask) with a transition to all 0's in the low-order bits.
- Use the desired range's base address as the value of **cfgRacTuneIpRangeAddr**. The 32-bit binary value of this address should have zeros in all the low-order bits where there are zeros in the mask.

### Configuring IP Blocking

IP blocking dynamically determines when excessive login failures occur from a particular IP address and blocks (or prevents) the address from logging in to iDRAC6 for a preselected time span.

The IP blocking features include:

- The number of allowed login failures (**cfgRacTuneIpBlkFailcount**)
- The time frame in seconds during which these failures must occur (**cfgRacTuneIpBlkFailWindow**)
- The amount of time in seconds that the blocked IP address is prevented from establishing a session after the allowed number of failures is exceeded (**cfgRacTuneIpBlkPenaltyTime**)

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

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

See the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals** for a complete list of **cfgRacTune** properties.

Table 13-5 lists the user-defined parameters.

**Table 13-5. Log In Retry Restriction (IP Blocking) Properties**

| Property | Definition |
|---|---|
| **cfgRacTuneIpBlkEnable** | Enables the IP blocking feature.<br>When consecutive failures (**cfgRacTuneIpBlkFailCount**) from a single IP address are encountered within a specific amount of time (**cfgRacTuneIpBlkFailWindow**), all further attempts to establish a session from that address are rejected for a certain time span (**cfgRacTuneIpBlkPenaltyTime**). |
| **cfgRacTuneIpBlkFailCount** | Sets the number of login failures from an IP address before the login attempts are rejected. |
| **cfgRacTuneIpBlkFailWindow** | The time frame in seconds during which the failure attempts are counted. When the failures exceed this limit, they are dropped from the counter. |
| **cfgRacTuneIpBlkPenaltyTime** | Defines the time span in seconds that login attempts from an IP address with excessive failures are rejected. |

#### Enabling IP Blocking

The following example prevents a client IP address from establishing a session for five minutes if that client has failed five login attempts in a one-minute period of time.

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindow 60
```

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 300
```

The following example prevents more than three failed attempts within one minute, and prevents additional login attempts for an hour.

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 3600
```

### Configuring iDRAC6 Telnet and SSH Services Using Local RACADM

The Telnet/SSH console can be configured locally (on the managed server) using RACADM commands.

**NOTE:** You must have **Configure iDRAC6** permission to execute the commands in this section.

**NOTE:** When you reconfigure Telnet or SSH settings in iDRAC6, any current sessions are terminated without warning.

To enable Telnet and SSH from the local RACADM, log in to the managed server and enter the following commands at a command prompt:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

To disable the Telnet or SSH service, change the value from `1` to `0`:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 0

racadm config -g cfgSerial -o cfgSerialSshEnable 0
```

Enter the following command to change the Telnet port number on iDRAC6:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort
<new port number>
```

For example, to change the Telnet port from the default 23 to 8022, enter this command:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort
8022
```

For a complete list of available RACADM CLI commands, see "Using the RACADM Command Line Interface" on page 275.

## Remote and SSH/Telnet RACADM

Remote RACADM is a client side utility, which can be executed from a management station through the out of band network interface. A remote capability option (**-r**) is provided that allows you to connect to the managed system and execute RACADM subcommands from a remote console or management station. To use the remote capability, you need a valid user name (**-u** option) and password (**-p** option), and iDRAC6 IP address. SSH/Telnet RACADM is used to refer to the RACADM command usage from a SSH or Telnet prompt.

The maximum number of simultaneous remote RACADM sessions is four. These sessions are independent and in addition to the Telnet and SSH sessions. iDRAC6 can simultaneously support four SSH sessions and four Telnet sessions, in addition to the four RACADM sessions.

**NOTE:** Configure the IP address on your iDRAC6 before using the RACADM remote capability.

**NOTE:** If the system from where you are accessing the remote system does not have an iDRAC6 certificate in its default certificate store, a message is displayed when you type a RACADM command.

```
Security Alert: Certificate is invalid - Name on
Certificate is invalid or does not match site name

Continuing execution. Use -S option for racadm to
stop the execution on certificate-related errors.
```

RACADM continues to execute the command. However, if you use the **–S** option, RACADM stops executing the command and displays the following message:

```
Security Alert: Certificate is invalid - Name on
Certificate is invalid or does not match site name

Racadm not continuing execution of the command.
```

```
ERROR: Unable to connect to iDRAC6 at specified
IP address
```

**NOTE:** When using the RACADM remote capability, you must have write permissions on the folders where you are using the RACADM subcommands involving file operations, for example:

```
racadm getconfig -f <file name>
```

or

```
racadm sslcertdownload -t <type> [-f <filename>]
```

### Remote RACADM Usage

```
racadm -r <iDRAC6 IP Address> -u <username> -p
<password> <subcommand> <subcommand options>
```

```
racadm -i -r <iDRAC6 IP Address> <subcommand>
<subcommand options>
```

For example:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
```

```
racadm -i -r 192.168.0.120 getsysinfo
```

If the HTTPS port number of iDRAC6 has been changed to a custom port other than the default port (443), the following syntax must be used:

```
racadm -r <iDRAC6 IP Address>:<port> -u <username> -p
<password> <subcommand> <subcommand options>
```

```
racadm -i -r <iDRAC6 IP Address>:<port> <subcommand>
<subcommand options>
```

### Remote RACADM Options

Table 13-6 lists the options for the remote RACADM command.

**Table 13-6. RACADM Command Options**

| Option | Description |
|---|---|
| -r <*racIpAddr*> | Specifies the controller's remote IP address. |
| -r <*racIpAddr*>:<*port number*> | Use:<*port number*> if iDRAC6 port number is not the default port (443) |

**Table 13-6. RACADM Command Options *(continued)***

| Option | Description |
|---|---|
| -i | Instructs RACADM to interactively query the user for user name and password. |
| -u <*usrName*> | Specifies the user name that is used to authenticate the command transaction. If the **-u** option is used, the **-p** option must be used, and the **-i** option (interactive) is not allowed. |
| -p <*password*> | Specifies the password used to authenticate the command transaction. If the **-p** option is used, the **-i** option is not allowed. |
| -S | Specifies that RACADM should check for invalid certificate errors. RACADM stops the execution of the command with an error message if it detects an invalid certificate. |

**NOTE:** The usage of characters other than the non-alpha numeric characters such as $ , % , <, > , | etc are not recommended for RACADM command arguments. Usage of them may result in unexpected behavior.

# Using an iDRAC6 Configuration File

An iDRAC6 configuration file is a text file that contains a representation of the values in iDRAC6 database. You can use the RACADM **getconfig** subcommand to generate a configuration file containing the current values from iDRAC6. You can then edit the file and use the RACADM **config -f** subcommand to load the file back into iDRAC6, or to copy the configuration to other iDRAC6s.

## Creating an iDRAC6 Configuration File

The configuration file is a plain text file. You can use any valid file name; however, the **.cfg** file extension is the recommended convention.

The configuration file can be:

- Created with a text editor
- Obtained from iDRAC6 with the RACADM **getconfig** subcommand

- Obtained from iDRAC6 with the RACADM **getconfig** subcommand and then edited

To obtain a configuration file with the RACADM **getconfig** command, enter the following command:

```
racadm -r <remote iDRAC6 IP> -u <user> -p <password>
getconfig -f myconfig.cfg
```

This command creates the file **myconfig.cfg** in the current directory.

### Configuration File Syntax

**NOTE:** Edit the configuration file with a plain text editor, such as **Notepad** on Windows or **vi** on Linux. The **racadm** utility parses ASCII text only. Any formatting confuses the parser and may corrupt iDRAC6 database.

This section describes the format of the configuration file.

- Lines that start with # are comments.

  A comment *must* start in the first column of the line. A # character in any other column is treated as a normal # character.

  **Example**:

  ```
  #
  # This is a comment
  [cfgUserAdmin]
  cfgUserAdminPrivilege=4
  ```

- 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 *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

  The following example displays a group name, object, and the object's property value.

  Example:

`[cfgLanNetworking]` (*group name*)

`cfgNicIpAddress=192.168.1.1` (*object name*)

- Parameters are specified as *object*=*value* pairs with no white space between the object, =, and value.

  White space that is included after the value is ignored. 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).

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

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

- 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 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:

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

- 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 *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

### Modifying iDRAC6 IP Address in a Configuration File

When you modify iDRAC6 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 will be 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
```

### Loading the Configuration File Into iDRAC6

The command `racadm config -f <filename>` parses the configuration file to verify that valid group and object names are present and that syntax rules are followed. If the file is error-free the command then updates iDRAC6 database with the contents of the file.

**NOTE:** To verify the syntax only and not update iDRAC6 database, add the -**c** option to the **config** subcommand.

Errors in the configuration file are flagged with the line number and a message that explains the problem. You must correct all errors before the configuration file can update iDRAC6.

**NOTE:** Use the **racresetcfg** subcommand to reset the database and iDRAC6 NIC settings to the original default settings and remove all users and user configurations. While the root user is available, other users' settings are also reset to the default settings.

Before you execute the `racadm config -f <filename>` command, you can run the `racresetcfg` subcommand to reset iDRAC6 to its default settings. Ensure that the configuration file you will load includes all desired objects, users, indexes, and other parameters.

To update iDRAC6 with the configuration file, execute the following command:

```
racadm -r <remote iDRAC6 IP> -u <user> -p <password>
config -f myconfig.cfg
```

After the command has completed, you can execute the RACADM **getconfig** subcommand to confirm that the update succeeded.

## Configuring Multiple iDRAC6s

Using a configuration file, you can configure other iDRAC6s with identical properties. Follow these steps to configure multiple iDRAC6s:

1. Create the configuration file from iDRAC6 settings you want to replicate to the others. Enter the following command:

   ```
   racadm -r <remote iDRAC6 IP> -u <user> -p
   <password> getconfig -f <filename>
   ```

   where *<filename>* is the name of a file to save iDRAC6 properties, such a **myconfig.cfg**.

   The below example shows how you can use remote RACADM commands to configure multiple iDRAC6s. Create a batch file on the management station and call remote racadm commands from the batch file.

   For example:

   ```
   racadm -r <Server IP 1> -u <user> -p <password>
   config -f myconfig.cfg

   racadm -r <Server IP 2> -u <user> -p <password>
   config -f myconfig.cfg

   ...
   ```

   See "Creating an iDRAC6 Configuration File" on page 297 for more information.

   **NOTE:** Some configuration files contain unique iDRAC6 information (such as the static IP address) that must be modified before you export the file to other iDRAC6s.

2. Edit the configuration file you created in the previous step and remove or comment-out any settings you *do not* want to replicate.
3. Copy the edited configuration file to a network drive where it is accessible to each managed server whose iDRAC6 you want to configure.
4. For each iDRAC6 you want to configure:
   a. Log in to the managed server and start a command prompt.
   b. If you want to reconfigure iDRAC6 from the default settings, enter the following command:

```
racadm racresetcfg
```

**c** Load the configuration file into iDRAC6 with the following command:

```
racadm -r <remote iDRAC6 IP> -u <user> -p
<password> config -f <filename>
```

where *<filename>* is the name of the configuration file you created. Include the full path if the file is not in the working directory.

**d** Reset iDRAC6 that was configured by entering the following command:

```
racadm racreset
```

# 14

# Power Monitoring and Power Management

Dell PowerEdge systems incorporate many new and enhanced power management features. The entire platform, from hardware to firmware to systems management software, has been designed with a focus on power efficiency, power monitoring, and power management.

**NOTE:** iDRAC6 power management logic utilizes a Complex Programmable Logic Device (CPLD) present in the blade server. A few platforms also support an extended CPLD. Updates to CPLD devices are available at the Dell Support website at **support.dell.com** under the **System Firmware** or **System Board** sections. It is recommended that you update your blade server with the latest CPLD firmware version. The current CPLD and the extended CPLD firmware versions (for applicable platforms) is displayed in iDRAC6 Web GUI.

Dell PowerEdge systems provide many features for monitoring and managing power:

- **Power Monitoring:** iDRAC6 collects a history of power measurements and calculates running averages, peaks, and so on. Using iDRAC6 Web interface, you can view the information on the **Power Monitoring** screen. You can also view the information in graph form by clicking **Show Graph** at the bottom of the **Power Monitoring** screen. See "Power Monitoring" on page 306 for more information.
- **Power Budgeting:** At boot, a system inventory enables a system power budget of the current configuration to be calculated. See "Power Budgeting" on page 309 for more information.
- **Power Control:** iDRAC6 enables you to remotely perform several power management actions on the managed system. See "Power Control" on page 314 for more information.

# Configuring and Managing Power

You can use iDRAC6 Web interface and RACADM command line interface (CLI) to manage and configure power controls on the Dell PowerEdge system. Specifically, you can:

- View the power status of the server. See "Viewing Power Monitoring" on page 307.
- View power budget information for the server, including the minimum and maximum potential power consumption. See "Viewing Power Budget" on page 311.
- View power budget threshold for the server. See "Power Budget Threshold" on page 312.
- View power allocated to the PCIe expansion-cards in the server. See "Viewing and Modifying PCIe Power Allocation" on page 313.
- Execute power control operations on the server (for example, power on, power off, system reset, power cycle, and graceful shutdown). See "Executing Power Control Operations on the Server" on page 314.

# Power Monitoring

iDRAC6 monitors the power consumption in Dell PowerEdge servers continuously. iDRAC6 calculates the following power values and provides the information through its Web interface or RACADM CLI:

- Cumulative System Power
- System Peak Power and System Peak Amperage
- Average, Minimum, and Maximum Power Consumption
- Power consumption (also shown in graphs in the Web interface)
- Max and Min Power Times

## Viewing Power Monitoring

### Using the Web Interface

To view the power monitoring data:

1. Log in to iDRAC6 Web interface.
2. In the system tree, select **Power Monitoring**.

   The **Power Monitoring** screen is displayed, displaying the following information:

#### Power Monitoring

- **Status**: A **green check** indicates that the power status is normal, **Warning** indicates that a warning alert was issued, and **Severe** indicates a failure alert was issued.
- **Probe Name**: Lists the name of the sensor.
- **Reading**: Indicates the wattage reported by the probe.
- **Warning Threshold**: Displays the acceptable power consumption (in Watts and BTU/hr) recommended for system operation. Power consumption that exceeds this value results in warning events and throttling the CPU.
- **Failure Threshold**: Displays the highest acceptable power consumption (in Watts and BTU/hr) required for system operation. Power consumption that exceeds this value results in critical/failure events and the blade will shutdown.

#### Amperage

- **Location**: Displays the name of the system board sensor.
- **Reading**: The current consumption in AC Amps.

#### Power Tracking Statistics and Peak Statistics

- Statistic:
  - **Cumulative System Power** displays the current cumulative energy consumption (in kWh) for the server. The value represents the total energy used by the system. You can reset this value to 0 by clicking **Reset** at the end of the table row.
  - **System Peak Power** specifies the system peak value in AC Watts.

- **System Peak Amperage** specifies the system peak amperage. The peak value is the highest value recorded between the **Measurement Start Time** and now. The peak time was the point in time when that peak value occurred. Click **Reset** at the end of the table row to set it back to the current instantaneous value (which, if the server is running, will not be 0). Clicking reset will also reset the measurement start time to the current time.
- **Measurement Start Time** displays the date and time recorded when the system energy consumption value was last cleared and the new measurement cycle began. For **Cumulative System Power**, **System Peak Amperage**, and **System Peak Power** statistics, the peak values when reset, will immediately reflect the current instantaneous value.
- **Measurement Current Time** for **Cumulative System Power** displays the current date and time when the system energy consumption was calculated for display. For **System Peak Amperage** and **System Peak Power**, the **Peak Time** fields display the time when these peaks occurred.
- **Reading**: The value of the appropriate statistic—**Cumulative System Power**, **System Peak Power**, and **System Peak Amperage** since the counter was started.

**NOTE:** Power Tracking Statistics are maintained across system resets and so reflect all activity in the interval between the stated Start and Current times. The power values displayed in the Power Consumption table are cumulative averages over the respective time interval (last minute, hour, day and week). Since the Start to Finish time intervals here may differ from those of the Power Tracking Statistics ones, peak power values (Max Peak Watts versus Max Power Consumption) may differ.

**Power Consumption**

- **Average Power Consumption**: Average over previous minute, previous hour, previous day, and previous week.
- **Max Power Consumption** and **Min Power Consumption**: The maximum and minimum power consumptions observed within the given time interval.
- **Max Power Time** and **Min Power Time**: The times (by minute, hour, day, and week) when the maximum and minimum power consumptions occurred.

#### Show Graph

Click **Show Graph** to display graphs illustrating iDRAC6 power consumption in Watts over the last hour, 24 hours, three days, and one week. Use the drop-down menu provided above the graph to select the time period.

**NOTE:** Each data point plotted on the graphs represents the average of readings over a 5 minute period. As a result, the graphs may not reflect brief fluctuations in power or current consumption.

## Power Budgeting

The **Power Budget** screen displays the power threshold limits, which cover the range of AC power consumptions a system under heavy workload will present to the datacenter.

Before a server powers up, iDRAC6 provides CMC with its power envelope requirement. The power envelop given by iDRAC to CMC before the system powers on is higher than the actual power that can be consumed by the blade. This power envelop is calculated based on the limited hardware inventory information. It may request a smaller power envelope 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, iDRAC6 may request an increase of the maximum potential power consumption thus increasing the power envelope. iDRAC6 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 will continue to request for more power if the power consumption exceeds the power allocated by CMC.

Once the system is powered on and initialized, iDRAC calculates a new power envelop which is based on the actual blade configuration. The blade will stay 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.

iDRAC6 also supports power allocation to the PCIe expansion-cards for applicable platforms. You can change the power allocated to the PCIe expansion-cards installed in the expansion slot in the server. Two PCIe cards can be installed in the applicable platforms. iDRAC dynamically adjusts the power envelope close to the actual system requirement for the blade, adds the power allocated for the expansion-card slot, and requests for the combined power from CMC. For more information about expansion-cards, see the *Hardware Owner's Manual* available on the Dell Support site at **support.dell.com/manuals**. For information about modifying the PCIe power allocation, see "Viewing and Modifying PCIe Power Allocation" on page 313.

After the blade powers on, BIOS will boot and detect the actual power consumption of the installed PCIe expansion cards. This occurs during POST. iDRAC maintains the value used in the pre-init phase for the expansion-cards if both cards are present. Once the updated value has been obtained based on the currently installed PCIe cards, iDRAC combines that value with the expansion card estimated power consumption and reports a new power value for the overall blade. If CMC does not allocate enough power, iDRAC will power off the blade. If CMC allocates enough power, BIOS is allowed to continue booting and the server can start up.

For example, if 500W is the value iDRAC assumes during pre-init, this value will be used unless you set a different value for the PCIe expansion slot allocation. If you set a different value, this value will always be used during pre-init. The value is preserved through AC power cycles. The input value will then be compared to the number of cards installed when the system reaches POST.

## Viewing Power Budget

The server provides power budget status overviews of the power subsystem on the **Power Budget** screen.

### Using the Web Interface

**NOTE:** To perform power management actions, you must have **Administrative** privilege.

1. Log in to iDRAC6 Web interface.
2. In the system tree, select **System**.
3. Click the **Power Management** tab, and then click **Power Budget**.

   The **Power Budget** screen is displayed.

The **Power Budget Information** table displays the minimum and maximum limits of power thresholds for the current system configuration. These cover the range of AC power consumptions a thresholded system under heavy workload will present to the datacenter.

- **Minimum Potential Power Consumption** represents the lowest Power Budget Threshold value.
- **Maximum Potential Power Consumption** represents the highest Power Budget Threshold value. This value is also the current system configuration's absolute maximum power consumption.

### Using RACADM

On a managed server, open a command line interface and enter:

```
racadm getconfig -g cfgServerPower
```

**NOTE:** For more information about cfgServerPower, including output details, see cfgServerPower in the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

### Power Budget Threshold

Power Budget Threshold, if enabled, enforces power limits for the system. System performance is dynamically adjusted to maintain power consumption near the specified threshold.

Actual power consumption may be less for light workloads and momentarily may exceed the threshold until performance adjustments have completed.

**NOTE:** Power Budget Threshold information is read-only and cannot be enabled or configured in iDRAC6.

#### Using the Web Interface

1. Log in to iDRAC6 Web interface.
2. In the system tree, select **System**.
3. Click the **Power Management** tab, and then click **Power Budget**.

   The **Power Budget** screen is displayed. The **Power Budget Threshold** table displays the following power limit information for the system:

   - **Enabled** indicates whether the system enforces the power budget threshold.
   - **Threshold in Watts** and **Threshold in BTU/hr** display the limit in AC Watts and BTU/hr respectively.
   - **Threshold in Percentage (of Maximum)** displays the percentage of power capping range.

#### Using RACADM

To view the Power Budget Threshold data from local RACADM, on the managed server, open a command line interface and enter:

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapWatts
```

returns <*power cap value in AC Watts*>

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapBTUhr
```

returns *<power cap value in BTU/hr>*

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapPercent
```

returns *<power cap value in %>*

**NOTE:** For more information about cfgServerPower, including output details, see cfgServerPower in the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

## Viewing and Modifying PCIe Power Allocation

The PCIe Power Allocation allows you to view and change the maximum power allocated to the PCIe expansion cards. The power allocated should be between 100W and 500W. Allocating too much power may result in the blade not powering on or may prevent other blades in the chassis from powering on. If the PCIe expansion card consumes more power than the allocation, the blade will power off. When modifying the PCIe power allocation, the new power allocation value is used when the system boots.

**NOTE:** The PCIe Power Allocation information does not apply to all platforms and will not display for platforms where it does not apply.

**NOTE:** You must have Administrator privileges (Configure iDRAC and Execute Server Control Commands) to edit the PCIe Power Allocation value.

### Using the Web Interface

1. Log in to iDRAC6 Web interface.
2. In the system tree, select **System**.
3. Click the **Power Management** tab, and then click **Power Budget**. The **PCIe Power Allocation** table displays the current power allocation in the **Power Threshold in Watts** field.
4. Enter a required value or click **Default Value** to specify a default value. Valid values are 100W - 500W. Default value is 500W.
5. Click **Apply** to save the new value. The new value is used when the system boots.

#### Using RACADM

To view the current power allocated for the PCIe expansion-cards using remote RACADM, on the remote system, open a command prompt and enter the following command:

```
racadm -r <idracip> -u <user> -p <password> config -g
cfgServerPower -o cfgServerPowerPCIeAllocation
```

Returns <*power cap value in AC Watts or BTU/hr*>. The default value is 500W.

To change the power allocation value (for example, 250W):

```
racadm -r <idracip> -u <user> -p <password> config -g
cfgServerPower -o cfgServerPowerPCIeAllocation 250
```

Sets the value to 250W

**NOTE:** The cfgServerPowerPCIeAllocation object is supported only on remote RACADM and not on local RACADM.

**NOTE:** For more information, see cfgServerPowerPCIeAllocation in the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

# Power Control

iDRAC6 enables you to remotely perform a power-on, power off, reset, graceful shutdown, non-masking interruption (NMI), or power cycle. Use the **Power Control** screen to perform an orderly shutdown through the operating system when rebooting and powering on or off.

### Executing Power Control Operations on the Server

**NOTE:** To perform power management actions, you must have **Administrator** privilege.

iDRAC6 enables you to remotely perform a power-on, reset, graceful shutdown, NMI, or power cycle.

#### Using the Web Interface

1. Log in to iDRAC6 Web interface.
2. In the system tree, select **System**.
3. Click the **Power Management** tab.

   The **Power Control** screen displays.
4. Select one of the following **Power Control Operations** by clicking its radio button:
   - **Power On System** turns on the server (the equivalent of pressing the power button when the server power is off). This option is disabled if the system is already powered on.
   - **Power Off System** turns off the server. This option is disabled if the system is already powered off.
   - **NMI (Non-Masking Interrupt)** generates an NMI to halt system operation. An NMI sends a high-level interrupt to the operating system, which causes the system to halt operation to allow for critical diagnostic or troubleshooting activities. This option is disabled if the system is already powered off.
   - **Graceful Shutdown** attempts to shut down the operating system, then powers off the system. Graceful shutdown requires an ACPI (Advanced Configuration and Power Interface)-aware operating system, which allows for system directed power management. This option is disabled if the system is already powered off.
   - **Reset System (warm boot)** reboots the system without powering off. This option is disabled if the system is already powered off.
   - **Power Cycle System (cold boot)** powers off and then reboots the system. This option is disabled if the system is already powered off.
5. Click **Apply**.

   A dialog box is displayed requesting confirmation.
6. Click **OK** to execute the power management action you selected.

### Using RACADM

To perform power actions from local RACADM, enter the below command at a command prompt:

```
racadm serveraction <action>
```

where <action> is powerup, powerdown, powercycle, hardreset, or powerstatus.

**NOTE:** For more information about serveraction, including output details, see serveraction in the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

# 15

# Using iDRAC6 Enterprise SM-CLP Command Line Interface

This section provides information about the Server Management Workgroup (SMWG) Server Management-Command Line Protocol (SM-CLP) that is incorporated in iDRAC6.

**NOTE:** This section assumes that you are familiar with the Systems Management Architecture for Server Hardware (SMASH) Initiative and the SMWG SM-CLP specifications. For more information on these specifications, see the Distributed Management Task Force (DMTF) website at **dmtf.org**.

iDRAC6 SM-CLP is a protocol driven by the DMTF and SMWG to provide standards for systems management CLI implementations. Many efforts are driven by a defined SMASH architecture that is targeted as a foundation for a more standardized systems management set of components. The SMWG SM-CLP is a subcomponent of the overall SMASH efforts driven by DMTF.

SM-CLP provides a subset of the functionality provided by the local RACADM command line interface, but with a different access path. SM-CLP executes within iDRAC6, while RACADM executes on the managed server. Also, RACADM is a Dell proprietary interface, where SM-CLP is an industry standard interface.

**NOTE:** Information about the Dell profiles and MOFs are available on the Dell Enterprise Technology Center at **delltechcenter.com** and all DMTF information is available on the DMTF website at **dmtf.org/standards/profiles/**. Further, Dell extensions are available at **delltechcenter.com/page/DCIM+-+Dell+CIM+Extensions**.

# System Management With SM-CLP

iDRAC6 SM-CLP enables you to manage the following system features from a command line:

- Server Power Management — Turn on, shutdown, or reboot the system
- System Event Log (SEL) Management — Display or clear the SEL records
- iDRAC6 user account management
- Active Directory configuration
- iDRAC6 LAN configuration
- SSL Certificate Signature Request (CSR) generation
- Virtual media configuration

# iDRAC6 SM-CLP Support

SM-CLP is hosted from iDRAC6 firmware, and supports Telnet and SSH connections. iDRAC6 SM-CLP interface is based on the SM-CLP Specification Version 1.0 provided by the DMTF organization.

The following sections provide an overview of the SM-CLP feature that is hosted from iDRAC6.

**NOTE:** If you have established an SM–CLP session through Telnet/SSH and the session is not closed successfully due to the network being disconnected, a message indicating that you have reached the maximum number of connections may be displayed. To resolve this, terminate the SM–CLP session in the Web GUI under **System→ iDRAC Settings→ Network/Security→ Sessions** before attempting to establish a new one.

**NOTE:** iDRAC6 supports up to 4 Telnet sessions and 4 SSH sessions simultaneously. However, only *one* of those 8 potential sessions may use SM-CLP. That is, iDRAC6 supports only one SM-CLP session at a time.

### How to start an SM–CLP session

- Connect to iDRAC6 through SSH/Telnet which takes you to the CLI (console).
- Enter "smclp" at the dollar prompt to start the SM–CLP console.

Syntax:

```
telnet <iDRAC6-ip-address>
$ (the CLI prompt is displayed)
$smclp (at the CLI prompt, type smclp)
```

# SM-CLP Features

The SM-CLP specification provides a common set of standard SM-CLP verbs that can be used for simple systems management through the CLI.

SM-CLP promotes the concept of verbs and targets to provide system configuration capabilities through the CLI. The verb indicates the operation to perform and the target is the entity (or object) on which the operation is performed.

The following is the syntax of the SM-CLP command line:

```
<verb> [<options>] [<target>] [<properties>]
```

Table 15-1 provides a list of the verbs iDRAC6 CLI supports, the syntax of each command, and a list of the options the verb supports.

**Table 15-1. Supported SM-CLP CLI Verbs**

| Verb | Description | Options |
|---|---|---|
| cd | Navigates through the managed system address space using the shell.<br>Syntax:<br>`cd [options] [target]` | –default, –examine, –help, –output, –version |
| delete | Deletes an object instance.<br>Syntax:<br>`delete [options] target` | –examine, –help, –output, –version |
| exit | Exits from the SM-CLP shell session.<br>Syntax:<br>`exit [options]` | –help, –output, –version |
| help | Displays help for SM-CLP commands.<br>`help` | -examine, -help, -output, -version |

**Table 15-1. Supported SM-CLP CLI Verbs *(continued)***

| Verb | Description | Options |
|---|---|---|
| reset | Resets the target.<br>Syntax:<br>`reset [options] [target]` | –examine, –help, –output, –version |
| set | Sets the properties of a target<br>Syntax:<br>`set [options] [target] <property name>=<value>` | –examine, –help, –output, –version |
| show | Displays the target properties, verbs, and subtargets.<br>Syntax:<br>`show [options] [target] <property name>=<value>` | -all, -default, –display, –examine, –help, –level, –output, –version |
| start | Starts a target.<br>Syntax:<br>`start [options] [target]` | –examine, –force, –help, –output, –version |
| stop | Shuts down a target.<br>Syntax:<br>`stop [options] [target]` | –examine, –force, –help, –output, –version, –wait |
| version | Displays the version attributes of a target.<br>Syntax:<br>`version [options]` | –examine, –help, –output, –version |

Table 15-2 describes the SM-CLP options. Some options have abbreviated forms, as shown in the table.

**Table 15-2. Supported SM-CLP Options**

| SM-CLP Option | Description |
|---|---|
| -all, -a | Instructs the verb to perform all possible functions. |
| -destination | Specifies the location to store an image in the dump command.<br>Syntax:<br>–destination <URI> |
| -display, -d | Filters the command output.<br>Syntax:<br>`-display <properties \| targets \| verbs>[, <properties \| targets \| verbs>]*` |
| -examine, -x | Instructs the command processor to validate the command syntax without executing the command. |
| -force, -f | If graceful shutdown is not successful, use this option to perform a forced shutdown of the target system.<br>Syntax:<br>`stop -force <target>` |
| -help, -h | Displays help for the verb. |
| -level, -l | Instructs the verb to operate on targets at additional levels beneath the specified target.<br>Syntax:<br>`-level <n \| all>` |
| -output, -o | Specifies the format for the output.<br>Syntax:<br>`-output format=<text \| clpcsv \| keyword \| clpxml>`<br>or<br>`-o format=<text \| clpcsv \| keyword \| clpxml>` |
| -version, -v | Displays the SM–CLP version number. |

# Navigating the MAP Address Space

**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.

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 iDRAC6. Navigate down from the root using the `cd` verb.

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.

### Targets

For a list of targets available through the SM-CLP, see the SM–CLP mapping document available on the Dell Enterprise Technology Center at **delltechcenter.com**.

# Using the 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/oemdcim_mfaaccount1
```

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
```

# iDRAC6 SM-CLP Examples

The following subsections provide examples on how to login to iDRAC6 using the SSH interface and start an SM-CLP session to perform the following operations:

- Server power management
- SEL management
- MAP target navigation
- Display system properties

## Server Power Management

Table 15-3 provides examples of using SM-CLP to perform power management operations on a managed server.

Enter "`smclp`" to start the SM-CLP console.

**Table 15-3. Server Power Management Operations**

| Operation | Syntax |
|---|---|
| Logging in to iDRAC6 using the SSH interface | `>ssh 192.168.0.120`<br>`>login: root`<br>`>password:`<br>Enter "`smclp`" to start the SM–CLP console. |
| Power down the server | `->stop /admin1/system1`<br>`system1 successfully stopped` |
| Power up the server from a powered-off state | `->start /admin1/system1`<br>`system1 successfully started` |
| Reboot the server | `->reset /admin1/system1`<br>`RESET successful for system1` |

## SEL Management

Table 15-4 provides examples of using the SM-CLP to perform SEL-related operations on the managed system.

## MAP Target Navigation

Table 15-5 provides examples of using the **cd** verb to navigate the MAP. In all examples, the initial default target is assumed to be /.

**Table 15-4. SEL Management Operations**

| Operation | Syntax |
|---|---|
| Viewing the SEL | `->show -d targets,properties,verbs /admin1/system1/logs1/log1`<br><br>Might return:<br>`Targets:`<br>`record1/`<br>`record2/...`<br><br>`Properties:`<br>`OverwritePolicy=7`<br>`LogState=4`<br>`CurrentNumberOfRecords=60`<br>`MaxNumberOfRecords=512`<br>`ElementName=Record Log 1`<br>`HealthState=5`<br>`EnabledState=2`<br>`RequestedState=12`<br>`EnabledDefault=2`<br>`TransitioningToState=12`<br>`InstanceID=DCIM: SEL Log`<br>`OperationalStatus={2}`<br><br>`Verbs:`<br>`show`<br>`exit`<br>`version`<br>`cd`<br>`help` |

**Table 15-4. SEL Management Operations *(continued)***

| Operation | Syntax |
|---|---|
| Viewing the SEL record | `->show /admin1/system1/logs1/log1/record4`<br>Might return:<br>`ufip=/admin1/system1/logs1/log1/record4`<br>`Associations:LogManagesRecord=`<br>`>/admin1/system1/logs1/log1`<br>`Properties:`<br>`RecordData=*0.0.65*4 2*1245152621*65`<br>`65*4*31*0*true*111*1*255*255*`<br>`RecordFormat=`<br>`*IPMI_SensorNumber.IPMI_OwnerLUN.IPMI_OwnerID*I`<br>`PMI_RecordID*IPMIRecordType*IPMI_TimeStamp*IPMI`<br>`_GeneratorID*IPMI_EvMRev*IPMI_SensorType*IPMI_S`<br>`ensorNumber*IPMI_AssertionEvent*IPMI_EventType*`<br>`IPMI_EventData1*IPMI_EventData2*IPMI_EventData3`<br>`*IANA*`<br>`Description=:0:Assert:OEM specific`<br>`ElementName=DCIM System Event Log Entry`<br>`InstanceID=DCIM:SEL LOG:4`<br>`LogInstanceID=idrac:Unknown:Unknown SEL Log`<br>`LogName=DCIM System Event Log Entry`<br>`RecordID=DCIM:SEL LOG:4`<br>`CreationTimeStamp=20090616114341.000000+000` |

**Table 15-4. SEL Management Operations *(continued)***

| Operation | Syntax |
|---|---|
| | Verbs:<br>show<br>exit<br>version<br>cd<br>help<br>delete |
| Clearing the SEL | ->delete /admin1/system1/logs1/log1/record*<br>Returns:<br>Records deleted successfully. |

**Table 15-5. Map Target Navigation Operations**

| Operation | Syntax |
|---|---|
| Navigate to the system target and reboot | ->cd admin1/system1<br>->reset<br>**NOTE:** The current default target is **/**. |
| Navigate to the SEL target and display the log records | ->cd admin1<br>->cd system1<br>->cd logs1<br>->cd log1<br>->show<br>is equivalent to<br>->cd admin1/system1/logs1/log1<br>->show |
| Display current target | ->cd . |
| Move up one level | ->cd .. |
| Exit the shell | ->exit |

# 16

# Using the WS-MAN Interface

Web Services for Management (WS–MAN) is a Simple Object Access Protocol (SOAP)–based protocol used for systems management. WS–MAN provides an interoperable protocol for devices to share and exchange data across networks. iDRAC6 uses WS–MAN 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 manipulated in a managed system. The Dell–embedded server platform management interfaces are organized into profiles, where each profile defines the specific interfaces for a particular management domain or area of functionality. Additionally, Dell has defined a number of model and profile extensions that provide interfaces for additional capabilities.

The data available through WS-MAN is provided by iDRAC6 instrumentation interface mapped to the DMTF profiles and Dell extension profiles.

## WS-Management Features

The WS–Management specification promotes interoperability between management applications and managed resources. By identifying a core set of Web service specifications and usage requirements to expose a common set of operations that are central to all systems management, WS–Management has the ability to:

- DISCOVER the presence of management resources and navigate between them
- GET, SET, CREATE, and DELETE individual management resources, such as settings and dynamic values

- ENUMERATE the contents of containers and collections, such as large tables and logs
- EXECUTE specific management methods with strongly typed input and output parameters

# Supported CIM Profiles

**Table 16-1. Supported CIM Profiles**

| Standard DMTF |
|---|
| **1** Base Server<br>Defines CIM classes for representing the host server. |
| **2** Base Metrics<br>Defines CIM classes for providing the ability to model and control metrics captured for managed elements. |
| **3** Service Processor<br>Defines CIM classes for modeling service processors. |
| **4** USB Redirection<br>Defines CIM classes for describing information about USB redirections. For keyboard, video, and mouse devices, this profile should be used if the devices are to be managed as USB devices. |
| **5** Physical Asset<br>Defines CIM classes for representing the physical aspect of the managed elements. iDRAC6 uses this profile to represent the host server's and its component's FRU information, as well as the physical topology. |
| **6** SM CLP Admin Domain<br>Defines CIM classes for representing CLP's configuration. iDRAC6 uses this profile for its own implementation of CLP. |
| **7** Power State Management<br>Defines CIM classes for power control operations. iDRAC6 uses this profile for the host server's power control operations. |
| **8** CLP Service<br>Defines CIM classes for representing CLP's configuration. iDRAC6 uses this profile for its own implementation of CLP. |
| **9** IP Interface<br>Defines CIM classes for representing an IP interface of a managed system. |

**Table 16-1. Supported CIM Profiles *(continued)***

**10** DHCP Client
Defines CIM classes for representing a DHCP client and its associated capabilities and configuration.

**11** DNS Client
Defines CIM classes for representing a DNS client in a managed system.

**12** Record Log
Defines CIM classes for representing different type of logs. iDRAC6 uses this profile to represent the System Event Log (SEL) and iDRAC6 RAC Log.

**13** Role Based Authorization
Defines CIM classes for representing roles. iDRAC6 uses this profile for configuring iDRAC6 account privileges.

**14** SMASH Collections
Defines CIM classes for representing CLP's configuration. iDRAC6 uses this profile for its own implementation of CLP.

**15** Profile Registration
Defines CIM classes for advertising the profile implementations. iDRAC6 uses this profile to advertise its own implemented profiles, as described in this table.

**16** Simple Identity Management
Defines CIM classes for representing identities. iDRAC6 uses this profile for configuring iDRAC6 accounts.

**17** Ethernet Port
Defines CIM classes for representing an Ethernet port, its associated controller, and Ethernet interfaces in a managed system. Associations with the port's physical aspects and profile–implementation version information are modeled in this profile.

**18** Sensor
Defines CIM classes used to describe the sensors in a managed system. It also defines association classes that describe the relationship of the sensors with the monitored devices.

**Dell Extensions**

**1** Active Directory Client
Defines CIM and Dell extension classes for configuring iDRAC6 Active Directory client and the local privileges for Active Directory groups.

**2** Virtual Media
Defines CIM and Dell extension classes for configuring iDRAC6 Virtual Media. Extends *USB Redirection* Profile.

**Table 16-1. Supported CIM Profiles *(continued)***

**3** OS Deployment
Defines CIM and Dell extension classes for representing the configuration of OS Deployment features. It extends the management capability of referencing profiles by adding the capability to support OS deployment activities by manipulating OS Deployment features provided by the service processor.

**4** Software Inventory
Defines CIM and Dell Extensions for representing currently installed BIOS, component firmware, Diagnostics, Unified Server Configurator, and Driver Pack versions. Also provides representation of versions of BIOS and firmware update images available in Lifecycle Controller for rollback and re-installation.

**5** Software Update
Defines CIM and Dell extensions for representing the service class and methods for updating BIOS, Diagnostics, driver pack, and component and Lifecycle Controller firmware. Update methods support update from CIFS, NFS, FTP, and HTTP network share locations and from update images located in the Lifecycle Controller. Update requests are formulated as jobs and can be scheduled immediately or later with a choice of types of reboot actions to apply the updates.

**6** Job Control
Defines CIM and Dell extensions for managing jobs generated by update requests. Jobs can be created, deleted, modified, and aggregated into job queues to sequence and perform multiple updates in a single reboot.

**7** LC Management
Defines CIM and Dell extensions for getting and setting attributes for managing Auto-Discovery and Part Replacement Lifecycle Controller features.

**8** Persistent Storage
Defines CIM and Dell extension classes for managing the partitions on the virtual flash media of Dell platforms.

**9** Simple NIC
Defines CIM and Dell extension classes to represent the configuration of NIC network controllers.

**10** BIOS and Boot Management
Defines CIM and Dell extension classes to represent Dell BIOS attributes and to configure host's boot sequence.

**11** Simple RAID
Defines CIM and Dell extension classes to represent the configuration of host's RAID storage.

**Table 16-1. Supported CIM Profiles *(continued)***

| | |
|---|---|
| **12** | iDRAC Card<br>Defines CIM and Dell extension classes to represent the iDRAC6 inventory information. |
| **13** | Memory<br>Defines CIM and Dell extension classes to represent the host's DIMM inventory information. |
| **14** | CPU<br>Defines CIM and Dell extension classes to represent the host's CPU inventory information. |
| **15** | System Info<br>Defines CIM and Dell extension classes to represent the host platform's inventory information. |
| **16** | PCI Device<br>Defines CIM and Dell extension classes to represent the host's PCI device inventory information. |
| **17** | Video<br>Defines CIM and Dell extension classes to represent the host's video card inventory information. |

iDRAC6 WS–MAN implementation uses SSL on port 443 for transport security, and supports basic authentication. Web services interfaces can be utilized by leveraging client infrastructure such as Windows WinRM and Powershell CLI, open source utilities like WSMANCLI, and application programming environments like
Microsoft .NET.

There are additional implementation guides, white papers, profiles, MOFs, and code samples available in the Dell Enterprise Technology Center at **delltechcenter.com**. For more information, also see the following:

- DMTF Web site: **dmtf.org/standards/profiles/**
- WS–MAN release notes or Readme file.

# 17

# Deploying Your Operating System Using iVMCLI

The Integrated Virtual Media Command Line Interface (iVMCLI) utility is a command-line interface that provides virtual media features from the management station to iDRAC6 in the remote system. Using iVMCLI and scripted methods, you can deploy your operating system on multiple remote systems in your network.

This section provides information on integrating the iVMCLI utility into your corporate network.

## Before You Begin

Before using the iVMCLI utility, ensure that your targeted remote systems and corporate network meet the requirements listed in the following sections.

### Remote System Requirements

- iDRAC6 is configured in each remote system.

### Network Requirements

A network share must contain the following components:

- Operating system files
- Required drivers
- Operating system boot image file(s)

  The image file must be an operating system CD or a CD/DVD ISO image with an industry-standard, bootable format.

# Creating a Bootable Image File

Before you deploy your image file to the remote systems, ensure that a supported system can boot from the file. To test the image file, transfer the image file to a test system using iDRAC6 Web user interface and then reboot the system.

The following sections provide specific information for creating image files for Linux and Windows systems.

### Creating an Image File for Linux Systems

Use the Data Duplicator (dd) utility to create a bootable image file for your Linux system.

To run the utility, open a command prompt and enter the following:

```
dd if=<input-device> of=<output-file>
```

For example:

```
dd if=/dev/sdc0 of=mycd.img
```

### Creating an Image File for Windows Systems

When choosing a data replicator utility for Windows image files, select a utility that copies the image file and the CD/DVD boot sectors.

# Preparing for Deployment

### Configuring the Remote Systems

1. Create a network share that can be accessed by the management station.
2. Copy the operating system files to the network share.
3. If you have a bootable, preconfigured deployment image file to deploy the operating system to the remote systems, skip this step.

   If you do not have a bootable, preconfigured deployment image file, create the file. Include any programs and/or scripts used for the operating system deployment procedures.

   For example, to deploy a Microsoft Windows operating system, the image file may include programs that are similar to deployment methods used by Microsoft Systems Management Server (SMS).

When you create the image file, do the following:

- Follow standard network-based installation procedures.
- Mark the deployment image as "read only" to ensure that each target system boots and executes the same deployment procedure.

4 Perform one of the following procedures:

- Integrate **IPMItool** and the Virtual Media command line interface (iVMCLI) into your existing operating system deployment application. Use the sample **ivmdeploy** script as a guide to using the utility.
- Use the existing **ivmdeploy** script to deploy your operating system.

**NOTE:** **ivmdeploy** internally uses the **iVMCLI** and **ipmitool**. You should have *IPMI over LAN* privilege to use this tool. Also, the virtual media should be in the attached state when using the **ivmdeploy** script.

# Deploying the Operating System

Use the iVMCLI utility and the **ivmdeploy** script included with the utility to deploy the operating system to your remote systems.

Before you begin, review the sample **ivmdeploy** script included with the iVMCLI utility. The script shows the detailed steps needed to deploy the operating system to remote systems in your network.

The following procedure provides a high-level overview for deploying the operating system on targeted remote systems.

1 List iDRAC6 IP addresses of the remote systems that will be deployed in the **ip.txt** text file, one IP address per line.

2 Insert a bootable operating system CD or DVD into the client media drive.

3 Run **ivmdeploy** at the command line.

To run the ivmdeploy script, enter the following command at the command prompt:

```
ivmdeploy -r ip.txt -u <idrac-user> -p <idrac-passwd>
-c {<iso9660-img> | <path>}
```

where:

- <*idrac-user*> is iDRAC6 user name—for example, **root**
- <*idrac-passwd*> is the password for iDRAC6 user—for example, **calvin**
- <*iso9660-img*> is the path to an ISO9660 image of the operating system installation CD or DVD
- <*path*> is the path to the device containing the operating system installation CD or DVD

The **ivmdeploy** script passes its command line options to the **iVMCLI** utility. See "Command Line Options" on page 340 for details about these options. The script processes the **-r** option slightly differently than the **iVMCLI -r** option. If the argument to the **-r** option is the name of an existing file, the script reads iDRAC6 IP addresses from the specified file and runs the **iVMCLI** utility once for each line. If the argument to the **-r** option is not a filename, then it should be the address of a single iDRAC6. In this case, the **-r** works as described for the **iVMCLI** utility.

The ivmdeploy script supports installation only from a CD/DVD or a CD/DVD ISO9660 image. If you need to install from a floppy disk or a floppy disk image, you can modify the script to use the **iVMCLI -f** option.

# Using the Virtual Media Command Line Interface Utility

The Virtual Media Command Line Interface (iVMCLI) utility is a scriptable command-line interface that provides virtual media features from the management station to iDRAC6.

The iVMCLI utility provides the following features:

**NOTE:** When virtualizing read-only image files, multiple sessions may share the same image media. When virtualizing physical drives, only one session can access a given physical drive at a time.

- Removable media devices or image files that are consistent with the Virtual Media plug-ins
- Automatic termination when iDRAC6 firmware boot once option is enabled
- Secure communications to iDRAC6 using Secure Sockets Layer (SSL)

Before you run the utility, ensure that you have Virtual Media user privilege to iDRAC6.

**CAUTION: It is recommended to use the interactive flag '-i' option, when starting up the iVMCLI command line utility. This ensures tighter security by keeping the username and password private because on many Windows and Linux operating systems, the username and password are visible in clear text when processes are examined by other users.**

If your operating system supports administrator privileges or an operating system-specific privilege or group membership, administrator privileges are also required to run the iVMCLI command.

The client system's administrator controls user groups and privileges, thereby controlling the users who can run the utility.

For Windows systems, you must have Power User privileges to run the iVMCLI utility.

For Linux systems, you can access the iVMCLI utility without administrator privileges by using the **sudo** command. This command provides a centralized means of providing non-administrator access and logs all user commands.

To add or edit users in the iVMCLI group, the administrator uses the **visudo** command. Users without administrator privileges can add the **sudo** command as a prefix to the iVMCLI command line (or to the iVMCLI script) to obtain access to iDRAC6 in the remote system and run the utility.

### Installing the iVMCLI Utility

The iVMCLI utility is located on the *Dell Systems Management Tools and Documentation* DVD, which is included with your Dell OpenManage system management software kit. To install the utility, insert the DVD into your system, and follow the on-screen instructions.

The *Dell Systems Management Tools and Documentation* DVD contains the latest systems management software products, including diagnostics, storage management, remote access service, and the RACADM utility. This DVD also contains readme files, which provide the latest systems management software product information.

The *Dell Systems Management Tools and Documentation* DVD also includes **ivmdeploy**—a sample script that illustrates how to use the iVMCLI and RACADM utilities to deploy software to multiple remote systems.

**NOTE:** The **ivmdeploy** script is dependent upon the other files that are present in its directory when it is installed. If you want to use the script from another directory, copy all the files with it.

### Command Line Options

The iVMCLI interface is identical on both Windows and Linux systems. The utility uses options that are consistent with the RACADM utility options. For example, an option to specify iDRAC6 IP address requires the same syntax for both RACADM and iVMCLI utilities.

The iVMCLI command format is as follows:

```
iVMCLI [parameter] [operating_system_shell_options]
```

Command-line syntax is case-sensitive. See "iVMCLI Parameters" on page 341 for more information.

If the remote system accepts the commands and iDRAC6 authorizes the connection, the command continues to run until either of the following occurs:

- The iVMCLI connection terminates for any reason.
- The process is manually terminated using an operating system control. For example, in Windows, you can use the Task Manager to terminate the process.

**NOTE:** When you are using the iVMCLI command, if the parameter values have spaces between words, you must use quotes for the complete parameter value. For example, consider the command to attach a DVD image from your system to the operating system on the server:
**F:\idrac>ivmcli -r 10.35.155.117 -u root -p calvin -c c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso**

where, -c is one of the parameters and **c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso** is the parameter value that contain spaces for 'documents and settings' and 'my documents'. Therefore, quotes is used for the complete image file path. Without the quotes, the command will fail. The following is also invalid:

**C:\"documents and settings"\.....**

## iVMCLI Parameters

### iDRAC6 IP Address

`-r <iDRAC-IP-address>[:<iDRAC-SSL-port>]`

This parameter provides iDRAC6 IP address and SSL port, which the utility needs to establish a Virtual Media connection with the target iDRAC6. If you enter an invalid IP address or DDNS name, an error message displays and the command terminates.

*<iDRAC-IP-address>* is a valid, unique IP address or iDRAC6 Dynamic Domain Naming System (DDNS) name (if supported). If *<iDRAC-SSL-port>* is omitted, port 443 (the default port) is used. The optional SSL port is not required unless you change iDRAC6 default SSL port.

#### iDRAC6 User Name

`-u <iDRAC-user-name>`

This parameter provides iDRAC6 user name that will run Virtual Media.

The <*iDRAC-user-name*> must have the following attributes:

- Valid user name
- iDRAC6 Virtual Media User permission

If iDRAC6 authentication fails, an error message displays and the command terminates.

#### iDRAC6 User Password

`-p <iDRAC-user-password>`

This parameter provides the password for the specified iDRAC6 user.

If iDRAC6 authentication fails, an error message displays and the command terminates.

#### Floppy/Disk Device or Image File

`-f {<device-name> | <image-file>}`

where <*device-name*> is a valid drive letter (for Windows systems) or a valid device file name, including the mountable file system partition number, if applicable (for Linux systems); and <*image-file*> is the filename and path of a valid image file.

This parameter specifies the device or file to supply the virtual floppy/disk media.

For example, an image file is specified as:

`-f c:\temp\myfloppy.img` (Windows system)

`-f /tmp/myfloppy.img` (Linux system)

If the file is not write-protected, Virtual Media may write to the image file. Configure the operating system to write-protect a floppy image file that should not be overwritten.

For example, a device is specified as:

`-f a:\` (Windows system)

`-f /dev/sdb4 # 4th partition on device /dev/sdb` (Linux system)

If the device provides a write-protection capability, use this capability to ensure that Virtual Media will not write to the media.

Omit this parameter from the command line if you are not virtualizing floppy media. If an invalid value is detected, an error message displays and the command terminates.

#### CD/DVD Device or Image File

`-c {<device-name> | <image-file>}`

where <*device-name*> is a valid CD/DVD drive letter (Windows systems) or a valid CD/DVD device file name (Linux systems) and <*image-file*> is the file name and path of a valid ISO-9660 image file.

This parameter specifies the device or file that will supply the virtual CD/DVD-ROM media:

For example, an image file is specified as:

`-c c:\temp\mydvd.img` (Windows systems)

`-c /tmp/mydvd.img` (Linux systems)

For example, a device is specified as:

`-c d:\` (Windows systems)

`-c /dev/cdrom` (Linux systems)

Omit this parameter from the command line if you are not virtualizing CD/DVD media. If an invalid value is detected, an error message is listed and the command terminates.

Specify at least one media type (floppy or CD/DVD drive) with the command, unless only switch options are provided. Otherwise, an error message displays and the command terminates and generates an error.

#### Root CA Certificate Validation

`-S`

This parameter is used to indicate if the iDRAC CA certificate is valid or not. If the certificate is not valid, the iVMCLI session is terminated and an error message is displayed indicating the certificate is not valid. If the certificate is valid, the iVMCLI session is established.

#### Version Display

`-v`

This parameter is used to display the iVMCLI utility version. If no other non-switch options are provided, the command terminates without an error message.

#### Help Display

`-h`

This parameter displays a summary of the iVMCLI utility parameters. If no other non-switch options are provided, the command terminates without error.

#### Manual Display

`-m`

This parameter displays a detailed "man page" for the iVMCLI utility, including descriptions of all of the possible options.

#### Encrypted Data

`-e`

When this parameter is included in the command line, iVMCLI will use an SSL-encrypted channel to transfer data between the management station and iDRAC6 in the remote system. If this parameter is not included in the command line, the data transfer is not encrypted.

### iVMCLI Operating System Shell Options

The following operating system features can be used in the iVMCLI command line:

- 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 iVMCLI utility.

  **NOTE:** The iVMCLI utility does not read from standard input (**stdin**). As a result, **stdin** redirection is not required.

- Background execution — By default, the iVMCLI utility runs in the foreground. Use the operating system's command shell features to cause 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.

The latter technique is useful in script programs, as it allows the script to proceed after a new process is started for the iVMCLI command (otherwise, the script would block until the iVMCLI program terminates).
When multiple iVMCLI instances are started in this way, and one or more of the command instances must be manually terminated, use the operating system-specific facilities for listing and terminating processes.

#### iVMCLI Return Codes

0 = No error

1 = Unable to connect

2 = iVMCLI command line error

3 = RAC firmware connection dropped

English-only text messages are also issued to standard error output whenever errors are encountered.

# 18

# Using iDRAC6 Configuration Utility

## Overview

iDRAC6 Configuration Utility is a pre-boot configuration environment that allows you to view and set parameters for iDRAC6 and for the managed system. Specifically, you can:

- View the firmware revision numbers for iDRAC6 and primary backplane firmware
- Configure, enable, or disable iDRAC6 local area network (LAN)
- Enable or disable IPMI Over LAN
- Configure LAN parameters
- Enable, disable, or cancel System Services
- Enable or disable Auto–Discovery and configure the Provisioning Server
- Attach or detach the Virtual Media devices
- Enable or Disable vFlash
- Enable or Disable Smart Card Logon and Single Sign On
- Configure System Services
- Change the administrative username and password
- Reset iDRAC6 configuration to the factory defaults
- View System Event Log (SEL) messages or clear messages from the log

The tasks you can perform using iDRAC6 Configuration Utility can also be performed using other utilities provided by iDRAC6 or Dell OpenManage software, including the Web interface, the SM-CLP command line interface, the local and remote RACADM command line interface and, in the case of basic network configuration, at iDRAC6 LCD during initial iDRAC6 configuration.

## Starting iDRAC6 Configuration Utility

You must use an iDRAC6 Virtual Console-connected console to access iDRAC6 Configuration Utility initially or after resetting iDRAC6 to the default settings.

1. At the keyboard connected to iDRAC6 Virtual Console, press <Print Screen> to display iDRAC6 **Virtual Console On Screen Configuration and Reporting (OSCAR)** menu. Use <Up Arrow> and <Down Arrow> to highlight the slot containing your server, then press <Enter>.
2. Turn on or restart the server by pressing the power button on the front of the server.
3. When you see the message `Press <Ctrl-E> for Remote Access Setup within 5 sec.....`, immediately press <Ctrl><E>. iDRAC6 Configuration Utility displays.

**NOTE:** If your operating system begins to load before you press <Ctrl><E>, allow the system to finish booting, then restart your server and try again.

The first two lines of the Configuration Utility provide information about iDRAC6 firmware and primary backplane firmware revisions. The revision levels can be useful in determining whether a firmware upgrade is needed.

iDRAC6 firmware is the portion of the firmware concerned with external interfaces, such as the Web interface, SM-CLP, and Web interfaces. The primary backplane firmware is the portion of the firmware that interfaces with and monitors the server hardware environment.

## Using iDRAC6 Configuration Utility

Beneath the firmware revision messages, the remainder of iDRAC6 Configuration Utility is a menu of items that you can access by using the up-arrow and down-arrow keys.

- If a menu item leads to a submenu or an editable text field, press <Enter> to access the item and <Esc> to leave it when you have finished configuring it.
- If an item has selectable values, such as **Yes/No** or **Enabled/Disabled**, press the left-arrow or right-arrow keys or the spacebar to choose a value.
- If an item is not editable, it is displayed in blue. Some items become editable depending upon other selections you make.

- The bottom line of the screen displays instructions for the current item. You can press <F1> to display help for the current item.
- When you have finished using iDRAC6 Configuration Utility, press <Esc> to view the exit menu, where you can choose to save or discard your changes or return to the utility.

The following sections describe iDRAC6 Configuration Utility menu items.

### iDRAC6 LAN

Use the left-arrow and right-arrow keys and the spacebar to select between **On** and **Off**.

iDRAC6 LAN is disabled in the default configuration. The LAN must be enabled to permit the use of iDRAC6 facilities, such as the Web interface, Telnet/SSH access to the SM-CLP command line interface, Virtual Console, and virtual media.

If you choose to disable the LAN the following warning displays:

```
iDRAC Out-of-Band interface will be disabled if the
LAN Channel is OFF.
```

The message informs you that in addition to facilities that you access by connecting to iDRAC6 HTTP, HTTPS, Telnet, or SSH ports directly, out-of-band management network traffic, such as IPMI messages sent to iDRAC6 from a management station, are not received when the LAN is disabled. The local RACADM interface remains available and can be used to reconfigure iDRAC6 LAN.

Press any key to clear the message and continue.

### IPMI Over LAN

Press the left-arrow and right-arrow keys and the spacebar to choose between **On** and **Off**. When **Off** is selected, iDRAC6 will not accept IPMI messages arriving over the LAN interface.

If you choose **Off**, a warning message is displayed.

Press any key to clear the message and continue. For an explanation of the message, see "iDRAC6 LAN" on page 349.

## LAN Parameters

Press <Enter> to display the LAN Parameters submenu. When you have finished configuring the LAN parameters, press <Esc> to return to the previous menu.

**Table 18-1. LAN Parameters**

| Item | Description |
|---|---|
| Common Settings | |
| MAC Address | This is the non-editable MAC address of iDRAC6 network interface. |
| VLAN Enable | Displays **On/Off**. **On** will enable the Virtual LAN filtering for iDRAC6. |
| VLAN ID | Displays any VLAN ID value between 1-4094. |
| VLAN | Displays the priority of the VLAN between 0-7 |
| Register iDRAC6 Name | Select **On** to register iDRAC6 name in the DNS service. Select **Off** if you do not want users to locate iDRAC6 name in DNS. |
| iDRAC6 Name | If **Register iDRAC Name** is set to **On**, press <Enter> to edit the **Current DNS iDRAC Name** text field. Press <Enter> when you have finished editing iDRAC6 name. Press <Esc> to return to the previous menu. iDRAC6 name must be a valid DNS host name. |
| Domain Name from DHCP | Select **On** if you want to obtain the domain name from a DHCP service on the network. Select **Off** if you want to specify the domain name. |
| Domain Name | If **Domain Name from DHCP** is set to **Off**, press <Enter> to edit the **Current Domain Name** text field. Press <Enter> when you have finished editing. Press <Esc> to return to the previous menu. The domain name must be a valid DNS domain, for example `mycompany.com`. |
| Host Name String | Press <Enter> to edit. Enter the name of the host for Platform Event Trap (PET) alerts. |
| LAN Alert Enabled | Select **On** to enable the PET LAN alert. |
| Alert Policy Entry 1 | Select **Enable** or **Disable** to activate the first alert destination. |

**Table 18-1. LAN Parameters *(continued)***

| Item | Description |
|---|---|
| Alert Destination 1 | if **LAN Alert Enabled** is set to **On**, enter the IP address where PET LAN alerts will be forwarded. |
| **IPv4 Settings** | Enable or disable support for the IPv4 connection. |
| IPv4 | Select **Enabled** or **Disabled** IPv4 protocol support.<br>The default is enabled. |
| RMCP+ Encryption Key | Press <Enter> to edit the value and <Esc> when finished. The RMCP+ Encryption key is a 40-character hexadecimal string (characters 0-9, a-f, and A-F). RMCP+ is an IPMI extension that adds authentication and encryption to IPMI. The default value is a string of 40 0s (zeros). |
| IP Address Source | Select between **DHCP** and **Static**. When DHCP is selected, the **Ethernet IP Address**, **Subnet Mask**, and **Default Gateway** fields are obtained from a DHCP server. If no DHCP server is found on the network, the fields are set to zeros.<br>When **Static** is selected, the **Ethernet IP Address**, **Subnet Mask**, and **Default Gateway** items become editable**.** |
| Ethernet IP Address | If the **IP Address Source** is set to **DHCP**, this field displays the IP address obtained from DHCP.<br>If the **IP Address Source** is set to **Static**, enter the IP address you want to assign to iDRAC6.<br>The default is **192.168.0.120**. |
| Subnet Mask | If the **IP Address Source** is set to **DHCP**, this field displays the subnet mask address obtained from DHCP.<br>If the **IP Address Source** is set to **Static**, enter the subnet mask for iDRAC6. The default is **255.255.255.0**. |
| Default Gateway | If the **IP Address Source** is set to **DHCP**, this field displays the IP address of the default gateway obtained from DHCP.<br>If the **IP Address Source** is set to **Static**, enter the IP address of the default gateway. The default is **192.168.0.1**. |
| DNS Servers from DHCP | Select **On** to retrieve DNS server addresses from a DHCP service on the network. Select **Off** to specify the DNS server addresses below. |

**Table 18-1. LAN Parameters *(continued)***

| Item | Description |
|---|---|
| DNS Server 1 | If **DNS Servers from DHCP** is **Off**, enter the IP address of the first DNS server. |
| DNS Server 2 | If **DNS Servers from DHCP** is **Off**, enter the IP address of the second DNS server. |
| **IPv6 Settings** | |
| IPv6 | Enable or disable support for the IPv6 connection. |
| IPv6 Address Source | Select between **AutoConfig** and **Static**. When **AutoConfig** is selected, the **IPv6 Address 1**, **Prefix Length**, and **Default Gateway** fields are obtained from DHCP.<br>When **Static** is selected, the **IPv6 Address 1**, **Prefix Length**, and **Default Gateway** items become editable. |
| IPv6 Address 1 | If the **IP Address Source** is set to **AutoConfig**, this field displays the IP address obtained from DHCP.<br>If the **IP Address Source** is set to **Static**, enter the IP address you want to assign to iDRAC6. |
| Prefix Length | Configures the Prefix length of the IPv6 address. It can be a value between 1 an 128, inclusive. |
| Default Gateway | If the **IP Address Source** is set to **AutoConfig**, this field displays the IP address of the default gateway obtained from DHCP.<br>If the **IP Address Source** is set to **Static**, enter the IP address of the default gateway. |
| IPv6 Link-local Address | This is the non-editable **IPv6 Link-local Address** of iDRAC6 network interface. |
| IPv6 Address 2-15 | This is the non-editable **IPv6 Address 2...IPv6 Address 15** of iDRAC6 network interface. |
| DNS Servers from DHCPv6 | Select **On** to retrieve DNS server addresses from a DHCP service on the network. Select **Off** to specify the DNS server addresses below. |
| DNS Server 1 | If **DNS Servers from DHCP** is **Off**, enter the IP address of the first DNS server. |
| DNS Server 2 | If **DNS Servers from DHCP** is **Off**, enter the IP address of the second DNS server. |

## Virtual Media Configuration

### Virtual Media

Use the left-arrow and right-arrow keys to select **Auto-Attached**, **Attached** or **Detached**.

- If you select **Attached**, the virtual media devices are attached to the USB bus, making them available for use during **Virtual Console** sessions.
- If you select **Detached,** users cannot access virtual media devices during **Virtual Console** sessions.
- If you select **Auto-Attached**, the Virtual Media devices are automatically attached to the server when a Virtual Media session is started.

**NOTE:** To use a USB Flash Drive with the Virtual Media feature, you must set **USB Flash Drive Emulation Type** to **Hard disk** in the BIOS Setup Utility. Access the BIOS Setup Utility by pressing <F2> during server start-up. If **USB Flash Drive Emulation Type** is set to **Auto**, the Flash Drive is displayed as a floppy drive to the system.

### vFlash

Use the left-arrow and right-arrow keys to select **Enabled** or **Disabled**.

- **Enabled** - vFlash is available for partition management.
- **Disabled** - vFlash is not available for partition management.

**CAUTION: vFlash cannot be disabled if one or more partitions are in-use or is attached.**

### Initialize vFlash

Choose this option to initialize the vFlash card. Initialize operation erases existing data on the SD card and all existing partitions are removed. You cannot perform initialize operation if one or more partitions are in use or attached. This option is accesible only if a card of size greated than 256 MB is present in the iDRAC Enterprise card slot and if vFlash is enabled.

Press <Enter> to initialize the vFlash SD card.

The initialize operation mail fail due to the following reasons:

- SD card is currently not present.
- vFlash is currently in use by another process.
- vFlash is not enabled.

- SD card is write-protected.
- One or more partitions are currently in-use.
- One or more partitions are currently attached.

#### vFlash Properties

Press <Enter> to view the following vFlash SD card properties:

- **Name** - Displays the name of the vFlash SD card inserted into the server's vFlash SD card slot. If it is a Dell SD card, it displays vFlash SD Card. If it is a non-Dell SD card, it displays SD Card.
- **Size** - Displays the vFlash SD card size in gigabytes (GB).
- **Available Space** - Displays the unused space on the vFlash SD card in megabytes (MB). This space is available to create more partitions on the vFlash SD card. For SD cards, the available space is displayed as 256 MB.
- **Write Protected** - Displays whether the vFlash SD card is write-protected or not.
- **Health** - Displays the overall health of the vFlash SD card. This can be:
  - OK
  - Warning
  - Critical

Press <Esc> to exit.

#### Smart Card/SSO

This option configures the **Smart Card Logon** and **Single Sign On** features. The available options are **Enabled** and **Disabled**.

**NOTE:** If you enable the **Single Sign On** feature, the **Smart Card Logon** feature is disabled.

## System Services

### System Services

Use the left-arrow and right-arrow keys to select **Enabled** or **Disabled**. If enabled, certain iDRAC6 features can be configured through the Lifecycle Controller. For more information, see the *Lifecycle Controller User Guide*, available on the Dell Support Website at **support.dell.com/manuals**.

**NOTE:** Modifying this option restarts the server when you **Save** and **Exit** to apply the new settings.

### Cancel System Services

Use the up-arrow and down-arrow keys to select **Yes** or **No**.

When you select **Yes**, all Lifecycle Controller sessions are closed, and the server restarts when you **Save** and **Exit** to apply the new settings.

### Collect System Inventory on Restart

Select **Enabled** to allow the collection of inventory during boot. See the *Dell Lifecycle Controller User Guide* available on the Dell Support website at **support.dell.com/manuals** for more information.

**NOTE:** Modifying this option restarts the server after you have saved your settings and exited from iDRAC6 Configuration Utility.

## LAN User Configuration

The LAN user is iDRAC6 administrator account, which is **root** by default. Press <Enter> to display the LAN User Configuration submenu. When you have finished configuring the LAN user, press <Esc> to return to the previous menu.

**Table 18-2. Lan User Configuration Screen**

| Item | Description |
|---|---|
| **Auto-Discovery** | The auto-discovery feature enables automated discovery of unprovisioned systems on the network; further, it *securely* establishes initial credentials so that these discovered systems can be managed. This feature enables iDRAC6 to locate the provisioning server. iDRAC6 and provisioning service server mutually authenticate each other. The remote provisioning server sends the user credentials to have iDRAC6 create a user account with these credentials. Once the user account is created, a remote console can establish WSMAN communication with iDRAC6 using the credentials specified in the discovery process and then send the secure instructions to iDRAC6 to deploy an operating system remotely.<br><br>For information on remote operating system deployment, see the *Dell Lifecycle Controller User Guide* available on the Dell Support website at **support.dell.com/manuals**.<br><br>Do the following prerequisite actions in a *separate* **iDRAC6 Configuration Utility** session *before manually enabling auto-discovery*:<br>• Enable NIC (blade servers)<br>• Enable IPv4 (blade servers)<br>• DHCP enable<br>• Get domain name from DHCP<br>• Disable admin account (account #2)<br>• Get DNS server address from DHCP<br>• Get DNS domain name from DHCP<br><br>Select **Enabled** to enable the auto-discovery feature. By default, this option is **Disabled**. If you have ordered a Dell system with the auto discovery feature **Enabled**, then iDRAC6 on the Dell system is shipped with DHCP enabled with no default credentials for a remote login. |

**Table 18-2. Lan User Configuration Screen *(continued)***

| Item | Description |
|---|---|
| **Auto–Discovery** *(continued...)* | Before adding your Dell system to the network and using the auto–discovery feature, ensure that:<br>• Dynamic Host Configuration Protocol (DHCP) server/Domain Name System (DNS) are configured.<br>• Provisioning Web services is installed, configured, and registered. |
| **Provisioning Server** | This field is used to configure the provisioning server. The provisioning server address can be a combination of IPv4 addresses or hostnames and should not exceed 255 characters. Each address or hostname should be separated by a comma.<br>If you have enabled the auto-discovery feature, user credentials are retrieved from the configured provisioning server to allow future remote provisioning after the auto-discovery process has completed successfully.<br>For more information, see the *Dell Lifecycle Controller User Guide* available on the Dell Support website at **support.dell.com/manuals**. |
| **Account Access** | Select **Enabled** to enable the administrator account. Select **Disabled** to disable the administrator account or when Auto-Discovery is enabled. |
| **IPMI LAN Privilege** | Select between **Admin**, **User**, **Operator**, and **No Access**. |
| **Account User Name** | Press <Enter> to edit the user name and press <Esc> when you have finished. The default user name is **root**. |
| **Enter Password** | Enter the new password for the administrator account. The characters are not echoed on the display as you enter them. |
| **Confirm Password** | Re-enter the new password for the administrator account. If the characters you enter do not match the characters you entered in the **Enter Password** field, a message displays and you must re-enter the password. |

### Reset to Default

Use the **Reset to Default** menu item to reset all of iDRAC6 configuration items to the factory defaults. This may be required, for example, if you have forgotten the administrative user password or if you want to reconfigure iDRAC6 from the default settings.

**NOTE:** In the default configuration, iDRAC6 networking is disabled. You cannot reconfigure iDRAC6 over the network until you have enabled iDRAC6 network in iDRAC6 Configuration Utility.

Press <Enter> to select the item. The following warning message is displayed:

```
Resetting to factory defaults will restore remote Non-
Volatile user settings. Continue?

< NO (Cancel)   >

< YES (Continue) >
```

To reset iDRAC6 to the defaults, select **YES** and press <Enter>.

Any of the following error messages is displayed if this operation fails:

- Reset command was not successful. Please try later- iDRAC is busy.
- Failed to restore settings to default values - Timeout.
- Not able to send Reset command. Please try later- iDRAC is busy.

### System Event Log Menu

The **System Event Log** Menu allows you to view System Event Log (SEL) messages and to clear the log messages. Press <Enter> to display the **System Event Log Menu**. The system counts the log entries and then displays the total number of records and the most recent message. The SEL retains a maximum of 512 messages.

To view SEL messages, select **View System Event Log** and press <Enter>. To navigate:

- Use the left-arrow key to move to the previous (older) message and the right-arrow key to move to the next (newer) message.
- Enter a specific record number to jump to that record.

Press <Esc> to exit the System Event Log.

**NOTE:** You can only clear the SEL in iDRAC6 Configuration Utility or in iDRAC6 Web interface.

To clear the SEL, select **Clear System Event Log** and press <Enter>.

When you have finished with the SEL menu, press <Esc> to return to the previous menu.

### Exiting iDRAC6 Configuration Utility

When you have finished making changes to iDRAC6 configuration, press the <Esc> key to display the Exit menu.

- Select **Save Changes and Exit** and press <Enter> to retain your changes. If this operation fails, one of the following message is displayed:
  - iDRAC6 Communication Failure—Displayed if iDRAC is not accessible.
  - Some of the settings cannot be applied—Displayed when few settings cannot be applied.
- Select **Discard Changes and Exit** and press <Enter> to ignore any changes you made.
- Select **Return to Setup** and press <Enter> to return to iDRAC6 Configuration Utility.

# 19

# Recovering and Troubleshooting the Managed System

This section explains how to perform tasks related to diagnosing and troubleshooting a remote managed system using iDRAC6 utilities. It contains the following subsections:

- Trouble indications — Helps you to find messages and other system indications that can lead to a diagnosis of the problem
- Problem-solving tools — Describes iDRAC6 tools that you can use to troubleshoot your system
- Troubleshooting and frequently asked questions — Answers to typical situations you may encounter

## Safety First – For You and Your System

To perform certain procedures in this section, you must work with the chassis, the Dell PowerEdge system, or other hardware modules. Do not attempt to service the system hardware except as explained in this guide and elsewhere in your system documentation.

**CAUTION: Many repairs may only be done by a certified service technician. 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.**

# Trouble Indicators

This section describes indications that there may be a problem with your system.

## LED Indicators

LEDs on the chassis or on components installed in the chassis are generally the first indicators of system trouble. The following components and modules have status LEDs:

- Chassis LCD display
- Servers
- Fans
- CMCs
- I/O modules
- Power supplies

The single LED on the chassis LCD summarizes the status of all of the components in the system. A solid blue LED on the LCD indicates that no fault conditions have been detected in the system. A blinking amber LED on the LCD indicates that one or more fault conditions have been detected.

If the chassis LCD has a blinking amber LED, you can use the LCD menu to locate the component that has a fault. See the *Dell Chassis Management Controller Firmware User Guide* for help using the LCD.

Table 19-1 describes the meanings of the LED on the Dell PowerEdge system:

**Table 19-1. Blade Server LED Indicators**

| LED indicator | Meaning |
|---|---|
| solid green (*only for power button*) | The server is powered on. Absence of the green LED means the server is not powered on. |
| solid blue | iDRAC6 is healthy. |
| flashing amber | iDRAC6 has detected a fault condition or may be in the process of updating firmware. |
| flashing blue | A user has activated the locator ID for this server. |

## Hardware Trouble Indicators

Indications that a module has a hardware problem include the following:

- Failure to power up
- Noisy fans
- Loss of network connectivity
- Battery, temperature, voltage, or power monitoring sensor alerts
- Hard drive failures
- USB media failure
- Physical damage caused by dropping, water, or other external stress

When these kinds of problems occur, inspect the damage caused, and then try to correct the problem using these strategies:

- Reseat the module and restart it
- Try inserting the module into a different bay in the chassis
- Try replacing hard drives or USB keys
- Reconnect or replace the power and network cables

If these steps do not correct the problem, consult the *Hardware Owner's Manual* for specific troubleshooting information for the hardware device.

## Other Trouble Indicators

**Table 19-2. Trouble Indicators**

| Look for: | Action: |
|---|---|
| Alert messages from the systems management software | See the systems management software documentation. |
| Messages in the System Event Log | See "Checking the System Event Log (SEL)" on page 365. |
| Messages in the start-up POST codes | See "Checking the Post Codes" on page 367. |
| Messages on the last crash screen | See "Viewing the Last System Crash Screen" on page 367. |
| Alert Messages on the Server Status Screen in the LCD | See "Checking the Server Status Screen for Error Messages" on page 369. |

**Table 19-2. Trouble Indicators *(continued)***

| Look for: | Action: |
|---|---|
| Messages in iDRAC6 Log | See "Viewing iDRAC6 Log" on page 377. |

# Problem Solving Tools

This section describes iDRAC6 utilities you can use to diagnose problems with your system, especially when you are trying to solve problems remotely.

- Checking the system health
- Checking the System Event Log for error messages
- Checking the POST codes
- Viewing the last crash screen
- Viewing the Most Recent Boot Sequences
- Checking the Server Status Screen on the LCD for Error Messages
- Viewing iDRAC6 log
- Viewing system information
- Identifying the managed server in the chassis
- Using the diagnostics console
- Managing power on a remote system

## Checking the System Health

When you log in to iDRAC6 Web interface, the **System Summary** screen displays the health of the system components. Table 19-3 describes the meaning of the system health indicators.

**Table 19-3. Server Health Indicators**

| Indicator | Description |
|---|---|
| | A green check mark indicates a healthy (normal) status condition. |
| | A yellow triangle containing an exclamation point indicates a warning (noncritical) status condition. |
| | A red X indicates a critical (failure) status condition. |
| | A question mark icon indicates that the status is unknown. |

Click any component on the **Server Health** section to see information about the component. Sensor readings are displayed for batteries, temperatures, voltages, and power monitoring, helping to diagnose some types of problems. iDRAC6 and CMC information screens provide useful current status and configuration information.

### Checking the System Event Log (SEL)

The **SEL Log** screen displays messages for events that occur on the managed server.

To view the **System Event Log**, perform the following steps:

1. Click **System** and then click the **Logs** tab.
2. Click **System Event Log** to display the **System Event Log** screen.

   The **System Event Log** screen displays a system health indicator (see Table 19-3), a time stamp, and a description of the event.
3. Click the appropriate **System Event Log** button to continue (see Table 19-4).

**Table 19-4. SEL Buttons**

| Button | Action |
|---|---|
| **Clear Log** | Clears the SEL.<br>**NOTE:** The **Clear Log** button is displayed only if you have **Clear Logs** permission. |

**Table 19-4. SEL Buttons *(continued)***

| Button | Action |
|---|---|
| Save As | Opens a pop-up window that enables you to save the SEL to a directory of your choice.<br>**NOTE:** If you are using Internet Explorer and encounter a problem when saving, be sure to download the Cumulative Security Update for Internet Explorer, located on the Microsoft Support website at **support.microsoft.com**.<br>**NOTE:** When using Internet Explorer, if you are not able to save the SEL Log using **Save As**, it may be due to a browser setting. To resolve this:<br>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 your local intranet, select **Local Intranet** and click **Custom level**....<br>2 In the **Security Settings** window, under **Downloads** ensure that the following options are enabled:<br>• Automatic prompting for file downloads<br>• File download<br>**CAUTION: To ensure that the computer used to access iDRAC is safe, under *Miscellaneous*, the *Launching applications and unsafe files* option must not be enabled.** |
| Advanced Settings | Opens the **System Event Log Advanced Settings** page that allows you to enable/disable the OEM event messages from the managed system displaying in the SEL. Click **Apply** to apply the setting. |

### Using the Command Line to View System Event Log

The command is:

```
racadm getsel <options>
```

If no arguments are specified, the entire log is displayed.

To display the number of SEL entries:

```
racadm getsel -i
```

**NOTE:** For more information about the options, see *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**.

The `clrsel` command removes all existing records from the SEL:

```
racadm clrsel
```

### Checking the Post Codes

The **Post Codes** screen displays the last system post code prior to booting the operating system. Post codes are progress indicators from the system BIOS, indicating various stages of the boot sequence from Power on Reset, and allow you to diagnose any faults related to system boot-up.

**NOTE:** View the text for POST code message numbers in the LCD display or in the *Hardware Owner's Manual.*

To view the Post Codes, click **System→ Logs→ Post Code**. The **Post Code** screen displays a system health indicator (see Table 19-3), a hexadecimal code, and a description of the code.

### Viewing the Last System Crash Screen

**NOTE:** The last crash screen feature must be configured in the Server Administrator and in iDRAC6 Web interface. See "Configuring the Managed Server to Capture the Last Crash Screen" on page 82 for instructions on configuring this feature.

The **Last Crash Screen** screen displays the most recent crash screen, which includes information about the events that occurred before the system crash. The last system crash image is saved in iDRAC6 persistent store and is remotely accessible. The last crash screen is availab le even if iDRAC resets since it is stored in NVRAM.

To view the **Last Crash Screen** screen, click **System→ Logs→ Last Crash Screen**. The **Last Crash Screen** screen displays the last saved crash screen.

Click **Save** to save the last crash screen to a directory of your choice.

Click **Delete** to delete the last crash screen.

**NOTE:** The **Save** and **Delete** buttons do not appear if there is no saved crash screen.

**NOTE:** Due to fluctuations in the Auto Recovery timer, the **Last Crash Screen** may not be captured when the System Reset Timer is configured with a value that is too high. The default setting is 480 seconds. Use Server Administrator or IT Assistant to set the System Reset Timer to 60 seconds and ensure that the **Last Crash Screen** functions properly. See "Configuring the Managed Server to Capture the Last Crash Screen" on page 82 for additional information.

## Viewing the Most Recent Boot Sequences

If you experience boot problems, you can view the screen activity of what happened during the last three boot sequences from the **Boot Capture** screen. Playback of the boot screens occurs at a rate of 1 frame per second. iDRAC6 records fifty frames during boot time. If iDRAC is reset, the boot capture video is not available since it is stored in RAM and is deleted when iDRAC resets.

Table 19-5 lists the available control actions.

**NOTE:** You must have administrator privileges to view playback of the Boot Capture sequences.

**Table 19-5. Boot Capture Options**

| Button/Option | Description |
|---|---|
| Select the boot sequence | Allows you to select the boot sequence to load and play.<br>• Boot Capture 1 — Loads the most recent boot sequence.<br>• Boot Capture 2 — Loads the (second most recent) boot sequence that occurred prior to Boot Capture 1.<br>• Boot Capture 3 — Loads the (third most recent) boot sequence that occurred prior to Boot Capture 2. |
| Save As | Creates a compressed .zip file that contains all boot capture images of the current sequence. The user must have administrator privileges to perform this action. |
| Previous Screen | Takes you to previous screen, if any, in the replay console. |
| Play | Starts the screenplay from current screen in the replay console. |
| Pause | Pauses the screenplay on the current screen being displayed in the replay console. |
| Stop | Stops the screenplay and loads the first screen of that boot sequence. |
| Next Screen | Takes you to next screen, if any, in the replay console. |
| Print | Prints the Boot Capture image that is displayed on the screen. |
| Refresh | Reloads the Boot Capture screen. |

### Viewing and Adding Work Notes

The **Work Notes** page displays the work note entries stored in the Lifecycle Log. To view the **Work Notes** page, expand the **System** tree and click **Systems→ Logs→ Work Notes**.

The time stamp recorded for each work note entry and the work note contents are displayed. The timestamp format is yyyy/mm/dd hh:mm:ss, based on a 24-hour clock.

Each user who logs in to iDRAC can add work notes to the log. A maximum of 50 characters is supported for each new work note. Click **Save** to add the note to the log.

**NOTE:** Do not use any special characters when you create a work note. If you use, they are converted to '%' character.

**NOTE:** You must have iDRAC login priviliges to add work notes. See "Adding and Configuring iDRAC6 Users" on page 99 for help configuring user permissions.

### Checking the Server Status Screen for Error Messages

When a flashing amber LED is lit, and a particular server has an error, the main Server Status Screen on the LCD will highlight 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. The following table lists all of the error messages and their severity.

**Table 19-6. Server Status Screen**

| Severity | Message | Cause |
|---|---|---|
| Warning | System Board Ambient Temp: Temperature sensor for System Board, warning event | Server ambient temperature crossed a warning threshold |
| Critical | System Board Ambient Temp: Temperature sensor for System Board, failure event | Server ambient temperature crossed a failure threshold |
| Critical | System Board CMOS Battery: Battery sensor for System Board, failed was asserted | CMOS battery is not present or has no voltage |

**Table 19-6. Server Status Screen *(continued)***

| Severity | Message | Cause |
|---|---|---|
| Warning | System Board System Level: Current sensor for System Board, warning event | Current crossed a warning threshold |
| Critical | System Board System Level: Current sensor for System Board, failure event | Current crossed a failure threshold |
| Critical | CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted | Voltage out of range |
| Critical | System Board <voltage sensor name>: Voltage sensor for System Board, state asserted was asserted | Voltage out of range |
| Critical | CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted | Voltage out of range |
| Critical | CPU<number> Status: Processor sensor for CPU<number, IERR was asserted | CPU failure |
| Critical | CPU<number> Status: Processor sensor for CPU<number>, thermal tripped was asserted | CPU overheated |
| Critical | CPU<number> Status: Processor sensor for CPU<number, configuration error was asserted | Incorrect processor type or in wrong location |
| Critical | CPU<number> Status: Processor sensor for CPU<number>, presence was deasserted | Required CPU is missing or not present |

**Table 19-6. Server Status Screen *(continued)***

| Severity | Message | Cause |
|---|---|---|
| Critical | System Board Video Riser: Module sensor for System Board, device removed was asserted | Required module was removed |
| Critical | Mezz B<slot number> Status: Add-in Card sensor for Mezz B<slot number>, install error was asserted | Incorrect Mezzanine card installed for IO fabric |
| Critical | Mezz C<slot number> Status: Add-in Card sensor for Mezz C<slot number>, install error was asserted | Incorrect Mezzanine card installed for I/O fabric |
| Critical | Backplane Drive <number>: Drive Slot sensor for Backplane, drive removed | Storage drive was removed |
| Critical | Backplane Drive <number>: Drive Slot sensor for Backplane, drive fault was asserted | Storage drive failed |
| Critical | System Board PFault Fail Safe: Voltage sensor for System Board, state asserted was asserted | This event is generated when the system board voltages are not at normal levels |
| Critical | System Board OS Watchdog: Watchdog sensor for System Board, timer expired was asserted | iDRAC6 watchdog timer expired and no action is set |
| Critical | System Board OS Watchdog: Watchdog sensor for System Board, reboot was asserted | iDRAC6 watchdog detected that the system has crashed (timer expired because no response was received from Host) and the action is set to reboot |
| Critical | System Board OS Watchdog: Watchdog sensor for System Board, power off was asserted | iDRAC6 watchdog detected that the system has crashed (timer expired because no response was received from Host) and the action is set to power off |

**Table 19-6. Server Status Screen *(continued)***

| Severity | Message | Cause |
|---|---|---|
| Critical | System Board OS Watchdog: Watchdog sensor for System Board, power cycle was asserted | iDRAC6 watchdog detected that the system has crashed (timer expired because no response was received from Host) and the action is set to power cycle |
| Critical | System Board SEL: Event Log sensor for System Board, log full was asserted | The SEL device detects that only one entry can be added to the SEL before it is full |
| Warning | ECC Corr Err: Memory sensor, correctable ECC ( <DIMM Location> ) was asserted | Correctable ECC errors reached a critical rate |
| Critical | ECC Uncorr Err: Memory sensor, uncorrectable ECC ( <DIMM Location> ) was asserted | An uncorrectable ECC error was detected |
| Critical | I/O Channel Chk: Critical Event sensor, I/O channel check NMI was asserted | A critical interrupt is generated in the I/O Channel |
| Critical | PCI Parity Err: Critical Event sensor, PCI PERR was asserted | Parity error was detected on the PCI bus |
| Critical | PCI System Err: Critical Event sensor, PCI SERR ( <Slot number or PCI Device ID>) was asserted | PCI error detected by device |
| Critical | SBE Log Disabled: Event Log sensor, correctable memory error logging disabled was asserted | Single bit error logging is disabled when too many SBE get logged |
| Critical | Logging Disabled: Event Log sensor, all event logging disabled was asserted | All error logging is disabled |
| Non-Recoverable | CPU Protocol Err: Processor sensor, transition to non-recoverable was asserted | The processor protocol entered a non-recoverable state |

**Table 19-6. Server Status Screen *(continued)***

| Severity | Message | Cause |
|---|---|---|
| Non-Recoverable | CPU Bus PERR: Processor sensor, transition to non-recoverable was asserted | The processor bus PERR entered a non-recoverable state |
| Non-Recoverable | CPU Init Err: Processor sensor, transition to non-recoverable was asserted | The processor initialization entered a non-recoverable state |
| Non-Recoverable | CPU Machine Chk: Processor sensor, transition to non-recoverable was asserted | The processor machine check entered a non-recoverable state |
| Critical | Memory Spared: Memory sensor, redundancy lost ( <DIMM Location> ) was asserted | Memory spare is no longer redundant |
| Critical | Memory Mirrored: Memory sensor, redundancy lost ( <DIMM Location> ) was asserted | Mirrored memory is no longer redundant |
| Critical | Memory RAID: Memory sensor, redundancy lost ( <DIMM Location> ) was asserted | RAID Memory is no longer redundant |
| Warning | Memory Added: Memory sensor, presence ( <DIMM Location> ) was deasserted | Added memory module was removed |
| Warning | Memory Removed: Memory sensor, presence ( <DIMM Location> ) was deasserted | Memory module was removed |
| Critical | Memory Cfg Err: Memory sensor, configuration error ( <DIMM Location> ) was asserted | Memory configuration is incorrect for the system |
| Warning | Mem Redun Gain: Memory sensor, redundancy degraded ( <DIMM Location> ) was asserted | Memory redundancy is downgraded but not lost |

**Table 19-6. Server Status Screen *(continued)***

| Severity | Message | Cause |
|---|---|---|
| Critical | PCIE Fatal Err: Critical Event sensor, bus fatal error was asserted | Fatal error is detected on the PCIE bus |
| Critical | Chipset Err: Critical Event sensor, PCI PERR was asserted | Chip error is detected |
| Warning | Mem ECC Warning: Memory sensor, transition to non-critical from OK (<DIMM Location> ) was asserted | Correctable ECC errors have increased from a normal rate |
| Critical | Mem ECC Warning: Memory sensor, transition to critical from less severe ( <DIMM Location> ) was asserted | Correctable ECC errors have reached a critical rate |
| Critical | POST Err: POST sensor, No memory installed | No memory detected on board |
| Critical | POST Err: POST sensor, Memory configuration error | Memory detected but is not configurable |
| Critical | POST Err: POST sensor, Unusable memory error | Memory configured but not usable |
| Critical | POST Err: POST sensor, Shadow BIOS failed | System BIOS shadow failure |
| Critical | POST Err: POST sensor, CMOS failed | CMOS failure |
| Critical | POST Err: POST sensor, DMA controller failed | DMA controller failure |
| Critical | POST Err: POST sensor, Interrupt controller failed | Interrupt controller failure |
| Critical | POST Err: POST sensor, Timer refresh failed | Timer refresh failure |
| Critical | POST Err: POST sensor, Programmable interval timer error | Programmable interval timer error |
| Critical | POST Err: POST sensor, Parity error | Parity error |

**Table 19-6. Server Status Screen *(continued)***

| Severity | Message | Cause |
|---|---|---|
| Critical | POST Err: POST sensor, SIO failed | SIO failure |
| Critical | POST Err: POST sensor, Keyboard controller failed | Keyboard controller failure |
| Critical | POST Err: POST sensor, System management interrupt initialization failed | System Management Interrupt initialization failure |
| Critical | POST Err: POST sensor, BIOS shutdown test failed | BIOS shutdown test failure |
| Critical | POST Err: POST sensor, BIOS POST memory test failed | BIOS POST memory test failure |
| Critical | POST Err: POST sensor, Dell remote access controller configuration failed | Dell Remote Access Controller configuration failure |
| Critical | POST Err: POST sensor, CPU configuration failed | CPU configuration failure |
| Critical | POST Err: POST sensor, Incorrect memory configuration | Incorrect memory configuration |
| Critical | POST Err: POST sensor, POST failure | General failure after video |
| Critical | Hdwar version err: Version Change sensor, hardware incompatibility was asserted | Incompatible hardware was detected |
| Critical | Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware) was asserted | Hardware is incompatible with the firmware |
| Critical | Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware and CPU mismatch) was asserted | CPU and firmware not compatible |

**Table 19-6. Server Status Screen *(continued)***

| Severity | Message | Cause |
|---|---|---|
| Critical | Mem Overtemp: Memory sensor, correctable ECC <DIMM Location> was asserted | Memory module overheating |
| Critical | Mem Fatal SB CRC: Memory sensor, uncorrectable ECC was asserted | South bridge memory failed |
| Critical | Mem Fatal NB CRC: Memory sensor, uncorrectable ECC was asserted | North bridge memory failed |
| Critical | WatchDog Timer: Watchdog sensor, reboot was asserted | Watch dog timer caused system to reboot |
| Critical | WatchDog Timer: Watchdog sensor, timer expired was asserted | Watch dog timer expired but no action taken |
| Warning | Link Tuning: Version Change sensor, successful software or F/W change was deasserted | Failed to update link tuning setting for proper NIC operation |
| Warning | Link Tuning: Version Change sensor, successful hardware change <device slot number> was deasserted | Failed to update link tuning setting for proper NIC operation |
| Critical | LinkT/FlexAddr: Link Tuning sensor, failed to program virtual MAC address (Bus # Device # Function #) was asserted | FlexAddress could not be programmed for this device |
| Critical | LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz <location>) was asserted | Option ROM does not support FlexAddress or linking tuning |
| Critical | LinkT/FlexAddr: Link Tuning sensor, failed to get link tuning or flex address data from BMC/iDRAC6 was asserted | Failed to obtain linking tuning or FlexAddress information from BMC/iDRAC6 |

**Table 19-6. Server Status Screen *(continued)***

| Severity | Message | Cause |
|---|---|---|
| Critical | LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or FlexAddress (Mezz XX) was asserted | This event is generated when the PCI device Option ROM for a NIC does not support link tuning or the Flex addressing feature |
| Critical | LinkT/FlexAddr: Link Tuning sensor, failed to program the virtual MAC address (<location>) was asserted | This event is generated when the BIOS fails to program the virtual MAC address on the given NIC device |
| Critical | I/O Fatal Err: Fatal IO Group sensor, fatal IO error (<location>) | This event is generated in association with a CPU IERR and indicates which device caused the CPU IERR |
| Warning | PCIE NonFatal Er: Non Fatal I/O Group sensor, PCIe error (<location>) | This event is generated in association with a CPU IERR |

## Viewing iDRAC6 Log

iDRAC6 **Log** is a persistent log maintained in iDRAC6 firmware. The log contains a list of user actions (such as log in, log out, and security policy changes) and alerts issued by iDRAC6. The log gets erased after iDRAC6 firmware update.

Where the **System Event Log** (SEL) contains records of events that occur in the managed server, iDRAC6 **Log** contains records of events that occur in iDRAC6.

To access iDRAC6 **Log**, click **System→ iDRAC Settings→ Logs.** The **iDRAC6 Log** screen is displayed. This screen provides the information listed in Table 19-7.

**Table 19-7. iDRAC6 Log Information**

| Field | Description |
|---|---|
| **Date/Time** | The date and time (for example, `Dec 19 16:55:47`).<br>iDRAC6 sets its clock from the managed server's clock at iDRAC6 initialization. If the managed server is off when iDRAC6 is started, then iDRAC6 sets its clock from the CMC in the chassis where the blade resides.<br>**NOTE:** Since the time source for iDRAC6 is different depending on the managed server's power state (at the time of iDRAC6 initialization), the managed server time should be set to match CMC time. If the system and CMC times do not match, inconsistent times may be reported in iDRAC6 logs after iDRAC initialization events. |
| **Source** | The interface that caused the event. |
| **Description** | A brief description of the event and the user name that logged in to iDRAC6. |

Click **Clear Log** to clear the log entries. The **Clear Log** button is displayed if you have Clear Logs permission.

Click **Save As** to to save iDRAC6 Log to a directory of your choice.

If you are using Internet Explorer and encounter a problem when saving, ensure to download the Cumulative Security Update for Internet Explorer, located on the Microsoft Support website at **support.microsoft.com**. When using Internet Explorer, if you are not able to save the iDRAC Log using **Save As**, it may be 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 your local intranet, select **Local Intranet** and click **Custom level**....
2. In the **Security Settings** window, under **Downloads** ensure that the following options are enabled:
   - Automatic prompting for file downloads
   - File download

**CAUTION: To ensure that the computer used to access iDRAC is safe, under *Miscellaneous*, the *Launching applications and unsafe files* option must not be enabled.**

## Viewing System Information

The **System Details** screen displays information about the following system components:

- Main system enclosure
- Integrated Dell Remote Access Controller 6—Enterprise

To access the system information, click **System→ Properties→ System Details**.

See "Recovering and Troubleshooting the Managed System" on page 361 for information on the system summary, main system enclosure, and iDRAC6.

## Identifying the Managed Server in the Chassis

The Dell PowerEdge M1000e chassis holds up to sixteen servers. To locate a specific server in the chassis, you can use iDRAC6 Web interface to turn on a blue flashing LED on the server. When you turn on the LED, you can specify the number of seconds that you want the LED to flash to ensure that you can reach the chassis while the LED is still flashing. Entering **0** leaves the LED flashing until you disable it.

To identify the server:

1. Click **System→ iDRAC Settings→ Troubleshooting**.
2. On the **Identify** screen, select **Identify Server**.
3. In the **Identify Server Timeout** field, enter the number of seconds that you want the LED to blink. Enter **0** if you want the LED to remain flashing until you disable it.
4. Click **Apply**.

A blue LED on the server will flash for the number of seconds you specified.

If you entered **0** to leave the LED flashing, follow these steps to disable it:

1. Click **System→ iDRAC Settings→ Troubleshooting**.
2. On the **Identify** screen, deselect **Identify Server**.
3. Click **Apply**.

## Using the Diagnostics Console

iDRAC6 provides a standard set of network diagnostic tools (see Table 19-8) that are similar to the tools included with Microsoft Windows or Linux-based systems. Using iDRAC6 Web interface, you can access the network debugging tools.

Click **Reset iDRAC6** to reset the iDRAC. A normal boot operation is performed on the iDRAC.

To access the **Diagnostics Console** screen, perform the following steps:

1. Click **System→ iDRAC Settings→ Troubleshooting**.
2. Select the **Diagnostics Console** tab.

Table 19-8 describes the commands that can be entered on the **Diagnostics Console** screen. Enter a command and click **Submit**. The debugging results appear in the **Diagnostics Console** screen.

Click the **Clear** button to clear the results displayed by the previous command.

To refresh the **Diagnostics Console** screen, click **Refresh**.

**Table 19-8. Diagnostic Commands**

| Command | Description |
|---|---|
| **arp** | Displays the contents of the Address Resolution Protocol (ARP) table. ARP entries may not be added or deleted. |
| **ifconfig** | Displays the contents of the network interface table. |
| **netstat** | Prints the content of the routing table. |
| **ping** *<IP Address>* | Verifies that the destination IP address is reachable from iDRAC6 with the current routing-table contents. A destination IP address must be entered in the field to the right of this option. An Internet control message protocol (ICMP) echo packet is sent to the destination IP address based on the current routing-table contents. |
| **ping6** *<IPv6 Address>* | Verifies that the destination IPv6 address is accessible from iDRAC6 with the current routing–table contents. A destination IPv6 address must be entered in the field to the right of this option. An ICMP (Internet control message protocol) echo packet is sent to the destination IPv6 address based on the current routing–table contents. |

**Table 19-8. Diagnostic Commands *(continued)***

| Command | Description |
|---|---|
| **traceroute** *<IP Address>* | Used to determine the route taken by packets across an IP network. |
| **traceroute6** *<IPv6 Address>* | Used to determine the route taken by packets across an IPv6 network. |
| **gettracelog** | Displays iDRAC6 trace log. For more information, see gettracelog in the *RACADM Command Line Reference Guide for iDRAC and CMC* available on the Dell Support website at **support.dell.com/manuals**. |

## Managing Power on a Remote System

iDRAC6 enables you to remotely perform several power management actions on the managed server. Use the **Power Management** screen to perform an orderly shutdown through the operating system when rebooting and powering on and off.

**NOTE:** You must have **Execute Server Action Commands** permission to perform power management actions. See "Adding and Configuring iDRAC6 Users" on page 99 for help configuring user permissions.

1. Click **System**, then click the **Power Management→ Power Control** tab.
2. Select a **Power Control Operation**, for example **Reset System (warm boot)**.
   Table 19-9 provides information about Power Control Actions.
3. Click **Apply** to perform the selected action.

**Table 19-9. Power Control Actions**

| | |
|---|---|
| **Power On System** | Turns on the system power (equivalent to pressing the power button when the system power is off). |
| **Power Off System** | Turns off the system power (equivalent to pressing the power button when the system power is on). |
| **NMI (Non-Masking Interrupt)** | Sends a high-level interrupt to the operating system, which causes the system to halt operation to allow for critical diagnostic or troubleshooting activities. |

**Table 19-9. Power Control Actions *(continued)***

| | |
|---|---|
| **Graceful Shutdown** | Attempts to cleanly shut down the operating system, then powers off the system. It requires an ACPI (Advanced Configuration and Power Interface) aware operating system, which allows for system directed power management.<br>**NOTE:** A graceful shutdown of the server operating system may not be possible when the server software stops responding, or if you are not logged as an administrator at a local Windows console. In these cases, you must specify a forced reboot instead of a graceful shutdown of Windows. In addition, depending on the version of the Windows OS, there might be a policy configured around the shutdown process that modifies shutdown behavior when triggered from iDRAC6. See Microsoft's documentation for the local computer policy "Shutdown: Allow system to be shut down without having to login." |
| **Reset System (warm boot)** | Reboots the system without powering off (warm boot). |
| **Power Cycle System (cold boot)** | Powers off, then reboots the system (cold boot). |

See "Power Monitoring and Power Management" on page 305 for more information.

# Troubleshooting and Frequently Asked Questions

Table 19-10 contains frequently asked questions about troubleshooting issues.

**Table 19-10. Frequently Asked Questions/Troubleshooting**

| Question | Answer |
|---|---|
| The LED on the server is blinking amber. | Check the SEL for messages and then clear the SEL to stop the blinking LED.<br>From iDRAC6 Web interface, see "Checking the System Event Log (SEL)" on page 365.<br>From SM-CLP, see "SEL Management" on page 324.<br>From iDRAC6 Configuration Utility, see "System Event Log Menu" on page 358. |
| There is a blinking blue LED on the server. | A user has activated the locator ID for the server. This is a signal to help them identify the server in the chassis. See "Identifying the Managed Server in the Chassis" on page 379 for information about this feature. |
| How can I find the IP address of iDRAC6? | **From CMC Web interface:**<br>**1** Click **Chassis→ Servers**, then click the **Setup** tab.<br>**2** Click **Deploy**.<br>**3** Read the IP address for your server from the table that is displayed.<br>**From the Virtual Console:**<br>• Reboot the server and enter **iDRAC6 Configuration Utility** by pressing <Ctrl><E>.<br>• Watch for the IP address which displays during BIOS POST.<br>• 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 *RACADM Command Line Reference Guide for iDRAC and CMC* for a complete list of CMC RACADM subcommands.<br>• Use the local RACADM **getsysinfo** command to view iDRAC6 IP address. |

**Table 19-10. Frequently Asked Questions/Troubleshooting *(continued)***

| Question | Answer |
|---|---|
| | For example:<br>`$ racadm getniccfg -m server-1`<br>`DHCP Enabled = 1`<br>`IP Address = 192.168.0.1`<br>`Subnet Mask = 255.255.255.0`<br>`Gateway = 192.168.0.1`<br><br>**From local RACADM:**<br>Enter the following command at a command prompt:<br>`racadm getsysinfo`<br>**From the LCD:**<br>1 On the Main Menu, highlight **Server** and press the check button.<br>2 Select the server whose IP address you seek and press the check button. |

**Table 19-10. Frequently Asked Questions/Troubleshooting *(continued)***

| Question | Answer |
|---|---|
| How can I find the IP address of CMC? | **From iDRAC6 Web interface:**<br>• Click **System→ iDRAC Settings→ CMC**.<br>CMC IP address is displayed on the CMC **Summary** screen.<br>**From the Virtual Console:**<br>• 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 *RACADM Command Line Reference Guide for iDRAC and CMC* for a complete list of CMC RACADM subcommands<br>`$ racadm getniccfg -m chassis`<br>`NIC Enabled = 1`<br>`DHCP Enabled = 1`<br>`Static IP Address = 192.168.0.120`<br>`Static Subnet Mask = 255.255.255.0`<br>`Static Gateway = 192.168.0.1`<br>`Current IP Address = 10.35.155.151`<br>`Current Subnet Mask = 255.255.255.0`<br>`Current Gateway = 10.35.155.1`<br>`Speed = Autonegotiate`<br>`Duplex = Autonegotiate`<br>**NOTE:** The above action can also be performed with remote RACADM. |
| iDRAC6 network connection is not working. | • Ensure that the LAN cable is connected to CMC.<br>• Ensure that NIC settings, IPv4 or IPv6 settings, and either Static or DHCP is enabled for your network. |
| I inserted the server into the chassis and pressed the power button, but nothing happened. | • iDRAC6 requires upto 2 minutes to initialize before the server can power up.<br>• Check CMC power budget. The chassis power budget may have exceeded. |

**Table 19-10. Frequently Asked Questions/Troubleshooting *(continued)***

| Question | Answer |
|---|---|
| I have forgotten iDRAC6 administrative user name and password. | You must restore iDRAC6 to its default settings.<br>**1** Reboot the server and press <Ctrl><E> when prompted to enter **iDRAC6 Configuration Utility**.<br>**2** On **iDRAC6 Configuration Utility** menu, highlight **Reset to Default** and press <Enter>.<br>**NOTE:** You can also reset iDRAC6 from local RACADM by issuing `racadm racresetcfg`.<br>For more information, see "Reset to Default" on page 358. |
| How can I change the name of the slot for my server? | **1** Log in to CMC Web interface.<br>**2** Open the **Chassis** tree and click **Servers**.<br>**3** Click the **Setup** tab.<br>**4** Enter the new name for the slot in the row for your server.<br>**5** Click **Apply**. |
| When starting a Virtual Console session from iDRAC6 Web interface, an ActiveX security popup is displayed. | iDRAC6 may not be a trusted site. To prevent the security popup from appearing every time you begin a Virtual Console session, add iDRAC6 to the trusted site list in the client browser:<br>**1** Click **Tools→ Internet Options→ Security→ Trusted sites**.<br>**2** Click **Sites** and enter the IP address or the DNS name of iDRAC6.<br>**3** Click **Add**.<br>**4** Click **Custom Level**.<br>**5** In the **Security Settings** window, select **Prompt** under **Download unsigned ActiveX Controls**. |
| When I start a Virtual Console session, the viewer screen is blank. | If you have **Virtual Media** privilege but not **Virtual Console** privilege, you are able to start the viewer so that you can access the virtual media feature, but the managed server's console will not display. |
| iDRAC6 is not responding during boot. | Remove and reinsert the server.<br>Check CMC Web interface to see if iDRAC6 is displayed as an upgradable component. If it does, follow the instructions in "Updating iDRAC6 Firmware Using CMC" on page 124.<br>If this does not correct the problem, contact technical support. |

**Table 19-10. Frequently Asked Questions/Troubleshooting *(continued)***

| Question | Answer |
|---|---|
| When attempting to boot the managed server, the power indicator is green, but there is no POST or no video at all. | This can happen if any of the following conditions is true:<br>• Memory is not installed or is inaccessible.<br>• The CPU is not installed or is inaccessible.<br>• The video riser card is missing or improperly connected.<br>Also, look for error messages in iDRAC6 log from iDRAC6 Web interface or from the LCD. |

# Index


## A

Active Directory
  adding DRAC 5 users, 144
  configuring access to the DRAC 5, 136
  managing certificates, 111
  objects, 133
  schema extensions, 132
  using with extended schema, 132
  using with standard schema, 152
  using with the DRAC 5, 127

ActiveX
  console redirection plug-in, 225

alert management. See *PEF*

arp command, diagnostics console, 380

ASR
  auto recovery timer, 83
  configuring, 120

attach or detach partition, 252

Auto Discovery, 356

Automated System Recovery, *See* ASR

## B

boot once, enabling, 265

boot to a partition, 255

bootable image file
  creating, 336

## C

Certificate Signing Request. See *CSR*

certificates
  Active Directory, 111
  exporting the root CA certificate, 130
  SSL and digital, 107
  viewing a server certificate, 111

chassis LCD panel, 33

Chassis Management Controller. See *CMC*

CMC
  about, 19
  configuring iDRAC6 during initialization, 35

CMC Web interface, 32
  configuring iDRAC6 network properties, 39
  locating iDRAC6 IP address, 383

configuration file
  creating, 297

configuring
  task overview, 35-39

configuring Local iDRAC6 users for Smart Card logon, 180
configuring multiple iDRACs with RACADM, 302
configuring Smart Card Login, 178
console redirection
configuring, 222
opening a session, 224
using, 219
CSR
about, 108
generating, 109

## D

delete a partition, 254
diagnostics console, 380
digital signature, verify, 53-56
Distributed Management Task Force (DMTF), 317
documents you may need, 27
DOS update utility, 58
DRAC 5
configuring, 146, 154

## E

e-mail alerts
configuring with RACADM, 289
configuring with the web interface, 96
Empty Partition, 245
Enabling or Disabling SD card, 244
extended schema
using with Active Directory, 132

## F

file system types, 249
Firefox
tab behavior, 87
firewall, opening ports, 25
firmware
recovering with CMC, 57, 123
updating, 52
updating with the web interface, 123
Format Partition, 249
frequently asked questions
using console redirection, 233
using the DRAC 5 with Active Directory, 165
using Virtual Media, 269

## G

gettracelog command, diagnostics console, 381
group permissions
table of, 106

## I

iDRAC
- creating a configuration file, 297
- log, viewing, 377
- recovering firmware, 124
- securing communications, 107
- updating the firmware, 52

iDRAC configuration utility
- configuring LAN user, 355

iDRAC KVM
- displaying OSCAR, 348

iDRAC service ports, 25

iDRAC6
- configuring standard schema Active Directory, 162
- resetting to factory defaults, 358
- SSH, 76

iDRAC6 configuration utility, 32
- configuring IPMI, 349
- configuring network properties, 349
- configuring virtual media, 353
- starting, 348

iDRAC6 firmware rollback, 125

iDRAC6 web interface, 32, 57

ifconfig command, diagnostics console, 380

iKVM
- disabling during console redirection, 231
- viewing status of the local console, 234

Image File, 247

instrumentation
- server, 81

Internet Explorer
- configuring, 66

IP blocking
- configuring with RACADM, 292
- configuring with the web interface, 92
- enabling, 293

IP filtering
- configuring with RACADM, 290
- configuring with the web interface, 92

IPMI, 34
- configuring LAN properties, 88
- configuring with iDRAC6 configuration utility, 349
- configuring with RACADM, 286
- configuring with the web interface, 98

iVMCLI, 33

iVMCLI utility
- about, 335
- deploying the operating system, 337
- operating system shell options, 345
- parameters, 341
- return codes, 345
- syntax, 340
- using, 339

ivmdeploy script, 337

## J

Java
  console redirection plug-in, 74, 225

## K

key, verify, 54, 56

## L

last crash screen
  capturing on the managed server, 82
  viewing, 367

Lifecycle Controller User Guide, 355

local RACADM, 33

localization, browser setup, 70

logs
  iDRAC, 377
  post codes, 367
  server, 81

lost administrative password, 358

## M

Manageability Access Point. See *MAP*

managed server
  capturing the last crash screen, 82
  configuring, 81

management
  storage, 81

management station
  configuring, 65-74
  configuring for console redirection, 221
  installing the software, 78-79
  network requirements, 65

MAP
  navigating

Media Redirection wizard, 266-267

mouse pointer
  synchronizing, 230

Mozilla Firefox
  disabling whitelist, 72
  supported versions, 72

## N

netstat command, diagnostics console, 380

network properties
  configuring manually, 284
  configuring with CMC Web interface, 39
  configuring with iDRAC6 configuration utility, 349
  configuring with RACADM, 284
  configuring with the Web interface, 88

## O

On Screen Configuration and Reporting. See *OSCAR*

OpenSSH, SSH client for Linux, 76

operating system
- installing (manual method), 268
- installing (scripted method), 335

OSCAR
- displaying, 348
- supported, 24

ports
- table of, 25

post codes, viewing, 367

power management
- using SM-CLP, 324
- using the web interface, 381

proxy server, web browser configuration, 69

public key, verify, 54, 56

PuTTY, Windows SSH client, 76

## P

password
- changing, 104
- lost, 358

PEF
- configuring with RACADM, 288
- configuring with the web interface, 95

PET
- configuring with RACADM, 288
- configuring with the web interface, 94-95, 288
- filterable platform events table, 94

ping command, diagnostics console, 380

ping6, 380

Platform Event Filter. See *PEF*

Platform Event Trap. See *PET*

platforms

## R

RACADM
- configuring e-mail alerts, 289
- configuring IP blocking, 292
- configuring IP filtering, 290
- configuring IPMI, 286
- configuring multiple iDRACS, 302
- configuring network properties, 284
- configuring PEF, 288
- configuring PET, 288
- configuring SOL, 286
- configuring SSH service, 294
- configuring telnet service, 294
- installing and removing, 73
- using, 275

RACADM subcommands
- clrraclog, 276
- clrsel, 276

config, 82, 276
getconfig, 234, 276, 297-298
getniccfg, 276
getraclog, 276
getractime, 276
getssninfo, 276
getsvctag, 276
getsysinfo, 277
gettracelog, 277
racreset, 277
racresetcfg, 277
serveraction, 277
setniccfg, 277
sslcertdownload, 278
sslcertupload, 278
sslcertview, 278
sslcsrgen, 278
testemail, 278
testtrap, 278

reboot option
disabling, 83

remote access connections
supported, 25

resetting iDRAC6 to defaults, 358

## S

safety, 361

screen resolutions, support, 221

scripts
ivmdeploy, 337

SD Card Properties, 241

secure shell. See *SSH*

Secure Sockets Layer (SSL)
importing the firmware certificate, 131

secure sockets layer. See *SSL*

security
using SSL and digital certificates, 107

See *RACADM*

SEL
managing with iDRAC6 configuration utility, 358
managing with the iDRAC6 configuration utility, 358
managing with the web interface, 365

server
instrumentation, 81
logs, 81

server certificate
viewing, 111

server features, integrated
instrumentation, 81
logs, 81

Server Management Command Line Protocol. See *SM-CLP*

server storage management, 81

services
configuring with the web interface, 120

signature, verify, 53-56

Simple Network Management Protocol. See *SNMP*

Single Sign-On, 175

Smart Card Authentication, 180

Smart Card Logon, 178

SM-CLP, 34
- features, 319
- navigating the MAP
- output formats, 323
- power management, 324
- syntax, 319
- targets, 322
- using the show verb, 322

snap-in
- installing the Dell extension, 143

SNMP
- testing trap alert, 284

SNMP Agent, 120

SOL
- configuring with RACADM, 286
- configuring with the web interface, 98

SSH
- client installation, 75
- configuring iDRAC service with RACADM, 294
- configuring service with the web interface, 120
- OpenSSH software for Linux, 76
- PuTTY client for Windows, 76

SSL
- about, 107

standard schema
- using with Active Directory, 152

standard SD card, 239

supported CIM profiles, 330

system health, viewing, 364

System Services Configuration Unified Server Configurator, 355

## T

telnet
- backspace configuration, 75
- client installation, 75
- configuring iDRAC service with the web interface, 120
- configuring iDRAC6 service with RACADM, 294

TFTP server, installing, 78

traceroute, 381

traceroute6, 381

Trivial File Transfer Protocol, see *TFTP*

troubleshooting
- indications, 362

trusted domains list, adding iDRAC, 69

Two-factor-authentication
- TFA, 178

## U

Unified Server Configurator, 355
- System Services, 355

Update Packages
verifying the digital signature, 53-56
USB flash drive emulation type, 353
user configuration, 103
users
adding and configuring with the web interface, 99
configuring LAN user with iDRAC6 configuration utility, 355
Using iDRAC6 with LDAP Directory Service, 161
using RACADM to configure iDRAC6 Users, 102-103
utilities
dd, 336
iVMCLI, 335
video viewer, 226

## V

verify
digital signature, 53-56
public key, 54, 56
vFlash Partitions, 239
vFlash SD Card, 239
vFlash SD Card Properties, 243
video viewer
using, 226
virtual media
about, 261
booting, 267
command line, 339
configuring with iDRAC6 configuration utility, 353
configuring with the web interface, 264
installing the operating system, 268
running, 265
VLAN, 88

## W

web browser
configuring, 66
proxy server configuration, 69
supported, 25
web interface
accessing, 86
browser configuration, 66
configuring ASR service, 120
configuring e-mail alerts, 96
configuring iDRAC services, 120
configuring IP blocking, 92
configuring IP filtering, 92
configuring IPMI LAN properties, 88, 98
configuring network properties, 88
configuring PEF, 95
configuring PET, 94-95, 288
configuring SOL, 98
configuring telnet service, 120
configuring the SSH service, 120

configuring the web server service, 120
logging in, 86
logging out, 87
updating firmware, 123
web server, iDRAC
configuring with the web interface, 120